NATIONAL FORENSIC SCIENCES UNIVERSITY
Sector-9, Gandhinagar-382007
Phone - 079-23977123/24 & Fax-079-232 47465

IMPORTANT INSTRUCTIONS / TERMS / CONDITIONS TO TENDERERS
FORMING PART & PARCEL OF ENQUIRY DOCUMENT:

TENDER ENQUIRY No: NFSU/PUR/ET-01(66)/UPSIFS/2024-25

ITEM : **66** : SHOWN AS UNDER

TENDER FEE : **Rs. 1500/- (Rs. One Thousand Five Hundred Only)**

SERIAL # OF P.T.F. :

NAME & ADDRESS OF TENDERER : _____

: _____

: _____

C.S.P.O., REGISTRATION GROUP NO. :

THIS TENDER DOCUMENT COMPRISES OF TWO PARTS LABELLED AS PART I & II

THIS TENDER ENQUIRY IS FOR **FIXED QTY. PURCHASE** OF ITEM AS UNDER:

DETAIL SPECIFICATIONS ARE GIVEN IN PART-I i.e. TECHNICAL BID.

Sr. No.	ITEM CODE	ITEM NAME	QTY.	PLACE OF DELIVERY & INSTALLATION	E.M.D. (Rs.)
03	66	**Mobile Forensic Extractor and Analysis with Cloud support**	02	UPSIFS, Lucknow	**2,40,000/-**

NOTE:

(1) **IF MANUFACTURER IS NOT AVAILABLE FOR IMPORTED COMPONENT (EQUIPMENT – MATERIALS) THEN THE REPUTED MANUFACTURERS / AUTHORIZED REPRESENTATIVE / DEALER APPOINTED EITHER BY PARENT COMPANY OR ITS SUBSIDIARY COMPANY SHALL BE ALLOWED TO QUOTE THE TENDER.**

(2) **THE TENDERER HAS TO SUBMIT ALL THE REQUIRED DETAILS / DOCUMENTS WITH THE TENDER. NO COMPILANCE WILL BE ACCEPTED AND CONSIDERED AFTER DUE DATE I.E OPENING OF THE TECHNICAL BID.**

(3) **ANNUAL MAINTENANCE CONTRACT (A.M.C.) & COMPREHENSIVE MAINTENANCE CONTRACT (C.M.C.) CHARGES FOR NEXT FIVE YEARS AFTER WARRANTY SHOULD BE QUOTED SEPARATELY. AMC/CMC CHARGES WILL NOT BE TAKEN INTO ACCOUNT FOR PRICE COMPARISION FOR DETERMINING THE LOWEST BIDDER.**

SIGNATURE & STAMP OF TENDERER

PART-I

TECHNICAL BID

T.E.NO: NFSU/PUR/ET-01(66)/UPSIFS/2024-25

Name of Item: Mobile Forensic Extractor and Analysis with Cloud support

Manufacture_____ Brand_____ Model_____

[A]	REQUIRED SPECIFICATIONS	SPECIFICATIONS AVAILABLE IN OFFERED MODEL
	Mobile Extraction Capabilities	
	The solution should be able to extract forensic evidence from supported mobile devices including mobile phones, handheld tablets, portable GPS devices and drones.	
	It should provide users with all physical, file system and advanced logical extraction capabilities for different devices and different Operating Systems as well as allow extraction of Cloud Data source tokens accessed by the Mobile Phone.	
	It should support more than 32,000 device profiles, 12,700 different mobile application versions and 400+ total unique applications. All the supported mobile device models and device profiles must be tested and verified by the OEM's R&D Team.	
	It should support automatic detection of supported devices. It should also support manual search for devices by manufacturer, model and IMEI number.	
	It shall have the ability to offer dynamic profiles of phones, based on IMEI, OS type, version and chipset.	
	It should come with a compact and lightweight case with necessary cables for the supported phones and operating systems. A multi-SIM adapter with support for Micro, Nano and standard SIM cards should be supplied.	
	Support Android, iOS, Blackberry, Bada, Symbian & Windows mobile device and generic capabilities for certain chipsets like MTK and Qualcomm, to obtain decrypted Physical Extractions.	
	The solution should be capable of cloning the SIM ID, which allows to extract phone data while preventing the mobile device from connecting to the network. Ability to perform SIM data extraction from a SIM or USIM card.	
	The solution must use custom-made OEM proprietary boot loaders instead of the 3rd party bootloaders.	
	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. This capability should allow user to perform other extractions at the same time.	
	The software should allow examiners to perform a quick selective extraction of specific applications or files, while doing Selective File System extraction for supported Android as well as iOS devices.	
	The software should also allow selective extraction of only cloud tokens from the phone while doing Selective File System extraction.	
	The software should also be able to quickly capture the chat data, by automatically taking screenshots from any Android device. It should also allow the user to perform a text search on the captured screens as well. This should support applications like WhatsApp, Signal, Instagram and Snapchat	

	The software should be able to categorize the applications and group these categories for applications found in mobile devices and user should be able to filter by category. This capability should be available for supported Android as well as iOS devices.	
	The software should have a workflow guidance widget to help managers and administrators to guide, control and enforce working procedures.	
	The software should include a copy functionality which allows selection of specific files such as images, videos, audio and documents from any unlocked device such as Android & iOS phones or removable drives.	
	The software should have the capability to allow the user to stop the Android File System extractions (except for Android Backup and APK downgrade) before they complete to save the partial extraction up to that point.	
	Users should be able to open a Support Ticket directly from the software GUI.	
	Extraction Support	
	It should support advanced unlocking capability to perform Full File-System extraction from locked Samsung Exynos FBE and FDE devices with Secure start-up. This capability should support devices S8, S9, S10, and A10-A50 series, running up to the Android 13. It should allow users to upload their own custom dictionary to enhance the unlocking process to make the process easier and faster.	
	There should be a capability which allows lock bypass and get full file system & physical data collection from Samsung S8, S8+, S9, Note8 and Note 9 models with Qualcomm chipset. As part of full file system extraction, there should also be ability to extract Samsung Secure Folder.	
	The software should support Full File System extraction for the latest unlocked Samsung Exynos high-end devices like S20, S21, S22 running on Android 11. S21 should be supported with Android 12 as well.	
	Full File-System extraction from latest Samsung devices like Galaxy A04, A04s, A04e, A14, A24, A34, A54, M04, M14, M54, F04, F14 and F54	
	Full File-System extraction from the latest devices with Snapdragon 8 Gen 2, Snapdragon 4 Gen 1 and Snapdragon 7 Gen 1 chipsets.	
	The software should support extraction of Full File System data from unlocked Qualcomm chipset-based Samsung devices like S9, S10, S20, S21, S21 Ultra 5G, S21 Plus, S22 devices running on latest security patch level and up to the most recent Android 11.	
	The software should allow full file system extraction for unlocked Huawei Kirin devices running Android 9 and higher.	
	The software should allow collection of data from applications like Signal Private Messenger, Samsung Health and Proton Mail that leverage keystore for additional security using methods like full file system extraction for wide range of Android devices.	
	The software should have support for a generic Full File System or Physical Extraction for unlocked high-end Android devices with Qualcomm chipsets. This capability should be available for the popular devices from major Android vendors such as Samsung, Huawei, Xiaomi, OPPO, OnePlus, VIVO, as well as devices from Nokia, LG and Motorola, running on Android Versions from 7 up to 11.	
	There should be support for Full File system extractions from latest high-end Android Qualcomm devices such as Samsung Galaxy S21, S21 Ultra 5G and S21 Plus, Xiaomi Mi 11, One Plus 9, Redmi K40 pro, and others.	

	The software should at least provide the following extraction methods to the user: Selective Filesystem Extraction, Selective App data extraction, Selective cloud token extraction, EDL extraction with decryption, 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.	
	The software should provide capability to perform Full File System or Physical extraction from unlocked MTK 64-bit devices running Android 9 and above for devices like Oppo A55, Realme 7, Vivo Y19, Xiaomi 11T and others with chipsets like mt6732, mt6735, mt6738, mt6763, mt6768, mt6769, mt6771, mt6781, mt6785, mt679, mt6983, mt8161, mt8163, mt8165,mt8732 and mt8752	
	The software should support vendor built-in backup for LG and Huawei for extraction of personal data like contacts, text message, call history, installed application data and system settings.	
	The software should provide capability to perform Full File System or Physical extraction from unlocked Exynos 64-bit devices running Android 9 and above for devices. It should support all Exynos chipsets up to Exynos 2200.	
	It should provide capability for Nokia feature phones with proprietary Nokia OS and MTK & Spreadtrum chipsets to get physical extraction from Nokia 105, 110, and 130 families.	
	The software should have support to bypass pattern, password and pin locks and overcome encryption challenges for a wide range of Qualcomm EDL, Qualcomm and Exynos based supported Samsung, Motorola, LG and Sony devices.	
	The software should retract a range of data e.g., Call Logs, Contacts, Calendar SMS, MMS, Video, Image, Apps Data, GPS Trail, Chat, E-mails etc.	
	It should have support for data extraction, decoding and analysis for unlocked devices running up to iOS 17.4.0.	
	The software should be able to support full file system extraction using Checkm8 capability for Apple iPhone 7,7+,8.8+ and X for iOS 15.7.3 depending on the iPhone device supported based on Apple official release.	
	Support for Various Phones:	
	Android Phones:	
	It should support unlocking with physical extraction for at least 100 Qualcomm and Exynos based Samsung devices, including S7, S7 Edge, S6, S6 Edge+, Note 5, A5, A7, J4+, J5, J6, J7 and J8 families.	
	It should have lock bypassing decrypted physical extraction capability for Qualcomm Android devices including LG, ZTE, Xiaomi, Huawei, Alcatel and Motorola	
	It should have decrypting bootloader capability for Huawei devices with HiSilicon Kirin chipsets and Samsung devices with Exynos processor.	
	It should support Physical Extraction via ADB for android devices directly to any USB storage or an SD card connected to the device. This method should be generic and should be supported across most Android phones available in the market. This method should support android devices including OS version 7.	
	It should have physical extraction method from more than 400 locked Android based devices bypassing any type of lock (Pattern/PIN/Password) using proprietary boot loaders, enabling a	

	forensically sound extraction process.	
	It should acquire apps data from Android devices via all extraction types including:	
	Facebook, Facebook Messenger, Google+, PingChat! (Touch), Skype, Twitter, Viber, Yahoo Messenger, WhatsApp, TigerText, Dropbox, QIP, Kik Messenger, Evernote, Kakao Talk, imo, ICQ, Vkontakte, HideSMS, Kakao Story, Kakao Map, MeetMe, Coco, Google Duo, FitBit, Zalo, Yubo, Zello	
	Samsung – Galaxy S7, Galaxy Note 7, Galaxy Note 5, Galaxy Note 8, Galaxy S6, Galaxy S8, Galaxy S8+, Galaxy S6 Edge, Galaxy S5, Galaxy S4, Galaxy SIII Family, Galaxy SII, Galaxy Note 4, Galaxy Note II, Galaxy Mega, Galaxy s5 duos, Galaxy alpha, J3 Neo, J5, J7, A5 and A7.	
	Indian Phones – Intex Aqua Amoled, Intex Aqua Core; Intex Cloud Y5; Intex Aqua i7; Karbonn A12+; Karbonn A25, Karboon S99 Titanium, Xolo A50zip0S; A114R Canvas Beat, Micromax A190 Canvas HD Plus, Intex Aqua ring.	
	Blackberry Phones:	
	It should enable physical extraction and decoding from BlackBerry devices running OS 4-7. Physical extraction should be performed using proprietary boot loaders, enabling a forensically sound process. Real-time decryption should be enabled for selected devices.	
	BlackBerry Messenger (BBM) messages including Deleted messages and chats, message attachments, contact photos, BBM from groups: Chats, contacts and shared photos.	
	Windows Phone:	
	It should support physical extraction and decoding of devices running Windows Phone devices running OS versions 8.0, 8.1 and 10. It should also support obsolete OS including 6.0 and 6.5.	
	The Devices supporting Physical Extraction should at least include HTC Pro, HTC HD2 T9193, Xperia X1, Nokia Lumia 520, LG GM750 and other popular models.	
	Nokia BB5 Phones:	
	It should support bit-for-bit physical extraction from locked and unlocked Nokia BB5 devices using proprietary boot loaders.	
	It should support decoding of Symbian databases including Decoding of intact and deleted contacts, SMS, MMS and call logs; Decoding support for multilingual content.	
	Portable GPS Device:	
	It should enable physical extraction and decoding of data from a range of portable GPS devices. The Decoded data should include: Entered locations, GPS fixes, Favorite locations, GPS info.	
	It should provide a solution to the encrypted TomTom trip-log files that reside in the TomTom device STATDATA folder. It should support Extraction and decoding of existing and deleted data from TomTom devices. TomTom extraction and decoding of information includes: Home, Favorites, Recent, User entered, Locations, Last journey, Location, Date & Time, Routes, GPS fixes (also deleted), Deleted locations (of all categories)	
	It should support Data Extraction from Garmin & Mio devices. Extracted data includes: Favorites, Past journey (containing all the fixes during the journey), deleted GPS fixes	
	Feature Phones:	
	It should enable physical, file system and logical extraction, and decoding from selected devices. Decoding of intact and deleted data: Phonebook, SMS, MMS, calendar entries, SIM ID and more.	

	The Supported Phones (for either Physical/ File System/ Logical) should at least include:	
	Nokia: 1280, 1616, 1650, 1661, 1661-2b, 1680 Classic, 1800, 2720 fold, 2720a-2b, 2730 Classic, 2760, 3109 Classic, 3110 Classic.	
	Samsung: SGH-C120, SGH-A127, SGH-M130L, SGH-A137, SGH-T139, SGH-J150, SGH-X150, SGH-X160, SGH-X166, SGH-X168, SGH-C170, GT-E1195, GT-E1230, SGH-E1310B, SGH-B2100.	
	Chinese Chipsets Based Phones:	
	Using proprietary boot loaders, it should perform a bit-by-bit physical extraction, from devices manufactured with Chinese chipsets, accessing the device's memory, whilst maintaining forensic integrity. The boot loaders prevent the tampering of data, during physical extraction.	
	The tool should provide generic extraction with Decrypting bootloader for MTK based chipsets including 6580, 6735, 6737, 6753, 6755, 6757 & 6797.	
	The software should be able to supports acquisition and decryption of 80+ MTK distinct chipsets and have the ability to conduct Physical or Full file system (FDE &FBE) extraction of unlocked MTK devices with ADB enabled. The Android OS supported should be up to version 9.	
	Decoding and Analysis Capabilities	
	Capability to provide powerful decoding and analysis solution for the extracted device data.	
	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.	
	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.	
	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.	
	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.	
	Should have the capability to parse windows computer data like DD, E01, RAW, L01,001 or BIN images in the same application.	
	Should have Registry Viewer to enable viewing of all Registry hives in a UI similar to the native Windows Registry Editor	
	Should be built on a database architecture to reopen cases quickly without having to reprocess the data.	
	Should have internal cryptocurrency enrichment to automatically identify the usage of cryptocurrencies and to detect wallet addresses and transactions within the device data.	
	It should also have an external 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.	
	Function to allow view of cloud data in the platform with a valid cloud extraction license. Users can review the device data and cloud data through a single software interface with a unified experience, for a seamless and simplified review process.	

	Enable highlighting of the exact position for each decoded content entry, enabling full tractability between the analyzed data and the Hex.	
	Support for image carving to recover deleted image files and fragments when only remnants are available. Also support for advanced location carving, by decoding more location data from unallocated spaces and unsupported databases.	
	It should perform an on-demand searches for viruses, spyware, Trojans and other malicious payloads in files.	
	Enable the user to identify the usage of cryptocurrency and detect addresses or transactions within the device data to provide coin data including value, currency type, artifact type and model type. Support for parsing of the crypto wallet apps like Coinbase Wallet, Metamask, BitPay, Trust Wallet and MyEtherWallet	
	Media classification capability to detect and categorize images and video frames into key categories. This capability should be selectable, allowing user to decide if he wants to run the media classification on a particular case.	
	The media classification capability based on machine learning to automatically identify media files related to 20+ key categories like Cars, Credit cards, Documents, Drugs, Faces, Photo ID, Flags, Food, Gatherings, Screenshots, Handwriting, Maps, Money, Nudity, Tattoos, Weapons and Suspected CSA (Child Sexual Abuse).	
	It should also be able to segregate the different media classifications into relevant groups like people, textual etc. to make the data review simpler and more efficient.	
	Capability to convert geographical location information to corresponding address directly from the software.	
	Decode network usage information to record the sending and receiving of information via various network connections.	
	Capability to identify unsupported apps in databases and surface data from them. It should leverage Artificial Intelligence to perform automatic analysis of any application database, and decode chats, contacts, user accounts and location artifacts without any prior knowledge of the application.	
	Support parsing of the Samsung wiped data to get the device factory reset data and also able to detect the time of last iOS data-wipe.	
	Support parsing of Apple pay data to get Apple wallet transactions and location data. Data should be available for transactions from both Safari and iMessages.	
	Capability to verify file integrity with use of MD5 and SHA 256.	
	Support applications such as WhatsApp, Skype, Facebook Messenger, Azar, Telegram, Discord, Tiktok, Wechat, Wickr, Reddit, Signal, Viber, Zalo, Cash App, imo, DuckDuck Go browser, Plus Messenger and WhatsApp dual mode.	
	Support the parsing of messages, calls and user accounts for the secure messaging app Threema for Android devices.	
	Support the parsing of messages, calls and user accounts for the secured Session Private Messenger for both iOS and Android devices.	
	It should have a built-in SQLite Viewer. Ability to save the queries created by the wizard and then run them again when the same application is encountered in other extractions.	
	Capability to match files extracted against Hash Databases and it should have built-in support for Project VIC and CAID hash databases.	
	Capability to allow user 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.	
	Support viewing of all locations on a single map. Enable viewing of	

	extracted locations using offline maps even without an Internet connection with an option to connect to offline maps from a shared central location.	
	Support viewing of text files including file information, content, and Hex.	
	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.	
	Provide a separate report with device information and user account information for quick reference of users.	
	It should enable chat messages to be exported in conversation format, in PDF reports. Support exporting of selected emails to EML format.	
	Support hash verification to ensure the extraction decoded is the same extraction received from the device.	
	Ability to merge multiple extractions in a single unified report for efficient reporting and investigation.	
	Option to adjust the timestamp according to the time zone and offset setting on the device.	
	Should provide a file format viewer which allows users to view, search and copy readable content from various file types like plist, bplist, etc.	
	Capability to extract Google advertisement ID (AD-ID) on advanced logical extraction and iOS advertisement ID on iPhones.	
	Allow playback of WhatsApp audio files in analysis software. Provide indication of reply for WhatsApp messages in application and reports generated.	
	Support decoding and review of secret messages from Facebook Messenger in Android, with support for vanish mode (self-destructing messages).	
	Support for parsing WhatsApp's disappearing messages and iOS "view once" media. Support for parsing of Signal iOS messages which were set to self-destruct at a specified date-time.	
	Support for parsing WhatsApp messages received while the device was locked and not yet written to the main WhatsApp database.	
	It should be possible to validate the image hash directly from the software GUI.	
	Ability to extract memory from Samsung devices to decrypt Samsung Health DB and support for Samsung Digital Wellbeing.	
	Decrypt and decode location information from Samsung Rubin service.	
	Support Samsung browser passwords and allow user to review the decrypted password data of the device owner.	
	Ability to parse the artifacts supported by iOS Biome service like wireless connection artifacts and device events like airplane mode status, lock status, orientation change plugged-in status, location and notes content.	
	Support for decoding of Snapchat stories to get location and media files uploaded by the user.	
	The software should support the following decoding capabilities:	
	➢ Decode the powering events, decode Samsung password manager and Samsung locked notes	
	➢ Decode iOS CashApp to parse user account, transactions, contacts, and credit card data	
	➢ Decode Microsoft Teams to parse chats, calls, contacts, user account, calendar events, and web artifacts	
	➢ Decode encrypted media from iOS Private Photo vault including location and transaction data, should include transactions done with Safari and iMessages	

	➢ Decode SkyPhone application to parse account information, address book and call history	
	➢ Decode Google Archive Files	
	➢ Decoding of backups for MTK based Android phones.	
	➢ Decoding of warrant return packages from WhatsApp, Facebook, Google, Snapchat, Instagram, Apple iCloud, Discord, TextNow and SkyECC	
	➢ Decoding of physical activity data from health and wellness applications	
	➢ Decoding of different WhatsApp variants like WhatsApp2Plus, obwhatsapp, ob2whatsapp, ob3whatsapp and ob4whatsapp	
	➢ Seamless process for cloud data decoding	
	➢ Automatic decoding of data from .zip and TAR files	
	➢ Decoding of the iCloud backup production set obtained from Apple devices and Instagram production set from other devices	
	➢ Decoding of Huawei backup and Huawei HiSuite backup.	
	➢ Decoding of ADB backup, MTK backup, iTunes backup, Blackberry 10 backup, Google Takeout (Google Archive) and LG backup	
	➢ User should be able to save and abort decoding process.	
	➢ Decoding of Berla ivx files	
	Keyword search capability to search within the decoded data and also in the contents of the files such as docx, pds, xls, DB, txt, plist and XML which are present in the extracted device.	
	Cloud Data Extraction Capability	
	Should allow access to remote cloud data sources to obtain, decode, save and perform analysis of this data.	
	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.	
	The data from the cloud sources should be from the private domain, including data from social-media applications, instant messaging applications, lifestyle applications, web pages, file storage sources and other content available on cloud using a process which is forensically sound.	
	The Software should allow access to remote cloud data sources using cloud login keys from mobile devices supporting iOS and Android. It should also identify & leverage cloud tokens & passwords from computer & browser to expand available cloud sources to investigate.	
	Support extraction of different content types from the data sources which includes messages, images, videos, files, contacts, calls, user profile, locations, user activities and backups.	
	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 option to cancel the process if required.	
	Allow users to gather private user data with appropriate legal authority from over 60 of the most popular social media and cloud-based sources, i.e. Facebook, Telegram, WhatsApp, Viber, Twitter, Gmail, AOL Mail, Dropbox, Uber, Skype, Instagram, , TikTok, Line, LinkedIn, SnapChat messages, Linkedin Public, Discord, Google Drive, etc., using login credentials provided by the subject, cloud login keys extracted from mobile devices or PCs, retrieved from personal files or via other discovery means to gain access to time-sensitive evidence.	
	Capability to create cloud tokens from manually entered credentials for future cloud extractions.	
	Allow extraction of Facebook location history data to provide	

	information about location of a device or account.	
	Should have the media classification capability to detect and categorize images and video frames into key categories. This capability should be selectable, and user should be able to decide if he wants to run the media classification on a particular case.	
	The media classification capability should be based on machine learning to automatically identify media files related to 35+ key categories like Cars, Credit cards, Documents, Drugs, Faces, Photo ID, Flags, Food, Gatherings, Screenshots, Handwriting, Maps, Money, Nudity, Tattoos, Weapons and Suspected CSA (Child Sexual Abuse).	
	Capability to use the QR code scan of the unlocked phone to access and extract the Telegram Web data including contacts, calls, user account, chats, channels data, instant messages including attachments, shared contacts and locations.	
	Capability to access WhatsApp Web data through QR code scan of the unlocked device to extract data including contacts, user account, chat data and chat instant messages.	
	Ability to validate data artifacts from iCloud data, iCloud drive, iCloud Photos, iCloud keychain, google contacts, calendar, task and photos. Support WhatsApp Google backup allowing extraction of WhatsApp backups using a Google User account, password and a mobile device.	
	Support extraction of Samsung backup files, including photos, calls, messages and notes.	
	Allow use of cloud login keys from the Mobile device and using cloud keys it should result in mimicking the mobile device thus leaving minimal login traces and generating little or no alerts to the end user. Also allow extraction from a variety of remote cloud data sources using known username and password.	
	Support 2FA authentication when accessing cloud data using username and password for at least Facebook, Google, Twitter and Dropbox	
	Support creation of PC browser tokens for Facebook, Google, Instagram and LinkedIn. It should also support creation of PC apps token for iCloud and One Drive.	
	Support reduction of extraction time from Cloud storage sources such as Google Drive, Dropbox, One Drive, etc. by pre-selection of specific files and directories for extraction	
	Support extraction of several files revisions from Cloud storage sources such as Google Drive, iCloud Drive, Dropbox, OneDrive, Outlook 365, Office 365, Box, and Magenta Cloud application	
	The software should support iCloud backups for iOS16. Support retrieving iCloud backups using iCloud login keys with support for 2FA.	
	Support downloading of WhatsApp & Viber cloud backup from iCloud and Google Drive. WhatsApp data download should also work for iCloud with 2FA.	
	Should display the location events chronologically. It should enable viewing of extracted locations using online as well as offline maps even without an internet connection.	
	Should automatically collect and hash digital evidence such as media files.	
	Allow access to user requests over popular IOT devices like Amazon Alexa and Google Home.	
	Support for extraction of Samsung Cloud backups.	
	Support Google's backup and extraction features saved notes on Google Keep, Google My Activity, Google passwords, Google recent devices from Google servers.	
	Ability to attach a photocopy or document that contains the legal	

	authority search warrant for the cloud extraction for each case. Ability for first time users to acknowledge that the method is used thoughtfully and with proper authority.	
	Reporting of extracted data from the Cloud to human readable format such as PDF, Word, Excel, HTML and XML. It should provide global setting to select/unselect items in a report. The software should provide additional security for protecting the reports. It should also allow to password protect the reports.	

[B]	**IMPORTANT TERMS AND CONDITION FOR SUPPLY**
	1. **Delivery :** The Director Uttar Pradesh State Institute of Forensic Science, Piparsand, Sarojini Nagar, Kanpur Road, Lucknow- 226008
	2. **Installation/Inspection:** Uttar Pradesh State Institute of Forensic Science, Lucknow
	3. **Payment**: By NFSU Gandhinagar Campus