TECHNICAL SPECIFICATIONS OF FORENSIC TOOL KIT (SOFTWARE & HARDWARE ITEMS) FOR DISTRICT CYBER POLICE STATIONS, DELHI.

S. No	Component	Detail Specifications
1.	Software to extract data from Mobile Devices-Universal Forensic Extraction Kit	Annexure A
2.	Mobile Phone, IoT, Wearables, Cloud, Link Anaytics and CDR Software	Annexure B
3.	Imaging Device	Annexure C
4.	Comprehensive Digital Investigation platform for forensic data extraction and analysis of live system, hard drives, mobile phones and cloud services	Annexure D
5.	Image & Video Analysis Software	Annexure E
6.	Forensic Workstation	Annexure F

ANNEXURE –"A"

SOFTWARE TO EXTRACT DATA FROM MOBILE DEVICES-UNIVERSAL FORENSIC EXTRACTION KIT

Sl. No.	Parameters	Specifications
1.	Data Extraction from phones	Should be able to take logical & Physical dump of all type of mobile devices from all type of manufactures of different OS based phones: i. Generic phones ii. Smart phones (Windows, iOS, Android, Palm, Blackberry etc) iii. data extraction portable GPS devices iv. Data extraction from Satellite Phones & Analysis v. SIM Cards (with cloning Facility) vi. Chinese Handset
		It should support data carving from unallocated space which enables to recover a greater amount of deleted data from unallocated space in the device's flash memory.
		It should be able to take dump by bypassing pin locked and pattern locked smart phones (Android based, iOS, Windows OS based etc. of different manufacturers)
		It should enable physical, file system and logical extraction, and decoding from selected devices. Decoding of intact and deleted data: Phonebook, SMS, and MMS, calendar entries, SIM ID and more.
2.	Analysis & Viewing	Should be able to recover the basic communication details like Logical extraction of data: Apps data, passwords, IM (instant messaging), contacts, SMS & MMS, emails, calendar, multimedia, call logs, phone details (IMEI/ESN),ICCID and IMSI, SIM location information (TMIS, MCC, MNC, LAC).
		It should be able to run Python scripts via plugins, and edit and create new decoding chains.
		It should support image carving, a powerful feature used to recover deleted image file and fragments when only remnants are available.
		It should perform on-demand searches for viruses,spyware, trojans and other malicious payloads in files
		It should enable visualizing of events over time, view distances between events and see the number of events within a defined timespan in a table/ graph view
		It should enable conversion of single or multiple locations to their corresponding address.
		It should support Viewing of all locations on a single map.
		It should enable viewing of extracted locations using offline maps even without an Internet connection. The offline maps should have an India version.
		It should support advanced search Based either on open text or specific parameters. It should support Quick search within decoded data.
		It should enable viewing of communications between sources in date and time order
		It should support Hexadecimal view of the extracted data enabling

		advanced search based on multiple parameters, regular expressions and more.
		It should be able to Generate and customize reports in different formats e. g. PDF, HTML, XML, Excel and Word.
		It should enable Chat messages to be exported in conversation format, in PDF reports.
		It should support Exporting selected emails to EML format.
		It should support hash verification to ensure the extraction decoded is the same extraction received from the device.
		Decryption of WhatsApp encrypted history database.
		Decoding of Apps data, passwords,
		emails, call history, SMS, contacts, calendar,
		Media files, location information etc.
		1 Android Phones : It should physical extraction method from locked Android based devices bypassing any type of lock (Pattern/PIN/Password) using proprietary boot loaders,enabling a forensically sound extraction process.
		Physical extraction from these devices should be done,regardless of their OS version, and should not require any permanent rooting
		It should also disable pattern/PIN/password locks on selected Samsung Android devices
		It should also support Physical extraction and advanced decoding, via USB debugging, for ALL Android OS versions preferably upto latest versions of Android. Physical extraction for any locked device should be available if the USB debugging has been switched on.
		It should support Decryption of encrypted Android physical extractions: Decrypt encrypted physical extractions from Android devices preferably latest version and below, with a known password. This includes generic Android and Samsung devices.
		It should acquire apps data from Android devices via all extraction types including but not limited to: Facebook, Facebook Messenger, Google+, PingChat! (akaTouch), Skype, Twitter, Viber, Yahoo Messenger, Whatsapp, TigerText, Dropbox, QIP, Kik Messenger, Evernote, Kakao Talk, ICQ, Vkontakte .
3.	Supported devices for Physical/Logical extraction	Physical Extraction of Major Device Support should at least including but not limited to the following phones: • HTC – HTC Evo, HTC One M8, Incredible, Desire 310, Desire C • Huawei – Ascend, Honor 3x, 5 vision • Motorola – Milestone, Milestone 2, Droid, Droid 2, Droid X, Droid Razr, Razr Maxx, Defy and more • Samsung – Galaxy S6, Galaxy 5S, Galaxy S4, Galaxy SIII Family, Galaxy SII, Galaxy Note 4, Galaxy Note II, Galaxy Mega , Galaxy s5 duos, Galaxy alpha • LG – G4, G3, Optimus, Optimus one, Optimus 3D, Optimus black. • Miscellaneous Phones - Intex Aqua Core; Intex Cloud Y5;Intex Aqua i7; Karbonn A12+; Karbonn A25; Xolo A500S ; A114R Canvas Beat • Sony - Experia edual, E1 Micromax
4.		**Blackberry Phones** It should enable physical extraction and decoding from BlackBerry

		devices running OS 4-7. Physical extraction should be performed using proprietary boot loaders, enabling a forensically sound process. Real-time decryption should be enabled for selected devices.
		It should support advanced decoding of existing and deleted data for Blackberry running OS 4-7 :
		BBM history (if enabled by the buyer)
		BlackBerry Messenger (BBM) messages including Deleted messages and chats, message attachments, contact photos,BBM from groups: Chats, contacts and shared photos.
		Recent email contacts (BB OS 6 and above, where available)
		Device Info (Model, IMEI\MEID, ICCID, PIN, OS version, Platform, Supported Networks)
		REM files – decryption of encrypted files on external memory
		Windows Phone It should support physical extraction and decoding of devices running Windows Phone devices running OS versions 8.0 and 8.1(Preferably latest) and below including 6.0 and 6.5.
		JTAG decoding of contacts, call logs and SMS from Windows Phone 8.x devices is enabled via physical extraction
		The Devices supporting Physical Extraction should at least include HTC Pro, HTC HD2 T9193, Xperia X1, Nokia Lumia 520 & Preferably latest versions like Lumina 535 etc., LG GM750.
		It should support applications for Windows Phone devices running latest version of OS, including Facebook, Facebook Messenger, Waze, WhatsApp, ooVoo, Skype, Voxer, Kik and Odnoklassniki etc.
		It should support bit-for-bit physical extraction from locked and unlocked Nokia BB5 devices using proprietary boot loaders.
		Portable GPS Device : It should enable physical extraction and decoding of data from a range of portable GPS devices (Garmin,Tom-Tom, Magellan etc). The Decoded data should include: Entered locations, GPS fixes, Favorite locations,GPS info.
		It should provide a solution to the encrypted including but not limited toTomTom triplog files that reside in the TomTom device STATDATA folder.
		It should support Extraction and decoding of existing and deleted data from GPS devices. GPS extraction and decoding of information Should include at least: 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, and MMS, calendar entries,SIM ID and more.
		The Supported Phones (for either Physical/ File System/Logical) should at least include:

		Nokia: 1280, 1616, 1650, 1661, 1661-2b, 1680 Classic, 1800, 2720 fold, 2720a-2b,
		2730 Classic, 2760, 3109 Classic, 3110 Classic.
		Samsung: SGH-C120, SGH-A127, SGH-M130L, SGH-A137, SGH-T139, SGH-J150, SGH-X150, SGH-X160, SGH-X166, SGH-X168, SGH-C170, GT-E1195, GT-E1230, SGH-E1310B, SGH-B2100.
		LG: KP175, KP202 i-mode, GB220, KG220, CG225, KG225, GB230 Julia, KG290, NTLG300GB, KG320, KG320S, KG328, L343i, KF350, KF600, KE800, KG800, KE850 Prada, KE970, Shine, C1100, L1100.
		Motorola: E1 ROKR, C113, C117, C118, C119, C115, C139,C140, V300, V303, V330, W375, E398, V400, V500, V505, V525, V551, V620, V635L, C975, E1000, V1050
		IOS Phones : It should enables forensically sound data extraction,decoding and analysis techniques to obtain existing and deleted data from these iOS Devices: up to iPhone 6Plus, and , iPad 4.
5.	Warranty Support	Three year from the date of Supply
6.	Licensing Details	1. It should be operated with a USB software license dongle. 2. The License should exclusively in the name of the buyer and the Certificate from OEM should be provided at the time supply mentioning their validity dates.
7.	Regular Updates/Patch management	1. The product should be supported at least three years. The OEM should provide support for new handsets released by different manufactures (With latest version of OS) that may come during the warranty period and accordingly upgrade the tool for data recovery for these devices. 2. The periodicity of such updates should be mentioned in quotation
8.	Training	Training for 03 Person

ANNEXURE-"B"

MOBILE PHONE, IOT, WEARABLES, CLOUD, LINK ANAYTICS AND CDR SOFTWARE

Sl. No.	Parameters	Features
1.	**Extraction and Feature Support**	• The solution must support most at least 39000+ unique device models of different companies and 20,000+ unique applications and 80+ cloud services. • The software must have capability to extract data from Mobile Devices operating on at least but not limited to following Operating Systems ➢ iOS ➢ Android ➢ Windows ➢ BlackBerry • The software must have capability to extract data from o Featured phones o Drones, o Cloud Extraction o IoT devices o Smart Watches. o Physical Support for Jio Phones. o MTK based Feature phones • The software must be able to extract any number of supported devices concurrently using all available USB ports present on the workstation/laptop using multiple instances.
2.	**License**	The software should be regularly updated to support additional versions and devices during the license and support period i.e. for 3 years. Should have a capability to use regular open market or Cell phone/Device manufacturer supplied data cables (and avoid restriction of special proprietary cable sets) as it is to be used across organisation at multiple locations (all locations may not have proprietary cable sets available during the hour of urgency).
3.	**Extraction Capability**	• The solution must have capability to automatically extract data from pre-configured handsets profiles supplied with the software handset profiles. • The solution should have capability to manually extract data using separate methods i.e. o Physical o File system o Logical method. • The solution should have a module in which if by any reason if the mobile device is not accessible then data should be

		extracted from its sync devices like laptop, computers running on several operating systems like Windows, MacOS& GNU/Linux. Atleast but not limited to following data should be extracted from the device : o Should able to extract tokens in Web browsers for interaction applications like Alexa. o Enable investigators to collect a host of new artifacts on macOS, including Apple Messages (comprising contacts, Apple Photos, SMS/MMS, iMessages, and their attachments), Apple Notes, and Apple Reminders. o Should be able to extract the WhatsApp QR token in WhatsApp desktop app and in Web browsers. o Extract the Google Refresh token in Google Chrome browser, Safari, Mozilla Firefox, Mozilla Thunderbird, Opera, WhatsApp Desktop and WhatsApp Web, Telegram Desktop and TamTam. o All tokens extracted from any app or service further should be imported to the tool to gain access to respective cloud services. o The solution should have capability to extract Jump Lists to track files and folders accessed by the user, even if related files are deleted. o Shell bags to allow the investigator to track the folder browsing history of the user and get the details of a folder that might no longer exist. o Should be able to extract USBSTOR registry for history of all USB connected devices to help finding the origin of malware infection, establishing data leaks, and proving USB device ownership. o Device backups and images can be decoded: iTunes, Android and BlackBerry backups, Android and Windows Phone JTAG images, Blackberry 10 Chip-off image etc. It be able to extract data from Data Hiding applications which can send private text messaging and can make secure calling. • The solution must have capability to do extraction based on Chipset Profiles of MTK & Spreadtrum chipsets. • The solution must have capability for Physical Extraction of locked handsets based on Qualcomm Chipset with methods like EDL extraction. • The solution should also be able to extract handsets based on Kirin Chipsets (for Huawei and other Chinese Phones). • The solution must have capability for Physical Extraction of Locked phones of several popular make like Samsung handsets, LG, Moto X Pure, Moto G 3rd gen and Moto G 5th

		gen. • Physical acquisition, and decrypt data from Huawei devices based on Kirin 980, 970, 710 and 710F chipsets and running Android OS 9 and 10, including the Huawei Honor 20, the Huawei Honor Magic 2 3D, the Huawei Honor 10 Premium (GT), and the Huawei Honor Note 10 • For fast extraction should support using Jet Imager technique for large capacity phones.
4.	**Analytics Features**	• The solution must have feature which can display the usage data of the device spread across Years, Month, Weeks, Days, Hours. And can show the matrix layout of the activities which can clearly segregate the high usage time of the device • The solution must have a feature in which when multiple devices are being analyzed then it can show common locations and contacts for several devices, events in a chronological order. • The solution must have a Dashboard to summarize and provide a quick review of the data acquired on a case as well as device level including the technical device details like, Make, Model, IMEI, Serial Number, Accounts present on devices, Graphical representation of types of data and applications etc. • The solution should have a capability to merge cloud data extracted using tokens or from any other device with a related case for combined analysis. • It must also perform the Call Data Record Analysis using the data provided by Service Provider. • A Call Data Records Analysis including the Data Visualization must be provided once a formatted normalized CDR file is imported in the solution. • A module must be in-built to provide a Social Graph visualizing the common connection points between suspects's using the extracted data like, Google Services, Contacts, Call Logs, Emails, Social Media Messages, Chat Applications, and Text Messages etc. • Should have an ability to search for and find similar images throughout the selected device or case using PhotoDNA • Hash calculation for physical dumps from several preferred hash sets: SHA1, SHA256, SHA3-256 or MD5.

		• The tool should also be able to perform below analytics. should create a unique set of reference images to identify in the extraction should conduct searches for specific faces in one or more extractions and can adjust the percentage of resemblance
5.	**Features related to Apple Devices:**	• Solution must be able to extract Apple Health data from the cloud account using either user credentials or token. • IT must have an ability to import and parse all available data from GrayKey images made from Apple iOS devices like contacts, calls, messages, applications, passwords, deleted information etc.
6.	**Extractions based on Chipsets:**	• It must decrypt Android physical dumps with a known password for Qualcomm devices using popular chipsets, at least but not limited to: MSM8917, MSM8937, MSM8940, MSM8953, including the devices with secure startup enabled. • Must decrypt Android physical images using hardware-backed keys and user passwords for chipsets, at least but not limited to, MTK 6737 and Qualcomm MSM8916, MSM8939, MSM8909, MSM8952, MSM8917, MSM8937, MSM8940, MSM8953. • Extract data from Android devices based on the following Spreadtrum chipsets: SC9850, SC9863, SC7731E, SC9832E. The supported devices must include teXet TM-5073, Fly Life Ace, Doogee N10, Alcatel 1C 2019 (5003D), DEXP BS650, Digma LINX Atom 3G, Meizu C9, Micromax Spark Go, and other popular models
7.	**Screen Lock disabling**	Methods to bypass or disable screen locks on the most popular mobile devices.
8.	**Features related to Graphics/Images:**	• A support for PhotoDNA algorithm must be present to search and cluster identical images in a case or device. • It must be able to categorize human faces with built-in facial recognition technology. • A further ability must be present to categorize the Photographs based on Age, gender, race, skin tone, emotions etc. • The ability to categorize/filter the images/photographs based on the Object Identification technique must be present in the solution.
9.	**Anti-Spyware**	Should have an in-built Spyware Detection on Android and Apple devices using known hash sets provided by user.
10.	**Drone Data**	• The solution must have capability to parse, extract and

		analyse data from physical dumps, drone logs and drone mobile applications. • It must be able to analyze the data like Flight Path with all attributes, Photos and videos etc. • The solution must be able to extract the data from widely used DJI Drones like: o Flight logs and technical data. o It must gain access to Skypixel cloud service data by rooting the DJI Drones or using login credentials for Skypixel. o It must extract account information, messages, notifications, media files, comments, Aerial Photographs and videos along with respective time stamps. • The solution must be able to extract and analyze the data from widely used Parrot drones flight logs and Parrot physical dumps like: o Geo coordinates with timestamps along with metadata that includes: altitude, velocity, ground speed, Wi-Fi signal, battery level, current satellite numbers etc. o Capability to extract Myparrot Cloud login credentials from web browser or connected device like laptop or computer to extract MyParrot cloud data to extract Flight history from cloud. o It must automatically find a token to MyParrot cloud in the installed FreeFlight Pro app in Apple iOS and Android devices.
11.	**Cloud Data extraction and Analysis (using tokens or user credentials):**	• iCloud Data - all associated devices with unique Apple ID, iCloud contacts and calendar (it must support the Latest Apple Cloud SMS Authentication method to extract data from iCloud.) • Google Cloud Services - Geo locations visited, Google Drive, browsing history etc. and visualize locations on online and offline maps. • Others cloud services like: Microsoft Live contacts and calendar, OneDrive, Dropbox and Box as well as from a wide range of social media including Twitter and Instagram. • It must import WhatsApp backups made in Android devices and decrypt them via phone number or WhatsApp Cloud token. • This solution must provide WhatsApp data by scanning a QR

		code from a mobile app or using the WhatsApp token from a PC (on WhatsApp Desktop App or Web Browser) extracted using special in-built module. • It must extract and analyze highly common cloud services for extraction with user credentials and Tokens found in user handsets from at least services mentioned herein: o Google - : Google Android Cloud Data, Google Bookmark, Google Calendar, Google Chrome, Google Contact, Google Drive, Google Keep, Google Location History, Google Mail, Google my activity, Google Photos, Google Task o Facebook :Facebook, Whatsappgoogle backup, Whatsappicloud backup, Instagram, Whatspp cloud, Workplace by Facebook. o Samsung : Samsung Cloud backup, Samsung Cloud data, Samsung secure filder backup o Apple : i-cloud calendar, i-cloud call history, i-cloudcontacts, i-cloud drive, i-tunes store, i-cloud notes, i-cloud photo stream, i-cloud photos, i cloud safari bookmarks, i-cloud safari history,i-cloud backup, i-cloud applications, Airbnb, o Microsoft : Microsoft Outlook, Outlook People, Outlook Calendars, One Drive, Windows Phone Cloud Data, live calendar, live contacts, IMAP o Twitter o Viber o IMO o Telegram o TamTam cloud o QQ Mail, o DJI Cloud o Dropbox, o Huawei Cloud Data, o JioChat o MI Cloud data, o Slack
12.	**Password & Encryption handling**	Should have In-built Passware module for automatically finding the encrypted device backups and images to unlock device data. - Should be able to take an advantage of Distributed processing, GPU Acceleration using ATI and NVIDIA cards -- Should at least be able to perform brute-force, dictionary, Xieve, etc
		Should allow to bypass screen lock passwords and create full physical dumps from Chinese chipset device.
		Allow the bypass of screen lock passcodes, locate passwords to encrypted backups, extract data from secure applications as well as recover deleted information.

		The Device should support the BruteForce using in-built password recovery module for at-least below handset models (and should have a scope of adding future capability for more handsets): -- brute force and decrypt encrypted user partitions using special exploit extracted out of LG devices in DFU Mode. -- Should at least support LG G5 and V10 devices
13.	**Application Data Parsing**	Should be able to extract data from Data Hiding applications like CoverMe.
		Should have an ability to extract and parse data from India Specific Applications like Elements, JioBrowser etc.
		Should acquires the complete evidence set from devices and backups: contacts, messages, calls, calendar, file system, data from applications (at least 400+ applications) and recovers deleted data.
14.	**IoT Device support**	• The device must support extraction of data from Amazon Alexa, Google Home using a user credentials or tokens. • The solution must have capability to extract data from Alexa which atleast includes but not limited to: account and device details, contacts, messages, calendars, notifications, lists, activities, skills, etc. • The least data required in Google Home includes: account and device details, voice commands, and information about users. • The tool should also extract Google Home data from Apple iOS and Android devices.
15.	**Free World Maps Support**	Should have Offline and Online maps so that if Internet connectivity is not available or not preferred, the offline maps engine should be able to plot the data on map. --The base map data should be available/included without any additional charge for the entire world.
16.	**CDR Analysis**	Should perform CDR Analysis using the data received from the Mobile Service Providers
		Call Data Records import Allows the import of call data records of any format received from wireless providers and conveniently guides the expert through the process of CDR importing and field mapping, easily converting the data to unified format.
		Once converted, it should allow forensic experts to analyze the processed CDR files and easily determine direct and indirect links between selected callers in a visual graph. The processed results can be saved as evidence for further analysis.

ANNEXURE-"C"

HARD DISK/ MEMORY FORENSICS/ANALYSIS TOOLS

Sl.No.	**HDD Imager with Network Tapping Module (**Imaging Devices)
1.	Should be portable kit for performing forensic acquisition from various storage media
2.	Should allow investigators to preview following suspected storage media in read only mode (Write Protected) using Laptop/Desktop web browser a. IDE/PATA 2.5" & 3.5" b. SATA 2.5" & 3.5" c. SAS 2.5" & 3.5" d. Fire wire Devices e. External USB 3.0/2.0/1.0 devices f. Multimedia cards g. Devices which can be accessed via PCIe interface like M.2 SATA/NVMe SSDs h. Network (iSCSI)
3.	Should allow investigators to create forensic images (Physical) of following types of storage media a. IDE/PATA 2.5" & 3.5" b. SATA 2.5" & 3.5" c. SAS 2.5" & 3.5" d. Fire wire Devices e. USB 3.0/2.0/1.0 devices f. Multimedia cards g. Devices which can be accessed via PCIe interface like M.2 SATA/NVMe SSDs h. Network (iSCSI)
4.	Should support following types of hash value to be calculated while performing forensic imaging or Hash Verification of Images. a. MD5 b. SHA1 c. SHA256 d. MD5 + SHA-1 e. MD5 + SHA-256
5.	Should support following modes of forensic duplication a. Disk to Disk (Clone) b. Disk to File (Image) c. Files and Folders (Logical)
6.	Should support following types of forensic image formats. a. For Physical Imaging i. E01 ii. DD(RAW) b. Logical i. L01
7.	Should support Temporarily or permanently removal of HPA/DCO
8.	Should Supports S.M.A.R.T. disk info
9.	Should support Various wiping standards like Clear Partition Table, Quick Erase, Custom Erase, Secure Erase Normal, Secure Erase Enhanced, DoD Clear, DoD Sanitize, NIST800-88 Clear, NIST800-88 Purge

10.	Should support imaging to a remote network location or share.
11.	Should have adapters and Cables for various types of Storage media like a. IDE 1.8", 2.5" & 3.5" b. SATA c. SAS d. FireWire e. Micro SATA & mSATA f. ZIF g. PCIe M2 SSD Adapter
12.	Should allow creation of multiple images from single source to multiple destination in USB 3.0 or SATA or Network simultaneously
13.	Should have a Network Tapping Module to capture the PCap Files when connected to the live network.
14.	Kit Should be portable enough to be carried by a single person inside a Ruggedized dustproof, waterproof case.
15.	Three years warranty support from the date of commissioning

ANNEXURE-"D"

COMPREHENSIVE DIGITAL INVESTIGATION PLATFORM FOR FORENSIC DATA EXTRACTION AND ANALYSIS OF LIVE SYSTEM, HARD DRIVES, MOBILE PHONES AND CLOUD SERVICES

Memory & Process Acquisitions Capabilities	• Should Support acquisition and analysis for computer, mobile, Cloud evidence sources. • Should have support for operating systems Windows, Mac OS and Linux platform. • Should support data acquisition at least from Android devices, IOS Devices, windows phone, Kindle Fire, MTP devices and SIM Card acquisition. • Support for popular distributions in Linux including Ubuntu, Red Hat, Debian, Kali, and more. • Should Support different file systems including NTFS, HFS+, HFSX, EXT2, EXT3, EXT4, FAT32, EXFAT, YAFFS2 • Should have capability to create image for Windows includes Page file, Hibernation File, Master File Table, USN Journal, Event Logs, Setup API Logs, Windows Registry Hives, LNK Files, User Profiles, Pre fetch Files. • Should Support capture of Physical Memory (RAM Dump) to analyse valuable artifacts that are often only found in memory. • Should also capture memory from individual running processes or a specific processes. • Should have option to acquire memory and individual process both using the GUI as well as Command Line to reduce the footprint on the suspect system. • Multiple Device Queuing – Automatically process multiple devices in a row without the need for examiner-run separate process.
Mobile devices acquisition capabilities	• Support data acquisition from supported Android devices using ADB and more advanced methods. • Ability to acquire the full image from Supported LG devices using Download mode • Ability to acquire the full image from supported Motorola devices using Boot loader Bypass methods • Ability to acquire the full image from supported Samsung devices using Recovery images • Support full image acquisition and password bypass from devices with supported MTK chipsets, Qualcomm Chipset using EDL mode • Support data logical acquisition from Kindle devices • Support data acquisition from SIM card. • Support data acquisition from iOS devices and save the image as .zip
Image types support Capabilities	• Ability to analyze data from forensic image file formats i.e. E01, Ex01, L01, Lx01, .AFF .AD1, .DD, .RAW, .BIN, .IMG, .DMG, .FLP, .VFD, .BIF, .VMDK, .VHD, .VDI, .XVA, .ZIP, .TAR. • Ability to analyze memory dumps in the format of .RAW,

	.CRASH, .VMSS, .HPAK, .ELF, .MEM, .DMP, .DD, .IMG, .IMA, .VFD, .FLP etc.
Decryption Capabilities	• Command-line utility that can quickly and non-intrusively check for encrypted volumes on a suspect computer system during incident response. • Support Full Drive Decryption, with the integrated capability, can detect and decrypt True Crypt, Bit Locker, McAfee, Vera Crypt and FileValut2 with known password or using brutal force attack.
Recovery/Extraction Capabilities	• Recover a wide range of system artifacts, such as user accounts, SSH keys, scheduled tasks, log files, Bash history, and recent files from Linux based images. • Targeted acquisition for Linux includes System logs, home, sleep images, tmp, etc, and usr and should also have Added support for recovering Bash information, including session ID, user, start date/time, end date/time, and session command history. • Should have support for recovering information about scheduled tasks, such as frequency, command, and paths of the directories, network interfaces information and their DHCP leases assigned by the local DHCP server. • Should have support for recovering Linux operation system installation information, SSH Keys information including file name/ key type/ encryption type/ MAC times, and file content, information about configured auto-run scripts that open when a Linux device starts. • Should have support for recovering items that a user has sent to the trash, including both deleted files and deleted directories and user account information such as the username, password hash, last password change date/time, user ID, account description, and more. • Quickly get photo, video, and chat evidence with an external or internal camera or by connecting to the victim or witness's mobile phone, or memory card. • Should have ability to recover PowerShell history, including the user that executed the command and the command text on windows. • Should have a utility for determining and retrieving user passwords based on keywords from a case file significantly reducing the time involved in trying to brute-force this password manually • Recovers more artefacts from both allocated and unallocated space by extracting data from full files or carving for deleted data and traces of data elements/fragments left behind by apps and websites, presenting it in an organized and easy to read format.
Search/filter capabilities	• Should support OCR support for extraction of text from PDF documents (including text in scanned documents and text from pictures in PDF documents) and from picture artefacts for

	Keyword Searching. • Should support search for keywords on both recovered artefact and sector level content both prior to processing the case as well as after processing the complete case with an option to select all added evidence sources or any particular evidence source. • Should have advance option to analyse media file using dedicated Media explorer to view, sort, and filter media evidence using criteria that are specific to pictures and videos. The Media explorer should stacks copies of the same picture or video that were found in different source locations. • Should allow investigator to filter media files by Investigation leads, including attributes such as camera serial numbers, Exif created dates, camera make & model, Items with Geolocation data, Deleted source, items matching social media platforms, Lens model & Serial Number, file extension, VICS attributes, media attributes, video attributes, and file attributes. The date / time filter is also available in the Filters bar. • Should allow investigator to Sort by option to organize the evidence in ascending or descending order based on attributes such as skin tone, media size. • Should allow investigator to filter video files with attributes such as video files within carving limit, media duration etc. • Inbuilt feature to Find similar Pictures and Build Picture comparison. • Ability to identify luring and sexual conversations. 15+ AI Categories to automatically identify and bifurcate images related to drugs, weapons, nudity, weapons, militants, vehicles, screen captures, documents, ID Cards, Human Faces, License Plates, Building, Child Abuse, etc • Filter stacking allows you to layer on several dimensions of filter criteria to pinpoint specific items in a large dataset. • Add hash sets to either filter out non-relevant files to enhance search performance and reduce false positives or add hash sets that will specifically call out and identify known bad pictures and videos. • Enhanced searching, sorting and filtering – search, sort and filter artefact data for relevant keywords, time/date stamps, tags or comments, or layer filter criteria to pinpoint items in a powerful and intuitive, but natural interface. Support filter stacking for multiple filters.

Reporting/GUI capabilities	• Ability to view SQLite database files using built-in SQLite viewer • Support case dashboard that displays high level details about the case, evidence sources and summaries of processed results of multiple digital evidence in one screen. • **Visualize connections between files, users, and devices.** Discover the full history of a file or artifact to build case and prove intent. Visualizes evidence from disk and memory to show where files came from, who they are connected to, and where they're stored. • Should have Timeline explorer to consolidate all the timestamps from files and artifacts in a single view, with colors and tags to differentiate timestamp categorizes. • Support multiple data views, including Column/Table view, Summary Row view, World Map view, Timeline view, Chat Threading view and Histogram view. • Support to export & merge portable case and share with other stakeholders without the need for the software license or the need to install the software, the user can select different types of items to be included according to tags, comments and categories. • Should have a feature to reduce overexposure to illicit/ disturbing content extracted to protect improve investigator wellness. This features should be configurable and optional, allowing examiners to work the way that they want. Blur or block media thumbnails, Mute audio on videos, Set timer reminders to take breaks or alerts to stop grading, View grading progress and set goals for amount of media graded • Quick hover over the picture for extend view of image and quick view of videos to reduce the time of exposure for Investigators.
Analysis Capabilities	• Ability to automatically find potential chat databases along with other valuable evidence from non-chat apps that aren't yet supported in an artifact. Users can then easily create an XML or Python artifact to be searched for in future cases. • Capability for parsing unsupported application database using GUI/Wizard-driven utility to make it easy to create custom artifacts for use within the main tool from CSV (and other delimited files) and SQ Lite databases. • Capability for parsing unsupported database using custom artifacts or Python Scripts for popular local applications like Tally, Airbnb, ccleaner, FakeGPS, Linkedin, onion browser bookmarks, Odnoklassniki etc.
Training	• Training for three persons covering topics
Updates	• Software Maintenance Support for 3 Years along with all latest updates for softwares supplied.

ANNEXURE-"E"

Image and Video Analysis and Authentication System		
Description-A software package for forensic image authentication and tamper detection on digital photos. It provides a suite of different tools to determine whether an image is an unaltered original, an original generated by a specific device, or the result of a manipulation with a photo editing software and thus may not be accepted as evidence.		
S.No.	**Parametres**	**Specifications**
1.	Image/ Video Analysis	Load, save, process, and analyze single images, sequences of pictures, or videos from a VMS or external source using the same methodology and software.
2.		Instant results: add, configure, move, and modify an unlimited number of filters, in real time during video playback.
3.		Automatically apply the same filters sequence to different files to avoid resetting all filters for different images from the same source or environment.
4.		Apply the filters only to a region of interest of the image, or select frames of interest in a sequence.
5.		Quickly seek for events in a long duration video with the integrated motion detection filter.
6.		Automatically remove duplicates or mismatched frames.
7.		Automatically de-multiplex multi-camera video feeds.
8.		Precise control over images: operate with pixel level precision on selections and measurements on images. Filters can work on the whole image, on a static selection or can automatically track a moving target.
9.		Crop quad multiplexed videos.
10.		Should automatically generate detailed reports (in .doc, .pdf, or .html formats) so that the investigations process is clearly documented. The report documents scientific methodology and includes all the technical details of the processing and relevant frames and processing steps selected by the user.
11.		View original and processed image or video side by side to easily show the results of your work.
12.		Fast redaction tool to hide sensitive details in the video by blurring, darkening or pixelating select areas – even while moving.
13.		Highlight sensitive details in the video blurring, darkening or pixelating selected areas.
14.		Load image files from the most common formats, such as bitmap, jpeg, tiff, targa, jpeg2000, png.
15.		16. Load video files from almost any digital format, sourced from NTSC, PAL and almost any other system such as mobile phones and internet content; users can decode most video formats by using internal libraries and codecs.
16.		All the video codecs should be preinstalled in the Tool
17.		Visualize the type of encoding of the current frame (I, P, B).
18.		The customizable player allows to define personal frame step for faster seeking or to use the mouse wheel as a jog control.
19.		Convert proprietary video files to a standard, viewable format.

20.		For unsupported proprietary DVR formats, it should allows to capture the screen without any loss of quality.
21.		Convert a sequence of static images to present and control as if it were video. Transcode video to a different format or transform it into a sequence of images or vice versa.
22.		Multiple video frames may be selected in either a consecutive or random sequence.
23.		Should able to check for unauthorized modifications by verifying the file hash-code to maintain strict evidence handling procedures to avoid contamination that could lose a case. You can also verify image EXIF and hash-code data.
24.		2Standard image editing features to instantaneously apply basic editing functions such as crop, flip, color to grayscale conversions, channel extraction, zoom and image rotation.
25.		Correct geometric distortions caused by wide angle lenses. Should allow the user to convert images taken from an omni directional camera to a panoramic format.
26.		Correct the perspective in order to see the picture of the scene from a different angle.
27.		Convert an interlaced video into a progressive one without loss of information.
28.		Shift the fields of an interlaced video to better view moving objects.
29.		Improve contrast and brightness manually, adjusting intensity curves, or speed workflow with automatic enhancement algorithms.
30.		Analyze images with various threshold and edge detection filters.
31.		Measure real world distances, heights, and lengths from images or video frames, Should also determine camera height as a cross-check of measurement accuracy.
32.		Improve image details (unsharp masking, laplacian sharpening).
33.		Reduce noise (averaging, Gaussian, median, bilateral, Wiener smoothing filters).
34.		Apply custom kernel filters.
35.		Reduce compression artifacts with our de-blocking algorithm.
36.		Remove interferences or image background (such as banknote watermark) with Fourier filter.
37.		Correct optical and motion blur resulting from fast movement or out of focus video.
38.		Correct the blur caused by air turbulence on long range surveillance videos.
39.		Remove noise from a video with temporal smoothing and frame integration.
40.		Improve shaking video with local or global image stabilization.
41.		Correct and modify the camera viewpoint in different frames with perspective alignment.
42.		Improve the resolution of the frames with a super resolutionalgorithm.
43.		Improve a video with bad weather conditions (fog, rain, flat light, sandstorm, etc.) and improve backlight images.
44.		View 360° dome camera images as panoramic.

45.		Export all frames as a PDF in one easy step.
46.	Image Authentication	Should be able to forensic image authentication and tamper detection on digital photos.
47.		Should able to determine whether an image is an unaltered original, an original generated by a specific device, or the result of manipulation with a photo editing software and thus may not be accepted as evidence.
48.		Should able to use Image ballistics tools to verify the camera used to shoot the image.
49.		Visual analysis of the image and comparison with a reference image.
50.		Automatic inspection of most common parameters that could indicate non originality of the image.
51.		Analysis and comparison of the histogram of DCT coefficients and its Fourier transform for detecting multiple resaves of the image.
52.		Analysis and comparison of correlation periodicities in the image pixels to analyze the presence and consistency of demosaicing or interpolation effects.
53.		Plot of the image with its recompressed version to identify signs of multiple compressions.
54.		Analysis of the histogram of the image that can help to spot excessive intensity adjustment.
55.		Creation of a PRNU (sensor noise) reference pattern from a user supplied set of pictures and identification of the device that generated the image by comparison with the reference pattern.
56.		Automatic identification of tampered areas of the image by comparison with the PRNU reference pattern of the image.
57.		Identification of similar areas of the image that can be the result of cloning.
58.		Identification of groups of similar points in the image that can be the result of cloning.
59.	Warranty Support	Three years from the date of supply
60.	Licensing Details	1. It should be operated with a USB software license dongle/ License which can be easily transferable to other workstations as per requirement. 2. The License should exclusively in the name of the user and the Certificate from OEM should be provided at the time supply mentioning the their validity dates.
61.	Regular Updates/Patch management	1. The product should be supported at least three years. The OEM should provide features that may come during the warranty period and accordingly upgrade the tool for data recovery and analysis. 2. The periodicity of such updates (If Any) should be mentioned in quotation

ANNEXURE-"F"

Forensic Workstation with Raid		
S.No	**Parameters**	**Specifications**
1.	Monitor	24" LED
2.	Processor	High Speed Dual Ten Core Intel ® Xeon Silver 4114 with clock frequency @ 2.2 Ghz (3.0 Ghz Turbo) or better
3.	Processor Cooling	Premium Grade Quiet Air Cooling Solutions
4.	Ram	128 GB DDR4 2400 Quad Channel Memory-ECC RAM and Expandable up to 1TB
5.	Graphic Card	NVIDIA GeForce RTX 2080Ti, 11GB GDDR6, CUDA Cores 4352, 1545MHz; with HDMI , Display Port x 3 and Dual-link DVI,
6.	Network Adaptor	2 x Gigabit LAN Controller(s)
7.	I/O Ports	Front Ports: 6 x USB (min. 4 x USB 3.0 and higher) 1 x eSATA 6Gb/s; 1 x Microphone; 1 x Headphone Rear Ports: 6 x USB (min.4x USB 3.1); 2 x RJ-45; 1x S/PDIF Out; Audio Ports,
8.	Operating System	Windows10 64 Bit Professional or latest and Linux Ubuntu server & Desktop edition (optional).
9.	Power Supply	1300 Watts or better SMPS
10.	Write Blocker	Integrated write protection for IDE/SATA/SAS/FireWire/USB3.0/PCIe ports.
		All Integrated write blocked ports should be simultaneously available for imaging/analysis. **Should provide Write Blocked access to 3 SATA (Most used) drives simultaneously**
11.	Cable & Adapter Set	Should have Adapters/Cables for write protected ports: 1. 3.5" IDE, 1.8" IDE, 1.8" ZIF, LIF 2. mSATA, microSATA and eSATA 3. M.2 PCIe, PCIe and mini- PCIe Cards
12.	Temp Drive	512GB M.2 32Gb/s SSD Drive
13.	OS Drive	512 GB SATA 6 Gbp/s SSD Drive
14.	Cache Drive	512 GB SATA 6 Gbp/s SSD Drive
15.	Active Evidence Drives	2 x 1 TB SATA 6 Gbp/s SSD Drives with RAID 0 setup giving total of 2TB high speed memory for Analysis Software like FTK & Encase.
16.	Data Drive	1 x 4TB SATA 7200 RPM 6Gb/s Drive
17.	RAID ARRAY	Raid of 5 x 4TB SATA 7200 RPM in RAID 5
18.	Onboard	7 x PCI Express (x16 slots; Version 3.0)
19.	Front Mounted Drive Bays	Optical Disk Drive - 1x 16 x Blu-Ray Burner
		6 x SATA SSD Trayless for OS, Temp, Cache and Active Evidence drives 1 x SATA Trayless for Data Drive;
20.	Cooling Bay	1 x Inserting/Extendable type integrated Drive Cooling Bay with Additional SATA 3.5" / 2.5" Write Blocker.
21.	Forensic Multi Card Reader	Should have Integrated Write Blocked Multi-Card Reader
22.	Key board/mouse	Wireless Keyboard & Mouse
23.	Software	Latest version of MS Office professional, Suitable Antivirus which should be capable of being upgraded offline.
		Any other Essential security related software may also be included.
24.	Warranty Support	Three year from the date of commissioning.