Request for proposal (RFP) Ref no;- **Dated: 13th March,2017**

RE-ISSUE OF INVITATION FOR BIDS IN TWO BID SYSTEM FOR PROCUREMENT, INSTALLATION, MAINTENANCE AND TRAINING OF PORTABLE FORENSIC KITS AT MUMBAI.

The Tata Institute of Social Sciences invites sealed bids in two bid system (Technical bid and Financial bid separately) from vendors preferably registered with DGS&D and satisfying the prescribed qualifications indicated here in for supply, installation, maintenance and training of Portable forensic kits of prescribed specifications as listed in the Annexures at Mumbai.

The sealed envelope (separately sealed for technical and financial bid) must be super scribed with the above title and the RFP number. The bids shall be addressed and sent to the following address on or before 20th March, 2017, on any working day between 10.30 a.m. and 5.00 p.m.

The Assistant Registrar (Purchase and Stores)
Tata Institute of Social Sciences
V.N. Purav Marg, Deonar,
Mumbai – 400 088.
Phone : 022-25525240
Queries if any, may be marked to:
Email: roja@tiss.edu
snbatliwalla@gmail.com
rohit.ganiga@tiss.edu

Important note; Bids received after the closing time and date will not be considered valid. Bids not following two bid system are liable to be rejected.

The RFP is being issued with no financial commitment and the Institute reserves the right to change or vary any part thereof at any stage including the option for AMC. The Institute also reserves the right to withdraw/cancel the RFP should it become necessary at any stage.

The scope of work and technical specification shall be as detailed in the Annexures to this RFP.

Bidders are advised to carefully read and understand the Annexures containing the scope and specifications. The Bidders should also provide the separate cost of material supply and the services and the applicable taxes for the same in detail in the bid as per the attached annexures.

General terms and conditions;

1. The price of the equipments should be quoted at per unit cost.
2. A complete profile of the company shall be submitted with the technical bid.
3. The audited statement of accounts of the last three financial years must be submitted.
4. Income tax returns for the last three years shall be submitted.
5. Profile of key personnel involved in this supply and installation.
6. Bidders must have designated office/ single point of contact in Mumbai. Address of the same must be submitted with the bid.
7. The bidder must submit the Manufacturer's Authorization Form (MAF) for the quoted equipments.
8. Successful bidder has to arrange for all necessary tools, measuring equipment for carrying out the job.
9. Successful bidder has to arrange for their own accommodation and transport during implementation, warranty and post warranty support periods.
10. All onsite personnel stationed by the vendor for operations and maintenance of the entire solution will have to be certified by respective OEMs and the documentary proof is to be furnished.
11. The bidders or his sub-contractor must possess valid licenses from the appropriate authority.
12. The bidder should have previous experience of supplying, installing, maintaining and training with regard to the equipments. (Relevant proofs to be attached).
13. Any alteration / modification of the original equipment will not be accepted.
14. Each page of the bid document must be signed by the bidder.

SCOPE OF WORK & TECHNICAL SPECIFICATTIONS

SCOPE OF WORK;

The successful bidder will be responsible for implementing the entire project on a turnkey basis.

The jobs to be carried out by the successful bidder are;

1. Set up the equipment at Mumbai.
2. AMC of supplied equipments, post warranty shall be undertaken by the bidder. The price of the same shall be indicated in the Price Bid, however the successful bidder will be chosen by TISS based on the Base Price and the AMC quoted.
3. Replacement of all defective equipment during warranty and AMC periods.
4. Supply of all hardware, original software and any required accessories to complete the entire project.
5. If maintenance is required at the power tapping point from the internal power supply, the vendor's personnel will inform Electrical Engineering Department and ask for shutdown.
6. The tools and tackles, transportation etc required for operation and maintenance of the entire system shall be arranged by the vendor.
7. Voltage, frequency and phase available will be 230V, 50Hz, single phase. The party will make appropriate arrangement like increasing the size of the cable, step up devices etc for getting the required quality of power for the equipment.
8. To provide adequate training to the concerned officers, who shall operate the equipments.

TECHNICAL SPECIFICATIONS: **ANNEXURE: I**

Portable forensic kits

1. Desktop Forensic Workstation Specifications:

- Intel Core i7-5820K CPU (Hex Core Processor), 3.3 GHz, 10MB Intel Smart Cache, 5 GT/s DMI
- 64 GB (4x8GB)PC3-17000 DDR4 2133 MHz Memory
- 1 x 512 GB Solid State SATA III Drive - OS Drive
- 1 x 512 GB Solid State SATA III Drive - Temp/Cache/DB Drive
- 1 x 4.0 TB 7200 RPM SATA III Hard Drive - Data Drive
- Nvidia GTX 750Ti 2GB 128 bit DDR5 PCI-Express Video Card with 1 VGA (D-Dub), 1 HDMI, and 2 DVI ports - supports up 4 displays
- 22" WideScreen LCD Monitor with Built-in Speakers
- Windows 10 Professional (64 bit)
- Hardware Write Blocking with touch screen display:
- Integrated IDE Drive Write Blocker
- Integrated SATA Drive Write Blocker
- Integrated SAS Drive Write Blocker
- Integrated USB 3.0/2.0 Write Blocker
- Integrated FireWire IEEE 1394b Write Blocker
- Integrated Forensic Media Card Reader - Read-Only and Read/Write switchable
- ATX Tower Case 12 x 5 1/4" Bays
- 1100 Watt Modular power supply
- i7 Motherboard with Intel X99 Chipset
- 2 RJ45 LAN ports (Intel I210-AT, 1 x Gigabit LAN Intel I218LM, 1 x Gigabit LAN Controllers)
- Minimum 10 USB 3.0/2.0 ports – 7 Back and 3 Front Mounted
- 2 USB 3.1 ports – Back Mounted
- 2 x Shock Mounted SATA Removable Hard Drive Bays (IDE Capable)
- 4 x HotSwap Shock Mounted Universal (IDE/SATA compatible) Removable Hard Drive Bays
- BD-R/BD-RE/DVDÂ±RW/CDÂ±RW Blu-ray Burner Dual-Layer Combo Drive
- Extendable/Retractable Imaging Workshelf with integrated ventilation
- 103 key Keyboard and Mouse Combo
- Toolbox containing: Adapters, Cables, Digital Camera, Security Screwdriver Set and OEM Documents
- Other Software included: Symantec Ghost and CD Authoring Software
- One licenced software Encase V7 or FTK 5 (latest version) for Forensic Analysis of digital storage media like Hard Disk, Pen Drive, Memory Card etc

Specific Terms:

- Product Offered should be of International Repute & Brand and should not be customised/ assembled Product from various sources
- Bidder should be OEM or direct Authorized Distributor or Reseller in India. In case of Distributor/ Reseller; OEM/ Manufacturer’s Authorization for Supply and Service should be attached with the Tender
- Bidder should have a minimum 03 years of existence in the field of Cyber/ Digital Forensics in India
- Bidder should have OEM trained Manpower for Installation and Training of the Product. OEM Certification to be attached for supporting the same.

2. Mobile Forensic Workstation Specifications:

A portable kit which contains a complete family of hardware write blockers for use in acquiring a forensically sound image of hard drive IDE, SATA, SAS or USB. It should contain all the write blockers, cables, adapters, and power supplies necessary for use in acquiring images in the field using a standard laptop with FireWire or USB support.

With multiple boot menu options (1) Windows 10 Professional 64 Bit and (2) Suse Linux Professional.

It should also has the ability to connect directly to a 10Mb, 100Mb, or even Gigabit Ethernet networks for use as a standard laptop when not processing or acquiring data. It should also have integrated 802.11a/b/g/n wireless capabilities. It should have facility for Network Analysis and to monitor network traffic.

Basic configuration of the computer hardware

- Intel Core i7-6700K Skylake Quad Core Processor, 4.0 GHz, 8MB Intel Smart Cache or better
- 16 GB PC4-17000 DDR4 2133 Memory or better
- Minimum 256 GB Solid State Internal SATA Drive
- Intel Z170 Express Chipset or better
- 15.6" Full HD (1920x1080) IPS Display or better
- NVIDIA GeForce GTX 1060 with 6 GB GDDR5 VRAM or better
- 1 RJ-45 LAN (10/100/1000Mbps)
- Intel Dual Band Wireless-AC 8260 - 802.11ac, Dual Band, 2x2 Wi-Fi + Bluetooth 4.2
- Card Reader 6-in-1 (MMC/RSMMC/SD/Mini-SD/SDHC/SDXC up to UHS-II)
- 2.0 Megapixel FHD Video Camera
- High Definition Audio
- Microphone
- Speakers (2)
- 19mm Full-Size Keyboard with numeric keypad - Illuminated
- Touch Pad pointing device(2 buttons)with multi-gesture and scrolling function
- 1 HDMI Port 2 Mini Display Port 1.3 ports 1 Thunderbolt 3 / USB 3.1 Gen 2 Combo Port (Type C) Minimum 1 USB 3.1 Gen 2 Port (Type C) Minimum 3 USB 3.0 ports Minimum 1 USB 2.0 Port 1 Headphone jack (2-in-1 Headphone/S/PDIF Optical) 1 Microphone jack 1 Line-In jack 1 Line-out jack.
- Suitable Smart Lithium -Ion Battery Pack Kensington Lock Slot Universal AC Adapter (100~240V AC 50/60hz) Windows 10 Professional (64 bit)
- SUSE Professional Linux (64 bit)
- Microsoft Office latest version
- Antivirus software of international repute
- Should be supplied with System Restore Media - Bootable Blu-ray disc containing restore environment and factory configured operating system images
- Symantec Ghost and CD-DVD Authoring Software
- System carrying bag should be Hard-sided, cushioned with pad
- USB 3.0 External 3.5” Hard Drive Enclosure
- Forensic Media Card Reader - Read-Only and Read/Write switchable
- One 2.0 TB SATA Hard Drive

Specific Terms:

- The system should be supplied with EnCase V7 or FTK V5. The bidder has to provide the latest license version available at the time of supply
- Warranty: 3 Years

- Training by the OEM certified trainer.
- On site live demonstrations of the product quoted by the bidder to get technically qualified.

3. Mobile Forensic Extraction device for the field

Specifications:

A. Software Features:

- It should support extraction of password for supported mobile devices
- It should support disabling of user lock for supported mobile devices
- It should support bypassing of user lock for supported mobile devices
- It should support Logical Extraction of mobile devices
- It should support File System Extraction of mobile devices
- The devices should be responding to a Centralized Management Console
- The Centralized Management Console must be able to push down profiles to the devices
- The Centralized Management Console must be able to push down key words or watch lists to the devices
- The Centralized Management Console must be able to push down user permissions to the devices
- The Centralized Management Console must be able to push down licenses to the devices
- The Centralized Management Console must be able to push down software updates to the devices
- The devices should provide reports to the Centralized Management Console which includes devices status, usage statistics and monitoring
- The devices should be able to send back all extractions gathered to the Central Management Console so that it can be stored in a Central Repository if needed
- The Devices and Central Management Console should have Role based Access
- The device should support extraction and decoding of data from messaging applications and social networking sites
- It should support Selective Extraction. There should be an option to specify a time range or a specific party (person, email or phone) and extract data related to this narrow criteria.
- It should support collecting evidence by capturing pictures or videos of a mobile device
- It should support capturing screenshots as photographic evidence from iOS, Android and BlackBerry devices.
- It should support Quick and selective copy that allows witnesses or victims to share specific evidence in an unobtrusive manner, leaving personal mobile device unaffected.
- It should automatically detect supported devices, providing the right workflow to extract data from that specific device
- It should allow quick searches by filtering data based on date, time , person and specific crime type watch lists.
- It should support sim data extraction
- It should support cloning of sim card
- It should include the provision of a case id as well as other relevant case-related information as part of the extraction report.
- It should support a location based event viewer

B. Hardware Specifications

- The software should run on a Laptop which should have atleast the following specifications:

    - CPU: *[Insert Value Here]*
    - RAM:*16 GB RAM*
    - Hard Disk: *[Insert Value Here]*
    - USB Ports: *[Insert Value Here]*
    - Power Supply: *[Insert Value Here]*
    - Monitor: *[Insert Value Here]*
    - SIM Card Reader
    - Camera

C. Advanced Specifications(Optional only not to be quoted by the bidder, Buyer should be able to upgrade to higher specifications without changing hardware but by upgrading licence only . The system should be capable of supporting the features through advanced Ultimate Licence)

- The InField system should support physical extraction capability using bootloader method with lock bypass for at least the following families:
  - Samsung Galaxy S5 (including Android OS 5.x firmware versions), including SM-G900V, SM-G900A, SM-G860P, SM-G900T
  - Samsung Galaxy S4 (including latest firmware versions), including SPH-L720, SCH-i545, GT-i9500, GT-i9506
  - Samsung Galaxy Note 3 (including Android OS 5.x firmware versions), including G900V, G900A, N900T N9005, N9006
  - Samsung Galaxy Y (including Android OS 5.x firmware versions), including GT-B5512, GT-S5360T
  - Samsung Galaxy Wave (including Android OS 5.x firmware versions), including GT-S5253, GT-S7250, GT-S8530
  - Motorola Android devices, including: NvidiaTegra 2: MB867 Milestone X2, MB870 Droid X2, MB860 Atrix 4G, TI OMAP 3xxx (3410/3430/3440/3610/3620/3630): MB526 Defy+, XT720 Milestone, A955 Droid 2
  - Nokia Lumia Windows Phone 8 with lock bypass, including Lumia 520, 820, 822, 920, 928, 1020
  - Physical extraction with password bypass from supported Nokia BB5 devices, including RAPUv21 chipset running on the following devices: Asha 300 (RM-781), Asha 302 (RM-813), Asha 311 (RM-714), 700 Benji (RM-670), 603 (RM-779)
  - Physical extraction (including NAND and NOR memory) from BlackBerry 7xxx/8xxx/9xxx devices, including 9930 Bold, 9800 Torch and 8330 Curve (for unlocked devices)
  - Built in Android temporary root (granting extra permissions) for supported Android devices that allow File system and Physical Extraction and decoding of Android devices utilizing operating systems from 4.2 up to and including 4.3. This should provide forensically sound extractions, eliminating the need of a 3rd party tool to accomplish such tasks
  - Temporary root (ADB) solution for selected Android devices running OS 4.3-5.1.1 - this capability enables file system and physical extraction methods and decoding from devices running OS 4.3-5.1.1 32-bit with ADB enabled. In addition, this capability enables extraction of apps data for logical extraction

- It should support disabling of user lock on leading Android Devices not limited to Samsung Note 2,3,4, Galaxy Tab, Samsung Galaxy S5, LG G3, G4, G5

- It should support iOS unlock capability for iOS versions 8.0 to 8.4.1 for iPhone 4S, 5 and 5C

- There should be at least 8 releases a year for new phone support lists

4. Mobile Forensic Hardware Tool Specifications:

A. Generic Features :

The Hardware extraction device shall have a standalone portable handheld device to extract and save data into a memory device; It Shall have minimum

- Three (3) RJ 45 Ethernet ports input;
- Two (2) USB ports input; one (1) mini-USB port input;
- Bluetooth function;
- Integrated SIM (Micro and Nano Sim) card reader; integrated SD card reader in the hardware device itself .
- The hardware device should be custom built with fully custom operating system and should not allow loading of any other third party application in it for security reasons.
- Portable integrated battery to allow the device to be portable for longer duration.
- Support High-resolution (1024), capacitive multi-touch display.
- Built-in multi-SIM
- Support DDR3 scalable memory
- Support USB 3.1 phase 1axillaries (Up to 5Mbps)
- Support inbuilt WiFi b\g\n\ac - (up to 350 Mbps)
- Support Larger and faster hard drive (SSD 128MB)
- Mini Display Port
- Work on Customized Windows 10

- Provide users with all physical, file system and logical extraction capabilities for different devices and different Operating Systems as well as allow extraction of Private Cloud Data accessed by the Mobile Phone with or without user name and password and show patterns and links between various extraction and data sources using link analysis feature all in an integrated platform which seamlessly interworks with each other from one single OEM.
- The extraction software should be touch screen enabled, allowing easy use on tablets
- It should come with a compact and lightweight case with all necessary cables for the phones/ os mentioned in section B)
- It should be operated with a USB software license dongle .
- 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 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 and 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 files 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 support file system extraction of blocked apps data using apk downgrade method.
- It should enable Viewing of statistics on communications and identifying relationship strengths and it should enable Visualizing of events over time, view distances between events and see the number of events within a defined time span 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 a 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 enable Quick reference pointer set to analyzed data item and data file item
- It should enable the Translation foreign-language content from your extractions to English. Translation should be possible atleast from Chinese, French, Arabic, German to English.
- It should support Decoding and analysis of a single unified project, and avoid analyzing duplicated data. The extracted data should be presented under one project tree, and include various type of extractions from

multiple devices.

- It should support merging any extraction into a single project. All the following extraction types may be combined: Logical, advanced logical, file system, physical, SIM card, JTAG, SD Card, Camera Evidence.
- The ability to re-enable the user lock and restore the device to its original state
- It should support hash verification to ensure the extraction decoded is the same extraction received from the device.

B. Physical Extraction , Logical and Advanced Logical Support for Various Phones:

1. Android Phones :

- It should support 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. Physical extraction from these devices should be done, regardless of their OS version, and should not require any permanent rooting
- It should support Temporary root (ADB) solution for selected Android devices running OS 4.3-5.1.1
- It should support Enhanced physical extraction while bypassing lock of atleast 25 Samsung Android devices with APQ8084 chipset using bootloader method.
- It should support physical extraction of more than 140 LG models, such as the MS3330 and VS880. This method should additionally allow the removal and restoration of the user screen lock.
- It should support Physical extraction while bypassing user lock and decoding support for 19 Huawei devices based on Hisilicon Chipsets.
- It should support Extraction of data from many popular apps via File system extraction using Android backup APK Downgrade method
- Physical extraction and decoding support for the latest TomTom devices (including Go 1000 Point Trading, 4CQ01 Go 2505 Mm, 4CT50, 4CR52 Go Live 1015 and 4CS03 Go 2405)
- Supported content types include contacts, calls and locations, (triplogs are not supported)
- It should also support Physical extraction and advanced decoding, via USB debugging, for ALL Android OS versions including Android 4.X (Ice Cream Sandwich). 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 4.2 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:
  Facebook, Facebook Messenger, Google+, PingChat! (aka Touch), Skype, Twitter, Viber, Yahoo Messenger, Whatsapp, TigerText, Dropbox, QIP, Kik Messenger, Evernote, Kakao Talk, ICQ, Vkontakte
- It should support physical extraction and decoding support for an atleast the following latest Motorola devices, include: XT1080 Droid Ultra, XT1028 Moto G, XT1030 Droid Mini, XT1060 Moto X

2. 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 user)
- 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

3. Windows Phone :

- It should support physical extraction and decoding of devices running Windows Phone devices running OS versions 8.0 and 8.1 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.
- It should support Physical extraction while bypassing user lock as well as decoding support for 3 Nokia 105 devices (RM-1133, RM-1134 and RM-1135
- The Devices supporting Physical Extraction should atleast include HTC Pro, HTC HD2 T9193, Xperia X1, Nokia Lumia 520, LG GM750.
- It should support applications for Windows Phone devices running OS 8.1 including Facebook, Facebook Messenger, Waze, WhatsApp, ooVoo, Skype, Voxer, Kik and Odnoklassniki.
- It should support unallocated carving for windows phone

4. 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.

5. 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

6. 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 atleast 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

7. Chinese Chipsets Based Phones :

- It should have a connectivity box acts as the interface between the phone and the Tool, enabling the automatic pin-out identification. By selecting “Chinese phones physical extraction” , the phone pin-out should be detected and the extraction will start automatically
- Using proprietary boot loaders, it should perform a bit-by-bit physical extraction, from devices manufactured

with Chinese chipsets, including knockoffs, 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.
- It should support the chipset auto detection function allows users to identify devices supported by Tool.
- Tool should enable decoding support for MTK chipsets: (for Indication of the SIM slot which is used for incoming/outgoing SMS and calls). Spreadtrum chipsets (for File system reconstruction, Phonebook, SMS, calls, Bluetooth devices and SIM slot used for SMS and Calls)Infineon chipsets: (Physical extraction of the inserted SIM data, including artifacts that reside on the device).

8. IOS Phones :

- It should enables forensically sound data extraction, decoding and analysis techniques to obtain existing and deleted data from these **iOS Devices using either of Logical/ advanced Logical/ File system extraction Methods:** iPhone 2G,iPhone 3G, iPhone 3GS, iPhone 4, iPhone 4S, iPhone 5,iPhone 5S, iPhone 5C, iPhone 6, iPhone 6Plus, iPod Touch 1G, iPod Touch 2G, iPod Touch 3G, iPod Touch 4G, iPod Touch 5G, iPad Mini, iPad 1, iPad 2, iPad3, iPad 4.iPhone SE

9. 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.

C. Cloud Data Analysis Features:

- The software should allow access to remote Cloud data sources using Cloud login keys decoded from Android mobile devices, including non-rooted ones.
- The software should allow access to remote Cloud data sources using Cloud login keys decoded from locked Android devices.
- Decoding should be enabled from the following specific locked Android devices families
  - Samsung devices including Galaxy S4, Galaxy S5, Galaxy Note 3, Galaxy Note 4
  - LG devices including Nexus 5
  - The software should allow access to remote Cloud data sources using Cloud login keys decoded from iOS devices.
  - The software should allow access to remote Cloud data sources using Cloud login keys decoded from locked iOS devices.
  - The software should allow decoding of Cloud login keys from logical, file system and physical extractions of Android devices (phones and tablets)
  - The software should allow decoding of Cloud login keys from advanced logical extractions of iOS devices (phones and tablets)
  - The software should allow use of cloud keys from iOS and Android to gain access into cloud data from the following cloud services: (list not limited too)
    - Facebook
    - Twitter
    - Gmail
    - Dropbox
    - Google drive
    - Google contacts
    - Google location history
    - Google search history
    - Instagram
    - VK

    - One Drive
  - The software should allow use of credential (username and password) to gain access into cloud data from the following cloud services:
    - Facebook
    - Twitter
    - Gmail
    - Dropbox
    - Google drive
    - Google contacts
    - Google location history
    - Google search history
    - Instagram
    - VK
    - One Drive
    - iCloud Contacts, Calendar, Reminder, Notes, Photos and Videos, Purchased items
    - iCloud Drive
    - Any email service that support IMAP protocol
- The software should allow complying with legal authority by extracting only information in a certain time range.
- The software should allow complying with legal authority by extracting only information of a certain category
- The software should allow complying with legal authority by extracting only email messages that are read by the user
- The software should allow use of cloud keys from the mobile device and using cloud keys it should result in bypass of security mechanism such as two factors authentication imposed by the cloud service provider that prevent access to the data.
- The software should support reduction of extraction time from Cloud storage sources such as Google Drive, Dropbox, OneDrive and iCloud Drive by pre-selection of specific files and directories for extraction
- The software should support reduction of extraction time from email services by extraction of headers only.
- The software should support extraction of several files revisions from Cloud storage sources such as Google Drive, Dropbox
- The software should allow forensics preservation of cloud data
- The software should support extraction of the following content types from Facebook:
  Posts, Direct messages, Comments, Likes, Images, Videos, Files, Contacts, Embedded location information, Facebook Events
- The software should support extraction of the following content types from Instagram:
  Images and Video posts, Direct messages, Group messages, Comments, Likes, Contacts, Embedded location information
- The software should support extraction of the following content types from Twitter:
  - Tweets, Direct messages, Contacts and pending contacts, Embedded location information
  - The software should support extraction of the following content types from VK:
    Posts, Direct messages, Comments, Likes, Images, Videos, Files, Contacts, Check-ins
- The software should support extraction of the following content types from Gmail:
  - Messages with attachments
- The software should support extraction of the following content types from IMAP based emails:
  - Messages with attachments
- The software should support extraction of the following content types from Google Drive:
  - Images, Video, Files and documents, Embedded location information
- The software should support extraction of the following content types from Dropbox:
  - Images, Video, Files and documents
- The software should support extraction of the following content types from OneDrive:

    - Images, Video, Files and documents
- The software should support extraction of the following content types from iCloud Drive:
    - Images, Video, Files and documents
- The software should support extraction of the following content types from Google location history: Location information
- The software should support extraction of the following content types from Google search history:
    - Search history, Voice search history, Device history, Visited pages (when signed into chrome) history
- The software should support extraction of the following content types from Google contacts:
    - Contacts
- The software should support extraction of the following content types from iCloud:
    - Photos and Videos, Contacts, Calendar, Reminders, Notes, Purchased app
- The software should support normalization of different data sources into the same look and feel so the same filters may be applied on data from different sources.
- The software should support analysis of data according to the time zone defined by the investigator.
- The software should support analysis of data in a chronological order.
- The software should support easy review and analysis of all files extracted from the Cloud.
- The software should support analysis of extracted location information on a map.
- The software should support correlation between social media posts and their comments.
- The software should support correlation between emails that are part of the same thread.
- The software should support reporting of extracted data from the Cloud to human readable format such as PDF.
- The software should allow hiding of thumbnails from the human readable report to avoid presentation of improper information at court.
- The software should support reporting of extracted data from the Cloud to a machine readable format so it can be digested by other analysis systems.
- The software should support export of extracted location data to excel and kml formats

D. Link Analysis Application Feature :

- It should Reveal and visualize connections of up to 100 extractions from mobile devices (logical, file system and physical extractions) and external data sources per case .It should reveal communication links between multiple mobile devices based on a complete range of existing, hidden and deleted data types: mutual contacts, calls, SMS, MMS, emails, chats, apps messages, locations etc.
- It should allow to View common connections based on communications and locations, narrow data using advanced filters and search, tag data based on specific needs and highlight case related data using watch lists
- It should analyze mutual locations of mobile device users on a single map
- It should enable sharing of findings with other investigators.
- It should provide Dynamic analysis tool for all mobile, operator, third party and cloud* data