DEPARTMENT OF JUSTICE

RECEIVED

OCT 30 2020

Procurement Management Division

Time: _____

TERMS OF REFERENCE

Renewal of and Forensic Investigation System for Mobile Phone Devices (UFED Touch 2 Ultimate)

I. INTRODUCTION

The **UFED Touch 2 Ultimate** is a portable mobile phone forensic system package consisting of both hardware and software used primarily to conduct, and enabling a digital forensic examiner to perform digital forensic analysis of mobile devices. It enables the user to acquire and examine potential electronic evidence from a wide array of devices. Hence, comprehensive reports can be produced using said tools.

II. OBJECTIVE

This aims to renew the software license of the existing **UFED Touch 2 Ultimate** previously procured by the Office of Cybercrime.

III. SCOPE

A tool for mobile phone, smartphone, and PDA forensics. It is a portable digital forensics solution that empowers law enforcement, military, intelligence and e-discovery personnel to speed the capture of critical forensic intelligence and evidence from the widest variety of mobile devices and operating systems.

A. General Features

1. The standalone portable hardware device should be custom built with fully custom operating system that is based on windows 10 and should not allow loading of any other third-party application in it for security reasons.
2. It should have portable integrated battery to allow the device to be portable for longer duration.
3. It should come with a compact and lightweight case with all necessary cables for the supported phones and operating systems.
4. The standalone portable hardware device should be touch screen enabled, allowing easy use.
5. 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 with or without consent.
6. It should support more than 31,110 device profiles and 10,800 different mobile application versions.

7. It should support management, upgrades and control from a centralized software.
8. The extraction software should be touch screen enabled, allowing easy use on tablets.
9. It should be operated with a USB software license dongle.
10. It should come with a compact and lightweight case with all necessary cables for the supported phones/OS).
11. 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.
12. It should support the decoding of the iCloud backup production set obtained from Apple devices and Instagram production set from other devices.
13. The software must have the function to extract cloud zip container.
14. It should enable Highlighting of the exact position for each decoded content entry, enabling full tractability between the analyzed data and the Hex.
15. It should enable using the Python shell to enhance the capabilities for content decoding.
16. It should be able to run Python scripts via plugins and edit and create new decoding chains.
17. It should support image carving, a feature used to recover deleted image files and fragments when only remnants are available.
18. It should support advanced location carving, by decoding more location data from unallocated spaces and unsupported databases.
19. The software should have an application emulator.
20. The software should have an extraction summaries interface.
21. It should perform on-demand searches for viruses, spyware, Trojans and other malicious payloads in files.
22. It should allow decoding & conversion of BSSID values (wireless networks) and cell ID values into physical location with map coordinates. This service should be available with in both online and offline mode.
23. It should support tagging of events using one or more labels via hotkeys
24. The software user interface supports the following, time bar, data files section in analyzed data and themes setting with dark and white theme to choose from.
25. It should be able to highlight platform for chat messages such as WhatsApp, Skype, Facebook Messenger, Azar, Telegram, Tiktok, Wechat, Wickr, Signal and WhatsApp dual mode
26. It should be able to decode powering events.
27. It should have a built-in SQLite Viewer.
28. It should have a wizard to visually map data from databases which are not automatically decoded by building queries.

29. 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.
30. It should have a built-in tool for researching databases recovered as part of the investigation using Fuzzy Model
31. It should have a research tools that helps to identify specific artifact from device database and have the ability to decode the databases when needed.
32. It should be able to read report file generated using corresponding Cloud extraction solution.
33. It should be able to integrate with Active Directory for user authentication.
34. 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.
35. It should be able to decode Google Archive Files.
36. It should be able to decode modified IMEI numbers for Android devices.
37. It should allow user to have the control to input IMEI number to decrypt WeChat database if needed.
38. 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.
39. 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.
40. It should enable conversion of single or multiple locations to their corresponding address.
41. It should support viewing of all locations on a single map.
42. It should enable viewing of extracted locations using offline maps even without an Internet connection.
43. The software should be able to load offline map
44. It should support the ability to highlight information based on predefined list of values.
45. It should support viewing of text files including file information, content, and Hex.
46. It should support quick search within decoded data.
47. It should enable viewing of communications between sources in date and time order.
48. It should enable quick reference pointer to set to analyzed data item and data file item.
49. It should support Hexadecimal view of the extracted data enabling advanced search based on multiple parameters, regular expressions and more.
50. It should enable the translation of foreign-language content from extractions to English. Translation should be possible from at least 5 languages. If required, then at least 70+ languages should be available at additional cost.
51. It should be able to Generate and customize reports in different formats e. g. PDF, HTML, XML, Excel and Word.

52. It should enable Chat messages to be exported in conversation format, in PDF reports.
53. It should provide global setting to select/unselect items in a report.
54. It should support Exporting selected emails to EML format.
55. It should support hash verification to ensure the extraction decoded is the same extraction received from the device.
56. It should be able to merge multiple extractions in a single unified report for efficient reporting and investigation.
57. 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.
58. Downgrading the APK should support shared data extractions, in addition to "no shared" data.
59. It should have the option to adjust the timestamp according to the time zone and offset setting on the device.
60. It should support extraction, decoding and media analysis from most popular drones from DJI with latest firmwares. It should also support the DJI Go app.
61. The software should provide additional security for protecting the reports. It should also allow to password protect the reports.
62. 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.
63. The software should allow decoding of backups for MTK based Android phones.
64. The software should support physical extraction capability using the emergency download mode.
65. The software should provide lock bypassing physical extraction support for devices with Coolsand based chipsets.
66. The software should be able to produce powerful visual reports which should include conversation screenshots, locations on the map and extraction summaries.
67. The software should provide greater access to supported applications with the use Android emulator. It should allow examiner to simulate exactly how the data appears from a user perspective.
68. The software should have the capability to provide internal screenshot and video function to capture the evidence data.
69. The software must be able to perform LG backup.
70. The software should be able to decode of Huawei backup, Huawei HiSuite backup, Facebook Takeout and Gogle Takeout.
71. The software also has the capability to extract Google advertisement ID (AD-ID) on advanced logical extraction.
72. The software should allow automatic decoding of data from .zip files.
73. The software should allow examiners to perform a quick selective extraction of selected applications.
74. It should provide generic pattern/pin/password lock screen removal and bypass method for various models from leading

vendors including Samsung, LG, Motorola, Sony, Xiaomi and others. It should support Android v6 and above with Full Disk Encryption and security patch older than August 2018.

75. It should provide a simple extraction flow with generic extraction for unsupported devices.
76. The software should allow direct upload of data from analysis software to analytics software.
77. The software should allow selective extraction of cloud tokens from the phone.
78. The software is able to Extract memory from Samsung devices to decrypt Samsung Health DB.
79. The software should be coupled with a USB 3.0 adapter for faster extraction.
80. The software should allow playback of WhatsApp audio files in analysis software.
81. The software should have a dashboard widget to show application insights.
82. The software should have a function to address unsupported application.
83. The software should be able to read interactionC database from IOS.
84. It should support Berla ivx files for decoding.
85. The software should have a capability to extract Qualcomm chipset phone in a generic option that support popular brand like Samsung and Huawei.
86. The software should have a capability to extract MTK chipset phone in a generic option.

B. Support for Various Phones

i. Android Phones:

1. It should support Android devices running up to and including v9 Pie.
2. It should support lock bypassing for at least 500 LG devices.
3. 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.
4. 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.
5. The software should able to support Samsung devices with full disk encryption such as Samsung S9 or Samsung Note 9 running on Android 10.
6. It should support lock bypass using file system extraction for latest Samsung devices like Galaxy J7, Galaxy S8, Galaxy Note8 and Galaxy S8+.

7. It should have lock bypassing decrypted physical extraction capability for Qualcomm Android devices including LG, ZTE, Xiaomi, Huawei, Alcatel and Motorola.
8. It should be able to perform selective file system extraction on popular Samsung models with the Qualcomm processor (SOC).
9. It should have decrypting bootloader capability for Huawei devices with HiSilicon Kirin chipsets and Samsung devices with Exynos processor.
10. The software should provide a unique decrypted physical extraction method for unlocked Android devices of latest generation.
11. 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 655, 658,659, 710, K710F 960 and 980 chipsets For Huawei and Huawei Honor must be running android 8 and 9.
12. 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.
13. It should support Physical Extraction over ADB for Samsung devices running up to Android OS v8.
14. It should support bootloader-based physical extraction for zte, alcatel and xiaomi devices running Qualcomm chipset.
15. It should support Partial File System extraction while bypassing User Lock for more than 100 Android devices.
16. 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.
17. It should also support Physical extraction and advanced decoding, via USB debugging, for Android OS version 4.X (Ice Cream Sandwich). Physical extraction for any locked device should be available if the USB debugging has been switched on.
18. It should provide a simple extraction flow with generic extraction for unsupported devices.
19. It should support Decryption of encrypted Android physical extractions: Decrypt encrypted physical extractions from Android devices 4.2 and below, with a known password. This includes generic Android and Samsung devices.
20. It should support automatic detection of supported devices. It should also support manual search for devices by manufacturer, model and IMEI number.

21. It should be able to perform physical, full file system and selective file system extraction on Smartphone with Samsung Qualcomm Processor.
22. It should be able to perform categorization when conducting selective extraction.
23. It should have the capability to add on categorization DB within the system.
24. 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.
25. Physical Extraction of Major Device Support should at least include the following phones:
    a) HTC – HTC Evo, HTC One M8, Incredible, Desire 310, Desire C, 2PS6500 10, U11, U-1w Ultra.
    b) 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.
    c) 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.
    d) LG – G5, G4, G3, Optimus, Optimus one, Optimus 3D, Optimus black, Nexus 5X, L51AL, Fiesta LTE, K10, G6, V30, Nexus 5x, H820 G5, LM-X210MA & MP260.
    e) 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.
    f) Huawei – Ascend, Honor 3x, 5 vision, Honor 5x, Honor 4c, H1611, Mi5, C8815, Nova 2i, U8600 Move, Mate 8, Honor 8, Nexus 6P, P10, Mate 10, P9.
    g) Sony: Xperia X, Xperia z5, Xperia e5, Xperia X Dual, XZ, L1, XA1 Plus, Xperia XA1.
    h) Xiaomi: M1908C3KG_DS Redmi 8A, M1810F6LE_DS Redmi 7, M1903F11I_DS Redmi K20 Pro, M1901F7S.
    i) Redmi Note 7 Pro, M1903F11G_DS Mi 9T Pro, M1903C3EG_DS Redmi 7A, M1903C3EI_DS Redmi.
    j) 7A, M1906G7E Redmi Note 8 Pro, M1904F3BG Mi 9 Lite, M1810F6I_DS Redmi Y3, M1903F11A.
    k) Redmi K20 Pro, M1906F9SI Mi A3, M1906G7G Redmi Note 8 Pro.
    l) Vivo: 1801_DS Y71i, 1813 Nex Dual, 1818_DS V15 Pro, 1901_DS.

m) Oppo: CPH1909_DS A5s, CPH1907 Reno 2, CPH1803_DS A3s, CPH1969 F11 Pro, CPH1613 F3 Plus, CPH1923_DS A1k.
n) Others: Asus Zenfone 4 Max, Xiaomi Redmi 3S/4, Oppo F3, Alcatel 5090i A7.

ii. Blackberry Phones

1. 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.
2. It should support advanced decoding of existing and deleted data for Blackberry running OS 4-7.
3. BBM history (if enabled by the user).
4. BlackBerry Messenger (BBM) messages including Deleted messages and chats, message attachments, contact photos, BBM from groups: Chats, contacts and shared photos.
5. 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).
6. Address book, SMS, MMS, Emails, PIN messages, Calendar entries, Memo pad notes, Web browser history, Web bookmarks, Bluetooth devices and Cookies.
7. Recent email contacts (BB OS 6 and above, where available).
8. Device Info (Model, IMEI\MEID, ICCID, PIN, OS version, Platform, Supported Networks).
9. REM files – decryption of encrypted files on external memory.

iii. Windows Phone

1. 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.
2. JTAG decoding of contacts, call logs and SMS from Windows Phone 8.x devices is enabled via physical extraction.
3. 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.
4. 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.
5. Support for .SDF files being used by Windows Phone apps.

iv. **Nokia BB5 Phones**

1. It should support bit-for-bit physical extraction from locked and unlocked Nokia BB5 devices using proprietary boot loaders.
2. It should enable Password extraction on selected devices.
3. It should support decoding of Symbian databases including Decoding of intact and deleted contacts, SMS, MMS and call logs; Decoding support for multilingual content.
4. It should support physical decoding of data obtained through Chip Off method for BB5 devices.

v. **Portable GPS Device**

1. 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.
2. 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).
3. 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.

vi. **Feature Phones:**

1. 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.
2. The Supported Phones (for either Physical/ File System/ Logical) should at least include:
   a) Nokia: 1280, 1616, 1650, 1661, 1661-2b, 1680 Classic, 1800, 2720 fold, 2720a-2b, 2730 Classic, 2760, 3109 Classic, 3110 Classic, TA-1047_DS Nokia 1, TA-1125 3.1 Plus, TA-1020 Nokia 3, TA-1109 X5, TA-1105 5.1 Plus.
   b) 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.
   c) 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.

d) 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.

vii. Chinese Chipsets Based Phones

1. 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.
2. In addition, it should bypass user lock code from these devices and decode the user lock from the extraction within Tool.
3. The tool should provide generic extraction with Decrypting bootloader for MTK based chipsets including 6580, 6735, 6737, 6753, 6755, 6757 & 6797.
4. 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.
5. The software should have a Qualcomm full file system or physical extraction capability on Qualcomm chipset and should support at least on the following brand, Xiaomi, OPPO, OnePlus, Samsung, Huawei and VIVO that runs Android version from 7 up to 10.

viii. iOS Phone

1. It should enable forensically sound data extraction, decoding and analysis techniques to obtain existing and deleted data from all major iOS devices.
2. The software should be able to support full file system extraction using Checkm8 capability from Apple iPhone 5S to X with a minimum IOS version from 12.3 to 13.5.X depending of the iPhone device supported base on Apple official release.
3. 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, 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.
4. It should have support for data extraction decoding and analysis for iOS devices running iOS 13.5 including encrypted iTunes backup.
5. It should decode URL parameters from popular search engines for iOS devices.

6. Decoding of additional iOS databases from KnowledgeC, Health App, Siri native messages and Telegram should be supported.

ix. **Unlocking Tool for Locked Phones:** The tool should provide a separate Unlocking software for unlocking the phone using brute force method. This should be integral part of the Tool.

x. **Phone Detection Application Features:**

1. The Phone Detection application should provide help to investigators quickly identify a mobile phone by its physical attributes, eliminating the need to open up the phone and risk phone lock.
2. It should be able to help to identify a phone by the user. answering key questions regarding the phone's appearance.
3. It should provide users with detailed extraction capabilities per device, connectivity details, device characteristics and more.

IV. DELIVERY DATE

Within thirty (30) days from the receipt of the notice to proceed. SUPPLIER must provide Manufacturer Letter of Authorization to bid, and provide demonstrable proficiency in providing technical support for mission-critical mobile forensic systems.

Inclusive of software maintenance service (SMS) for one (1) year.

V. PENALTY CLAUSE

When the service provider fails to satisfactorily deliver the software under the contract within the specified delivery schedule, inclusive of duly granted time extensions, if any, it shall be liable for liquidated damages for at least equal to one-tenth of one percent (0.001) of the cost of the unperformed portion for every day of delay until the software is finally delivered and accepted by the DOJ. Such amount shall be deducted from any money due or which may become due to the service provider.

Once the cumulative amount of liquidated damages reaches ten percent (10%) of the amount of the contract, the DOJ may rescind or terminate the contract, without prejudice to other courses of action and remedies available under the circumstances.

VI. TERMS OF PAYMENT

The approved budget for the contract, which is Five Hundred Thousand Pesos (Php500,000.00) inclusive of VAT, and all other applicable government taxes and charges, which shall cover payment for subscription

of software license for the UFED Touch 2 Ultimate for One (1) year from the delivery, chargeable against the funds of the Office of Cybercrime, subject to the usual government accounting and auditing rules.

The payment shall be made upon delivery of the software license for the UFED Touch 2 Ultimate and acceptance of DOJ.

VII. TERMINATION

The Department of Justice has the right to test and evaluate the software license before acceptance. Prospected bidder must be Certified Distributor and have authority to sell, deploy, manage and provide support services issued by the product owner/manufacturer.