GOVERNMENT OF KERALA
POLICE DEPARTMENT
Vazhuthacaud, Thiruvananthapuram - 695010
Ph: 0471-2722566 Fax: 0471- 2722566
e-mail: aig2phq.pol@kerala.gov.in
www.keralapolice.gov.in

e-Government Procurement (e-GP)
NOTICE INVITING TENDER

H9/168185/2026/PHQ **Dated: 21/08/2026**

The Director General of Police & State Police Chief, Kerala Police Department, Government of Kerala invites online bids from reputed firms/agencies experienced in cyber security, digital forensics, malware analysis solutions and turnkey laboratory infrastructure works for the Establishment of Integrated Cyber Capability Centre for Training, Research, AI-Driven Threat Analytics & Digital Forensics at the 2nd Floor, Police Training College under the Scheme for "Technology Upgradation of Cyber Crime Investigation" under Assistance to States and UTs for Modernisation of Police 2026-27 (ASUMP 2026-27).

The tender includes the **Supply, installation and commissioning of the Tiered Digital Forensics Architecture Tools/Equipments** as specified in the enclosed technical specifications and conditions.

1	**Tender No.**	**KPET/29/2026/PHQ Dated 21.08.2026**	
2	**Name of Project**	**Supply, installation and commissioning of the Tiered Digital Forensics Architecture Tools/ Equipments**	
3	**Tools/Equipments to be supplied**	**I. Advanced Data Extraction Capabilities for Mobile Devices**	For Cyber - Tiered Digital Forensics Architecture **- 21 Nos** For Cyber Range & Cyber Training Centre **– 02 Nos** Cyber Crime Research & Advanced Crime Labs **– 02 Nos** **Total – 25 Nos**
		II. Advanced Mobile Extraction Capabilities	For Cyber - Tiered Digital Forensics Architecture **- 01 No**
		III. High-End Analysis Workstation	For Cyber - Tiered Digital Forensics Architecture **- 21 Nos**
		IV. Digital Evidence Acquisition and	For Cyber - Tiered Digital

		Examination Software – 3-Year Subscription License	Forensics Architecture **- 05 Nos** For Artificial Intelligence Threat Lab **– 01 No** **Total – 06 Nos**
		V. Video Enhancement Software- Perpetual License with 3 Years Support	For Cyber - Tiered Digital Forensics Architecture **- 21 Nos**
		VI. Image Authentication Software-Perpetual License with 3 Years Support	For Cyber - Tiered Digital Forensics Architecture - **05 Nos** For Artificial Intelligence Threat Lab **– 01 No** **Total – 06 Nos**
		VII. DVR Data Extraction Tool	For Cyber - Tiered Digital Forensics Architecture **- 05 Nos**
		VIII. Logicube Falcon NEO 2 - 3 Years Hardware Warranty (High-speed digital forensic imager and duplicator)	For Cyber - Tiered Digital Forensics Architecture **- 21 Nos**
		IX. FRED - Forensic Workstation	For Cyber - Tiered Digital Forensics

			Architecture **- 21 Nos** For Cyber Range & Cyber Training Centre **– 01 No** **Total – 22 Nos**
		X. Financial Investigation and Analytics Software (Perpetual License with 3 Years Support)	For Cyber - Tiered Digital Forensics Architecture - **06 Nos**
		XI. Blockchain Investigation and Cryptocurrency Analysis Software for 8 Users- 3 Years Subscription License For Cyber - Tiered Digital Forensics Architecture **– 06 users** For Cyber Crime Research & Advanced Crime Labs **– 02 Users**	For Cyber - Tiered Digital Forensics Architecture **01 Nos**
4	**Locations**	**Police Training College, Thiruvananthapuram**	
5	**Estimated Amount**	**Rs. 29.10 Crores**	
6	**Tender Fees**	(through online mode only) Rs. 28,750 /- [Rupees Twenty eight thousand seven hundred and fifty Only] (GST extra) 18% GST amount on tender fees mentioned above shall be paid to GST Department directly by the bidder.	
7	**Earnest Money Deposit**	Rs. 29,10,000/- (Rupees Twenty nine lakh and ten thousand Only) (through online mode/Bank Guarantee)	

8	**Specifications**	Attached in the Tender document.
9	**Date and Time of Publication of e Tender**	**21.08.2026, 06:00 PM**
10	**Date of submission of e-Tender**	**21/08/2026, 06:00 PM To 05/09/2026,12:00 NOON**
11	**Last date and time for online Submission of e Tender**	**05.09.2026, 12.00 NOON**
12	**Date and time of opening of e-Tender**	**07.09.2026, 03.00 PM**
13	**Place of opening**	Police Headquarters, Vazhuthacaud, Thiruvananthapuram- 695010
14	**Date of Technical Evaluation**	**Bidders should be ready to attend the Technical Evaluation on any day within 1 week after bid opening date on short notice.**
15	**Address of Tender Inviting Authority**	State Police Chief, Kerala, Vazhuthacaud, Thiruvananthapuram - 695010 Ph: 0471-2722566 Mobile No. 9497996998 Fax: 0471-2722566 e-mail: aig2phq.pol@kerala@gov.in Website: www.keralapolice.gov.in
16	**Bid Validity**	(Total Number of Days up to which the rates are to be firm) 180 **days**

The scope of work covers:

Supply, installation and commissioning of the following Tiered Digital Forensics Architecture Tools/Equipments from reputed firms.

I. Advanced Data Extraction Capabilities for Mobile Devices

1. Technical Specifications

1. The solution should provide advanced access extraction capabilities to provide Full-File System extraction from unlocked File-based encryption devices and Physical extraction from unlocked Full-disk encryption devices from leading Android vendors in the Indian smartphone market such as Vivo, Samsung, Oppo, Xiaomi, Realme and OnePlus.
2. The solution should include all necessary adapters, cables, and accessories to perform the supported advanced access operations on the iOS and Android devices.
3. The solution should come with all the relevant documentation including supported devices, user manual, release notes and video tutorials.
4. The solution should also allow Full File-system extraction of unlocked iOS devices with greater data extraction. It should support Full File-system extraction from unlocked iOS devices running on chipsets A8 to A13 for iPhone 6 to 11.
5. The solution should be able to conduct Full File-system extraction from unlocked iPhone 11, 12, 13, 14,15,16 with chips running on A13, A14, A15, A16, A17 to A18.
6. The solution should be able to conduct Full File-system extraction for the unlocked iPhone 17.
7. The solution should allow users to perform selective extraction at the level of the individual installed applications for both iOS and Android devices.
8. The solution should work in a secured environment in a client – cloud exploit server mode.
9. The solution must provide advanced access capabilities from a Central Cloud exploit server to multiple extraction endpoints.
10. An advanced security mechanism should be available to allow the advanced exploit to be pushed down from the Central Cloud exploit server to the client endpoints only on need basis.
11. The solution should be supported to run on an active internet connection with a recommended speed of a minimum of 100 Mbps.
12. The solution should be regularly updated to support additional operating system versions and devices during the valid license and support period.
13. The solution should also have the ability to upgrade the license in the future to provide the device unlocking capability using brute-force for the supported locked Android and iOS devices.

14. It should allow the user to define a workflow at the beginning of the process to ensure the complete decoding, enrichment, and reporting functions are automated without any human intervention.
15. There should be the capability to automatically search for relevant device information during the access phase of the device based on the device state.
16. The solution should be able to provide information related to device identifiers like IMSI, device name and IMEI along with device user identification information.
17. The automated workflow and searching device information capabilities should be available for the advanced access extractions for both iOS and Android devices.

2. Mobile Extraction Capabilities

a) The solution should be able to extract forensic evidence from supported mobile devices including mobile phones, handheld tablets, portable GPS devices and drones.

b) It should provide users with available physical, file system and advanced logical extraction capabilities for different supported devices and Operating Systems as well as allow extraction of Cloud Data source tokens accessed by the supported Mobile Phones. It should support automatic detection of supported devices. It should also support manual search for devices by manufacturer, model and IMEI number

c) A multi-SIM adapter with support for Micro, Nano and standard SIM cards should be supplied. Ability to perform SIM data extraction from a SIM or USIM card.

d) 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.

e) 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, Unisoc Live, Kirin Live, 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.

3. Decoding, Review and Reporting Capabilities

a) Should have Case Management capability, which allows users to create and manage cases and to provide case details and exhibit information. It

should enable users to include multiple extractions and to apply the different enrichments.

b) Should include dashboard view to provide a quick visual overview and display insights into the extracted data including commonly used applications, the most recent messages and enable the investigator to quickly and easily drill down into the data of interest.

c) Dedicated location analysis view to clearly categorize the location records like device visited locations, locations of some significance, media derived locations and any other location data for detailed user analysis.

d) Capability to identify the origin of media items found within the device data to collect various metrics about a media item and apply logic to try to identify how the item originated, providing the user with information about the determined origin and the reasoning for that determination.

e) Should have the ability to parse Windows computer data like DD, E01, RAW, L01,001 or BIN images in the same application.

f) Should be built on a database architecture to reopen cases quickly without having to reprocess the data.

g) Should have cryptocurrency enrichment feature to automatically identify the usage of cryptocurrencies and to detect wallet addresses and transactions within the device data.

h) It should also have an advanced cryptocurrency enrichment ability to provide a detailed analysis of the cryptocurrency assets associated with detected wallet addresses and highlight potential illicit activity. The enrichment should further provide risk severity and graphs on currency sent and received insights. This crypto enrichment result should be exportable to a report for individual wallet addresses.

i) Support for image carving and location carving

j) It should conduct on demand searches for viruses, spyware, Trojans and other malicious payloads in files.

k) Media classification capability to detect and categorize images and video frames into 20+ key categories. This capability should be selectable, allowing the user to decide if he wants to run the media classification on a particular case.

l) Capability to verify file integrity with use of MD5 and SHA 256.

m) It should have a built-in SQLite Viewer.

n) Capability to match files extracted against Hash Databases and it should have built-in support for Project VIC, CAID and NCMEC hash databases.

o) Capability to allow users to include Case ID as well as other relevant case-related information as part of the extraction report and allow filtering based on specified date range.

p) Ability to generate and customize reports in different formats e.g. PDF, HTML, XML, Excel and Word. Global setting to select/unselect items in a report with the ability to password protect the reports.

q) Provide a separate report with device information and user account information for quick reference of users.

4. Cloud Data Extraction Capabilities

a. Should allow access to remote cloud data sources to obtain, decode, save and perform analysis of this data.

b. There should be a single software interface in which users can review device data and cloud data through a single tool and with a unified experience, for a seamless and simplified review process.

c. Software should allow access to remote cloud data sources using cloud login keys from mobile devices supporting iOS and Android.

d. Support extraction of different content types from the supported data sources which includes messages, images, videos, files, contacts, calls, user profile, locations, user activities and backups.

e. Provide visibility of the cloud extraction progress to the user. It should provide a view of the current status of each data source extraction with an option to cancel the process if required.

f. Allow users to gather private user data with appropriate legal authority from over 50 of the most popular social media and cloud-based sources.

g. Capability to create cloud tokens from manually entered credentials for future cloud extractions.

h. Reporting of extracted data from the Cloud to human readable formats such as PDF, Word, Excel, HTML and XML. It should provide a global setting to select/unselect items in a report. The software should allow for password protection of the reports.

5. Tender Specific Authorization Certificate from the OEM in favour of the Indian Distributor/Reseller/Bidder is mandatory for participation in the tender.

6. 3-year subscription license without Unlocks

7. One-day training must be provided at the time of installation and setup. The training should be conducted on-site by an OEM-certified engineer.

8. The training must cover both basic fundamentals and hands-on sessions to ensure familiarity with all functionalities of the tool.

II. Advanced Mobile Extraction Capabilities

1. Technical Specifications

a) The solution should provide advanced access capabilities with brute-force, unlocking and data extraction from supported iOS and Android mobile phones.

b) The solution should provide maximum unlocks and unlimited extractions with a term-based license through a USB dongle.

c) It should have brute-force capability for both Android and iOS devices on the same software interface.

d) The solution should be able to provide Full File-System extraction for File-based encryption (FBE) devices and Physical extraction for full-disk encryption (FDE) devices from leading Android vendors in the Indian smartphone market such as Vivo, Samsung, Oppo, Xiaomi, Realme and OnePlus.

e) The solution should support autonomous & connected Brute-Force for a wide range of supported FDE and FBE Android devices.

f) The solution should identify, extract and decrypt Samsung Secure folder, Huawei Private Space and Xiaomi second space.

g) The solution should provide brute-force capabilities for supported iPhones in Cold/BFU State on chip A8 all the way to A13 (iPhone 11 and iPhone SE Gen 2) to determine the device passcode.

h) The solution should be able to conduct After-First Unlock (AFU) based Full Filesystem extraction from iPhone 12, 13, 14 in Hot/AFU State with chip running on A14, A15 to A16.

i) The solution must allow a Full File-system extraction of supported unlocked iOS devices up to iPhone 16.

j) The solution should be able to support autonomous Brute-Force for iOS devices.

k) The solution shall support application selective data extraction allowing fast extraction of specific application data.

l) The solution should allow the user to enter potential passcodes while performing brute-force on iOS and Android devices without affecting the ongoing process.

m) The solution should be able to perform Before-First-Unlock (BFU) extraction for supported iPhone and Android phones

n) The solution must include the software, cables and adapter to allow the solution to perform the access of Android and iOS mobile devices.

o) The solution should work in a secured environment in a client – cloud exploit server mode.

p) The solution must provide advanced access capabilities from a Central Cloud exploit server to multiple extraction end points.

q) An advanced security mechanism should be available to allow the advanced exploit to be pushed down from the Central Cloud exploit server to the client endpoints only on need basis.

r) The solution should be supported to run on an active internet connection with a recommended speed of a minimum of 100 Mbps.

s) The solution should come with all the relevant documentation including supported devices, user manual, release notes and video tutorials.

t) The solution should be regularly updated to support additional operating system versions and devices during the valid license and support period.

u) It should allow the user to define a workflow in the beginning of the process to ensure the complete decoding, enrichment and reporting functions are automated without any human intervention.

v) There should be the capability to automatically search for relevant device information during the access phase of the device based on the device state.

w) Solution should be able to provide information related to device identifiers like IMSI, device name and IMEI along with device user identification information.

x) The automated workflow and searching device information capabilities should be available for the advanced access extractions for both iOS and Android devices.

2. Mobile Extraction Capabilities

a) The solution should be able to extract forensic evidence from supported mobile devices including mobile phones, handheld tablets, portable GPS devices and drones.

b) It should provide users with available physical, file system and advanced logical extraction capabilities for different supported devices and Operating Systems as well as allow extraction of Cloud Data source tokens accessed by the supported Mobile Phones.

c) It should support automatic detection of supported devices. It should also support manual search for devices by manufacturer, model and IMEI number

d) A multi-SIM adapter with support for Micro, Nano and standard SIM cards should be supplied. Ability to perform SIM data extraction from a SIM or USIM card.

e) 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.

f) 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, Unisoc Live, Kirin Live, 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.

3. Decoding, Review and Reporting Capabilities

a) Should have Case Management capability which allows users to create and manage cases and to provide case details and exhibit information. It should enable users to include multiple extractions and to apply the different enrichments.

b) Should include dashboard view to provide quick visual overview and display insights into the extracted data including commonly used applications, the most recent messages and enable investigator to quickly and easily drill down into the data of interest.

c) Dedicated location analysis view to clearly categorize the location records like device visited locations, locations of some significance, media derived locations and any other location data for detailed user analysis.

d) Capability to identify the origin of media items found within the device data to collect various metrics about a media item and apply logic to try to identify how the item originated, providing the user with information about the determined origin and the reasoning for that determination.

e) Should have the ability to parse windows computer data like DD, E01, RAW, L01, 001 or BIN images in the same application.

f) Should be built on a database architecture to reopen cases quickly without having to reprocess the data.

g) Should have a cryptocurrency enrichment to automatically identify the usage of cryptocurrencies and to detect wallet addresses and transactions within the device data.

h) It should also have an advanced cryptocurrency enrichment ability to provide a detailed analysis of the cryptocurrency assets associated with detected wallet addresses and highlight potential illicit activity. The enrichment should further provide risk severity and graphs on currency sent and received insights. This crypto enrichment result should be exportable to a report for individual wallet addresses.

i) Support for image carving and location carving

j) It should conduct on demand searches for viruses, spyware, Trojans and other malicious payloads in files.

k) Media classification capability to detect and categorize images and video frames into 20+ key categories. This capability should be selectable, allowing user to decide if he wants to run the media classification on a particular case.

l) Capability to verify file integrity with use of MD5 and SHA 256.

m) It should have a built-in SQLite Viewer.

n) Capability to match files extracted against Hash Databases and it should have built-in support for Project VIC, CAID and NCMEC hash databases.

o) Ability to generate and customize reports in different formats e.g., PDF, HTML, XML, Excel and Word. Global setting to select/unselect items in a report with ability to password protect the reports.

p) Provide a separate report with device information and user account information for quick reference of users.

4. Cloud Data Extraction Capabilities

a) Should allow access to remote cloud data sources to obtain, decode, save and perform analysis of this data.

b) There should be a single software interface in which users can review device data and cloud data through a single tool and with a unified experience, for a seamless and simplified review process.

c) Software should allow access to remote cloud data sources using cloud login keys from mobile devices supporting iOS and Android.

d) Support extraction of different content types from the supported data sources which includes messages, images, videos, files, contacts, calls, user profile, locations, user activities and backups.

e) Provide visibility of the cloud extraction progress to the user. It should provide a view of the current status of each data source extraction with an option to cancel the process if required.

f) Allow users to gather private user data with appropriate legal authority from over 50 of the most popular social media and cloud-based sources.

g) Capability to create cloud tokens from manually entered credentials for future cloud extractions.

h) Reporting of extracted data from the Cloud to human readable formats such as PDF, Word, Excel, HTML and XML. It should provide a global setting to select/unselect items in a report. The software should allow to password protect the reports.

5. Provide 2 TB SSD Hard disk for keeping backup storage facilities.

6. Tender Specific Authorization Certificate from the OEM in favour of the Indian Distributor/Reseller/Bidder is mandatory for participation in the tender.

7. **3 Years Subscription License**
8. **One-day training must be provided at the time of installation and setup. The training should be conducted on-site by an OEM-certified engineer.**
9. **The training must cover both basic fundamentals and hands-on sessions to ensure familiarity with all functionalities of the tool.**

III. High-End Analysis Workstation

Technical Specifications

1. A high-end analysis workstation is the Non-Plus Ultra when it comes to indexing and processing IT forensic cases at the workplace.
2. A high-end analysis workstation series is globally recognized and popular for its speed, reliability and durability.
3. A high-end analysis workstation is certified and tested for the use of the programs of the leading software manufacturers (like Access Data, OpenText, Magnet Forensics, etc.).
4. Chassis: Must be a Big Tower Case: 306(W) x 651(H) x 639(D) mm 11x 5.25 Bay Chassis.
5. Processor: Should have CPU 24-Core Intel® Core™ Ultra 9 Processor 285K (36M Cache, up to 5.70 GHz).
6. RAM: Should have RAM 128 GB (expandable up to 192GB).
7. Internal Storage:
    a. 1x 1TB SSD M.2 NVMe PCIe 4.0 x4 for OS.
    b. 1x 1TB SSD M.2 NVMe PCIe 4.0 for Cache.
    c. 1x 10TB Enterprise HDD SATA III for DATA.
8. Graphics Card: NVIDIA GF RTX, min. 6GB Memory, PCIe, min. 1x HDMI & 1x DisplayPort.
9. Mainboard: Should Intel Z890 LGA 1851 ATX-Mainboard with:
    a. 2x PCIe® 5.0 x16 slots.
    b. 1x PCIe 4.0 x16 slot.
    c. 5x M.2-Slots.
    d. Max. 256GB DDR5.
    e. Intel WIFI 7.
    f. 1x 10Gb Ethernet.
    g. 1x 2.5 Gb Ethernet.
    h. HDMI®.
    i. USB 3.2 Gen 2x2 Type-C®.

j. Front USB 3.2 Gen 2 Type-C®.

k. 2x Thunderbolt™ 5.

l. Aura Sync.

10. Should have integrated a Silent edition Write Blocker with IDE, SATA, USB, SAS, FIREWIRE, PCIe interface.
11. Must have a retractable ice tray internal cooler for suspected drive Two fans and Auto On / OFF.
12. Backplane:
    a. 3x Backplane, screwless hot-swap for additional 3.5" HDDs (2x empty, 1x occupied by HDD).
13. Power Supply: 1000WATT Modular Power Supply ATX, EPS12V, PS/2
14. Should have 1 RJ45 LAN port (Gigabit LAN controller).
15. Should have Optical Drives READ WRITE - SATA.
16. Front I/O:
    a. 1x USB 3.1 Type-C.
    b. 4x USB 3.0 Type-A.
    c. 1x FAN-/ RGB-LED-Control Unit.
    d. 1x Audio In/Out.
17. Should have 2x USB 3.1 ports (1 port at Type A, 1 port at Type C) Back Mounted.
18. Should have a 24-inch LED Monitor with Full HD (1920x1080) resolution, a keyboard and a mouse combo.
19. Forensic Card Reader with integrated 3-port USB Hub:
    a. Compact Flash = V6.0, PIO mode 6 / Ultra DMA mode 7 and LBA48.
    b. SD & micro SD: V1.0, V1.1, V2.0, SDHC, SDXC, V3.0 (UHS-1), V4.0 (UHS-II), MMC, RS-MMC, MMCmicro, MMCmobile.
    c. Memory Stick: MS V1.43, MS PRO V1.05, MS Micro V1.04, MS PRO HG Duo 1.03, MS XC Duo v1.00, MS XC HG Duo v1.00, MS XC Micro V1.00, MS XC HG Micro v1.00, MARS.
    d. Multi-LUN: access to several card slots during the same time.
    e. "Read Only / Read & Write" switch for all card slots, with LED indicator:
        - Red = Read Only.
        - Green = Read & Write.
    f. White LED indicator for card access.

g. 1x USB 3.1-port Type-A & 2x USB 3.1-port Type-C (5 Gbit/s) (downstream) Read & Write mode.

20. Adapters and Cables: Cables and adapters to image and process internal/external drives including:
    a. SAS.
    b. SATA.
    c. IDE.
    d. microSATA.
    e. SATA LIF.
    f. MacBook Air Blade Type SSDs.
    g. mini/micro-SSD cards.
    h. 1.8-inch IDE (iPod).
    i. 2.5-inch IDE (laptop).
    j. PCIe Card SSD Adapter.
    k. PCIe M.2 SSDS Adapter.
    l. PCIe Apple SSD Adapter.
    m. PCIe Cable.
21. Preinstalled Software:
    a. Windows 11 Pro with recovery media.
    b. Should have the capability for rapid, automated data acquisition.
    c. Should have support for digital data capture from removable media, mobile devices, computers, drones, and hard drives.
    d. Should have a simple, intuitive interface for users to perform media acquisition efficiently.
    e. Should have functionality that enables quick analysis of multiple devices.
    f. Should have live data viewing capabilities during the acquisition process to support real-time decision-making.
    g. Should have the ability to simultaneously secure and analyse data from multiple removable devices.
    h. Should have advanced inspection tools to display the target's file tree before initiating data extraction.
    i. Should have live streaming views of logical data as it is being captured into the platform.
    j. Should have powerful data carving tools to recover deleted data effectively.

k. Should have the ability to acquire data from hard drives extracted from damaged systems.

l. Should have a patented red-amber-green visual alert system for automated alerts on suspicious data.

m. Should have automation capabilities using predefined criteria for streamlined analysis.

n. Forensic Imaging Software:
   - FTK Imager.
   - Magnet Acquire.
   - EnCase Imager.
   - Tableau Imager.

22. Should have an External bootable HDD with pre-installed Backup Software.
23. Should be passed through 12/24 hours Burn-in Test with accurate results.
24. Incorporates features supporting forensic evidence handling and documentation practices.
25. OEM must be ISO 9001:2015 certified and the workstation should have a BIS (Bureau of Indian Standards) Certificate and a TUV quality certificate.
26. Product should carry a 3 (Three) Years On-Site Warranty.
27. Any Software/Firmware updates to be provided during the Warranty Period.
28. Tender Specific Authorization Certificate from the OEM in favor of the Indian Distributor/Reseller/Bidder is mandatory for participation in the tender.

IV. Digital Evidence Acquisition and Examination Software – 3-Year Subscription License

Technical specifications

1. Imaging and Triage Tool

a. Should provide comprehensive all-in-one capability to handle booted or live triage, targeted data collection, and forensic imaging for both Windows and Mac systems from a single USB device.

b. The product must enable booting both supported Mac and Windows systems from a single USB device, eliminating the need for multiple platform-specific devices.

c. The product should have the ability to deploy forensic analysis software on both Windows and Mac workstations.

d. Product should be able to triage and create images of Apple Silicon (M1-M4 chips) and T2 chips computers running macOS Big Sur 11 through macOS Tahoe 26, either running live on the host operating system, or running by booting from the product.

e. Should be able to create physical decrypted images of Apple's latest Mac computers utilizing the Apple T2 and M series chips. It should also produce a physical image of APFS fusion drives.

f. For T2 chipset, it should support decryption with password or recovery key.

g. For FileVault and CoreStorage, it should support decryption with keychain, password, or recovery key.

h. Should support AFF4 image format for imaging Mac computers with APFS Fusion or with T2 chips.

i. Ability to create images of selected files to a folder or the L01 logical evidence file format.

j. Should support writing to evidence storage configured with APFS, HFS+, exFAT, or NTFS file systems.

k. Provide the ability to format evidence storage onsite by using built-in tools without external dependency.

l. Ability to preview file contents prior to acquisition using a dedicated view, and to locate specific files using custom filters or keyword searches through a dedicated search interface

m. Ability to triage before data collection in both live and booted mode with the option to create predefined collection templates for rapid and repeatable collections.

n. Provide in-built tools for evidence storage management and compatibility with all major file systems.

o. Product must be able to boot the supported Mac and Windows systems via a single USB device.

p. Should support forensic imaging of macOS computers with APFS, HFS+, CoreStorage, FileVault, T2, M series, and Fusion in any combination.

q. Should support forensic imaging of computers running Windows with or without BitLocker enabled, NTFS/FAT, etc.

r. Should authenticate collected computer data using any or all MD5, SHA-1, or SHA-256 hash functions for the image and individual files.

2. Analysis Tool

a. Product should be able to give analysis platform to review computer forensic extractions to provide actionable intelligence from both Windows and Mac systems.

b. Product should run on Windows or Mac forensic workstations.

c. Product must be able to conduct search, filtering, and sifting through large data sets with simple or complex group filtering.

d. The filter criteria should include file name, file kind, file size, file extension, date created, date modified, date accessed, picture metadata attributes, including GPS coordinates and camera (iPhone/iPad device) type

e. Product must be able to support Windows artifacts such as device history from Microsoft Volume shadow copies, windows registry and Windows memory

f. Product should be able to automatically parse account information, web history, downloads and Windows 10 activity

g. Product should have support for different Windows OS artifact like jump list, shellbags, prefetch, volume shadow copies, link files, event logs, superfetch, recycle bin, user info, connected devices, last executed, NTFS ACL, file downloads, recent items, memory analysis, new Window activity, srum, notifications, Registry: amcache, bam, comdlg32, muicache, recentapps, shimcache.

h. Product must be able to support all macOS systems from Hierarchical File System (HFS) with File Vault or Core storage to APFS with T2 chips or fusion drives.

i. Product should be able to conduct review on device history from Apple File System (APFS) snapshots and Time Machine backups

j. Product must support E01, EX01, L01, RAW, DD, DMG and AFF4, AFF4-L file format.

k. Product should be able to display and search Unified logs, spotlight and built-in APOLLO support for Mac systems

l. Should support processing and analysis of the macOS Unified Logs

m. Product should be able to review health data, wallet transactions and calendar activity

n. The product should have powerful activity correlation for Windows and show how an artifact came to be and how it relates to other artifacts.

o. Product supports smart indexing and image categorization such as Porn, Weapons, Drugs, Extremism, Gore, Alcohol, Swim/Underwear, Documents, ID, Currency, CSAM, Chat, and Vehicles.

p. Product should support advanced timeline capabilities to allow the user to narrow activity and artifacts to a specific time frame.

q. Product should support extraction of text from documents, pictures and PDF using built in Optical Character Recognition (OCR).

r. Product must be able to link with child exploitation media database and must be able to integrate with Project VIC, Semantics21 and C4All.

s. It must be able to support ingestion of Berla vehicle forensic extractions for analysis

t. Must have the capability to share access to case data for offline review for both Windows and Mac systems:

u. A portable case file with case data, which can be exported along with a reader application for review of the case file

v. Export reports in a variety of formats including HTML, PDF, CSV, Excel and tab delimited formats.

3. **Provide 2 TB SSD Hard disk for keeping backup storage facilities**
4. **Tender Specific Authorization Certificate from the OEM in favour of the Indian Distributor/Reseller/Bidder is mandatory for participation in the tender.**
5. **3 Years Subscription License.**
6. **One-day training must be provided at the time of installation and setup. The training should be conducted on-site by an OEM-certified engineer.**
7. **The training must cover both basic fundamentals and hands-on sessions to ensure familiarity with all functionalities of the tool.**

V. Video Enhancement Software- Perpetual License with 3 Years Support

Technical specifications

1. General Specification

1. Must have at least 140 different filters and tools to enhance and process images and video files.
2. Must be a single stand-alone system protected by a USB dongle or by a digital license.
3. Must be able to decode video files with these codec frameworks: FFmpeg, FFMS, FFMS with Audio, DirectShow, Video for Windows, QuickTime (if installed on the system).
4. Must be able to bookmark frames and filters and customize their names, description, and folder.
5. Must provide batch renaming options of bookmarks, to easily locate them after the export.
6. Must be able to convert and export videos in proprietary formats, most of them without transcoding. Must support one or more variant of (at least) these formats: Milestone .xml/.pqz, USB Play archive, 000, 001… up to 099, 2, 264, 264001, 400, 600, 787, acsm, aira, ajp, ami, amv, aov, arv, ary, asf, asx, av, ava, av3, avc, avd, ave, avf, avi, avr, avs, awlive, bdb, bes, bfs, bin, bix, blk, bms, body, box, bpv, bu, bvr, bwm, bwv, car, cam, cbf, cme, cms, cv2, cx3, d, da, dar, dat, data, dav, db, dbx, dce, dcr, dga, djp, dmd, dmi, dmskm, dpv, drv, dv4, dv5, dvr, dvs, dvt, dxa, e, edr, eds, ethe,

evf, exe, exp, eye, ezvp, fl4, flm, g64, g64a, g64x, gbf, gop, h263, h264, h265, h64, har, hav, hevc, hgd, hik, hkv, hme, hvs, icf, ifs, igd, ifv, image, imf, img, irf, iva, ivf, jdr, kvf, jv, k26, l64, lmp, lvf, lwx, lxf, m2t, m2ts, m2v, m4v, m65, master, max, mdt, media, mgv, mjp, mjpg, mkv, mod, mov, mp4, mpc, mpg, mpg2, mrd, mts, mul, mva, mxg, noext, nov, n3r, nr3, nvf, nvr, nvt3, omv, par, pef, pic, pns, ps, psf, psx, pvf, pw3, qbx, raw, re4, rec, rf, rgm, rms, rmv, rsv, s, sm, sdc, sdr, sdv, sec, shv, snx, ssf, strg, stw, svs, synav, tav, teb, tmp, ts, tvr, ubv, umv, v, v264, var, vcr, vdd, vdx, vfs4, vid, video, video.data, vision, vls, vmf, vp6, vse, vmhrcd, vsr, webm, wmv, wnm, wsb, xa1, xi1, xba, xpa.

7. Must allow the selection of the timing source (average PTS, average FPS or data timestamp) when exporting a video.
8. Must be able to mux audio-only files into a video format
9. Must be able to create a writing queue to batch-export multiple video files.
10. Must be able to export variable and constant frame rate videos.
11. Must support any standard video format (avi, mp4, mkv, flv, 3gpp, wmv, mov…), also without the need of the codec installed on the system. Expandable by system codecs.
12. Must be able to perform the batch conversion of multiple video files, even if they have different file extensions and/or are distributed across different folders.
13. Must support any standard digital image format (i.e., jpeg (also HEIC-encoded), tiff, png, bmp, targa, tiff, jpeg2000, heif…) as well as at least one variant of the following ones: ico, gif, dcm, emf, eps, pcd, psd, xpm, 3fr, ari, arw, srf, sr2, bay, cr2, cap, iiq, eip, dcs, drf, k25, kdc, dng, erf, fff, mef, mos, mrw, nef, orf, ptx, pxn, R3D, raf, raw, rw2, rwl, dng, rwz, x3f, wbmp, webp.
14. Must be able to organize loaded images and videos in folders, possibly nested.
15. Must support Undo/Redo actions.
16. Must support GPU-accelerated encoding when transcoding videos with the H264 and H265 codec for conversion or export, either with CUDA or Intel Quick Sync Video.
17. Must be able to load more videos all at once.
18. Must be able to concatenate, extract the timestamp and demultiplex some proprietary video files during conversion
19. Must be able to track areas or target of interest (such as people or objects) through static, dynamic, manual, and keyframe-based tracking. MUST allow the copy of tracking data among multiple annotations so that they have matching movements when following a target.

20. Must be able to display frame type (I, P, B) for video files.
21. Must allow for all operations performed by the user to be logged on a text file, together with system info and other critical information. The feature can be optionally disabled.
22. Must be integrated with Milestone XProtect server, both connecting to the server and playing the exported images without prior conversion.
23. Must be able to load a subtitle file (in SRT or SMI format) and renders its text on the video.
24. Must be able to export the current video frames to a PDF with the number of images per page and paper size configurable by the user.
25. Must be able to export the original video/image as well as the processed one. If the chosen output codec for exporting a video is H264, different quality options are available.
26. Must be able to export the audio stream of a video if present.
27. Must be able to select only the Intra-coded Frames of a video (I-Frames).
28. Must have the project format in a simple and readable text which instructs the system on the filters and parameters to apply on specific files.
29. Must be able to import a project folder originally exported by Amped Replay.
30. Must provide the automatic generation of a report and must contain all the scientific methodology and details of the processing steps, settings, and the bibliographic references to the algorithms in HTML, PDF (optionally protected) or DOCX format.
31. Must allow for report generation in several different paper sizes
32. Must provide different report templates and must allow the creation of customized templates too. Must also allow for customization of destination folder and filename of the report.
33. Must be able to add footers and page numbers to the report.
34. Must provide volume and mute controls when audio is enabled.
35. Must allow for audio hearing when navigating the video frame by frame.
36. Must support multichannel audio for some formats.
37. Must be able to redact audio.
38. Must be able to add an audio stream to a video
39. Must be able to support audio-video synchronization, adding or subtracting a delay to an audio stream
40. Must be able to automatically add black frames when the audio track is longer than the video stream

41. Must allow to inspect the video file with different tools (FFMS, MediaInfo, FFProbe and ExifTool) and must offer the option to save the provided information onto a log file.
42. Must provide the RIFF Viewer tool to inspect the structure of files wrapped in an AVI video container.
43. Must be able to perform file analysis frame by frame, reporting detailed information about each frame and allowing to filter the results by frame type (video, audio, other data).
44. Must be able to perform video mixer overlays or display two different videos side by side.
45. Must be able to combine and sync multiple videos together.
46. Must support synchronization of video streams and similarity metrics computation.
47. Must be able to merge the audio and video streams from different filters. Must be able to put in sequence or side by side multiple videos, Must allow synchronizing the videos playback.
48. Must be able to apply the Picture in Picture effect to display a small image or video over a larger one
49. Must be able to convert a video with juxtaposed fields into an interlaced video.
50. Must correct the geometric distortion caused by capturing optics (barrel, pincushion, and fisheye lens distortion). Must support the selection of multiple lines for the estimation of the curvature to compensate.
51. Must include a camera calibration tool that allows generating and applying a distortion profile to accurately correct lens distortion.
52. Must be able to convert an omnidirectional image into a panoramic one.
53. Must have a homomorphic filter to adjust separately the contrast of the illumination and detail in an image.
54. Must have a Smart Adjust filter that automatically adjusts the local contrast and brightness in an image whilst mitigating halo artifacts.
55. Must be able to correct an uneven illumination in the image using the Retinex algorithm.
56. Must have a colour deconvolution filter to maximize the differences between specific colours in the image.
57. Must be able to perform component separation to separate signals due to different informative components in the image.
58. Must be able to calculate the input file hash code to check data integrity when loading the project. Must support several hashing algorithms.

59. Must be able to calculate the frame hash code with MD5 or SHA1 algorithms.
60. Must be able to correct the blur caused by linear motion, even when the motion parameters change between frames.
61. Must be able to correct the blur caused by wrong focus
62. Must be able to correct the blur by non-linear motion defined by the user.
63. Must be able to correct the blur caused by air turbulence on long distances or by high ambient air temperature/humidity.
64. Must be able to align the perspective of different images of the same object, taken from different points of view. Must support any kind of motion (shift, rotation, zoom, perspective changes).
65. Must be able to perform automatic perspective stabilization of the same object taken by different angles.
66. Must be able to visualize the macroblock type and motion vectors from a MPEG based video.
67. Must have a CTU analysis filter to examine the compression on h265/HEVC-based videos, with an option to visualize the variable size of the blocks.
68. Must have a super resolution feature that must generate a single higher resolution image by merging all the frames with subpixel motion estimation, even with different perspectives.
69. Must be able to stabilize a video focusing on an object with either static, dynamic or manual tracking.
70. Must be able to stabilize a shaking video automatically.

71. Must be able to adapt the video frame rate by duplicating or dropping frames retaining the original speed.
72. Must be able to change the video frame rate to export or play a video with a customized duration.
73. Must be able to perform video redaction to pixelate, darken or blur an area of interest in a video (for privacy reasons, witness protection, or sensitive subjects). Must be able to invert a hide selection and apply feathering to soften the edges of a hidden area.
74. Must support different tracking methods (either manual, software assisted or keyframe-based) and inverse selection.
75. Must be able to annotate images or videos with arrows, shapes, freehand drawings, magnification and spotlight effects. Each annotation Must be able to track a specific target (manually, with software assisted tracking, or by setting keyframes). It Must be possible to set a different colour for

each annotation, also by using an eyedropper tool to pick colour from image pixels

76. Must support for visual hints and snapping, to assist the user to align annotations.
77. Must support the grouping of annotations. Grouped annotations Must be able to track object together.
78. Must be able to freeze a selected frame for a set amount of time.
79. Must be able to create an empty video showing a coloured frame or a still image for a specified time
80. Must be able to display subtitles on the video frames with customizable font, colour, size and position.
81. Must be able to indicate date and time for the current frame and font, colour, size and position must be customizable.
82. Must be able to superimpose a grid onto the image or video which is useful for compression estimation and other analysis.
83. Must be able to play back the video in the reverse direction.
84. Must be able to take a measurement on the image with a reconstruction model of the perspective. Must support error calculation.
85. Must be able to estimate the speed of an object that is moving over a flat surface. Must support uncertainty calculation.
86. Must be able to copy the evidence files stored in an external removable device, verifying the match between the source hash codes and the destination hash codes in order to check the integrity for a safe acquisition. Must generate an automatic report/log of the action performed.
87. Must be able to directly load the securely copied multimedia files into the software and must be able to send user-selected videos directly to the batch conversion engine.
88. Must be able to add the information related to the secure copy into the report of the project.
89. Must support playback of variable frame rate video based on presentation timestamps.
90. Must support playback speed based on timestamp values.
91. Must allow adding, shifting, interpolating and refining timestamps. Must also allow for region selection and tracking in the filter options.
92. Must be able to reduce the blocking artifacts caused by JPEG compression.

93. Must have multiple denoising, sharpening and intensity adjustment filters.
94. Must be able to invert and replace the colour channels of an image with another.
95. Must be able to process and optionally record live video from a DirectShow compatible source.
96. Must be able to load multiple images together to work on them as if they were frames of a single video file.
97. Must include a special seek function which allows to move on user specified intervals based on units of (frames, Iframes, or different time units).
98. Must include a decimation function to remove frames based on a user-defined step value.
99. Must be able to send, with a single click, the current image to Word, PowerPoint or copy it onto the clipboard for pasting in any other tool.
100. Must have the notes panel always available on screen and the notes Must be automatically saved with the project.
101. Must have the ability to integrate screen capture with the option to save standard uncompressed video files for maximum quality and compatibility.
102. Must be able to view, grab and process any stream coming from a DirectShow compatible device.
103. Must include more than 50 different sample projects and files to learn how to apply the software in numerous situations.
104. Must be able to select frames of the video within an interval with an optional frame step. MUST support the trimming of the original video stream without transcoding.
105. Must be able to select a list of frames that are defined by the user.
106. Must be able to select frames at a discretional interval, to retain a constant pattern of frames and remove all the others (e.g. to quickly demultiplex videos with a fixed pattern).
107. Must allow to correct the perspective of objects in an image (e.g., rectifying a license plate).
108. Must be able to reduce the noise integrating current and previous frames and avoiding halos on moving objects.
109. Must be able to put side by side the original and the processed image.
110. Must be able to add logos, text with dynamic macros and shapes on images and videos.

111. Must allow users to validate results by automating the pixel verification of processed images and videos between projects created using different versions of the software and/or different host computers.

2. **Provide 4 TB SSD Hard disk for keeping backup storage facilities.**
3. **Tender Specific Authorization Certificate from the OEM in favour of the Indian Distributor/Reseller/Bidder is mandatory for participation in the tender.**
4. **Perpetual License with 3 Years Support.**
5. **One-day training must be provided at the time of installation and setup. The training should be conducted on-site by an OEM-certified engineer.**
6. **The training must cover both basic fundamentals and hands-on sessions to ensure familiarity with all functionalities of the tool.**

VII. Image Authentication Software-Perpetual License with 3 Years Support

Technical Specifications

1. Must have at least 40 analysis filters with optional user-customizable configuration and post-processing parameters (levels, scale to enhance the displayed image).
2. Must be compatible with all the most common image formats and many of the uncommon ones too: BMP, GIF, JPEG, JPEG 2000, TIFF, PNG, TGA, ICO, DICOM, EMF, EPS, Photo PCD, XPM, PSD, HEIF, AVIF and RAW camera formats from most manufacturers.
3. Must be compatible with all the most common video formats (MP4, MOV, MKV, 3GP).
4. Must allow the image, video or project loading by means of drag and drop onto the GUI.
5. Must automatically apply all filters to one image or all images in a folder and include support for nested folders.
6. Must provide hints for each filter by hovering over them with the mouse.
7. Must display RGB values and luminance (Y) when hovering the mouse over pixels. The inspected values can be copied to the clipboard.
8. Must generate an automatic output image and report with all processing results on one or more images and the user can customize the output image size and the custom destination folder.
9. Must be able to create and save projects.
10. Must be able to generate a project report in HTML, PDF (optionally protected), and DOCX format.

11. Must perform a quick automatic analysis of the format of all images in a folder to find suspicious files (triage).
12. Must export a multiple image file format analysis results table directly to Microsoft Excel for further processing.
13. Must display image and video location in Google Maps.
14. Must search for similar images on Google Lens, starting from the evidence image or video frame.
15. Must be able to check sun position for image or video location and date on Suncalc.
16. Must search for images from a specific camera model on Flickr and support advanced image features filtering.
17. Must search for images from a specific camera model on Camera Forensics and support advanced image features filtering.
18. Must extract JPEG images embedded in any file type (image files, PDF, PPT, DOC, disk image...) for questioned document authentication support. MUST be able to automatically load into the program the images extracted from the PDF.
19. Must be able to perform customization of all the criteria for evaluating the camera original files.
20. Must be able to check whether the image likely comes from a known social media platform.
21. Must be able to make the filter's label appear in red, if the analysis of an image detects signs of manipulation.
22. Must be able to display/compare main JPEG markers.
23. Must have integrated hexadecimal viewer with search capabilities.
24. Must display/compare JPEG Huffman Tables of the main image, embedded thumbnail, and preview.
25. Must perform analysis of the colour space usage of the image in the HSV and Lab coordinates to help spot excessive colour adjustment.
26. Must identify manipulated areas of the image based on DCT-domain analysis of aligned double JPEG quantization artifacts (ADJPEG).
27. Must identify manipulated areas of the image based on DCT-domain analysis of non-aligned double JPEG quantization artifacts (NADJPEG).
28. Must identify manipulated areas of the image based on the joint analysis of JPEG Ghosts Map, Blocking Artifacts, ADJPEG and NADJPEG.
29. Must perform automatic identification of tampered areas of the image by comparison with the PRNU reference pattern of the image.

30. Must allow to inspect the video file with different tools (FFMS, Media Info, FF Probe and Exif Tool) and MUST offer the option to save the provided information onto a log file.
31. Must run the PRNU analysis to images and video frames (within the technical limitations) and MUST compare two different camera reference patterns. Must be able to extract video frames for generating the camera reference pattern file, without using external tools.
32. Must include a PRNU video tampering tool.
33. Must detect geometrical transformations (such as scaling and rotation) while carry out the PRNU analysis on videos.
34. Must be able to perform VPF (Variation of Prediction Footprint) Analysis to detect whether a video was encoded twice during its life cycle.
35. Must allow the range-based analysis on videos.
36. Must identify similar areas of the image that can be the result of cloning.
37. Must identify groups of similar points in the image that can be the result of cloning.
38. Must be able to detect faces in the image and classify each face as being a deepfake generated by a GAN (Generative Adversarial Network) or not. It must provide a confidence score for either class.
39. Must be able to detect synthetic deepfake images generated by several Diffusion models, including Stable Diffusion, DALL-E, Midjourney, Flux, Nano Banana, GPT Image and Grok. It must provide a confidence score for the binary output (compatible or not compatible with a known AI model). Must be able to carry out such an analysis by batch processing the entire evidence folder.
40. Must check the consistency of cast and attached shadows within an image or video frame.
41. Must check the consistency of reflections within an image or video frame.
42. Must automatically add to the generated report a warning concerning inconsistency of shadows or reflections
43. Must check if elements within an image or video frame have a consistent perspective.
44. Must be able to hide sensitive visual details by means of blur, pixelation and blackening, with also the possibility of applying an inverted selection.
45. Must support bookmarking output images and MUST support drawing graphical annotations on bookmarked output images.
46. Must allow to copy annotations from one bookmark to another.

47. Must allow to inspect the macroblocks type and their compression level in MPEG based videos (with H264 codec), and MUST allow the generation of a customizable plot.
48. Must allow to inspect Coding Tree Unit (CTU) block types and related motion vectors in HEVC/H265 videos.
49. Must have the RIFF Viewer tool to inspect the structure of files wrapped in an AVI video container.
50. Must allow to inspect the coding details of a video at the frame level (PTS data, decoding and display frame order, packet size).
51. Must allow computing the pixel hash of all frames in a video and export it to TSV format
52. Must allow visualizing blocks that remained unchanged between consecutive frames, and MUST allow the generation of a customizable plot.
53. Must allow extracting and displaying a specific colour channel of an image or a video.
54. Must allow for file relocation when loading a project whose original input media was moved
55. Tender Specific Authorization Certificate from the OEM in favour of the Indian Distributor/Reseller/Bidder is mandatory for participation in the tender.
56. Perpetual License with 3 Years Support.
57. One-day training must be provided at the time of installation and setup. The training should be conducted on-site by an OEM-certified engineer.
58. The training must cover both basic fundamentals and hands-on sessions to ensure familiarity with all functionalities of the tool.

VI. DVR Data Extraction Tool

Technical Specifications

1. The software shall possess the capability to extract and recover video evidence from Digital Video Recorders (DVRs) in a forensically sound manner, ensuring end-to-end data integrity is maintained throughout the investigative lifecycle.
2. It shall be compatible with more than 50 widely used video formats, encompassing proprietary formats and standard formats such as H.264, MOV, MP4, and AVI, from a wide array of recording equipment, including DVRs.
3. The platform shall facilitate video evidence retrieval from cloud-based surveillance systems, including Ring and Arlo, using authorized access credentials.

4. It must enable the recovery and examination of video data and related metadata from various sources such as body-worn cameras, dashcams, drones, and mobile phones, while supporting decoding of Open AVI and MP4 files using appropriate encoding standards.
5. The software shall compute and log MD5, SHA-1, and SHA-256 hash values for all acquired video files to maintain forensic authenticity.
6. Upon connecting a DVR storage or forensic image, the system must automatically present granular detection information, including the file system's label, version, format type, and output details.
7. The tool shall provide keyboard shortcuts for essential functionalities like case initiation, report creation, incident tagging, bookmark insertion, application settings, and toggling case views, improving examiner productivity.
8. A dedicated dashboard panel must offer an at-a-glance reference of all available keyboard shortcuts for ease of use during investigations.
9. Separate processing workflows shall be offered for accessible and inaccessible scans, allowing for faster processing when direct file access is available or deeper bit-level scanning when needed.
10. The system should include the ability to bypass indexing processes during video extraction or scan operations to improve speed and efficiency.
11. Targeted scan options should allow investigators to limit analysis to accessible video files only when known evidence exists.
12. A streamlined interface should permit direct launch of previously accessed cases from the startup screen for improved investigation continuity.
13. Post-scan export functions shall be configurable to execute automatically upon scan completion, enabling batch exports in PDF or Excel format to user-defined destinations with chosen media encoding and hashing options.
14. Investigators should be able to define parameters for post-scan exports in advance, including filters for date/time range, camera channels, and thumbnail selection from particular source devices.
15. The application shall support pre-configurable scan filters and time offset settings prior to extraction to reduce analysis time and enhance result relevance.
16. A synchronized matrix viewing capability must allow simultaneous preview of a minimum of four video feeds to support comparative video analysis.
17. The tool should support the ability to add notes, labels, and bookmarks to video clips to aid in review, collaboration, and final report generation.
18. Users must be able to isolate and export relevant segments from larger video files through sub-clipping functionalities to focus on specific evidence.

19. The platform shall allow filtering of video evidence using date, time, recurring time ranges, or specific days of the week.
20. Clip lists must be filterable by attributes such as file size, clip duration, source, camera channel, unknown channels, bookmark status, and tag status.
21. The system must eliminate the need for passwords or third-party decryption tools and offer a seamless user interface without complex navigation.
22. Evidence collected from multiple locations and devices must be organized within a hierarchical case structure to streamline complex investigations.
23. The software should facilitate recovery of deleted or partially overwritten video footage from supported DVR devices.
24. The sub-clipping tool must allow precision trimming of footage to capture seconds of critical evidence from hours-long video content.
25. Playback controls shall offer multiple speed options including 0.5x, 1x, 2x, 4x, 8x, and 16x for efficient video review.
26. Users shall be able to visually highlight significant clips, segments, or frames, while attaching annotations using tags and bookmarks that can be shared with stakeholders.
27. Default configuration values and workflow preferences shall be customizable to apply consistently across all future investigations.
28. A color-coded notification system (red, yellow, green, white) shall indicate alert levels and status messages clearly.
29. The system shall support pause and resume functionality for any job or process currently in execution.
30. Pre-scan diagnostics shall offer advanced settings such as forcing sector size to 512, manual sector count specification, and selective file system detection to handle problematic media.
31. Automatic thumbnail generation shall be supported for all compatible video files, with an option to manually select thumbnails directly from the playback timeline.
32. Column headers within clip views shall be repositionable using drag-and-drop interaction and allow grouping of video clips by selected attributes.
33. Users should be able to explore and build custom playlists and clip lists, queueing items for batch export on-the-fly or at a later stage.
34. The application must generate forensically secure reports at any stage during the video extraction or upon closing a case.
35. An interactive reporting tool shall be embedded to generate diverse formats of reports such as summaries, clip tables, gallery previews, audit trails, and export documentation.

36. Multiple report exports should be supported simultaneously to different folder destinations without any functional restriction.
37. Supported evidence sources shall include physical DVR drives, forensic image formats (DD, E01), video clips from a variety of devices, and cloud-hosted videos from Ring and Arlo with multi-factor authentication.
38. The application must allow forensic correction of timestamp inaccuracies by applying offsets to individual or grouped video clips.
39. Exported clips must be capable of displaying corrected date/time information as overlay text to reflect accurate forensic timelines.
40. The tool must include built-in prompts and notifications for software updates and newer versions.
41. A complete audit logging mechanism shall capture and record every investigator action, filter used, and system event, with export options for oversight and case documentation.
42. Export tasks must support queueing of clips directly from the clip view or during real-time playback preview.
43. A dedicated Case Summary section must be provided that consolidates all relevant case information such as Incident Details, Locations, Source Devices, Case Metrics, and the complete action log.
44. The software shall offer both dark and light visual modes, allowing examiners to switch themes to reduce visual fatigue during prolonged case reviews.
45. The platform shall feature a utility tool designed for frontline officers to capture and document transient digital evidence, allowing it to be installed and operated concurrently on any number of Windows laptops or tablets to record DVR footage in a forensically valid format, applying timestamp and cryptographic hash (MD5 & SHA).
46. This utility must allow documentation of date and time discrepancies present in the DVR system directly at the scene of the crime.
47. The tool must enable acquisition of photos and videos using built-in or connected cameras, as well as through devices like memory cards or phones belonging to witnesses or victims, embedding metadata such as geolocation, source device ID, and hash values into generated reports.
48. 3 Year Subscription License
49. One-day training must be provided at the time of installation and setup, conducted on site by an OEM-certified engineer. Training must cover both basic fundamentals and hands-on sessions to ensure familiarity with all functionalities of the tool.
50. Tender Specific Authorization certificate from the OEM in favour of the Indian Distributor/Reseller/Bidder is mandatory for participation in the tender.

51. Provide a 2 TB SSD External Hard disk for backup storage facilities.

VIII. Logicube Falcon NEO 2 - 3 Years Hardware Warranty

Technical Specifications

1. The Forensic Field Imager represents the pinnacle of forensic imaging technology, designed to deliver unprecedented speed, efficiency, and versatility in data acquisition.
2. The device should have the capability to surpass 100GB/min E01 capture speeds, making it the first field imager to achieve such performance. It should be able to image SAS-3 SSDs at speeds up to 115GB/min and handle PCIe drives at speeds exceeding 100GB/min.
3. The device should have a SAS-3 (12 Gbps SAS) architecture and should support up to 5 simultaneous tasks.
4. The device should include built-in security features to protect data integrity and prevent unauthorized access, ensuring that sensitive forensic data remains secure.
5. Capable to imaging/clone data from one to one, two to two or one to many destination media.
6. The device should be equipped with an extensive array of ports to support various imaging tasks:
    a. Source Ports: Should have up to 10 source ports to connect multiple devices.
    b. Destination Ports: Should have up to 11 destination ports for efficient data transfer.
    c. USB Ports: Should have USB 3.2 Gen-2 (10Gbps) ports for fast and reliable connections.
    d. Network Ports: Should have two 10GbE ports for imaging to and from network repositories, facilitating high-speed network-based acquisitions.
7. Support multiple Imager Formats, copy, dd image, .dmg image, e01, ex01, supports MD5, SHA1, SHA256 and dual-hash (MD5+SHA-1) authentication.
8. The device should be portable and lightweight, making it easy to transport and deploy in various field locations.
9. Should have Cloud Storage Acquisition (now included as a standard feature) allows you to acquire files from OneDrive, Dropbox, or Google Drive. Capture to any destination drive or network repository connected.
10. 10 write-blocked source ports include 4 SAS/SATA drives supported with 1 port, 2 USB 3.2 (Gen 2), 1 PCIe, 2 I/O ports for use with optional I/O cards including Thunderbolt™ 3/USB-C, 10GbE.

11. Multiple Imaging Ports:
    I. **Write-protected source ports include**:
        a. 1 SAS/SATA (SAS-3/12Gbps) that supports up to 4 drives with a single cable.
        b. 2 USB 3.2 Gen 2 (can be converted to SATA using an optional USB to SATA adapter).
        c. 1 PCIe.
        d. 2 I/O ports for use with optional I/O cards including Future Expansion Thunderbolt 3/USB-C.
    II. **Multiple destination ports include**:
        a. 1 SAS/SATA (SAS-3/12Gbps) that supports up to 4 drives with a single cable.
        b. 4 USB 3.2 Gen 2 (can be converted to SATA using an optional USB to SATA adapter).
        c. 1 PCIe.
        d. 1 I/O ports for use with optional I/O cards including Future Expansion Thunderbolt 3/USB-C.
12. Should have Two 10GbE network ports for network connectivity.
13. 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.
14. 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.
15. Capable Web Browser/Remote Operation to allows to connect with device from a web browser.
16. Capable to cross copy support for IDE, SATA, e SATA, microSATA, SAS, ZIF and USB interface and combine-SATA etc. 3 | P a g e
17. Should image CD/DVD/Blu-ray media by using a USB optical drive connected to the USB port on the device.
18. Capable to Detect and capture Host Protected Areas (HPA) and Device Configuration Overlay (DCO) hidden areas on the source (suspect) drive.
19. Should capture network traffic, internet activity and VOIP.
20. Capable to Generate Audit Trail Reporting/Log Files in XML, HTML or PDF format.

21. Should secure sensitive evidence data with whole-drive AES 256-bit encryption.
22. 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.
23. Forensic, Filter-Based File Copy, users can filter and then image by the file extension (such as .PDF, .xls, .JPEG, .mov etc.).
24. Capable to acquire data over a network.
25. Capable to generate the log of the processes.
26. Capable to boot/mount the suspect media virtually in a write-protected environment for the preview of live data.
27. HDMI Port for connecting display.
28. Incorporates features supporting forensic evidence handling and documentation practices.
29. Should come with:
    a. 1 x M.2 to PCIe Adapter (F-ADP-M2-PCIE3)
    b. 1 x Mini PCIe (mPCIe) to PCIe Adapter (F-ADP-MINI-PCIE)
    c. 1 x M.2 to SATA Adapter (F-ADP-M.2-SATA)
    d. 1 x PCIe to PCIe extender cable (F-ADP-PCIE-CBL)
30. **Product should carry 3 Years On-Site Warranty. Any Software/Firmware updates to be provided during the Warranty Period.**
31. **Tender Specific Authorization Certificate from the OEM in Favor of the Indian Distributor/Reseller/Bidder is mandatory for participation in the tender.**

IX. Technical Specification for FRED- Forensic Workstation

Technical specifications

SL No.	Parameters	Specification
1	Processor	Intel Ultra 9 285K, also 24 Cores, 8 P/16 E Cores, up to 5.7 GHz, 36 MB Intel Smart Cache
2	RAM	128 GB Memory PC5-38500 DDR5 4800 MHz- (4X32GB)

3	OS, Cache & Storage Drives	a) OS Drive - Internal PCIe M.2 NVMe SSD: 2 TB M.2 NVMe PCIe Solid State Drive - 990 PRO Series b) Drive 2 - Internal PCIe M.2 NVMe SSD: 2 TB M.2 NVMe PCIe Solid State Drive - 990 Pro Series c) Drive 3 - Internal PCIe M.2 NVMe SSD: 2 TB M.2 NVMe PCIe Solid State Drive - 990 Pro Series d) Drive 4 - Internal PCIe M.2 NVMe SSD: Available for future upgradability e) Drive 5 - SATA Interface: 4 TB 7200 rpm SATA Hard Drive f) Drive 6 - SATA Interface: Available for future upgradability g) Drive 7 - USB 3.2 Interface: Available for future upgradability h) Drive 8 - USB 3.2 Interface: Available for future upgradability i) Drive 9 - USB 3.2 Interface: Available for future j) Upgradability k) Drive 10 - USB 3.2 Interface: Available for future upgradability
4	Graphic Card	NVIDIA RTX 3050, 8 GB, 128-bit GDDR6, 2560 CUDA Cores
5	Display	24” LED
6	Operating System	Licensed Windows 11 Professional (64-bit), Additional Linux with Dual Boot Option
7	Include Hardware Write Blocker with the following support for:	a) USB 3/2/1.1 b) PCIe c) SATA, IDE d) Firewire 800/400 e) SAS
8	Integrated Hardware Write Blocker should have listed features:	a) Touch screen interface b) Connected to the board on USB 3.1 c) Write-Block and Read/Write visibility via Lock/Unlock LEDs d) Read and write mode capabilities for all device ports controlled via LCD Menu to enable the investigator to use the Write Blocker as a Drive Wiper for USB/SATA/IDE/FIREWIRE/SAS/PCIe drives when required by the users e) Allows simultaneous imaging of 2 attached devices on the integrated Write Blocker Allows forensic imaging of at least 4 SATA Drives simultaneously
9	Memory Card Writer Blocker:	Integrated Forensic Media Card Reader Read-Only or Read-Write mode capable
10	Dock with cooling system for Evidence Hard Drive	Integrated Retractable imaging shelf (fully retracts into the system when not in use). Dual fans for maximum cooling and surface coverage auto on/off switch when the shelf is opened or closed. Slotted, cushioned, nonconductive, non-skid, surface supports all popular Drive sizes (3-1/2", 2-1/2", 1.8", etc)

11	Hot swappable bays and Optical Drive	a) 2 x Shock Mounted SATA Removable Hard Drive Bays b) 4 x Hot Swap Shock Mounted Universal Removable Hard Drive Bays. All Hot- Swap Bays should be Read-Only or Read- Write mode capable. c) BD-R/BD-RE/DVD±RW/CD±RW Blu-ray Burner Dual-Layer Combo Drive
12	Others integrated components	a) 1 X RJ45 LAN port b) USB 3.1 (Minimum 2 ports) c) USB 3.1 Type-C (Minimum 1 port) d) USB 3.0 (Minimum 8 ports) e) USB 2.0 (Minimum 2 ports) f) Keyboard and Mouse Combo
13	Internal connections	All components such as the Integrated Write Blocker, Hot Swap bays and USB Hub should not be connected on the motherboard and should have different connections to avoid IRQ hardware confliction.
14	Toolkits	Adapters and Cables: Cables and adapters to image and process internal/ external drives including SAS, SATA, IDE, Micro SATA, SATA LIF, MacBook Air Blade Type SSDs, mini/micro-SSD cards, PCIe SSD m.2 NVMe, PCIe SSD MacBook Pro and Server Class PCIe SSD Security. **Screwdriver Set: A varied assortment of popular security bits for opening computer enclosures that may have been locked down in a corporate environment.**
15	Warranty	The product should carry a 3 (Three) Years On-Site Warranty. Any Software/Firmware updates should be provided in the Warranty Period.
16	Proof of Manufacturing of Forensic Workstation	Product offered should be of International Repute & Brand and should not be a customised/assembled Product from various sources. Either the Manufacturing License of the OEM should be attached or the Product Offered should have at least 23 Components which are marked by the OEM Name preferably on the various PCB's used in the offered Forensic Workstations.
17	MAF	A Tender Specific Authorization Certificate from the OEM in favour of the Indian Distributor/Reseller/Bidder is mandatory for participation in the tender.
18	Training	Training to be done by an OEM-certified engineer at the time of Installation and as per request.

X. Financial Investigation and Analytics Software (Perpetual License with 3 Years Support)

General Specifications

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.
2. The system should ensure the automated acquisition and processes individual files or it should be done in batch mode.
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
    a. Value Date
    b. Description (ATM Withdrawal, To Transfer, RTGS, NEFT, Cash)
    c. Reference Number, Cheque No.
    d. Debit
    e. Credit
    f. Balance
5. The system should allow users to categorize the data on various parameters 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 an individual account.
7. The system able to identify high value/low value debit/credit transaction with conditions (>, <, =) specified amount.
8. The system to identify high value/low value debit/credit transactions between two entities over a specified period of time.
9. The system able to identify and list all transactions done in one account by different modes like NEFT, RTGS, Cheque and Cash
10. The system able to identify and list all debit/credit transactions where the transaction type is cash. (or any other mode like NEFT, RTGS, Cash)
11. The system should be able to identify the frequency of transactions between two accounts. The system should also be able to identify on the basis of the 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.

14. The system to enable the user to analyze 'text fields' of the transaction data. (i.e., Transaction Description)
15. The system should allow users to analyze cumulative data of all the years by merging different files together.
16. The system should allow users to merge transaction data of one or more individuals spread over a single or multiple entities, further spread over single or multiple entity branches.
17. The system should allow the 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.
19. The system should allow users to perform customized searches using logical and financial formulae. (And, Or Not). The system should allow users to cross manipulate among different result sets.
20. **Provide 2 TB SSD External Hard disk for backup storage facilities.**
21. **Tender Specific Authorization Certificate from the OEM in favour of the Indian Distributor/Reseller/Bidder is mandatory for participation in the tender.**
22. **Perpetual License with 3 Years Support.**
23. **One-day training must be provided at the time of installation and setup. The training should be conducted on-site by an OEM-certified engineer.**
24. **The training must cover both basic fundamentals and hands-on sessions to ensure familiarity with all functionalities of the tool.**

XI. Blockchain Investigation and Cryptocurrency Analysis Software for 6 Users - 3-Year Subscription License

Technical Specifications

1. The solution should offer an interactive visual representation of transactions across multiple layers, tracing from the input address to the final exchange.
2. **The solution must provide full coverage for a minimum of 30 blockchains, including but not limited to Bitcoin, Ethereum, Linea, Tron, SUI, Aleo, VerifiedX, Platon, Canton and ICP. It should offer coverage for over 3,000 tokens and enable unlimited analytical capabilities across all supported blockchain networks.**
3. The solution should provide access to crypto-currency forensic investigation platform for a period of three (3) years, with the capability to create and manage up to 6 user accounts within the organization.

4. The OEM shall provide a warranty for a period of three (3) years from the date of activation, which includes regular product updates, feature enhancements, and maintenance support during the warranty period.
5. The solution should depict both direct and indirect exposure of transactions to any suspicious activities involving real-world entities, such as exchange transfers, unnamed service scams, P2P exchanges, mixers, mining pools, high risk exchanges, gambling, terrorist financing, CSAM, narcotics, and similar activities.
6. **The solution should offer clearly differentiated functionalities for address/wallet tracing and transaction-level tracing, enabling users to perform each type of analysis independently through dedicated interfaces.**
7. It should allow real-time database updates within an active session without the need to close the application interface.
8. Support for automated investigations to instantly expand and visualize both direct and indirect wallet exposures to real-life entities with a single click without having to manually expand every node.
9. Provision of comprehensive training on the tool, its technology, and usage for users designated to mentor and assist others within the organization. Regular periodic training, including updates, should be provided for the tool, along with complete technical support for the entire team.
10. Should have coverage of digital assets that represent at least 97% of total global crypto market capitalization.
11. **Support for cross-chain tracing of at least 45+ de-fi bridges including but not limited to Thorchain, Synapse protocol and offer seamless visualizations of such transactions**.
12. The solution must include a risk alerting and transaction monitoring capability, with AI-driven chat-based functionality to generate concise summaries and contextual insights from risk alerts.
13. Ability to share password protected graphs across users within the organizations and outside of organizations
14. Support for continuous monitoring of real-time transactions with a customizable real-time alerting feature.
15. Access to a directory of Virtual Asset Service Providers (VASPs) for contact details and legal processes
16. Support for clustering selected wallets, assigning custom names and colours, and viewing aggregate transaction values for the entire cluster.
17. The platform should provide deconfliction intelligence, highlighting whether specific wallet addresses or entities under investigation have already been flagged by other law enforcement or government agencies using the tool.

18. Should adhere to security frameworks and standards, including ISO 27001, SOC II, and GDPR certifications.
19. Should have the ability to split/delete transactions between addresses to segregate tokens from native assets and to separate out transactions or assets which are important for the case and either hide the rest or display them separately.
20. Support for sequential and custom investigation board layout with an option to toggle between both curved and straight-line transfer links between wallets
21. Should provide specific exchange clusters and associated deposit addresses with real-time data.
22. Ability to download filtered data as reports in CSV format for analysis and documentation.
23. Must have the ability to filter exposure and counterparties by categories and sub categories of illicit activities for both receiving and sending transactions.
24. The tool should have the ability to display both complete transaction values with all decimal points and rounded values as needed.
25. The tool shall allow investigators to manually add custom nodes on the investigation board, enabling the incorporation of off-chain intelligence. These nodes should be linkable to on-chain wallet addresses, supporting comprehensive case-building and contextual analysis.
26. Support for adding comments/notes on the graph to highlight findings, with an option to disable them.
27. The tool should have enhanced search functionality to retrieve addresses by entity name, partial wallet addresses, and allow fetching multiple addresses and transactions simultaneously.
28. Support for analyzing smart contracts, viewing similar contracts, and exploring other contracts created by the same owner.
29. The solution must support attribution derived from Open-Source Intelligence (OSINT), with references to the original intelligence sources made available to the user for deeper analysis and validation.
30. Should support real-time identification and clustering of certain high-risk jurisdiction VASP wallets.
31. Ability to search UTXO transactions from an address node, select the relevant transactions for the case, and selectively include certain senders and receivers while excluding others.
32. The tool should maintain robust deterministic evidence for attributions and include an in-built option to directly share intelligence with the team, which will be reflected in the product upon validation.

33. The tool should have the ability to add off-chain custom nodes to the investigation board.

34. The OEM must have a registered R&D office in India and must possess a 'Make in India' certificate. Participating vendors must provide an authorization certificate issued by the OEM.

35. Tender Specific Authorization Certificate from the OEM in favour of the Indian Distributor/Reseller/Bidder is mandatory for participation in the tender.

36. 3-Year Subscription License

37. One-day training must be provided at the time of installation and setup. The training should be conducted on-site by an OEM-certified engineer.

38. The training must cover both basic fundamentals and hands-on sessions to ensure familiarity with all functionalities of the tool.

Warranty, Support & Maintenance

- All supplied hardware, software and systems shall be covered under the applicable OEM warranty/support period specified in the tender.
- The bidder shall coordinate with respective OEMs for warranty support.
- The bidder shall provide installation and configuration support during the warranty period.
- Defective equipment/components shall be repaired or replaced as per the applicable warranty terms.
- Software licenses and subscriptions shall remain valid for the specified license period.
- The bidder shall provide technical support and troubleshooting for the complete integrated solution.

1. Overall Responsibility

The bidder shall be responsible for the complete end-to-end supply, delivery, installation, configuration, integration, testing, commissioning, training, documentation and handover of the entire infrastructure covered under the BOM, including all necessary components, accessories, licenses, cables, connectors, mounting hardware, power connections and other items required for a fully functional solution, whether or not each individual item is explicitly mentioned in the BOQ.

2. Contract Period

The selected firm shall complete the delivery, installation, configuration and commissioning of all items listed in the Tender notice within **90 days (Ninety Days)** from the date of issue of Work Order/Supply Order.

The timelines specified are mandatory and must be strictly adhered to by the firm.

- After successful installation, testing, and acceptance by the Department, the firm shall provide free maintenance, technical support, and necessary software/firmware upgrades for all supplied hardware, software, tools, and systems in the specified period.
- The selected firm shall execute an Agreement with the Department covering:
- All delivered items must remain fully operational, updated, and properly maintained throughout the entire contractual period. The Department reserves the right to impose penalties or take action as per norms in SLA for any lapse in performance, maintenance, or support.

3. Eligibility Criteria

Sl No	Technical Criteria	Supporting Documents
1	The Bidder must be registered in India and have been in operations for a minimum of 3 (three) years as on the date of bid opening.	Copy of GST Registration Certificate and PAN or COI
2	The bidder shall have achieved an average annual turnover of at least ₹50 Crores from IT Infrastructure business during the last three (3) financial years.	Audited financial statements for the last 3 FYs
3	The bidder must not have been blacklisted, debarred, or suspended by any Central Government, State Government, or PSU organization during the last three (3) years as on the date of bid submission.	Undertaking on company letterhead signed by Authorized Signatory.
4	Bidder must have positive net worth for each of the last 3 financial years.	Audited Balance Sheet and/or CA Certificate clearly stating net worth.
5	The bidder must be an authorized reseller/partner for all quoted products and solutions	Manufacturer's Authorization Form specific to this tender for all the quoted items
6	The bidder/OEM from a country which shares a land border with India will be eligible only if they are registered with the competent authority as per Govt. of India order, issued by Ministry of Finance vide No.F.No.6/18/2019-PPD dated 23/07/2020	Attach supporting documents
7	OEM should submit the undertaking stating that the items offered are not nearing end of life or end of support until the end of warranty	Attach supporting documents

8	The bidder must meet at least one of the following project experience criteria, with all projects having been executed within the past Five (5) years 1. The bidder must have successfully executed at least one (1) turnkey project comprising Servers, Storage, and Room Furnishing under a single Purchase Order, with a minimum project value of ₹10 Crore. OR 2. Two Projects Requirement The bidder must have successfully executed at least two (2) projects with a combined project value of not less than ₹15 Crore. OR 3. Three Projects Requirement The bidder must have successfully executed at least three (3) projects with a combined project value of not less than ₹20 Crore.	Attach PO copies and completion reports
9	Clarifications	For any clarifications regarding this tender, bidders may contact the Cyber Operations Wing, Kerala Police: Contact No. 09074458789 Email: cyberops-sec.pol@kerala.gov.in
10	Payment Terms:	a. 45% (Forty Five Percent) Advance against Bank Guarantee b. 25% (Twenty Five Percent) of the contract value will be released after confirmation of shipment and acceptance by Kerala Police of each item. c. c. 20% (Twenty Percent) of the contract price will be released after satisfactory installation, testing & commissioning of the item/equipment and on receipt of successful installation report of each item. d. The balance 5% amount can be

		released against the submission of bank guarantee from a Nationalized/scheduled Bank
11	Other Payment Terms	a. PBG in Director General of Police, Kerala State b. Valid for contract period +3months c. Advance will be adjusted in subsequent bills. d. No advance without BG as per KFC Rule 182A & KSPM Clause 15.15.

4. **General Conditions**

1. The Department reserves the right to accept or reject any or all bids, in full or in part, without assigning any reason. The contract may be awarded to the lowest evaluated bidder or to a technically qualified firm whose proposal is considered most advantageous.
2. The Department may adjust quantities, combine or shorten line items, or exceed the quoted amount within the approved budget to meet operational requirements.
3. Strict confidentiality of all departmental data, systems, and information must be maintained by the bidder.
4. No data or information shall be copied, transferred, or exported outside India under any circumstances.
5. The selected firm must commence work immediately upon issuance of the Work Order and signing of the Agreement.
6. Subcontracting of any part of the work is allowed only with prior written approval from the Department.
7. Penalties or liquidated damages shall apply for delays, non-performance, or breach of contractual obligations, as per the tender terms.
8. Bidders may propose equivalent or superior items to those listed in the annexures, subject to technical evaluation and approval by the Department.
9. The decision of the Department on all matters relating to bid evaluation, award, and execution shall be final and binding, and no correspondence will be entertained.
10. The OEM/Solution Provider should submit the duly filled compliance statement as per the format. Non submission of compliance statement will lead to rejection of bid.
11. The bidder should ensure that all the quoted items are not declared End of Sale for the next five years period from the date of submission of the bid.

5. **Mode of submission of bids: -** Online. All Bid documents shall be submitted only in the online procedure through the eGP website '*www.etenders.kerala.gov.in*' in their designated online covers. Details of covers are given separately. No other mode of submission shall be accepted, such tenders will be rejected outright.

6. **Cover details: - No. of covers – 2 : -** i) Technical Bid ii) Financial Bid. In the case of foreign equipment, the rate must be quoted in Indian Rupees. The documents to be uploaded under each online cover are specified on the website.

7. **Downloading of e-Tender documents: -** The tender documents can be downloaded from the e-GP website *www.etenders.kerala.gov.in* from the date and time of publication of the e-tender onwards to the last date and time for online submission of the e-tender. Downloading of tender documents will not be possible after the date specified above.

8. **Submission of e-Tender documents:-** The digitally signed tender document and other specified documents shall be submitted online through the e-GP website other specified documents shall be submitted online through the e GP website *www.etenders.kerala.gov.in* well in advance before the last date and time mentioned above. No submission shall be allowed after the last date mentioned above.

9. **Payment of Tender Fees: -** A non-refundable tender fee shall be paid in online mode through the e-GP website *www.etenders.kerala.gov.in* at the time of bid submission. No other mode of payment shall be accepted.

THE TENDERS OR BIDDERS WHO DO NOT REMIT FEES THROUGH ONLINE WILL BE REJECTED OUTRIGHT.

10. **Payment of Earnest Money Deposit (EMD): -** The EMD shall be paid in online mode through the e-GP website *www.etenders.kerala.gov.in* at the time of bid submission. No other mode of remittance shall be accepted.

11. **Exemption from payment of EMD: -** Bidders who are registered with Store Purchase Department, Kerala or National Small Scale Industries Corporation Ltd., New Delhi (for the items tendered) are exempted from submission of EMD. Those bidders claiming exemption shall submit valid registration certificate from the SPD, Kerala or NSSIC, New Delhi. Tenders of bidders who do not remit EMD online or do not upload documental proof (digitally signed) for exemption of EMD will be rejected outright.

12. **Withdrawal and re-submission of e-Tender: -** The Bidders are at liberty to withdraw the submitted tender/documents and to submit fresh tender/documents till the last date and time of submission of e-tender after which withdrawal/re-submission will not be allowed.

13. **Opening of e-Tenders: -**
The bids shall be opened online through the eGP website www.etenders.kerala.gov.in at the Office of State Police Chief, Kerala, Thiruvananthapuram on the date and time mentioned above in the presence of the Bidders/ authorized representatives who wish to attend at the above address. If the tender opening date happens to be a holiday or non-working day due to any valid reason, the tender opening process will be done on the next working day at the same time and place specified. Any change in the opening date/time/venue due to other reasons shall be informed by way of Corrigendum published in the eGP website. The Technical Bids will, be evaluated by a Technical Evaluation committee and those that do not conform to the specifications or to the satisfaction of the committee will be rejected. The

financial bids of the Technically qualified tenderer only will be considered for opening. The date of opening of financial bids will be intimated to the concerned technically qualified tenderer, over phone/e-mail.

14. **Technical Evaluation: -** All tenderers who quote for the supply of above items are required to be ready for technical evaluation to be held in the Office of the State Police Chief Kerala Thiruvananthapuram and the date will be intimated in due course. Any clarification/doubts regarding the specification or related matters pertaining to the items tendered may be freely got cleared by contacting the Assistant Sub Inspector of Police, Cyber Security and Advanced Crimes, Cyber Operations, Police Headquarters. Ph. 9895258496. All Bidders who participate in e-tender should produce hard copies of all relevant documents related to e-tender at the time of technical evaluation, without fail.

15. **Note to Bidders: -**

i. Bidders have to procure a legally valid Digital Certificate (Class III) as per Information Technology Act, 2000 for digitally signing their electronic bids. Bidders can procure the same from any of the license certifying authority of India. For more details, please visit the e-GP website www.etenders.kerala.gov.in

ii. Bidders are advised to note the Tender ID and Tender No. & Date for future reference.

iii. All uploaded documents should contain the signature and the office seal of the bidder/authorized persons and should be digitally signed while uploading. Documents uploaded without digital signature shall entitle rejection of the tender.

iv. In the case of Foreign Equipment, the rate should be quoted in Indian Rupees. Preference will be given to those who are ready to supply the item without opening a Letter of Credit. Ordinarily, no advance payment will be made for procuring the above item.

v. For obtaining Digital Signature Certificate and help on e-tendering process, contact Kerala State IT Mission, eGovernment Procurement PMU & Help desk, Basement floor of Pension Treasury Building, Uppalam Road, Statue, Thiruvananthapuram; Ph:0471-2577088, 2577 IBB; Toll free no: 18002337315; e-mail: etendershelo@kerala.gov.in; Website: www.etenders.kerala.gov.in, on all government working days from 9:30 am to 5:30 pm.

16. The successful bidder should execute a service level agreement format available at the Office of IGP Cyber Operations, Pattom, Thiruvananthapuram. Cost of stamp paper for SLA is one rupee for every rupee 1000 or part thereof on the amount agreed in the contract, subject to a minimum of rupees 200 and a maximum of rupees one lakh.

17. **Contact for Clarifications**

For any clarifications regarding this tender, bidders may contact the Cyber Operations Wing, Kerala Police: Email: cyberops-sec.pol@kerala.gov.in.

All queries should be sent well in advance of the bid submission deadline to ensure a response in time.

NOTE: - BIDDERS ARE ADVISED TO GO THROUGH THE CONDITIONS IN THE NOTICE INVITING TENDER AND THE TENDER DOCUMENT CAREFULLY AND COMPLY WITH THEM TO AVOID OUTRIGHT REJECTION OF THEIR TENDER.

Bidders are requested to make online payment of EMD and tender fee before 72 hours in advance of last date.

Forany litigation relating to this order, the jurisdiction will be Thiruvananthapuram City.

Compliance Statement: -

I. Advanced Data Extraction Capabilities for Mobile Devices

SL.No	SPECIFICATIONS	COMPLIANCE (YES/NO)
1	**General Specifications**	
a	The solution should provide advanced access extraction capabilities to provide Full-File System extraction from unlocked File-based encryption devices and Physical extraction from unlocked Full-disk encryption devices from leading Android vendors in the Indian smartphone market such as Vivo, Samsung, Oppo, Xiaomi, Realme and OnePlus	
b	The solution should include all necessary adapters, cables, and accessories to perform the supported advanced access operations on the iOS and Android devices.	
c	The solution should come with all the relevant documentation including supported devices, user manual, release notes and video tutorials.	
d	The solution should also allow Full File-system extraction of unlocked iOS devices with greater data extraction. It should support Full File-system extraction from unlocked iOS devices running on chipsets A8 to A13 for iPhone 6 to 11.	
e	The solution should be able to conduct Full File-system extraction from unlocked iPhone	

	11, 12, 13, 14,15,16 with chips running on A13, A14, A15, A16, A17 to A18.	
f	The solution should be able to conduct Full File-system extraction for the unlocked iPhone 17.	
g	The solution should allow users to perform selective extraction at the level of the individual installed applications for both iOS and Android devices.	
h	The solution should work in a secured environment in a client – cloud exploit server mode.	
i	The solution must provide advanced access capabilities from a Central Cloud exploit server to multiple extraction endpoints.	
j	An advanced security mechanism should be available to allow the advanced exploit to be pushed down from the Central Cloud exploit server to the client endpoints only on need basis.	
k	The solution should be supported to run on an active internet connection with a recommended speed of a minimum of 100 Mbps.	
l	The solution should be regularly updated to support additional operating system versions and devices during the valid license and support period.	
m	The solution should also have the ability to upgrade the license in the future to provide the device unlocking capability using brute-force for the supported locked Android and iOS devices.	
n	It should allow the user to define a workflow at the beginning of the process to ensure the complete decoding, enrichment, and reporting functions are automated without any human intervention.	
o	There should be the capability to automatically search for relevant device information during the access phase of the device based on the device state.	
p	Solution should be able to provide information related to device identifiers like IMSI, device name and IMEI along with device user identification information.	
q	The automated workflow and searching device information capabilities should be available for the advanced access extractions for both iOS and Android devices.	
2	**Mobile Extraction Capabilities**	

a	The solution should be able to extract forensic evidence from supported mobile devices including mobile phones, handheld tablets, portable GPS devices and drones.	
b	It should provide users with available physical, file system and advanced logical extraction capabilities for different supported devices and Operating Systems as well as allow extraction of Cloud Data source tokens accessed by the supported Mobile Phones. It should support automatic detection of supported devices. It should also support manual search for devices by manufacturer, model and IMEI number	
c	A multi-SIM adapter with support for Micro, Nano and standard SIM cards should be supplied. Ability to perform SIM data extraction from a SIM or USIM card.	
d	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.	
e	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, Unisoc Live, Kirin Live, 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.	
3	**Decoding, Review and Reporting Capabilities**	
a	Should have Case Management capability, which allows users to create and manage cases and to provide case details and exhibit information. It should enable users to include multiple extractions and to apply the different enrichments.	
b	Should include dashboard view to provide a quick visual overview and display insights into the extracted data including commonly used applications, the most recent messages and enable the investigator to quickly and easily drill down into the data of interest.	
c	Dedicated location analysis view to clearly	

	categorize the location records like device visited locations, locations of some significance, media derived locations and any other location data for detailed user analysis.	
d	Capability to identify the origin of media items found within the device data to collect various metrics about a media item and apply logic to try to identify how the item originated, providing the user with information about the determined origin and the reasoning for that determination.	
e	Should have the ability to parse Windows computer data like DD, E01, RAW, L01,001 or BIN images in the same application.	
f	Should be built on a database architecture to reopen cases quickly without having to reprocess the data.	
g	Should have cryptocurrency enrichment feature to automatically identify the usage of cryptocurrencies and to detect wallet addresses and transactions within the device data.	
h	It should also have an advanced cryptocurrency enrichment ability to provide a detailed analysis of the cryptocurrency assets associated with detected wallet addresses and highlight potential illicit activity. The enrichment should further provide risk severity and graphs on currency sent and received insights. This crypto enrichment result should be exportable to a report for individual wallet addresses. • Support for image carving and location carving	
i	It should conduct on demand searches for viruses, spyware, Trojans and other malicious payloads in files.	
j	Media classification capability to detect and categorize images and video frames into 20+ key categories. This capability should be selectable, allowing the user to decide if he wants to run the media classification on a particular case.	
k	Capability to verify file integrity with use of MD5 and SHA 256.	
l	It should have a built-in SQLite Viewer.	
m	Capability to match files extracted against Hash Databases and it should have built-in support for Project VIC, CAID and NCMEC hash databases.	
n	Capability to allow users to include Case ID as well as other relevant case-related information as part of the extraction report and allow	

	filtering based on specified date range.	
o	Ability to generate and customize reports in different formats e.g. PDF, HTML, XML, Excel and Word. Global setting to select/unselect items in a report with the ability to password protect the reports.	
p	Provide a separate report with device information and	
4	**Cloud Data Extraction Capabilities**	
a	Should allow access to remote cloud data sources to obtain, decode, save and perform analysis of this data.	
b	There should be a single software interface in which users can review device data and cloud data through a single tool and with a unified experience, for a seamless and simplified review process.	
c	Software should allow access to remote cloud data sources using cloud login keys from mobile devices supporting iOS and Android.	
d	Support extraction of different content types from the supported data sources which includes messages, images, videos, files, contacts, calls, user profile, locations, user activities and backups.	
e	Provide visibility of the cloud extraction progress to the user. It should provide a view of the current status of each data source extraction with an option to cancel the process if required.	
f	Allow users to gather private user data with appropriate legal authority from over 50 of the most popular social media and cloud-based sources.	
g	Capability to create cloud tokens from manually entered credentials for future cloud extractions.	
h	Reporting of extracted data from the Cloud to human readable formats such as PDF, Word, Excel, HTML and XML. It should provide a global setting to select/unselect items in a report. The software should allow for password protection of the reports.	
5	**Tender Specific Authorization Certificate from the OEM in favour of the Indian Distributor/Reseller/Bidder is mandatory for participation in the tender.**	
6	**3-year subscription license without Unlocks**	
7	**One-day training must be provided at the time of installation and setup. The training**	

	should be conducted on-site by an OEM-certified engineer.	
8	**The training must cover both basic fundamentals and hands-on sessions to ensure familiarity with all functionalities of the tool.**	

II. Advanced Mobile Extraction Capabilities

SL. No	SPECIFICATIONS	COMPLIANCE (YES/NO)
I	**General Specifications**	
a	The solution should provide advanced access capabilities with brute-force, unlocking and data extraction from supported iOS and Android mobile phones.	
b	The solution should provide maximum unlocks and unlimited extractions with a term-based license through a USB dongle.	
c	It should have brute-force capability for both Android and iOS devices on the same software interface.	
d	The solution should be able to provide Full File-System extraction for File-based encryption (FBE) devices and Physical extraction for full-disk encryption (FDE) devices from leading Android vendors in the Indian smartphone market such as Vivo, Samsung, Oppo, Xiaomi, Realme and OnePlus.	
e	The solution should support autonomous & connected Brute-Force for a wide range of supported FDE and FBE Android devices.	
f	The solution should identify, extract and decrypt Samsung Secure folder, Huawei Private Space and Xiaomi second space.	
g	The solution should provide brute-force capabilities for supported iPhones in Cold/BFU State on chip A8 all the way to A13 (iPhone 11 and iPhone SE Gen 2) to determine the device passcode.	
h	The solution should be able to conduct After-First Unlock (AFU) based Full Filesystem extraction from iPhone 12, 13, 14 in Hot/AFU State with chip running on A14, A15 to A16.	
i	The solution must allow a Full File-system extraction of supported unlocked iOS devices up to iPhone 16.	
j	The solution should be able to support autonomous Brute-Force for iOS devices.	
k	The solution shall support application selective data extraction allowing fast extraction of	

	specific application data.	
l	The solution should allow the user to enter potential passcodes while performing brute-force on iOS and Android devices without affecting the ongoing process.	
m	The solution should be able to perform Before-First-Unlock (BFU) extraction for supported iPhone and Android phones	
n	The solution must include the software, cables and adapter to allow the solution to perform the access of Android and iOS mobile devices.	
o	The solution should work in a secured environment in a client – cloud exploit server mode.	
p	The solution must provide advanced access capabilities from a Central Cloud exploit server to multiple extraction end points.	
q	An advanced security mechanism should be available to allow the advanced exploit to be pushed down from the Central Cloud exploit server to the client endpoints only on need basis.	
r	The solution should be supported to run on an active internet connection with a recommended speed of a minimum of 100 Mbps.	
s	The solution should come with all the relevant documentation including supported devices, user manual, release notes and video tutorials.	
t	The solution should be regularly updated to support additional operating system versions and devices during the valid license and support period.	
u	It should allow the user to define a workflow in the beginning of the process to ensure the complete decoding, enrichment and reporting functions are automated without any human intervention.	
v	There should be the capability to automatically search for relevant device information during the access phase of the device based on the device state.	
w	Solution should be able to provide information related to device identifiers like IMSI, device name and IMEI along with device user identification information.	
x	The automated workflow and searching device information capabilities should be available for the advanced access extractions for both iOS and Android devices.	
2	**Mobile Extraction Capabilities**	
a	The solution should be able to extract forensic	

	evidence from supported mobile devices including mobile phones, handheld tablets, portable GPS devices and drones.	
b	It should provide users with available physical, file system and advanced logical extraction capabilities for different supported devices and Operating Systems as well as allow extraction of Cloud Data source tokens accessed by the supported Mobile Phones.	
c	It should support automatic detection of supported devices. It should also support manual search for devices by manufacturer, model and IMEI number	
d	A multi-SIM adapter with support for Micro, Nano and standard SIM cards should be supplied. Ability to perform SIM data extraction from a SIM or USIM card.	
e	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.	
f	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, Unisoc Live, Kirin Live, 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.	
3	**Decoding, Review and Reporting Capabilities**	
a	Should have Case Management capability which allows users to create and manage cases and to provide case details and exhibit information. It should enable users to include multiple extractions and to apply the different enrichments.	
b	Should include dashboard view to provide quick visual overview and display insights into the extracted data including commonly used applications, the most recent messages and enable investigator to quickly and easily drill down into the data of interest.	
c	Dedicated location analysis view to clearly categorize the location records like device visited	

	locations, locations of some significance, media derived locations and any other location data for detailed user analysis.	
d	Capability to identify the origin of media items found within the device data to collect various metrics about a media item and apply logic to try to identify how the item originated, providing the user with information about the determined origin and the reasoning for that determination.	
e	Should have the ability to parse windows computer data like DD, E01, RAW, L01, 001 or BIN images in the same application.	
f	Should be built on a database architecture to reopen cases quickly without having to reprocess the data.	
g	Should have a cryptocurrency enrichment to automatically identify the usage of cryptocurrencies and to detect wallet addresses and transactions within the device data.	
h	It should also have an advanced cryptocurrency enrichment ability to provide a detailed analysis of the cryptocurrency assets associated with detected wallet addresses and highlight potential illicit activity. The enrichment should further provide risk severity and graphs on currency sent and received insights. This crypto enrichment result should be exportable to a report for individual wallet addresses.	
i	Support for image carving and location carving	
j	It should conduct on demand searches for viruses, spyware, Trojans and other malicious payloads in files.	
k	Media classification capability to detect and categorize images and video frames into 20+ key categories. This capability should be selectable, allowing user to decide if he wants to run the media classification on a particular case.	
l	Capability to verify file integrity with use of MD5 and SHA 256.	
m	It should have a built-in SQLite Viewer.	
n	Capability to match files extracted against Hash Databases and it should have built-in support for Project VIC, CAID and NCMEC hash databases.	
o	Ability to generate and customize reports in different formats e.g., PDF, HTML, XML, Excel and Word. Global setting to select/unselect items in a report with ability to password protect the reports.	
p	Provide a separate report with device information and user account information for	

	quick reference of users.	
4	**Cloud Data Extraction Capabilities**	
a	Should allow access to remote cloud data sources to obtain, decode, save and perform analysis of this data.	
b	There should be a single software interface in which users can review device data and cloud data through a single tool and with a unified experience, for a seamless and simplified review process.	
c	Software should allow access to remote cloud data sources using cloud login keys from mobile devices supporting iOS and Android.	
d	Support extraction of different content types from the supported data sources which includes messages, images, videos, files, contacts, calls, user profile, locations, user activities and backups.	
e	Provide visibility of the cloud extraction progress to the user. It should provide a view of the current status of each data source extraction with an option to cancel the process if required.	
f	Allow users to gather private user data with appropriate legal authority from over 50 of the most popular social media and cloud-based sources.	
g	Capability to create cloud tokens from manually entered credentials for future cloud extractions.	
h	Reporting of extracted data from the Cloud to human readable formats such as PDF, Word, Excel, HTML and XML. It should provide a global setting to select/unselect items in a report. The software should allow to password protect the reports.	
5	**Provide 2 TB SSD Hard disk for keeping backup storage facilities.**	
6	**Tender Specific Authorization Certificate from the OEM in favour of the Indian Distributor/Reseller/Bidder is mandatory for participation in the tender.**	
7	**3 Years Subscription License**	
8	**One-day training must be provided at the time of installation and setup. The training should be conducted on-site by an OEM-certified engineer.**	
9	**The training must cover both basic fundamentals and hands-on sessions to ensure familiarity with all functionalities of the tool.**	

III. High-End Analysis Workstation

SL. No	SPECIFICATIONS	COMPLIANCE (YES/NO)
Technical Specifications		
1	A high-end analysis workstation is the Non-Plus Ultra when it comes to indexing and processing IT forensic cases at the workplace.	
2	A high-end analysis workstation series is globally recognized and popular for its speed, reliability and durability.	
3	A high-end analysis workstation is certified and tested for the use of the programs of the leading software manufacturers (like Access Data, OpenText, Magnet Forensics, etc.).	
4	Chassis: Must be a Big Tower Case: 306(W) x 651(H) x 639(D) mm 11x 5.25 Bay Chassis.	
5	Processor: Should have CPU 24-Core Intel® Core™ Ultra 9 Processor 285K (36M Cache, up to 5.70 GHz).	
6	RAM: Should have RAM 128 GB (expandable up to 192GB).	
7	Internal Storage: a. 1x 1TB SSD M.2 NVMe PCIe 4.0 x4 for OS. b. 1x 1TB SSD M.2 NVMe PCIe 4.0 for Cache. c. 1x 10TB Enterprise HDD SATA III for DATA	
8	Graphics Card: NVIDIA GF RTX, min. 6GB Memory, PCIe, min. 1x HDMI & 1x DisplayPort.	
9	Mainboard: Should Intel Z890 LGA 1851 ATX-Mainboard with: a. 2x PCIe® 5.0 x16 slots. b. 1x PCIe 4.0 x16 slot. c. 5x M.2-Slots. d. Max. 256GB DDR5. e. Intel WIFI 7. f. 1x 10Gb Ethernet. g. 1x 2.5 Gb Ethernet. h. HDMI®. i. USB 3.2 Gen 2x2 Type-C®. j. Front USB 3.2 Gen 2 Type-C®. k. 2x Thunderbolt™ 5. l. Aura Sync.	
10	Should have integrated a Silent edition Write Blocker with IDE, SATA, USB, SAS, FIREWIRE, PCIe interface.	
11	Must have a retractable ice tray internal cooler for suspected drive Two	
12	Backplane: 3x Backplane, screwless hot-swap for additional 3.5" HDDs (2x empty, 1x occupied by HDD).	

13	Power Supply: 1000WATT Modular Power Supply ATX, EPS12V, PS/2	
14	Should have 1 RJ45 LAN port (Gigabit LAN controller).	
15	Should have Optical Drives READ WRITE - SATA.	
16	Front I/O: a. 1x USB 3.1 Type-C. b. 4x USB 3.0 Type-A. c. 1x FAN-/ RGB-LED-Control Unit. d. 1x Audio In/Out.	
17	Should have 2x USB 3.1 ports (1 port at Type A, 1 port at Type C) Back Mounted.	
18	Should have a 24-inch LED Monitor with Full HD (1920x1080) resolution, a keyboard and a mouse combo.	
19	Forensic Card Reader with integrated 3-port USB Hub: a. Compact Flash = V6.0, PIO mode 6 / Ultra DMA mode 7 and LBA48. b. SD & micro SD: V1.0, V1.1, V2.0, SDHC, SDXC, V3.0 (UHS-1), V4.0 (UHS-II), MMC, RS-MMC, MMCmicro, MMCmobile. c. Memory Stick: MS V1.43, MS PRO V1.05, MS Micro V1.04, MS PRO HG Duo 1.03, MS XC Duo v1.00, MS XC HG Duo v1.00, MS XC Micro V1.00, MS XC HG Micro v1.00, MARS. d. Multi-LUN: access to several card slots during the same time. e. "Read Only / Read & Write" switch for all card slots, with LED indicator: - Red = Read Only. - Green = Read & Write. f. White LED indicator for card access. g. 1x USB 3.1-port Type-A & 2x USB 3.1-port Type-C (5 Gbit/s) (downstream) Read & Write mode.	
20	Adapters and Cables: Cables and adapters to image and process internal/external drives including: a. SAS. b. SATA. c. IDE. d. microSATA. e. SATA LIF. f. MacBook Air Blade Type SSDs. g. mini/micro SSD cards. h. 1.8-inch IDE (iPod). i. 2.5-inch IDE (laptop). j. PCIe Card SSD Adapter. k. PCIe M.2 SSDS Adapter.	

	l. PCIe Apple SSD Adapter. m. PCIe Cable.	
21	Preinstalled Software: a. Windows 11 Pro with recovery media. b. Should have the capability for rapid, automated data acquisition. c. Should have support for digital data capture from removable media, mobile devices, computers, drones, and hard drives. d. Should have a simple, intuitive interface for users to perform media acquisition efficiently. e. Should have functionality that enables quick analysis of multiple devices. f. Should have live data viewing capabilities during the acquisition process to support real-time decision-making. g. Should have the ability to simultaneously secure and analyse data from multiple removable devices. h. Should have advanced inspection tools to display the target's file tree before initiating data extraction. i. Should have live streaming views of logical data as it is being captured into the platform. j. Should have powerful data carving tools to recover deleted data effectively. k. Should have the ability to acquire data from hard drives extracted from damaged systems. l. Should have a patented red-amber-green visual alert system for automated alerts on suspicious data. m. Should have automation capabilities using predefined criteria for streamlined analysis. n. Forensic Imaging Software: - FTK Imager. - Magnet Acquire. - EnCase Imager. - Tableau Imager.	
22	Should have an External bootable HDD with pre-installed Backup Software.	
23	Should be passed through 12/24 hours Burn-in Test with accurate results.	
24	Incorporates features supporting forensic evidence handling and documentation practices.	
25	OEM must be ISO 9001:2015 certified and the workstation should have a BIS (Bureau of	

	Indian Standards) Certificate and a TUV quality certificate.	
26	Product should carry a 3 (Three) Years On-Site Warranty.	
27	Any Software/Firmware updates to be provided during the Warranty Period.	
28	Tender Specific Authorization Certificate from the OEM in favor of the Indian Distributor/Reseller/Bidder is mandatory for participation in the tender.	

IV. Digital Evidence Acquisition and Examination Software – 3-Year Subscription License

SL. No	SPECIFICATIONS	COMPLIANCE (YES/NO)
1	**Imaging and Triage Tool**	
a	Should provide comprehensive all-in-one capability to handle booted or live triage, targeted data collection, and forensic imaging for both Windows and Mac systems from a single USB device.	
b	The product must enable booting both supported Mac and Windows systems from a single USB device, eliminating the need for multiple platform-specific devices.	
c	The product should have the ability to deploy forensic analysis software on both Windows and Mac workstations.	
d	Product should be able to triage and create images of Apple Silicon (M1-M4 chips) and T2 chips computers running macOS Big Sur 11 through macOS Tahoe 26, either running live on the host operating system, or running by booting from the product.	
e	Should be able to create physical decrypted images of Apple's latest Mac computers utilizing the Apple T2 and M series chips. It should also produce a physical image of APFS fusion drives.	
f	For T2 chipset, it should support decryption with password or recovery key.	
g	For FileVault and CoreStorage, it should support decryption with keychain, password, or recovery key.	
h	Should support AFF4 image format for imaging Mac computers with APFS Fusion or with T2 chips.	
i	Ability to create images of selected files to a folder or the L01 logical evidence file format.	
g	Should support writing to evidence storage	

	configured with APFS, HFS+, exFAT, or NTFS file systems.	
k	Provide the ability to format evidence storage onsite by using built-in tools without external dependency.	
l	Ability to preview file contents prior to acquisition using a dedicated view, and to locate specific files using custom filters or keyword searches through a dedicated search interface	
m	Ability to triage before data collection in both live and booted mode with the option to create predefined collection templates for rapid and repeatable collections.	
n	Provide in-built tools for evidence storage management and compatibility with all major file systems.	
o	Product must be able to boot the supported Mac and Windows systems via a single USB device.	
p	Should support forensic imaging of macOS computers with APFS, HFS+, CoreStorage, FileVault, T2, M series, and Fusion in any combination.	
q	Should support forensic imaging of computers running Windows with or without BitLocker enabled, NTFS/FAT, etc.	
r	Should authenticate collected computer data using any or all MD5, SHA-1, or SHA-256 hash functions for the image and individual files.	
2	**Analysis Tool**	
a	Product should be able to give analysis platform to review computer forensic extractions to provide actionable intelligence from both Windows and Mac systems.	
b	Product should run on Windows or Mac forensic workstations.	
c	Product must be able to conduct search, filtering, and sifting through large data sets with simple or complex group filtering.	
d	The filter criteria should include file name, file kind, file size, file extension, date created, date modified, date accessed, picture metadata attributes, including GPS coordinates and camera (iPhone/iPad device) type	
e	Product must be able to support Windows artifacts such as device history from Microsoft Volume shadow copies, windows registry and Windows memory	
f	Product should be able to automatically parse account information, web history, downloads and Windows 10 activity	

g	Product should have support for different Windows OS artifact like jump list, shellbags, prefetch, volume shadow copies, link files, event logs, superfetch, recycle bin, user info, connected devices, last executed, NTFS ACL, file downloads, recent items, memory analysis, new Window activity, srum, notifications, Registry: amcache, bam, comdlg32, muicache, recentapps, shimcache.	
h	Product must be able to support all macOS systems from Hierarchical File System (HFS) with File Vault or Core storage to APFS with T2 chips or fusion drives.	
i	Product should be able to conduct review on device history from Apple File System (APFS) snapshots and Time Machine backups	
j	Product must support E01, EX01, L01, RAW, DD, DMG and AFF4, AFF4-L file format.	
k	Product should be able to display and search Unified logs, spotlight and built-in APOLLO support for Mac systems	
l	Should support processing and analysis of the macOS Unified Logs	
m	Product should be able to review health data, wallet transactions and calendar activity	
n	The product should have powerful activity correlation for Windows and show how an artifact came to be and how it relates to other artifacts.	
o	Product supports smart indexing and image categorization such as Porn, Weapons, Drugs, Extremism, Gore, Alcohol, Swim/Underwear, Documents, ID, Currency, CSAM, Chat, and Vehicles.	
p	Product should support advanced timeline capabilities to allow the user to narrow activity and artifacts to a specific time frame.	
q	Product should support extraction of text from documents, pictures and PDF using built in Optical Character Recognition (OCR).	
r	Product must be able to link with child exploitation media database and must be able to integrate with Project VIC, Semantics21 and C4All.	
s	It must be able to support ingestion of Berla vehicle forensic extractions for analysis	
t	Must have the capability to share access to case data for offline review for both Windows and Mac systems:	

u	A portable case file with case data, which can be exported along with a reader application for review of the case file	
v	Export reports in a variety of formats including HTML, PDF, CSV, Excel and tab delimited formats.	
3	**Provide 2 TB SSD Hard disk for keeping backup storage facilities**	
4	**Tender Specific Authorization Certificate from the OEM in favour of the Indian Distributor/Reseller/Bidder is mandatory for participation in the tender.**	
5	**3 Years Subscription License.**	
6	**One-day training must be provided at the time of installation and setup. The training should be conducted on-site by an OEM-certified engineer.**	
7	**The training must cover both basic fundamentals and hands-on sessions to ensure familiarity with all functionalities of the tool.**	

V. Video Enhancement Software- Perpetual License with 3 Years Support

SL. No	SPECIFICATIONS	COMPLIANCE (YES/NO)
1	**General Specification**	
1	Must have at least 140 different filters and tools to enhance and process images and video files.	
2	Must be a single stand-alone system protected by a USB dongle or by a digital license.	
3	Must be able to decode video files with these codec frameworks: FFmpeg, FFMS, FFMS with Audio, DirectShow, Video for Windows, QuickTime (if installed on the system).	
4	Must be able to bookmark frames and filters and customize their names, description, and folder.	
5	Must provide batch renaming options of bookmarks, to easily locate them after the export.	
6	Must be able to convert and export videos in proprietary formats, most of them without transcoding. Must support one or more variant of (at least) these formats: Milestone .xml/.pqz, USB Play archive, 000, 001… up to 099, 2, 264, 264001, 400, 600, 787, acsm, aira, ajp, ami, amv, aov, arv, ary, asf, asx, av, ava, av3, avc, avd, ave, avf, avi, avr, avs, awlive, bdb, bes, bfs, bin, bix, blk, bms, body, box, bpv, bu, bvr, bwm, bwv, car, cam, cbf, cme, cms, cv2, cx3, d, da, dar, dat, data, dav, db, dbx, dce, dcr, dga, djp, dmd, dmi, dmskm, dpv, drv, dv4, dv5, dvr, dvs, dvt, dxa, e, edr, eds, ethe, evf, exe, exp, eye, ezvp, fl4, flm, g64, g64a, g64x, gbf, gop, h263, h264, h265, h64, har, hav, hevc, hgd, hik, hkv, hme, hvs, icf, ifs, igd, ifv, image, imf, img, irf, iva, ivf, jdr, kvf, jv, k26, l64, lmp, lvf, lwx, lxf, m2t, m2ts, m2v, m4v, m65, master, max, mdt, media, mgv, mjp, mjpg, mkv, mod, mov, mp4, mpc, mpg, mpg2, mrd, mts, mul, mva, mxg, noext, nov, n3r, nr3, nvf, nvr, nvt3, omv, par, pef, pic, pns, ps, psf, psx, pvf, pw3, qbx, raw, re4, rec, rf, rgm, rms, rmv, rsv, s,	

	sm, sdc, sdr, sdv, sec, shv, snx, ssf, strg, stw, svs, synav, tav, teb, tmp, ts, tvr, ubv, umv, v, v264, var, vcr, vdd, vdx, vfs4, vid, video, video.data, vision, vls, vmf, vp6, vse, vmhrcd, vsr, webm, wmv, wnm, wsb, xa1, xi1, xba, xpa.	
7	Must allow the selection of the timing source (average PTS, average FPS or data timestamp) when exporting a video.	
8	Must be able to mux audio-only files into a video format	
9	Must be able to create a writing queue to batch-export multiple video files.	
10	Must be able to export variable and constant frame rate videos.	
11	Must support any standard video format (avi, mp4, mkv, flv, 3gpp, wmv, mov…), also without the need of the codec installed on the system. Expandable by system codecs.	
12	Must be able to perform the batch conversion of multiple video files, even if they have different file extensions and/or are distributed across different folders.	
13	Must support any standard digital image format (i.e., jpeg (also HEIC-encoded), tiff, png, bmp, targa, tiff, jpeg2000, heif…) as well as at least one variant of the following ones: ico, gif, dcm, emf, eps, pcd, psd, xpm, 3fr, ari, arw, srf, sr2, bay, cr2, cap, iiq, eip, dcs, drf, k25, kdc, dng, erf, fff, mef, mos, mrw, nef, orf, ptx, pxn, R3D, raf, raw, rw2, rwl, dng, rwz, x3f, wbmp, webp.	
14	Must be able to organize loaded images and videos in folders, possibly nested.	
15	Must support Undo/Redo actions.	
16	Must support GPU-accelerated encoding when transcoding videos with the H264 and H265 codec for conversion or export, either with CUDA or Intel Quick Sync Video.	
17	Must be able to load more videos all at once.	
18	Must be able to concatenate, extract the timestamp and demultiplex some proprietary video files during conversion	
19	Must be able to track areas or target of interest (such as people or objects) through static, dynamic, manual, and keyframe-based tracking. MUST allow the copy of tracking data among multiple annotations	

	so that they have matching movements when following a target.	
20	Must be able to display frame type (I, P, B) for video files.	
21	Must allow for all operations performed by the user to be logged on a text file, together with system info and other critical information. The feature can be optionally disabled.	
22	Must be integrated with Milestone XProtect server, both connecting to the server and playing the exported images without prior conversion.	
23	Must be able to load a subtitle file (in SRT or SMI format) and renders its text on the video.	
24	Must be able to export the current video frames to a PDF with the number of images per page and paper size configurable by the user.	
25	Must be able to export the original video/image as well as the processed one. If the chosen output codec for exporting a video is H264, different quality options are available.	
26	Must be able to export the audio stream of a video if present.	
27	Must be able to select only the Intra-coded Frames of a video (I-Frames).	
28	Must have the project format in a simple and readable text which instructs the system on the filters and parameters to apply on specific files.	
29	Must be able to import a project folder originally exported by Amped Replay.	
30	Must provide the automatic generation of a report and must contain all the scientific methodology and details of the processing steps, settings, and the bibliographic references to the algorithms in HTML, PDF (optionally protected) or DOCX format.	
31	Must allow for report generation in several different paper sizes	
32	Must provide different report templates and must allow the creation of customized templates too. Must also allow for customization of destination folder and filename of the report.	
33	Must be able to add footers and page	

	numbers to the report.	
34	Must provide volume and mute controls when audio is enabled.	
35	Must allow for audio hearing when navigating the video frame by frame.	
36	Must support multichannel audio for some formats.	
37	Must be able to redact audio.	
38	Must be able to add an audio stream to a video	
39	Must be able to support audio-video synchronization, adding or subtracting a delay to an audio stream	
40	Must be able to automatically add black frames when the audio track is longer than the video stream	
41	Must allow to inspect the video file with different tools (FFMS, MediaInfo, FFProbe and ExifTool) and must offer the option to save the provided information onto a log file.	
42	Must provide the RIFF Viewer tool to inspect the structure of files wrapped in an AVI video container.	
43	Must be able to perform file analysis frame by frame, reporting detailed information about each frame and allowing to filter the results by frame type (video, audio, other data).	
44	Must be able to perform video mixer overlays or display two different videos side by side.	
45	Must be able to combine and sync multiple videos together.	
46	Must support synchronization of video streams and similarity metrics computation.	
47	Must be able to merge the audio and video streams from different filters. Must be able to put in sequence or side by side multiple videos, Must allow synchronizing the videos playback.	
48	Must be able to apply the Picture in Picture effect to display a small image or video over a larger one	
49	Must be able to convert a video with juxtaposed fields into an interlaced video.	
50	Must correct the geometric distortion caused by capturing optics (barrel,	

	pincushion, and fisheye lens distortion). Must support the selection of multiple lines for the estimation of the curvature to compensate.	
51	Must include a camera calibration tool that allows generating and applying a distortion profile to accurately correct lens distortion.	
52	Must be able to convert an omnidirectional image into a panoramic one.	
53	Must have a homomorphic filter to adjust separately the contrast of the illumination and detail in an image.	
54	Must have a Smart Adjust filter that automatically adjusts the local contrast and brightness in an image whilst mitigating halo artifacts.	
55	Must be able to correct an uneven illumination in the image using the Retinex algorithm.	
56	Must have a colour deconvolution filter to maximize the differences between specific colours in the image.	
57	Must be able to perform component separation to separate signals due to different informative components in the image.	
58	Must be able to calculate the input file hash code to check data integrity when loading the project. Must support several hashing algorithms.	
59	Must be able to calculate the frame hash code with MD5 or SHA1 algorithms.	
60	Must be able to correct the blur caused by linear motion, even when the motion parameters change between frames.	
61	Must be able to correct the blur caused by wrong focus	
62	Must be able to correct the blur by non-linear motion defined by the user.	
63	Must be able to correct the blur caused by air turbulence on long distances or by high ambient air temperature/humidity.	
64	Must be able to align the perspective of different images of the same object, taken from different points of view. Must support any kind of motion (shift, rotation, zoom, perspective changes).	
65	Must be able to perform automatic perspective stabilization of the same object	

	taken by different angles.	
66	Must be able to visualize the macroblock type and motion vectors from a MPEG based video.	
67	Must have a CTU analysis filter to examine the compression on h265/HEVC-based videos, with an option to visualize the variable size of the blocks.	
68	Must have a super resolution feature that must generate a single higher resolution image by merging all the frames with subpixel motion estimation, even with different perspectives.	
69	Must be able to stabilize a video focusing on an object with either static, dynamic or manual tracking.	
70	Must be able to stabilize a shaking video automatically.	
71	Must be able to adapt the video frame rate by duplicating or dropping frames retaining the original speed.	
72	Must be able to change the video frame rate to export or play a video with a customized duration.	
73	Must be able to perform video redaction to pixelate, darken or blur an area of interest in a video (for privacy reasons, witness protection, or sensitive subjects). Must be able to invert a hide selection and apply feathering to soften the edges of a hidden area.	
74	Must support different tracking methods (either manual, software assisted or keyframe-based) and inverse selection.	
75	Must be able to annotate images or videos with arrows, shapes, freehand drawings, magnification and spotlight effects. Each annotation Must be able to track a specific target (manually, with software assisted tracking, or by setting keyframes). It Must be possible to set a different colour for each annotation, also by using an eyedropper tool to pick colour from image pixels	
76	Must support for visual hints and snapping, to assist the user to align annotations.	
77	Must support the grouping of annotations. Grouped annotations Must be able to track object together.	

78	Must be able to freeze a selected frame for a set amount of time.	
79	Must be able to create an empty video showing a coloured frame or a still image for a specified time	
80	Must be able to display subtitles on the video frames with customizable font, colour, size and position.	
81	Must be able to indicate date and time for the current frame and font, colour, size and position must be customizable.	
82	Must be able to superimpose a grid onto the image or video which is useful for compression estimation and other analysis.	
83	Must be able to play back the video in the reverse direction.	
84	Must be able to take a measurement on the image with a reconstruction model of the perspective. Must support error calculation.	
85	Must be able to estimate the speed of an object that is moving over a flat surface. Must support uncertainty calculation.	
86	Must be able to copy the evidence files stored in an external removable device, verifying the match between the source hash codes and the destination hash codes in order to check the integrity for a safe acquisition. Must generate an automatic report/log of the action performed.	
87	Must be able to directly load the securely copied multimedia files into the software and must be able to send user-selected videos directly to the batch conversion engine.	
88	Must be able to add the information related to the secure copy into the report of the project.	
89	Must support playback of variable frame rate video based on presentation timestamps.	
90	Must support playback speed based on timestamp values.	
91	Must allow adding, shifting, interpolating and refining timestamps. Must also allow for region selection and tracking in the filter options.	
92	Must be able to reduce the blocking artifacts caused by JPEG compression.	
93	Must have multiple denoising, sharpening	

	and intensity adjustment filters.	
94	Must be able to invert and replace the colour channels of an image with another.	
95	Must be able to process and optionally record live video from a DirectShow compatible source.	
96	Must be able to load multiple images together to work on them as if they were frames of a single video file.	
97	Must include a special seek function which allows to move on user specified intervals based on units of (frames, Iframes, or different time units).	
98	Must include a decimation function to remove frames based on a user-defined step value.	
99	Must be able to send, with a single click, the current image to Word, PowerPoint or copy it onto the clipboard for pasting in any other tool.	
100	Must have the notes panel always available on screen and the notes Must be automatically saved with the project.	
101	Must have the ability to integrate screen capture with the option to save standard uncompressed video files for maximum quality and compatibility.	
102	Must be able to view, grab and process any stream coming from a DirectShow compatible device.	
103	Must include more than 50 different sample projects and files to learn how to apply the software in numerous situations.	
104	Must be able to select frames of the video within an interval with an optional frame step. MUST support the trimming of the original video stream without transcoding.	
105	Must be able to select a list of frames that are defined by the user.	
106	Must be able to select frames at a discretional interval, to retain a constant pattern of frames and remove all the others (e.g. to quickly demultiplex videos with a fixed pattern).	
107	Must allow to correct the perspective of objects in an image (e.g., rectifying a license plate).	
108	Must be able to reduce the noise integrating current and previous frames and avoiding	

	halos on moving objects.	
109	Must be able to put side by side the original and the processed image.	
110	Must be able to add logos, text with dynamic macros and shapes on images and videos.	
111	Must allow users to validate results by automating the pixel verification of processed images and videos between projects created using different versions of the software and/or different host computers.	
2	**Provide 4 TB SSD Hard disk for keeping backup storage facilities.**	
3	**Tender Specific Authorization Certificate from the OEM in favour of the Indian Distributor/Reseller/Bidder is mandatory for participation in the tender.**	
4	**Perpetual License with 3 Years Support.**	
5	**One-day training must be provided at the time of installation and setup. The training should be conducted on-site by an OEM-certified engineer.**	
6	**The training must cover both basic fundamentals and hands-on sessions to ensure familiarity with all functionalities of the tool.**	

V. Image Authentication Software-Perpetual License with 3 Years Support

SL. No	SPECIFICATIONS	COMPLIANCE (YES/NO)
	Specifications	
1	Must have at least 40 analysis filters with optional user-customizable configuration and post-processing parameters (levels, scale to enhance the displayed image).	
2	Must be compatible with all the most common image formats and many of the uncommon ones too: BMP, GIF, JPEG, JPEG 2000, TIFF, PNG, TGA, ICO, DICOM, EMF, EPS, Photo PCD, XPM, PSD, HEIF, AVIF and RAW camera formats from most manufacturers.	

3	Must be compatible with all the most common video formats (MP4, MOV, MKV, 3GP).	
4	Must allow the image, video or project loading by means of drag and drop onto the GUI.	
5	Must automatically apply all filters to one image or all images in a folder and include support for nested folders.	
6	Must provide hints for each filter by hovering over them with the mouse.	
7	Must display RGB values and luminance (Y) when hovering the mouse over pixels. The inspected values can be copied to the clipboard.	
8	Must generate an automatic output image and report with all processing results on one or more images and the user can customize the output image size and the custom destination folder.	
9	Must be able to create and save projects.	
10	Must be able to generate a project report in HTML, PDF (optionally protected), and DOCX format.	
11	Must perform a quick automatic analysis of the format of all images in a folder to find suspicious files (triage).	
12	Must export a multiple image file format analysis results table directly to Microsoft Excel for further processing.	
13	Must display image and video location in Google Maps.	
14	Must search for similar images on Google Lens, starting from the evidence image or video frame.	
15	Must be able to check sun position for image or video location and date on Suncalc.	
16	Must search for images from a specific camera model on Flickr and support advanced image features filtering.	
17	Must search for images from a specific camera model on Camera Forensics and support advanced image features filtering.	
18	Must extract JPEG images embedded in any file type (image files, PDF, PPT, DOC, disk image...) for questioned document authentication support. MUST be able to automatically load into the program the	

	images extracted from the PDF.	
19	Must be able to perform customization of all the criteria for evaluating the camera original files.	
20	Must be able to check whether the image likely comes from a known social media platform.	
21	Must be able to make the filter's label appear in red, if the analysis of an image detects signs of manipulation.	
22	Must be able to display/compare main JPEG markers.	
23	Must have integrated hexadecimal viewer with search capabilities.	
24	Must display/compare JPEG Huffman Tables of the main image, embedded thumbnail, and preview.	
25	Must perform analysis of the colour space usage of the image in the HSV and Lab coordinates to help spot excessive colour adjustment.	
26	Must identify manipulated areas of the image based on DCT-domain analysis of aligned double JPEG quantization artifacts (ADJPEG).	
27	Must identify manipulated areas of the image based on DCT-domain analysis of non-aligned double JPEG quantization artifacts (NADJPEG).	
28	Must identify manipulated areas of the image based on the joint analysis of JPEG Ghosts Map, Blocking Artifacts, ADJPEG and NADJPEG.	
29	Must perform automatic identification of tampered areas of the image by comparison with the PRNU reference pattern of the image.	
30	Must allow to inspect the video file with different tools (FFMS, Media Info, FF Probe and Exif Tool) and MUST offer the option to save the provided information onto a log file.	
31	Must run the PRNU analysis to images and video frames (within the technical limitations) and MUST compare two different camera reference patterns. Must be able to extract video frames for generating the camera reference pattern file, without using external tools.	

32	Must include a PRNU video tampering tool.	
33	Must detect geometrical transformations (such as scaling and rotation) while carry out the PRNU analysis on videos.	
34	Must be able to perform VPF (Variation of Prediction Footprint) Analysis to detect whether a video was encoded twice during its life cycle.	
35	Must allow the range-based analysis on videos.	
36	Must identify similar areas of the image that can be the result of cloning.	
37	Must identify groups of similar points in the image that can be the result of cloning.	
38	Must be able to detect faces in the image and classify each face as being a deepfake generated by a GAN (Generative Adversarial Network) or not. It must provide a confidence score for either class.	
39	Must be able to detect synthetic deepfake images generated by several Diffusion models, including Stable Diffusion, DALL-E, Midjourney, Flux, Nano Banana, GPT Image and Grok. It must provide a confidence score for the binary output (compatible or not compatible with a known AI model). Must be able to carry out such an analysis by batch processing the entire evidence folder.	
40	Must check the consistency of cast and attached shadows within an image or video frame.	
41	Must check the consistency of reflections within an image or video frame.	
42	Must automatically add to the generated report a warning concerning inconsistency of shadows or reflections	
43	Must check if elements within an image or video frame have a consistent perspective.	
44	Must be able to hide sensitive visual details by means of blur, pixelation and blackening, with also the possibility of applying an inverted selection.	
45	Must support bookmarking output images and MUST support drawing graphical annotations on bookmarked output images.	
46	Must allow to copy annotations from one bookmark to another.	

47	Must allow to inspect the macroblocks type and their compression level in MPEG based videos (with H264 codec), and MUST allow the generation of a customizable plot.	
48	Must allow to inspect Coding Tree Unit (CTU) block types and related motion vectors in HEVC/H265 videos.	
49	Must have the RIFF Viewer tool to inspect the structure of files wrapped in an AVI video container.	
50	Must allow to inspect the coding details of a video at the frame level (PTS data, decoding and display frame order, packet size).	
51	Must allow computing the pixel hash of all frames in a video and export it to TSV format	
52	Must allow visualizing blocks that remained unchanged between consecutive frames, and MUST allow the generation of a customizable plot.	
53	Must allow extracting and displaying a specific colour channel of an image or a video.	
54	Must allow for file relocation when loading a project whose original input media was moved	
55	Tender Specific Authorization Certificate from the OEM in favour of the Indian Distributor/Reseller/Bidder is mandatory for participation in the tender.	
56	Perpetual License with 3 Years Support.	
57	One-day training must be provided at the time of installation and setup. The training should be conducted on-site by an OEM-certified engineer.	
58	The training must cover both basic fundamentals and hands-on sessions to ensure familiarity with all functionalities of the tool.	

VI. DVR Data Extraction Tool

SL. No	SPECIFICATIONS	COMPLIANCE (YES/NO)
	Specifications	
1	The software shall possess the capability to extract and recover video evidence from Digital Video Recorders (DVRs) in a forensically sound manner, ensuring end-	

	to-end data integrity is maintained throughout the investigative lifecycle.	
2	It shall be compatible with more than 50 widely used video formats, encompassing proprietary formats and standard formats such as H.264, MOV, MP4, and AVI, from a wide array of recording equipment, including DVRs.	
3	The platform shall facilitate video evidence retrieval from cloud-based surveillance systems, including Ring and Arlo, using authorized access credentials.	
4	It must enable the recovery and examination of video data and related metadata from various sources such as body-worn cameras, dashcams, drones, and mobile phones, while supporting decoding of Open AVI and MP4 files using appropriate encoding standards.	
5	The software shall compute and log MD5, SHA-1, and SHA-256 hash values for all acquired video files to maintain forensic authenticity.	
6	Upon connecting a DVR storage or forensic image, the system must automatically present granular detection information, including the file system's label, version, format type, and output details.	
7	The tool shall provide keyboard shortcuts for essential functionalities like case initiation, report creation, incident tagging, bookmark insertion, application settings, and toggling case views, improving examiner productivity.	
8	A dedicated dashboard panel must offer an at-a-glance reference of all available keyboard shortcuts for ease of use during investigations.	
9	Separate processing workflows shall be offered for accessible and inaccessible scans, allowing for faster processing when direct file access is available or deeper bit-level scanning when needed.	
10	The system should include the ability to bypass indexing processes during video extraction or scan operations to improve speed and efficiency.	
11	Targeted scan options should allow investigators to limit analysis to accessible	

	video files only when known evidence exists.	
12	A streamlined interface should permit direct launch of previously accessed cases from the startup screen for improved investigation continuity.	
13	Post-scan export functions shall be configurable to execute automatically upon scan completion, enabling batch exports in PDF or Excel format to user-defined destinations with chosen media encoding and hashing options.	
14	Investigators should be able to define parameters for post-scan exports in advance, including filters for date/time range, camera channels, and thumbnail selection from particular source devices.	
15	The application shall support pre-configurable scan filters and time offset settings prior to extraction to reduce analysis time and enhance result relevance.	
16	A synchronized matrix viewing capability must allow simultaneous preview of a minimum of four video feeds to support comparative video analysis.	
17	The tool should support the ability to add notes, labels, and bookmarks to video clips to aid in review, collaboration, and final report generation.	
18	Users must be able to isolate and export relevant segments from larger video files through sub-clipping functionalities to focus on specific evidence.	
19	The platform shall allow filtering of video evidence using date, time, recurring time ranges, or specific days of the week.	
20	Clip lists must be filterable by attributes such as file size, clip duration, source, camera channel, unknown channels, bookmark status, and tag status.	
21	The system must eliminate the need for passwords or third-party decryption tools and offer a seamless user interface without complex navigation.	
22	Evidence collected from multiple locations and devices must be organized within a hierarchical case structure to streamline complex investigations.	
23	The software should facilitate recovery of deleted or partially overwritten video footage	

	from supported DVR devices.	
24	The sub-clipping tool must allow precision trimming of footage to capture seconds of critical evidence from hours-long video content.	
25	Playback controls shall offer multiple speed options including 0.5x, 1x, 2x, 4x, 8x, and 16x for efficient video review.	
26	Users shall be able to visually highlight significant clips, segments, or frames, while attaching annotations using tags and bookmarks that can be shared with stakeholders.	
27	Default configuration values and workflow preferences shall be customizable to apply consistently across all future investigations.	
28	A color-coded notification system (red, yellow, green, white) shall indicate alert levels and status messages clearly.	
29	The system shall support pause and resume functionality for any job or process currently in execution.	
30	Pre-scan diagnostics shall offer advanced settings such as forcing sector size to 512, manual sector count specification, and selective file system detection to handle problematic media.	
31	Automatic thumbnail generation shall be supported for all compatible video files, with an option to manually select thumbnails directly from the playback timeline.	
32	Column headers within clip views shall be repositionable using drag-and-drop interaction and allow grouping of video clips by selected attributes.	
33	Users should be able to explore and build custom playlists and clip lists, queueing items for batch export on-the-fly or at a later stage.	
34	The application must generate forensically secure reports at any stage during the video extraction or upon closing a case.	
35	An interactive reporting tool shall be embedded to generate diverse formats of reports such as summaries, clip tables, gallery previews, audit trails, and export documentation.	
36	Multiple report exports should be supported simultaneously to different folder	

	destinations without any functional restriction.	
37	Supported evidence sources shall include physical DVR drives, forensic image formats (DD, E01), video clips from a variety of devices, and cloud-hosted videos from Ring and Arlo with multi-factor authentication.	
38	The application must allow forensic correction of timestamp inaccuracies by applying offsets to individual or grouped video clips.	
39	Exported clips must be capable of displaying corrected date/time information as overlay text to reflect accurate forensic timelines.	
40	The tool must include built-in prompts and notifications for software updates and newer versions.	
41	A complete audit logging mechanism shall capture and record every investigator action, filter used, and system event, with export options for oversight and case documentation.	
42	Export tasks must support queueing of clips directly from the clip view or during real-time playback preview.	
43	A dedicated Case Summary section must be provided that consolidates all relevant case information such as Incident Details, Locations, Source Devices, Case Metrics, and the complete action log.	
44	The software shall offer both dark and light visual modes, allowing examiners to switch themes to reduce visual fatigue during prolonged case reviews.	
45	The platform shall feature a utility tool designed for frontline officers to capture and document transient digital evidence, allowing it to be installed and operated concurrently on any number of Windows laptops or tablets to record DVR footage in a forensically valid format, applying timestamp and cryptographic hash (MD5 & SHA).	
46	This utility must allow documentation of date and time discrepancies present in the DVR system directly at the scene of the crime.	
47	The tool must enable acquisition of photos	

	and videos using built-in or connected cameras, as well as through devices like memory cards or phones belonging to witnesses or victims, embedding metadata such as geolocation, source device ID, and hash values into generated reports.	
48	3 Year Subscription License	
49	One-day training must be provided at the time of installation and setup, conducted on site by an OEM-certified engineer. Training must cover both basic fundamentals and hands-on sessions to ensure familiarity with all functionalities of the tool.	
50	Tender Specific Authorization certificate from the OEM in favour of the Indian Distributor/Reseller/Bidder is mandatory for participation in the tender.	
51	Provide a 2 TB SSD External Hard disk for backup storage facilities.	

VII. Technical Specifications for Logicube Falcon NEO 2 - 3 Years Hardware Warranty

SL. No	SPECIFICATIONS	COMPLIANCE (YES/NO)
	Technical Specifications	
1	The Forensic Field Imager represents the pinnacle of forensic imaging technology, designed to deliver unprecedented speed, efficiency, and versatility in data acquisition.	
2	The device should have the capability to surpass 100GB/min E01 capture speeds, making it the first field imager to achieve such performance. It should be able to image SAS-3 SSDs at speeds up to 115GB/min and handle PCIe drives at speeds exceeding 100GB/min.	
3	The device should have a SAS-3 (12 Gbps SAS) architecture and should support up to 5 simultaneous tasks.	
4	The device should include built-in security features to protect data integrity and prevent unauthorized access, ensuring that sensitive forensic data remains secure.	
5	Capable to imaging/clone data from one to one, two to two or one to many destination media.	

6	The device should be equipped with an extensive array of ports to support various imaging tasks: a. Source Ports: Should have up to 10 source ports to connect multiple devices. b. Destination Ports: Should have up to 11 destination ports for efficient data transfer. c. USB Ports: Should have USB 3.2 Gen-2 (10Gbps) ports for fast and reliable connections. d. Network Ports: Should have two 10GbE ports for imaging to and from network repositories, facilitating high-speed network-based acquisitions.	
7	Support multiple Imager Formats, copy, dd image, .dmg image, e01, ex01, supports MD5, SHA1, SHA256 and dual-hash (MD5+SHA-1) authentication.	
8	The device should be portable and lightweight, making it easy to transport and deploy in various field locations.	
9	Should have Cloud Storage Acquisition (now included as a standard feature) allows you to acquire files from OneDrive, Dropbox, or Google Drive. Capture to any destination drive or network repository connected.	
10	10 write-blocked source ports include 4 SAS/SATA drives supported with 1 port, 2 USB 3.2 (Gen 2), 1 PCIe, 2 I/O ports for use with optional I/O cards including Thunderbolt™ 3/USB-C, 10GbE.	
11	Multiple Imaging Ports: **I. Write-protected source ports include**: a. 1 SAS/SATA (SAS-3/12Gbps) that supports up to 4 drives with a single cable. b. 2 USB 3.2 Gen 2 (can be converted to SATA using an optional USB to SATA adapter). c. 1 PCIe. d. 2 I/O ports for use with optional I/O cards including Future Expansion Thunderbolt 3/USB-C. **II. Multiple destination ports include**:	

	a. 1 SAS/SATA (SAS-3/12Gbps) that supports up to 4 drives with a single cable. b. 4 USB 3.2 Gen 2 (can be converted to SATA using an optional USB to SATA adapter). c. 1 PCIe. d. 1 I/O ports for use with optional I/O cards including Future Expansion Thunderbolt 3/USB-C.	
12	Should have Two 10GbE network ports for network connectivity.	
13	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.	
14	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.	
15	Capable Web Browser/Remote Operation to allows to connect with device from a web browser.	
16	Capable to cross copy support for IDE, SATA, e SATA, microSATA, SAS, ZIF and USB interface and combine-SATA etc.	
17	Should image CD/DVD/Blu-ray media by using a USB optical drive connected to the USB port on the device.	
18	Capable to Detect and capture Host Protected Areas (HPA) and Device Configuration Overlay (DCO) hidden areas on the source (suspect) drive.	
19	Should capture network traffic, internet activity and VOIP.	
20	Capable to Generate Audit Trail Reporting/Log Files in XML, HTML or PDF format.	
21	Should secure sensitive evidence data with whole drive AES 256-bit encryption.	

22	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.	
23	Forensic, Filter-Based File Copy, users can filter and then image by the file extension (such as .PDF, .xls, .JPEG, .mov etc.).	
24	Capable to acquire data over a network.	
25	Capable to generate the log of the processes.	
26	Capable to boot/mount the suspect media virtually in a write-protected environment for the preview of live data.	
27	HDMI Port for connecting display.	
28	Incorporates features supporting forensic evidence handling and documentation practices.	
29	Should come with: a. 1 x M.2 to PCIe Adapter (F-ADP-M2-PCIE3) b. 1 x Mini PCIe (mPCIe) to PCIe Adapter (F-ADP-MINI-PCIE) c. 1 x M.2 to SATA Adapter (F-ADP-M.2-SATA) d. 1 x PCIe to PCIe extender cable (F-ADP-PCIE-CBL)	
30	**Product should carry a 3-year on-site warranty. Any Software/Firmware updates to be provided during the Warranty Period.**	
31	**Tender Specific Authorization Certificate from the OEM in Favor of the Indian Distributor/Reseller/Bidder is mandatory for participation in the tender.**	

VIII. Technical Specification for FRED- Forensic Workstation

SL No.	Parameters	Specification	COMPLIANCE (YES/NO)
1	Processor	Intel Ultra 9 285K, also 24 Cores, 8 P/16 E Cores, up to 5.7 GHz, 36 MB Intel Smart Cache	
2	RAM	128 GB Memory PC5-38500 DDR5 4800 MHz- (4X32GB)	
3	OS, Cache & Storage Drives	a) OS Drive - Internal PCIe M.2 NVMe SSD: 2 TB M.2 NVMe PCIe Solid State	

		Drive - 990 PRO Series b) Drive 2 - Internal PCIe M.2 NVMe SSD: 2 TB M.2 NVMe PCIe Solid State Drive - 990 Pro Series c) Drive 3 - Internal PCIe M.2 NVMe SSD: 2 TB M.2 NVMe PCIe Solid State Drive - 990 Pro Series d) Drive 4 - Internal PCIe M.2 NVMe SSD: Available for future upgradability e) Drive 5 - SATA Interface: 4 TB 7200 rpm SATA Hard Drive f) Drive 6 - SATA Interface: Available for future upgradability g) Drive 7 - USB 3.2 Interface: Available for future upgradability h) Drive 8 - USB 3.2 Interface: Available for future upgradability i) Drive 9 - USB 3.2 Interface: Available for future j) Upgradability k) Drive 10 - USB 3.2 Interface: Available for future upgradability	
4	Graphic Card	NVIDIA RTX 3050, 8 GB, 128-bit GDDR6, 2560 CUDA Cores	
5	Display	24” LED	
6	Operating System	Licensed Windows 11 Professional (64-bit), Additional Linux with Dual Boot Option	
7	Include Hardware Write Blocker with the following support for:	a) USB 3/2/1.1 b) PCIe c) SATA, IDE d) Firewire 800/400 e) SAS	
8	Integrated Hardware Write Blocker should have listed features:	a) Touch screen interface b) Connected to the board on USB 3.1 c) Write-Block and Read/Write visibility via Lock/Unlock LEDs d) Read and write mode capabilities for all device ports controlled via LCD Menu to enable the investigator to use the Write Blocker as a Drive Wiper for USB/SATA/IDE/FIREWIRE/SAS/PCIe drives when required by the users e) Allows simultaneous imaging of 2 attached devices on the integrated Write Blocker Allows forensic imaging	

		of at least 4 SATA Drives simultaneously	
9	Memory Card Writer Blocker:	Integrated Forensic Media Card Reader Read-Only or Read-Write mode capable	
10	Dock with cooling system for Evidence Hard Drive	Integrated Retractable imaging shelf (fully retracts into the system when not in use). Dual fans for maximum cooling and surface coverage auto on/off switch when the shelf is opened or closed. Slotted, cushioned, nonconductive, non-skid, surface supports all popular Drive sizes (3-1/2", 2-1/2", 1.8", etc)	
11	Hot swappable bays and Optical Drive	a) 2 x Shock Mounted SATA Removable Hard Drive Bays b) 4 x Hot Swap Shock Mounted Universal Removable Hard Drive Bays. All Hot- Swap Bays should be Read-Only or Read- Write mode capable. c) BD-R/BD-RE/DVD±RW/CD±RW Blu-ray Burner Dual-Layer Combo Drive	
12	Others integrated components	a) 1 X RJ45 LAN port b) USB 3.1 (Minimum 2 ports) c) USB 3.1 Type-C (Minimum 1 port) d) USB 3.0 (Minimum 8 ports) e) USB 2.0 (Minimum 2 ports) f) Keyboard and Mouse Combo	
13	Internal connections	All components such as the Integrated Write Blocker, Hot Swap bays and USB Hub should not be connected on the motherboard and should have different connections to avoid IRQ hardware confliction.	
14	Toolkits	Adapters and Cables: Cables and adapters to image and process internal/ external drives including SAS, SATA, IDE, Micro SATA, SATA LIF, MacBook Air Blade Type SSDs, mini/micro-SSD cards, PCIe SSD m.2 NVMe, PCIe SSD MacBook Pro and Server Class PCIe SSD Security. **Screwdriver Set: A varied assortment of popular security bits for opening computer enclosures that may have been locked down in a corporate environment.**	
15	Warranty	The product should carry a 3 (Three) Years On-Site Warranty. Any Software/Firmware updates should be provided in the Warranty Period.	

16	Proof of Manufacturing of Forensic Workstation	Product offered should be of International Repute & Brand and should not be a customised/assembled Product from various sources. Either the Manufacturing License of the OEM should be attached or the Product Offered should have at least 23 Components which are marked by the OEM Name preferably on the various PCB's used in the offered Forensic Workstations.	
17	MAF	A Tender Specific Authorization Certificate from the OEM in favour of the Indian Distributor/Reseller/Bidder is mandatory for participation in the tender.	
18	Training	Training to be done by an OEM-certified engineer at the time of Installation and as per request.	

X. Financial Investigation and Analytics Software (Perpetual License with 3 Years Support)

SL. No	SPECIFICATIONS	COMPLIANCE (YES/NO)
	General Specifications	
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.	
2	The system should ensure the automated acquisition and processes individual files or it should be done in batch mode.	
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: a. Value Date b. Description (ATM Withdrawal, To Transfer, RTGS, NEFT, Cash) c. Reference Number, Cheque No. d. Debit e. Credit f. Balance	

5	The system should allow users to categorize the data on various parameters 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 an individual account.	
7	The system able to identify high value/low value debit/credit transaction with conditions (>, <, =) specified amount.	
8	The system to identify high value/low value debit/credit transactions between two entities over a specified period of time.	
9	The system able to identify and list all transactions done in one account by different modes like NEFT, RTGS, Cheque and Cash	
10	The system able to identify and list all debit/credit transactions where the transaction type is cash. (or any other mode like NEFT, RTGS, Cash)	
11	The system should be able to identify the frequency of transactions between two accounts. The system should also be able to identify on the basis of the 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.	
14	The system to enable the user to analyze 'text fields' of the transaction data. (i.e., Transaction Description)	
15	The system should allow users to analyze cumulative data of all the years by merging different files together.	
16	The system should allow users to merge transaction data of one or more individuals spread over a single or multiple entities, further spread over single or multiple entity branches.	
17	The system should allow the 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.	
19	The system should allow users to perform customized searches using logical and financial	

	formulae. (And, Or Not). The system should allow users to cross manipulate among different result sets.	
20	**Provide 2 TB SSD External Hard disk for backup storage facilities.**	
21	**Tender Specific Authorization Certificate from the OEM in favour of the Indian Distributor/Reseller/Bidder is mandatory for participation in the tender.**	
22	**Perpetual License with 3 Years Support.**	
23	**One-day training must be provided at the time of installation and setup. The training should be conducted on-site by an OEM-certified engineer.**	
24	**The training must cover both basic fundamentals and hands-on sessions to ensure familiarity with all functionalities of the tool.**	

XI. Blockchain Investigation and Cryptocurrency Analysis Software for 6 Users - 3-Year Subscription License

SL. No	SPECIFICATIONS	COMPLIANCE (YES/NO)
	Specifications	
1	The solution should offer an interactive visual representation of transactions across multiple layers, tracing from the input address to the final exchange.	
2	**The solution must provide full coverage for a minimum of 30 blockchains, including but not limited to Bitcoin, Ethereum, Linea, Tron, SUI, Aleo, VerifiedX, Platon, Canton and ICP. It should offer coverage for over 3,000 tokens and enable unlimited analytical capabilities across all supported blockchain networks.**	
3	The solution should provide access to crypto-currency forensic investigation platform for a period of three (3) years, with the capability to create and manage up to 6 user accounts within the organization.	
4	The OEM shall provide a warranty for a period of three (3) years from the date of activation, which includes regular product updates, feature enhancements, and maintenance support during the warranty period.	

5	The solution should depict both direct and indirect exposure of transactions to any suspicious activities involving real-world entities, such as exchange transfers, unnamed service scams, P2P exchanges, mixers, mining pools, high risk exchanges, gambling, terrorist financing, CSAM, narcotics, and similar activities.	
6	**The solution should offer clearly differentiated functionalities for address/wallet tracing and transaction-level tracing, enabling users to perform each type of analysis independently through dedicated interfaces.**	
7	It should allow real-time database updates within an active session without the need to close the application interface.	
8	Support for automated investigations to instantly expand and visualize both direct and indirect wallet exposures to real-life entities with a single click without having to manually expand every node.	
9	Provision of comprehensive training on the tool, its technology, and usage for users designated to mentor and assist others within the organization. Regular periodic training, including updates, should be provided for the tool, along with complete technical support for the entire team.	
10	Should have coverage of digital assets that represent at least 97% of total global crypto market capitalization.	
11	**Support for cross-chain tracing of at least 45+ de-fi bridges including but not limited to Thorchain, Synapse protocol and offer seamless visualizations of such transactions**.	
12	The solution must include a risk alerting and transaction monitoring capability, with AI-driven chat-based functionality to generate concise summaries and contextual insights from risk alerts.	
13	Ability to share password protected graphs across users within the organizations and outside of organizations	
14	Support for continuous monitoring of real-time transactions with a customizable real-time alerting feature.	
15	Access to a directory of Virtual Asset Service	

	Providers (VASPs) for contact details and legal processes	
16	Support for clustering selected wallets, assigning custom names and colours, and viewing aggregate transaction values for the entire cluster.	
17	The platform should provide deconfliction intelligence, highlighting whether specific wallet addresses or entities under investigation have already been flagged by other law enforcement or government agencies using the tool.	
18	Should adhere to security frameworks and standards, including ISO 27001, SOC II, and GDPR certifications.	
19	Should have the ability to split/delete transactions between addresses to segregate tokens from native assets and to separate out transactions or assets which are important for the case and either hide the rest or display them separately.	
20	Support for sequential and custom investigation board layout with an option to toggle between both curved and straight-line transfer links between wallets	
21	Should provide specific exchange clusters and associated deposit addresses with real-time data.	
22	Ability to download filtered data as reports in CSV format for analysis and documentation.	
23	Must have the ability to filter exposure and counterparties by categories and sub categories of illicit activities for both receiving and sending transactions.	
24	The tool should have the ability to display both complete transaction values with all decimal points and rounded values as needed.	
25	The tool shall allow investigators to manually add custom nodes on the investigation board, enabling the incorporation of off-chain intelligence. These nodes should be linkable to on-chain wallet addresses, supporting comprehensive case-building and contextual analysis.	
26	Support for adding comments/notes on the graph to highlight findings, with an option to disable them.	
27	The tool should have enhanced search	

	functionality to retrieve addresses by entity name, partial wallet addresses, and allow fetching multiple addresses and transactions simultaneously.	
28	Support for analyzing smart contracts, viewing similar contracts, and exploring other contracts created by the same owner.	

Sd/-
Assistant Inspector General of Police, Procurement
For DIRECTOR GENERAL OF POLICE &
STATE POLICE CHIEF, KERALA