- **Item No. 1**
- **Name of the Item: MAGNET AXIOM COMPLETE PERPETUAL LICENSE WITH ONE YEAR SUPPORT**
- **Quantity: 1 Nos**

Technical Specifications/features:

1. Should Support acquisition and analysis for computer and mobile sources.
2. Should have dedicated workflow for Windows, MacOS and Linux platform.
3. Should support data acquisition from Android devices and Logical acquisition from IOS Devices, windows phone, Kindle Fire, MTP devices and SIM Card acquisition.
4. Support for popular distributions in Linux including Ubuntu, Red Hat, Debian, Kali, and more.
5. Should Support different file systems including NTFS, HFS+, HFSX, EXT2, EXT3, EXT4, FAT32, EXFAT, YAFFS2
6. Targeted image for Windows includes Pagefile, Hibernation File, Master File Table, USN Journal, Event Logs, Setup API Logs, Windows Registry Hives, LNK Files, User Profiles, Prefetch Files.
7. 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.
8. 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.
9. 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.
10. 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.
11. 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.
12. Should have utility to empower frontline officers to collect and report on fleeting digital evidence. The tool should be capable to Maintain privacy and build trust with the public while capturing crucial but fleeting digital evidence from consenting victims and witnesses.
13. 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.
14. Should Support capture of Physical Memory (RAM Dump) to analyse valuable artifacts that are often only found in memory.
15. Should also capture memory from individual running processes. When investigators are short on time or are only interested in specific processes, the

utility can retrieve specific processes and also provide less fragmented data and better recovery of larger data types.

16. 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.
17. Should have ability to recover PowerShell history, including the user that executed the command and the command text on windows.
18. Command-line utility that can quickly and non-intrusively check for encrypted volumes on a suspect computer system during incident response.
19. Support data acquisition from supported Android devices using ADB and more advanced methods.
20. Ability to acquire the full image from Supported LG devices using Download mode.
21. Ability to acquire the full image from supported Motorola devices using Bootloader Bypass methods.
22. Ability to acquire the full image from supported Samsung devices using Recovery images.
23. Support full image acquisition and password bypass from devices with supported MTK chipsets.
24. Support full image acquisition and password bypass from supported devices with Qualcomm Chipset using EDL mode.
25. Support data logical acquisition from Kindle devices.
26. Support data acquisition from SIM card.
27. Support data logical acquisition from iOS devices and save the image as .zip
28. 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.
29. Ability to analyze memory dumps in the format of .RAW, .CRASH, .VMSS, .HPAK, .ELF, .MEM, .DMP, .DD, .IMG, .IMA, .VFD, .FLP etc.
30. Support Full Drive Decryption, with the integrated capability, can detect and decrypt TrueCrypt, BitLocker, McAfee, VeraCrypt and FileValut2 with known password or using brutal force attack.
31. 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.
32. Multiple Device Queueing – Automatically process multiple devices in a row without the need for examiner-run separate process.
33. Filter stacking allows you to layer on several dimensions of filter criteria to pinpoint specific items in a large dataset.
34. Ability to view SQLite database files using built-in SQLite viewer.
35. Should support OCR support for extraction of text from PDF documents (including text in scanned documents and text from pictures in PDF documents) and from picture artifacts for Keyword Searching.
36. Should support search for keywords on both recovered artifact and sector level content both prior to processing the case as well as after processing the complete

case with an option to select all added evidence sources or any particular evidence source.

37. Recovers more artifacts from both allocated and unallocated space by extracting data from full files or carving for deleted data and traces of data elements/fragments left behind by apps and websites, presenting it in an organized and easy to read format.
38. 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.
39. 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.
40. 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.
41. 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.
42. Should allow investigator to filter video files with attributes such as video files within carving limit, media duration etc.
43. Inbuilt feature to Find similar Pictures and Build Picture comparison.
44. 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.
45. **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.
46. 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.
47. 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.
48. 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 SQLite databases.

49. 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.
50. 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.
51. Enhanced searching, sorting and filtering – search, sort and filter artifact data for relevant keywords, time/date stamps, tags or comments, or layer filter criteria to pinpoint items in a powerful and intuitive, but natural interface. Support filter stacking for multiple filters.
52. Should capture web pages as they are at a specific point in time for situations where the web pages need to be displayed in an environment where Internet access is not available (such as a court room).
53. Support multiple data views, including Column/Table view, Summary Row view, World Map view, Timeline view, Chat Threading view and Histogram view.
54. 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.
55. Should have a feature to reduce overexposure to illicit/ disturbing content extracted to protect improve investigator wellness. This f**e**atures 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
56. Quick hover over the picture for extend view of image and quick view of videos to reduce the time of exposure for Investigators.
57. **Tender Specific Authorization Certificate from the OEM is mandatory for participation in the tender in favor of the Indian Distributor/Reseller/Bidder.**
58. **Perpetual License with One Year Support.**
59. **Training - One Day Training to be provided on-site.**

- **Item No. 2**
- **Name of the Item: Cellebrite UFED 4PC with One Year Subscription License**
- **Quantity 1 Nos**

Technical Specifications/features:

1.	**Scope**	Supply of Mobile Phone Forensic Solution
2.	**Specifications**	The Mobile phone forensic solution should provide the below capabilities:
	Extraction Capabilities	• **Generic Features:**

		• The solution should be able to capture critical forensic evidence from mobile devices including mobile phones, handheld tablets, portable GPS devices, drones and devices manufactured with Chinese chipsets. • 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 and 12,400 different mobile application versions. All the supported mobile device models and device profiles must be tested and verified by the OEM's R&D Team. • The solution should be able to integrate with a central management platform that can oversee usage, permissions, SOPs, configurations, licensing, and SW updates. • The extraction software should be touch screen enabled, allowing easy use on tablets. • The solution should have an autodetect function to locate and identify the mobile device. • 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 all necessary cables for the supported phones/OS). • 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 technically capable to clone the SIM ID, which allows to extract phone data while preventing the mobile device from connecting to the network. • The solution should be technically capable to copy a SIM ID from one SIM card to another SIM card or to a vendor's SIM ID access card.

		• The solution should be technically capable to perform SIM data extraction, i.e., the extraction of information from a SIM or USIM card. • It should be able to support file system extraction of blocked application data by downgrading the APK version temporarily for Android devices running on Android 6 and above. • The solution should be technically capable to extract flight data and multimedia files from supported drones, i.e., to perform physical extractions, as well capture images of drones. • The solution must support the use of custom-made proprietary boot loaders instead of the 3rd party bootloaders. • The software should provide lock bypassing physical extraction support for devices with Coolsand based chipsets. • 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 • The software should allow the users to select specific files and folders in the file system for extraction • The software should allow examiners to perform a quick selective extraction of specific applications or files, while doing Full File System extraction for supported Android as well as iOS devices. • The software should also allow selective extraction of only cloud tokens from the phone while doing Full File System extraction. • It should provide a simple extraction flow with generic extraction for unsupported devices. • The software should be supplied with USB 3.0 adapter which connects to PC's USB port for faster extraction. This adapter should also have a RJ45 port for device connectivity.

		• The software should also be supplied with a multi-SIM adapter with support for Micro, Nano and standard SIM cards. • 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. • **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 11. 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. • It should allow full backup of the Signal database from unlocked Android devices. • The software should support Full File System extraction for the latest unlocked Samsung Exynos high-end devices like S20, S21 running on Android 11. S21 should be supported with Android 12 as well. • The software should support extraction of Full File System data from unlocked Qualcomm chipset-based Samsung devices like S9, S10, S20, S21, S21 Ultra 5G, S21 Plus devices running on latest security patch level and up to the most recent Android 11. • 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 Mai 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, 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, mt6797,mt6983, mt8161, mt8163, mt8165,mt8732 and mt8752 • 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 support custom boot loaders to ensure forensically sound bit-by -bit physical extractions, without tampering the data. • It should have support for data extraction, decoding and analysis for unlocked devices running up to iOS 16.0. • 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 depending on the iPhone device supported based on Apple official release

		Additional Points: • Support for different handsets brands like Apple, SANYO, KYOCERA, Motorola, ASUS, Sharp, Lenovo, HUAWEI, CASIO, NOKIA, NEC, Samsung, iPhone, Xiaomi, OPPO, VIVO, OnePlus, HYUNDAI, BlackBerry, ZTE, LG, Acer, Qtek, Vodafone, Telit, Toshiba, Plam, i-mate, Ubiquam, Haier, Zonda, Sony Ericsson, Samsung, HP, Jaga, Sagem, Alcatel, Mediatek, HTC, etc. • It should be able to integrate with Active Directory for user authentication. **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 • The software should be able to support full file system extraction on more than 12 Samsung Exynos devices which includes S10,S10+,S10e and A10-A50 phone model. • The software should able to support Samsung devices with full disk encryption such as Samsung S9 or Samsung Note 9 running on Android 10. • It should support lock bypass using file system extraction for popular Samsung devices like Galaxy J7, Galaxy S8, Galaxy Note8 and Galaxy S8+. • It should have lock bypassing decrypted physical extraction capability for Qualcomm Android devices including LG, ZTE, Xiaomi, Huawei, Alcatel and Motorola • It should be able to perform selective file system extraction on popular Samsung models with the Qualcomm processor (SOC).

		• The software should have a capability to extract Qualcomm chipset phone in a generic option that support popular brand like Samsung and Huawei. . • The software should have a capability to extract MTK chipset phone in a generic option. • It should have decrypting bootloader capability for Huawei devices with HiSilicon Kirin chipsets and Samsung devices with Exynos processor • It should be able to allows users to perform a full file system and selective extraction on smartphones with the Huawei HiSilicon KIRIN 970 processor and other popular devices with the KIRIN 659, 960 and 980 chipsets For Huawei and Huawei Honor must be running android 8 and 9. • 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 support Physical Extraction over ADB for Samsung devices running up to Android OS v8 • It should support bootloader-based physical extraction for zte, alcatel and xiaomi devices running Qualcomm chipset • It should support Partial File System extraction while bypassing User Lock for more than 100 Android devices • 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 support automatic detection of supported devices. It should also support manual search for devices by manufacturer, model and IMEI number. • It should be able to perform physical, full file system and selective file system extraction on Smartphone with Samsung Qualcomm Processor • It should acquire apps data from Android devices via all extraction types including: Facebook, Facebook Messenger, Google+, PingChat! (aka Touch), Skype, Twitter, Viber, Yahoo Messenger, WhatsApp, TigerText, Dropbox, QIP, Kik Messenger, Evernote, Kakao Talk, ICQ, Vkontakte, HideSMS, Kakao Story, MeetMe, Coco, Google Duo, FitBit, Zalo, Yubo, Zello • Physical Extraction of Major Device Support should at least include the following phones: • HTC – HTC Evo, HTC One M8, Incredible, Desire 310, Desire C, 2PS6500 10, U11, U-1w Ultra • Motorola – Milestone, Milestone 2, Droid, Droid 2, Droid 3, Droid X, Droid Razr, Razr Maxx, Defy, Moto X Play, Moto G, XT1710-02 Z2 Play, G4, G5, Nexus 6. • Samsung – Galaxy S7, Galaxy Note 7, Galaxy Note 5, Galaxy Note 8, Galaxy S6, Galaxy S8, Galaxy S8+, Galaxy S6 Edge, Galaxy S5, Galaxy S4, Galaxy SIII Family, Galaxy SII, Galaxy Note 4, Galaxy Note II, Galaxy Mega , Galaxy s5 duos, Galaxy alpha, J3 Neo, J5, J7, A5 and A7 • Indian Phones – Intex Aqua Amoled, Intex Aqua Core; Intex Cloud Y5; Intex Aqua i7; Karbonn A12+; Karbonn A25, Karboon S99 Titanium, Xolo A50zip0S ; A114R Canvas Beat, Micromax A190 Canvas HD Plus, Intex Aqua ring. • **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

		• Installed applications data: WhatsApp, Facebook, Twitter, Google Talk (Gtalk), UberSocial (WhatsApp data retrieval includes decryption of the database and recovery of contacts, chats, chat attachments and user account). • Address book, SMS, MMS, Emails, PIN messages, Calendar entries, Memo pad notes, Web browser history, Web bookmarks, Bluetooth devices and Cookies. • 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, 8.1 and 10. It should also support obsolete OS 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, LG GM750 and other popular models. • It should support applications for Windows Phone devices running OS 8.1 including apps such as Facebook, Facebook Messenger, Waze, WhatsApp, ooVoo, Skype, Voxer, Kik and Odnoklassniki. • Support for .SDF files being used by Windows Phone apps. • **Nokia BB5 Phones:** • It should support bit-for-bit physical extraction from locked and unlocked Nokia BB5 devices using proprietary boot loaders. • It should enable Password extraction on selected devices. • It should support decoding of Symbian databases including Decoding of intact and deleted contacts, SMS, MMS and call logs; Decoding support for multilingual content.

		• It should support physical decoding of data obtained through Chip Off method for BB5 devices. • **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.

		• In addition, it should bypass user lock code from these devices and decode the user lock from the extraction within Tool. • 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. • **IOS Phones:** • The full list of supported iOS devices should minimally include the following: iPhone 2G, iPhone 3G, iPhone 3GS, iPhone 4, iPhone 4S, iPhone 5, iPhone 5S, iPhone 5C, iPhone 6, iPhone 6Plus, iPhone 6s, iPhone 6s Plus, iPhone 7, iPhone 7 Plus, iPhone 8, iPhone 8 Plus, iPhone X, iphone XS, iphone 11, iphone 11 Pro, iphone 11 Pro Max, iphone 12 mini, iphone 12, iphone 12 Pro, iphone 12 Pro Max, iphone 13, iphone 13 mini, iphone 13 pro max, iPod Touch 1G, iPod Touch 2G, iPod Touch 3G, iPod Touch 4G, iPod Touch 5G, iPad Mini, iPad 1, iPad 2, iPad3, iPad 4, iPad Pro, iPad Air, iPad Air 2. • Decoding of additional iOS databases from KnowledgeC, Health App, Siri native messages and Telegram should be supported.
	Decoding and Analysis Capability	• Capability to provide powerful decoding and analysis solution for the extracted device data and simplify the task of navigating through the device's data structures and to assist in the complex tasks of intelligence gathering, investigative research, and providing legal evidence in the form of reports. • It should provide the capability to decode selected applications rather than the complete phone extraction file to decrease the time to evidence. This selective decoding capability should be optional, and user should be able to choose to use this. • It should support advanced data carving algorithms, by recovering database records to recover additional deleted data from unallocated space. • It should support the decoding of the iCloud backup production

		set obtained from Apple devices and Instagram production set from other devices. • It should have a function to allow view of cloud data in the platform with a valid cloud extraction license. Users can review the device data and cloud data through a single software interface with a unified experience, for a seamless and simplified review process. • The software must have the function to extract cloud zip container. • It should enable highlighting of the exact position for each decoded content entry, enabling full tractability between the analyzed data and the Hex. • It should enable using the Python shell to enhance the capabilities for content decoding. • It should be able to run Python scripts via plugins and edit and create new customized decoding chains. • It should support image carving, a feature used to recover deleted image files and fragments when only remnants are available. • It should support advanced location carving, by decoding more location data from unallocated spaces and unsupported databases. • It should have an in-built fully automated android emulator where selected APKs can be loaded for viewing. It should allow examiner to simulate exactly how the data appears from a user perspective. • The software should have an extraction summaries interface. • It should perform an on-demand searches for viruses, spyware, Trojans and other malicious payloads in files. • The software should enable the user to identify the usage of cryptocurrency and detect addresses or transactions within the

		device data to provide coin data including value, currency type, artifact type and model type. • The software user interface should have time bar, data files section in analyzed data and themes setting with dark and white theme to choose from. • It should allow the user to extract and preserve public domain, forensically sound data in one workflow. The user can enrich the extracted data sources, and quickly reveal evidence based on available public data on Facebook, Instagram, and Twitter. • The software should have the media classification capability to detect and categorize images and video frames into key categories. This capability should be selectable and user should be able to decide if he wants to run the media classification on a particular case. • The media classification capability should be 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) • The software should also be able to segregate the different media classifications into relevant groups like people, textual etc. to make the data review simpler and more efficient. • It should have the capability to convert geographical location information to corresponding address directly from the software. • It should be able to decode network usage information to record the sending and receiving of information via various network connections. • It should have 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.

		• It should be able to support parsing of the Samsung wiped data to get the device factory reset data and also able to detect the time of last iOS data-wipe • It should support parsing of Apple pay data to get Apple wallet transactions and location data. Data should be available for transactions from both Safari and iMessages. • It shall verify file integrity with use of MD5 and SHA 256. • It should support tagging of events using one or more labels via hotkeys. It should have capability to import and export tags from one system to another as XML files. • It should be able to support the applications such as WhatsApp, Skype, Facebook Messenger, Azar, Telegram, Discord, Tiktok, Wechat, Wickr, Reddit, Signal, Viber, Zalo, Cash App, imo, DuckDuck Go browser, Plus Messenger and WhatsApp dual mode. • It should support the parsing of messages, calls and user accounts for the secure messaging app Threema for Android devices • It should have a built-in SQLite Viewer. • It should have a wizard to visually map data from databases which are not automatically decoded by building queries. • It should be able to save the queries created by the wizard and then run them again when the same application is encountered in other extractions. • It should have a built-in tool for researching databases recovered as part of the investigation using Fuzzy Model. • It should be able to match files extracted against Hash Databases and it should have built-in support for Project VIC and CAID hash databases.

		• It should allow user to have the control to input IMEI number to decrypt WeChat database if needed. • It should include the provision of a case id as well as other relevant case-related information as part of the extraction report and allow filtering based on specified date range. • 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. • It should support viewing of all locations on a single map. It should enable viewing of extracted locations using offline maps even without an Internet connection. There should be an option to connect to offline maps from a shared central location. • It should support the ability to highlight information based on predefined list of values. • It should support viewing of text files including file information, content, and Hex. • It should support quick search within decoded data. • It should enable quick reference pointer to set to analyzed data item and data file item. • It should support Hexadecimal view of the extracted data enabling advanced search based on multiple parameters, regular expressions and more. • It should enable the translation of foreign-language content from extractions to English. In-built offline translation should be possible from at least 5 languages. If required, then at least 70+ languages should be available at additional cost. • It should be able to Generate and customize reports in different formats e. g. PDF, HTML, XML, Excel and Word. It should provide global setting to select/unselect items in a report. The software should also allow to password protect the reports.

		• There should be a time range filter for the reports to display data from a specific date and time range • It should be able to 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. • 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. • It should be able to merge multiple extractions in a single unified report for efficient reporting and investigation. • It should have the option to adjust the timestamp according to the time zone and offset setting on the device. • The software should provide a file format viewer which allows users to view, search and copy readable content from various file types like plist, bplist, etc. • It shall have an in-built screen capture capability to visually document (via pictures and/ or by video recording) and capture the examination process for sharing with stakeholders and easily insert it in a report. • The software also has the capability to extract Google advertisement ID (AD-ID) on advanced logical extraction and iOS advertisement ID on iphones. • The software should allow playback of WhatsApp audio files in analysis software. It should also provide indication of reply for WhatsApp messages in application and reports generated. • It should have support decoding and review of secret messages from Facebook Messenger in Android, with support for vanish

		mode (self-destructing messages). • It should have support for parsing WhatsApp's disappearing messages and iOS "view once" media. Should also supporting parsing of Signal iOS messages which were set to self-destruct at a specified date-time. • It should be possible to validate the image hash directly from the software GUI • The software is able to extract memory from Samsung devices to decrypt Samsung Health DB • The software should decrypt and decode location information from Samsung Rubin service • The software should be able to decrypt the Facebook messenger offline account on an iOS mobile device and parse the messages, calls and contacts. • The software should support Samsung browser passwords and allow user to review the decrypted password data of the device owner. • The software should be able to read interactionC database from IOS. • The software should support the following decoding capabilities: o Decode the powering events, decode Samsung password manager and Samsung locked notes o Decode iOS CashApp to parse user account, transactions, contacts, and credit card data o Decode Microsoft Teams to parse chats, calls, contacts, user account, calendar events, and web artifacts o Decode encrypted media from iOS Private Photo vault including location and transaction data, should include transactions done with Safari and iMessages o Decode SkyPhone application to parse account information, address book and call history o Decode Google Archive Files o Decoding of backups for MTK based Android phones. o Decoding of warrant return packages from WhatsApp,

		Facebook, Google, Snapchat, Instagram, Apple iCloud, Discord, TextNow and SkyECC o Decoding of physical activity data from health and wellness applications o Decoding of different WhatsApp variants like WhatsApp2Plus, obwhatsapp, ob2whatsapp, ob3whatsapp and ob4whatsapp o Seamless process for cloud data decoding o Automatic decoding of data from .zip and TAR files o Decoding of the iCloud backup production set obtained from Apple devices and Instagram production set from other devices o Decoding of Huawei backup and Huawei HiSuite backup. o Decoding of ADB backup, MTK backup, iTunes backup, Blackberry 10 backup, Google Takeout (Google Archive) and LG backup o User should be able to save and abort decoding process o Decoding of Berla ivx files • The software should have the 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. • **Should also provide a 64GB Pen drive.** • **1 Year Subscription License.** • **Tender Specific Authorization Certificate is mandatory from the OEM for participation in the tender in favor of the Indian Distributor/Reseller/Bidder.** • **Training - One Day Training to be provided on-site.**

- **Item No. 3**
- **Name of the Item: FORENSIC ACQUISTION OF WEBSITE- FAW (One Year Subscription License)**
- **Quantity 1 Nos**

Technical Specifications/features:

1. Perform the acquisition of a Web page using Browser Scroll.
2. Verification of acquisition locally: the program checks the integrity of the two files Acquisition.txt and Acquisition.xml and shows the result of the verification.
3. Verification of online acquisition: If the acquisition data has also been saved on the server, it is possible to check the integrity of the Acquisition.txt and Acquisition.xml files by comparing it with the data stored in the database.
4. The program should allow to automatically send the acquisition made to an e-mail box. To avoid the sending of attachments that are too heavy, only the Acquisition.txt, Acquisition.xml and Checking. files are sent.

5. In addition to the classic software there are 9 new tools allow new, more safe and automatic type of acquisition:
6. It should allow to capture two screenshots of the same page at different times, while keeping the screencast and network sniffer recording active.
7. It should allow making acquisitions of the same web page in a scheduled way. It should allow capture of web pages in Darkweb with TOR network. The operation is identical to the tool; the only difference is that a session is opened on the TOR network to navigate.
8. Its extension should allow crawler searches all the web pages relate to the main pages, extracting URL and height to create an index.
9. It should allow automatic capture of a list of web pages. It is suitable to perform fast and automatic capture full web sites.
10. It should allow to download an entire website via FTP protocol without altering the date and time of the files, as they are on the web server.
11. It should allow generating a report of all acquisitions performed within the same Case ID.
12. It should allow acquiring WhatApp Web chats including all the multimedia elements contained in them.
13. The tool should allow acquisition of the Face book profile is based on the user ID.
14. It shall provide partial or total acquisition of web pages. It shall acquisition Frame pages.
15. It shall acquire all graphics elements.
16. It shall Acquisition of the html code of the web pages.
17. It shall automatically capture of all objections linked to the webpage It shall provide change User agent.
18. It shall provide acquisition Edit host file It shall acquiring network traffic.
19. It shall provide screen cast audio / video.
20. It shall provide case management and acquisitions.
21. It shall provide multiuser (used by different investigators.)
22. It shall provide automatic calculation of hash MD5, SHa1, and sha256 of all captured files.
23. It shall provide log files for each capture.
24. It shall verification of the integrity of the acquisition It shall provide store capture data on remote server It shall send mail and PEC with acquisition Data.
25. It shall acquisition of SSL /TLS server and client certificates. It shall provide script injection on the page (bookmarklet).
26. It shall provide Manual Referral setting.
27. It shall provide acquiring page and audio /video media content for any length of time.
28. It shall provide scheduled acquisition of web pages.
29. It shall provide web site acquisitions on TOR network (Darkweb) It shall provide automatic search of pages lined to the main page.
30. It shall provide automatic search of pages linked to the main page in websites protected by login.

31. It shall provide automatic acquisitions of web pages from a list (xml File).
32. It shall provide Acquiring websites in FTP preserving the original metadata on the server.
33. It shall provide automatic generation acquisition reporting.
34. It shall provide acquisition Edit host file It shall acquiring network traffic.
35. It shall provide screen cast audio / video.
36. It shall provide case management and acquisitions.
37. It shall provide multiuser (used by different investigators.)
38. It shall provide automatic calculation of hash MD5, SHa1, and sha256 of all captured files.
39. It shall provide log files for each capture.
40. It shall verification of the integrity of the acquisition It shall provide store capture data on remote server It shall send mail and PEC with acquisition.
41. Data It shall acquisition of SSL /TLS server and client certificates.
42. It shall provide script injection on the page (boomarklet)
43. It shall provide Manual Referral setting.
44. It shall provide acquiring page and audio /video media content for any length of time.
45. It shall provide scheduled acquisition of web pages.
46. It shall provide web site acquisitions on TOR network (Darkweb) It shall provide automatic search of pages lined to the main page.
47. It shall provide automatic search of pages linked to the main page in websites protected by login.
48. It shall provide automatic acquisitions of web pages from a list (xml File).
49. It shall provide Acquiring websites in FTP preserving the original metadata on the server.
50. It shall provide automatic generation acquisition reporting.
51. **One Year Subscription License.**
52. **Tender Specific Authorization Certificate is mandatory from the OEM for participation in the tender in favor of the Indian Distributor/Reseller/Bidder.**
53. **Training - One Day Training to be provided on-site.**