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(67)/UPSIFS/2024-25

ITEM : 67 : 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.)
04	67	**Mobile Forensic Acquisition and Analysis Tool**	02	UPSIFS, Lucknow	**1,80,000/-**

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(67)/UPSIFS/2024-25
Name of Item: Mobile Forensic Acquisition and Analysis Tool
Manufacture_____ Brand_____ Model_____

[A]	REQUIRED SPECIFICATIONS	SPECIFICATIONS AVAILABLE IN OFFERED MODEL
	The mobile forensic solution should offer a choice of software license or USB hardware dongle(CodeMeter) license. The license should be pereptual.	
	The mobile forensic solution should provide a case binder for all the cables.	
	The mobile forensic solution should provide a SIM Card Reader with support of Standard, Micro and Nano SIM cards.	
	The mobile forensic solution should provide SIM-ID Cloner Cards.	
	The mobile forensic solution should provide a Write Protected Universal Memory Card Reader.	
	The mobile forensic solution should have at least 47,000+ mobile forensic profiles.	
	It should support more than 440+ Applications and 4400+ different versions of these applications.	
	The mobile forensic solution should have a image content recognition capability and utilising NVidia GPUs toaccelerate image classification times.	
	The mobile forensic solution should allow for the extraction of at least up to 3 mobile devices simultaneously with just a single license key if required.	
	The mobile forensic solution should have fast file opening and users should not need to wait longer than a maximum of 60 seconds to visualize the extracted data.	
	The mobile forensic solution shall provide options for support of mobile devices via Generic Profiles to allow for support of new and untested devices. Required generic profiles :	
	a) Android generic, Apple iOS generic, RIM Blackberry generic, Windows generic.	
	b) Android MediaTek generic, Android Spreadtrum generic, Qualcomm generic, Samsung exynos generic.	
	c) Mediatek generic, Spreadtrum generic, Coolsand generic.	
	d) LG Android generic Qualcomm, Samsung generic, Sony generic.	
	The mobile forensic solution should support searching of content on text-based documents.It must have capability to search for specific words in different file formats such as pdf, txt, xml, html, and SQL databases.	
	The mobile forensic solution should have a viewer to save and recall a quick view to avoid recreating the same set of filter repeatedly.	
	The mobile forensic solution should have a viewer to show extraction from single or multiple devices.	
	The mobile forensic solution should have a viewer to show extraction in multiple tab and multi-monitor mode.	
	The mobile forensic solution should have a viewer to easily tag an item as Important with one mouse click.	
	The mobile forensic solution should have a viewer to create new tag	

	with desire tag name and colour. User created tag can be transferred to another computer easily.	
	The mobile forensic solution should have a viewer to create, customize or delete any filter.	
	The mobile forensic solution should have a viewer to provide four investigator views(List, Column, Gallery and File Tree).	
	The mobile forensic solution should have a viewer to show data in Source Mode, SQL Viewer and Map View without using the native or 3rd party application.	
	The mobile forensic solution should have a text filter to search on the entire extraction and show the result instantly.	
	The mobile forensic solution should have scalable Overview page with Recently Opened Extraction, Case Content, Exhibits, Quick View, Artifacts information, Exhibit Data, Summary & Statistic, General Information, Device Overview and Extraction Log.	
	The mobile forensic solution should have options for export of data into the standard file formats of XLS, PDF, WORD, GPX, KMZ, VIC, FILE, EXTENDED XML, HTML, OpenDocument Text, OpenDocument SpreadSheet	
	The mobile forensic solution must be able to import Python Script to assists on the decoding and analysis. It should use python v3.4.3 or above.	
	The mobile forensic solution must be able to bookmark Hex data.	
	The mobile forensic solution must have App database mapper tool for unsupported apps to manually map data in SQLite database tables to artifacts. Once mapped it should have option to save the template for future use.	
	The mobile forensic solution must be able to manually reconstruct of Hex data.	
	The mobile forensic solution should generate hex-dumps from the phone memory, typically by bypassing the device operating system.	
	The mobile forensic solution must be able to provide Project VIC functionality.	
	The mobile forensic solution must be able to provide PLIST, XML & SQL Database Viewers.	
	The mobile forensic solution must be able to group duplicate artifacts.	
	The mobile forensic solution must be able to provide Known Data Filtering.	
	The solution must be able to provide file anomalies filter.	
	If Drone data and information is available, The mobile forensic solution must be able to display the data and information on a Drone Tab.	
	The mobile forensic solution must be able to allow Column export in WYSIWYG format from column view.	
	The mobile forensic solution should be a software based solution, complete with all necessary hardware for recovering data from device in a secured manner.	
	The mobile forensic solution should be able to extract device data logically and physically. Both the methods should be available in The mobile forensic solution along with photon method of screen capturing.	
	The mobile forensic solution should be able to extract SIM Card data.	
	The mobile forensic solution should support bypass and recovery of lock codes for mobile devices.	
	The mobile forensic solution must have option to bruteforce encrypted iTunes backup.	
	The mobile forensic solution should have selective app extraction option for targeting extraction to only recover data from selected apps.	

	The mobile forensic solution should support Bluetooth and Hosted Wifi Extraction for mobile devices.	
	The mobile forensic solution should utilize the latest 64Bit software technology to ensure future capability and support of large multi-gigabyte mobile devices.	
	The mobile forensic solution should be able to extract vital application data on device running but not limited to below OS:	
	a) iOS	
	b) Android	
	c) Blackberry OS	
	d) Windows Phone/Mobile/CE/RT	
	e) Asha Platform	
	f) KaiOS	
	g) Tizen OS	
	The mobile forensic solution shall provide options for support of mobile devices via Generic Profiles to allow for support of new and untested devices.	
	The mobile forensic solution should be regularly updated with new releases containing updates to device and app support as part of the license.	
	The mobile forensic solution should perform extraction, decoding and indexing on a single operation.	
	The mobile forensic solution must use Windows Certified and signed USB drivers to avoid interference with any other software running on the computer and for IT Security reasons: https://docs.microsoft.com/en-gb/windows-hardware/drivers/develop/signing-a-driver to ensure the foolproof security in terms of IT equipments.	
	The mobile forensic solution should normalize timestamps from all mobile devices extracted to ensure that exported data formats are all consistently reported to 3rd party tools.	
	The mobile forensic solution support extraction and decoding of data from applications, minimally including WhatsApp, Skype, Telegram, WeChat, Snapchat, Line, Facebook Messenger, Facebook, Twitter, Instagram, Tinder, Skout, Gmail, Yahoo Mail, Outlook, SMS, etc.	
	The mobile forensic solution should be able to extract the internet and download history from common web browsers.	
	The mobile forensic solution should support Rapid hash match functionality that enables you to acquire information about the device data before the extraction has even finished. Hash matching functionality should support MD5, SHA1 and SHA 256 hash algorithms.	
	The mobile forensic solution should adhere to the fundamentals of digital forensic principles:	
	a) A secured data file container to avoid allegations of interference with electronic evidence after extraction;	
	b) An audit log to show exactly what functions the forensic tool performed on the digital device;	
	c) Hash Algorithm options for enhanced file security and cross referencing;	
	d) To provide password protection on extraction data;	
	e) Examinations should not assume file extensions can be relied upon and instead it should only read the raw digital data.	
	The mobile forensic solution should have a fully documented manual that:	

	a) Manually lists all devices and apps supported via the extraction software to aid investigators;	
	b) List what data types can be extracted on specific device profile;	
	c) List what data types cannot be extracted on specific device profile;	
	d) Available via mobile phone app to manually lists all devices and apps supported to aid investigators.	
	The mobile forensic solution should have a fully documented manual that lists out the device or application based on:	
	a) Device Type;	
	b) Manufacturer;	
	c) Form Factor;	
	d) Device Operating System;	
	e) Application Category;	
	f) Application Operating System.	
	The mobile forensic solution should have built in decoders for the recovery of the following artifacts:	
	a) Deleted Video and Image Carving	
	b) Audio Files	
	c) Picture Files	
	d) Document Files	
	e) Smartphone App data	
	The mobile forensic solution should natively enable connection to a mobile device via any USB port on the installed PC. No hardware converter devices should be required to be installed.	
	The mobile forensic solution should be able to perform device cleanup by specifying individually or the whole list.	
	The mobile forensic solution must support physical extraction using Raspberry Pi Zero.	
	The mobile forensic solution should support Application Downgrade Method on at least 55+ latest Android OS non-system applications. For example (Whatsapp, Skype, WeChat, Instagram, KakaoTalk, Line, Facebook Messenger, Facebook, QQ and etc).	
	The mobile forensic solution should be able to extract kaios operating system based devices from various vendors like Nokia, JioPhone, LYF, Energizer, Alcatel, Caterpillar etc.	
	The mobile forensic solution should perform various logical extraction methods like Agent, Backup, Filesystem and app downgrade all in one go and user need not to perform each method i.e. Agent, Backup, Filesystem and app downgrade Seprately.	
	The mobile forensic solution should have capability to modify existing extraction profile's or create a new profile and configure extraction and decoding option based on user requirements.	
	The mobile forensic solution should have feature to specify the time span allowing to limit all the artifacts in extraction to a certain time span.	
	The mobile forensic solution should have feature to select all apps or a limited set of apps to include in the extraction.	
	The mobile forensic solution should have a feature to specify categories to reduce the extraction time and size by excluding non-important artifacts categories.	
	The mobile forensic solution should have Triage mode with android extraction option of rooted and non rooted device.	
	The mobile forensic solution should be able to extract evidence from mobile device where a screenshot is the only way to capture relevant evidence and help validate device extraction results. Capturing	

	screenshot should be available for both Android as well as iOS devices.	
	The mobile forensic solution should automatically generate a detailed audit log file of the forensic process for each extraction for peer review.	
	The mobile forensic solution should have support for Telegram Android clones like Graph Messenger, Plus Messenger and Mobogram.	
	The mobile forensic solution should support decoding of geolocation information from KMZ files.	
	The mobile forensic solution should have an automated version of manual app examination on Whatsapp, signal, Telegram, Whatsapp for Business and dual instances of these apps with the benefit of storing image, text data and Emoji in a searchable way. Stored text data and Emoji must be presented with 100% accuracy. Method should also support of Manual app examination to capture app data from any application by manually opening app from which user wants to capture data.	
	The mobile forensic solution should have offline maps integrated.	
	The mobile forensic solution should have AI person's capability.	

[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. <u>Installation/Inspection:</u> Uttar Pradesh State Institute of Forensic Science, Lucknow
	3. <u>Payment</u>: By NFSU Gandhinagar Campus