MOBILE FORENSIC TOOL

Sl. No.	Specifications	Compliance (Yes/No)
A.	**Advanced Mobile Extraction Capabilities**	
1	The solution should provide advanced access capabilities with brute-force, unlocking and data extraction from supported iOS and Android mobile phones.	
2	The solution should provide 40 unlocks and unlimited extractions with a term-based license through a USB dongle.	
3	It should have brute-force capability for both Android and iOS devices on the same software interface.	
4	The solution should be able to provide Full File-System extraction for File-based encryption (FBE) devices and Physical extraction for the Full-disk encryption (FDE) devices from leading android vendors in India smartphone market such as Vivo, Samsung, Oppo, Xiaomi, Realme and OnePlus.	
5	The solution should support autonomous & connected Brute-Force for a wide range of supported FDE and FBE Android devices.	
6	The solution should identify, extract and decrypt Samsung Secure folder, Huawei Private Space and Xiaomi second space.	
7	The solution should provide brute-force capabilities for supported iPhones in Cold/BFU State on chip A8 all the way to A13 (iPhone 11 and iphone SE Gen 2) to determine the device passcode.	
8	The solution should be able to conduct After-First Unlock (AFU) based Full File-system extraction from iPhone 12, 13, 14 in Hot/AFU State with chip running on A14, A15 to A16	
9	The solution must allow a Full File-system extraction of supported unlocked iOS devices up to iPhone 16.	
10	The solution should be able to support autonomous Brute-Force for iOS devices.	
11	The solution shall support application selective data extraction allowing fast extraction of specific applications data.	
12	The solution should allow the user to enter potential passcodes while performing brute-force on iOS and Android devices without affecting the ongoing process.	
13	The solution should be able to perform Before-First-Unlock (BFU) extraction for supported iPhone and Android phones	
14	The solution must include the software, cables and adapter to allow the solution to perform the access of Android and iOS mobile devices.	
15	The solution should work in a secured environment in a client – cloud exploit server mode.	
16	The solution must provide advanced access capabilities from a Central Cloud exploit server to multiple extraction end points.	
17	An advanced security mechanism should be available to allow the advanced exploit to be pushed down from the Central Cloud exploit server to the client endpoints only on need basis. The solution should be supported to run on an active internet connection with a reliable speed and bandwidth.	

18	The solution should come with all the relevant documentation including supported devices, user manual, release notes and video tutorials.	
19	The solution should be regularly updated to support additional operating system versions and devices during the valid license and support period.	
20	The solution shall support rapid forensic triage of iOS and Android devices without requiring full data extraction. It shall enable configurable profile-based targeted scanning, simultaneous acquisition and decoding of supported metadata, real-time review of matched artifacts and generation of comprehensive triage reports indicating matched artifacts and their severity.	
21	It should allow the user to define a workflow in the beginning of the process to ensure the complete decoding, enrichment and reporting functions are automated without any human intervention.	
22	There should be capability to automatically search for relevant device information during the access phase of the device based on the device state.	
23	Solution should be able to provide information related to device identifiers like IMSI, device name and IMEI along with device user identification information.	
24	The automated workflow and searching device information capabilities should be available for the advanced access extractions for both iOS and Android devices.	
B	**Mobile Extraction Capabilities**	
26	The solution should be able to extract forensic evidence from supported mobile devices including mobile phones, handheld tablets, portable GPS devices and drones.	
27	It should provide users with available physical, file system and advanced logical extraction capabilities for different supported devices and Operating Systems as well as allow extraction of Cloud Data source tokens accessed by the supported Mobile Phones.	
28	It should support automatic detection of supported devices. It should also support manual search for devices by manufacturer, model and IMEI number	
29	A multi-SIM adapter with support for Micro, Nano and standard SIM cards should be supplied. Ability to perform SIM data extraction from a SIM or USIM card.	
30	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.	
31	The software should at least provide the following extraction methods to the user: Selective Filesystem Extraction, Selective App data extraction, Selective cloud token extraction, EDL extraction with decryption, Unisoc Live, Kirin Live, Exynos Live, MTK Live, Qualcomm Live, Smart ADB, Samsung Qualcomm, Samsung Decrypting Exynos, Samsung MTK, Samsung Spreadtrum, Samsung Exynos Physical Bypass, Generic Android Unlock using Lockpick, APK Downgrade (Android 6 & above), Huawei Kirin extraction, LG LAF, Advanced ADB, TWRP, Coolsand chipset extraction.	
C	**Decoding, Review and Reporting Capabilities**	

33	Should have Case Management capability which allows users to create and manage cases and to provide case details and exhibit information. It should enable users to include multiple extractions and to apply the different enrichments.	
34	Should include dashboard view to provide quick visual overview and display insights into the extracted data including commonly used applications, the most recent messages and enable investigator to quickly and easily drill down into the data of interest.	
35	Dedicated location analysis view to clearly categorize the location records like device visited locations, locations of some significance, media derived locations and any other location data for detailed user analysis.	
36	Capability to identify the origin of media items found within the device data to collect various metrics about a media item and apply logic to try to identify how the item originated, providing the user with information about the determined origin and the reasoning for that determination.	
37	Should have the ability to parse windows computer data like DD, E01, RAW, L01,001 or BIN images in the same application.	
38	Should be built on a database architecture to reopen cases quickly without having to reprocess the data.	
39	Should have a cryptocurrency enrichment to automatically identify the usage of cryptocurrencies and to detect wallet addresses and transactions within the device data.	
40	It should also have an advanced cryptocurrency enrichment ability to provide a detailed analysis of the cryptocurrency assets associated with detected wallet addresses and highlight potential illicit activity. The enrichment should further provide risk severity and graphs on currency sent and received insights. This crypto enrichment result should be exportable to a report for individual wallet addresses.	
41	Support for image carving and location carving	
42	It should conduct on demand searches for viruses, spyware, Trojans and other malicious payloads in files.	
43	Media classification capability to detect and categorize images and video frames into 20+ key categories. This capability should be selectable, allowing user to decide if he wants to run the media classification on a particular case.	
44	Capability to verify file integrity with use of MD5 and SHA 256.	
45	It should have a built-in SQLite Viewer.	
46	Capability to match files extracted against Hash Databases and it should have built-in support for Project VIC, CAID and NCMEC hash databases.	
47	Ability to generate and customize reports in different formats e.g. PDF, HTML, XML, Excel and Word. Global setting to select/unselect items in a report with ability to password protect the reports.	
48	Provide a separate report with device information and user account information for quick reference of users.	
D	**Cloud Data Extraction Capabilities**	
50	Should allow access to remote cloud data sources to obtain, decode, save and perform analysis of this data.	
51	There should be a single software interface in which users can review device data and cloud data through a single tool and with a unified experience, for a seamless and simplified review process.	

52	Software should allow access to remote cloud data sources using cloud login keys from mobile devices supporting iOS and Android.	
53	Support extraction of different content types from the supported data sources which includes messages, images, videos, files, contacts, calls, user profile, locations, user activities and backups.	
54	Provide visibility of the cloud extraction progress to the user. It should provide a view of the current status of each data source extraction with an option to cancel the process if required.	
55	Allow users to gather private user data with appropriate legal authority from over 50 of the most popular social media and cloud-based sources.	
56	Capability to create cloud tokens from manually entered credentials for future cloud extractions.	
57	Reporting of extracted data from the Cloud to human readable formats such as PDF, Word, Excel, HTML and XML. It should provide a global setting to select/unselect items in a report. The software should allow to password protect the reports.	