

POLICE



DEPARTMENT

**No. C1-7390/2020/FSL**

Forensic Science Laboratory,

Thiruvananthapuram

✉ [dirfsl.pol@kerala.gov.in](mailto:dirfsl.pol@kerala.gov.in)

☎ 04712721533

Dated. 12-10-2020

### **E-tender Notice**

#### **e-Government Procurement (e-GP) NOTICE INVITING TENDER**

The Director, Forensic Science Laboratory, Kerala Police Department, Government of Kerala invites online bids from reputed manufacturers/ authorized dealers or reputed vendors for the under mentioned **Cyber Forensic Tools for Forensic Science Laboratory and Regional Forensic Science Laboratories**. The bidders should comply with the following general conditions in addition to the additional conditions of the instant tender.

#### **General**

1. The Bidder should be a reputed Original Equipment Manufacturers (OEM) or authorized dealer of OEM, who is having an Authorization Certificate from the OEM to participate in the tender floated by Kerala Police. Certificate from the OEM for sales and service, to be produced.
  2. One bidder can not represent two suppliers/OEMs or quotes on their behalf in a particular tender.
  3. The OEM/Bidder should have a well equipped service centre functioning in India (preferably in Kerala) to cater to immediately after sales requirement; copy of Service Centre details must be enclosed along with Tender document. (Preferably bidder should have a Service Centre in Kerala/South India).
- 
1. A reputed vendor can participate in the tender provided the vending outfit is functioning in the market for at least 10 years.
  2. The Bidder should have valid GST registration. Copy of GST registration certificate should be enclosed along with the tender.
  3. The bidder should have valid PAN/Taxation Index Number. Copy of PAN/Taxation Index Number allocation letter should be enclosed along with the tender.
  4. The Bidder must fulfil the following minimum qualification criteria to prove the techno-commercial competence and submit the documents in support thereof:
    1. Valid Authorization letter from the OEM to attend this particular Tender.
    2. Certificate of Registration/Incorporation Certificate of the Bidder. c). Last 3 year's financial status of the Bidder's/P&L and Balance Sheet/audit report of last 3 years.



C1-7390/2020/FSL



b8cccf

1. The bidder (authorized dealer/distributor) should have the dealership/distributionship for at least 3 (three) continuous consecutive years with the OEM.
2. The Bidder has to submit a Warranty Certificate along with invoices. f). In case of a proprietary item, a certificate by the OEM to be attached.

SI No	Name of Equipment	Quantity Required
1	<b>Forensic DVR Examiner with 3 year licence</b>	1.00
2	<b>FRED Lap Top with one year licence</b>	1.00
3	<b>Forensic Tableau TX-1 Imager with 3 year warranty</b>	2.00
4	<b>Access Data FTK Latest version with 3year licence</b>	1.00

5	<b>Magnet Axiom with Magnet Cloud Module with 3 year licence</b>	1.00
6	<b>XRY Physical/Logical &amp; XAMN (Mobile Device and Cloud Storage Analysis Software/Hardware kit)with 3 year licence</b>	2.00
7	<b>UFED 4PC Ultimate (3 Years license)</b>	2.00
8	<b>Forensic Recovery of Evidence Device (FRED)</b>	3.00
9	<b>Encase Software- Latest version with 3 year licence</b>	2.00

		TENDER NO 12/2020-21 Dated
--	--	----------------------------



C1-7390/2020/FSL



b8cccf

1	Tender No. & Date	06/10/2020
2	Item	<b>Cyber Forensic Tools for Forensic Science Laboratory and Regional Forensic Science Laboratories</b> "
3	Quantity	List attached

4	Estimated Amount	Rs. 90 Lakhs
5	Tender Fees	Rs. 15530+GST =Rs.18325/-
6	Earnest Money Deposit	Rs. 90000/-
7	Date and time of publication of e-Tender	06/10/2020 06:00 PM
9	Date of submission of e-Tender	07/10/2020, 06:00 PM To 17/11/2020,12:00 NOON



C1-7390/2020/FSL



b8cccf

10	Last date and time for online submission of e-tender	<b>17/11/2020, 12:00 NOON</b>
11	Date and time of opening of e-Tender	18/11/2020, 3:00 PM

12	Place of opening	Forensic Science Laboratory, Thiruvananthapuram
13	Date, Time and Place of Technical Evaluation	<b>Will be informed later</b>
14	Bid Validity (Total Number of Days up to which the rates are to be firm)	180 days
15	Address of Tender Inviting Authority	Forensic Science Laboratory, Kerala, Vazhuthacaud, Thiruvananthapuram - 695010 Ph: 04712721533 e-mail: dirfsl.pol@kerala@gov.in Website: www.keralapolice.gov.in

- 1. Mode of submission of bids: - Online.** All Bid documents shall be submitted only in online procedure through the e-GP website [www.etenders.kerala.gov.in](http://www.etenders.kerala.gov.in) in their designated online covers. Details of covers are given separately. No other mode of submission shall be accepted and such tenders will be rejected outright.
- 2. Cover details: -** No. of covers - 2. i) Technical Bid cum and Financial Bid. The CMC/AMC/ATS after warranty period also to be quoted in the Financial Bid. In the case of Foreign Equipments, the rate must be quoted in Indian Rupees. The documents to be uploaded under each online covers are specified in the website.
- 3. Downloading of e-Tender documents: -** The tender document can be downloaded from the e-GP website [www.etenders.kerala.gov.in](http://www.etenders.kerala.gov.in) from the date and time of publication of e-tender onwards to last date and time for online submission of e-tender. Downloading of tender documents will not be possible after the date specified above.
- 4. Submission of e-Tender documents: -** The digitally signed tender document and other specified documents shall be submitted online through the

e-GP website [www.etenders.kerala.gov.in](http://www.etenders.kerala.gov.in) well in advance before the last date and time mentioned above. No submission shall be allowed after the last date mentioned above.

- 1. Payment of Tender Fees: -** A non-refundable tender fee shall be paid in online



C1-7390/2020/FSL



b8cccf

mode through the e-GP website [www.etenders.kerala.gov.in](http://www.etenders.kerala.gov.in) at the time of bid submission. No other mode of payment shall be accepted. **The tenders of bidders who do not remit fees through online will be rejected outright.**

2. **Payment of Earnest Money Deposit (EMD):** - The EMD shall be paid in online mode through the e-GP website [www.etenders.kerala.gov.in](http://www.etenders.kerala.gov.in) at the time of bid submission. No other mode of remittance shall be accepted.
3. **Exemption from payment of EMD:** - Bidders who are registered with Store Purchase Department, Kerala or National Small Scale Industries Corporation Ltd., New Delhi (for the items tendered) are exempted from submission of EMD. Those bidders claiming exemption shall submit valid registration certificate from the SPD, Kerala or NSSIC, New Delhi.

**Tenders of bidders who do not remit EMD online or do not upload documental proof (digitally signed) for exemption of EMD will be rejected outright.**

1. **Withdrawal and re-submission of e-Tender:** - The Bidders are at liberty to withdraw the submitted tender/documents and to submit fresh tender/documents till the last date and time of submission of the e-Tender after which withdrawal/re-submission will not be allowed.
2. **Opening of e-Tenders:** - The bids shall be opened online through the e-GP website [www.etenders.kerala.gov.in](http://www.etenders.kerala.gov.in) at the Police Headquarters, Vazhuthacaud, Thiruvananthapuram on the date and time mentioned above in the presence of the Bidders/ authorized representatives who wish to attend at the above address. If the tender opening date happens to be a holiday or non-working day due to any valid reason, the tender opening process will be done on the next working day at the same time and place specified. Any change in the opening date/time/venue due to other reasons shall be informed by way of Corrigendum published in the e- GP website. The Technical Bids will be evaluated by a Technical Evaluation Committee and those that do not conform to the specifications or to the satisfaction of the Committee will be rejected. The financial bids of the Technically qualified Tenderers only will be considered for opening. The date of opening of financial Bids will be intimated to the concerned technically qualified tenderers, over phone/Fax/e-mail. This will be with in 7 to 10 days of evaluation of technical bid.
3. **Technical Evaluation:** - All tenderers who quote for the supply of above equipment are required to be ready for live demonstration to be held in Forensic Science Laboratory, **TVPM and the date of the venue which will be intimated in due course. In the event of firms not able to show live**

**demonstration, they need to convince the Technical Evaluation Committee about such inability and resort to documentary/power point presentation with original product brochures/CDs/scale models/ videos/ slide shows etc. to the utmost satisfaction of the Technical Evaluation Committee.**

1. **All Bidders who participates in e-tender should produce hard copies of all relevant documents related to e tender at the time of technical evaluation, without fail.**

**1. Note to Bidders:**

- i. Bidders have to procure legally valid Digital Certificate (Class III) as per Information Technology Act, 2000 for digitally signing their electronic bids. Bidders can procure the same from any of the license certifying authority of India. For more details, please visit the e-GP website [www.etenders.kerala.gov.in](http://www.etenders.kerala.gov.in).
- ii. Bidders are advised to note the Tender\_Id and Tender No. & Date for future



- reference.
- iii. All uploaded documents should contain the signature and the office seal of the bidder/ authorized persons and should be digitally signed while uploading. Documents uploaded without digitally signing shall entitle rejection of the tender.
  - iv. In the case of Foreign Equipments, the rate should be quoted in Indian Rupees. Preference will be given to those who are ready to supply the item without opening Letter of Credit. Ordinarily, no advance payment will be made for procuring the above item. In case advance payment has to be made, a clear case has to be made out by the Tenderee. However this will be only on extraordinary circumstances.
  - v. For obtaining Digital Signature Certificate and help on e-tendering process, contact

Kerala State IT Mission, e-Government Procurement PMU & Helpdesk, Basement floor of Pension Treasury Building, Uppalam Road, Statue, Thiruvananthapuram; Ph: 0471-2577088, 2577188; Toll free no: 18002337315; e-mail:etendershelp@kerala.gov.in; Website: www.etenders.kerala.gov.in on all government working days from 9:30 am to 5:30 pm.

vi) The Director,Forensic Science Laboratory is empowered to reject any tender without assigning any reason.

- i. For any clarifications regarding the terms and conditions in this tender notice or the tender document, please contact Director,FSL , Or Manager FSL,

Thiruvananthapuram – 10 on all Government working days from 10:30 am to 5:00 pm.  
(Ph. No. 0471-2722136)(Ph. No. 0471- 2722155)



For any litigation relating to this order, the jurisdiction will be Thiruvananthapuram City.

## **Specification**

### **1. Forensic DVR Examiner WITH 3 YEAR LICENCE**

- Bypass DVR Passwords: The tool shall eliminate the need for any passwords menus and should have all the features of DME Forensics DVR Examiner.
- Non-Working DVRs: The tool shall be able to recover the video without the DVR machine
- The tool shall allow the retrieval of videos from the DVR hard drive directly
- The tool shall allow previewing the video directly from the application
- Facility for Sorting, Filtering and Date Adjustment for getting the adjusted DVR times to real time
- The extracted video-shall not be proprietary to the DVRs. The extracted video shall be playable using the openly available video players
- Whether extracting all videos or exporting a few clips, the tool shall be able to export



C1-7390/2020/FSL



b8cccf

- quickly in the background without switching the flash drives or CDs
  - It shall provide the report with all pertinent details keeping the track of what is exported and when
  - The DVR Examination tool shall be able to work for all DVR hard drives of the branded as well as unbranded DVRs.
  - The offered product should have facility to adjust Date/Time offset adjustment to adjust DVR times to real times
  - Support for 100+ DVR Proprietary File Systems including NVP\_3000P file system, new variant of the STL file system, UWARE\_264 file system, NAFS\_264, Mirage\_HiSi and Mirage\_IVNET filesystems
  - The tool shall support 1000+ DVR's
  - The DVR Examination tool should have facility to add Profiler of the unsupported DVR within the Software to add its support from OEM in future releases
- 
- Offered product should have at-least 4 Updates every year which should have new Features, File Systems, DVR's and Bug-fixes
  - Product Offered should be of International Repute
  - 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
  - Vendor has to provide demonstration of the complete solutions at site and provide ample training required.
  - Vendor should be in Business of Digital Forensics/Investigation and allied products & Services for minimum period of 5 (Five) Years

## 2.FRED Lap Top

Sr. No.	Features required	
1.	MOBILE FORENSIC WORKSTATION	<ul style="list-style-type: none"> <li>•Motherboard Chipset: Intel® Z370 Express Chipset</li> <li>•Motherboard</li> <li>•OS: Windows 10 Pro 64-bit</li> <li>•CPU: i7-9700K 8 Core 3.6GHz (4.9 Turbo), 12MB</li> </ul>
		<ul style="list-style-type: none"> <li>•RAM: 64GB PC4-19200 DDR4 2400</li> </ul>
		<ul style="list-style-type: none"> <li>•Graphics Card: NVIDIA GeForce RTX 2060 6GB GDDR6</li> </ul>
		<ul style="list-style-type: none"> <li>•Drive 1 - OS Drive: 512 GB M.2 NVMe PCIe Solid State Drive</li> </ul>
		<ul style="list-style-type: none"> <li>• Drive 2 - SATA Interface: 2 TB 5400 rpm SATA Hard Drive</li> </ul>



•Drive 3- Internal PCIe M.2 SSD Interface: To be available for future expansion

•Drive 4 - SATA Interface: To be available for future expansion

•External USB BR-RE/CDRW/DVDRW BluRay Burner Drive

Standard features:

Windows 10 Professional (64 bit)

Other Operating System included:openSUSE Tumbleweed (64 bit)

System Restore Media:

Bootable Blu-ray disc containing restore environment and factory configured operating system images.

Detailed Specifications:

- Intel Z370 Express Chipset
- 15.6" Full HD (1920x1080) IPS Display with G-Sync Technology, Matte Finish
- 1 RJ-45 LAN (10/100/1000Mbps)
- Intel Dual Band Wireless-AC 8265 - 802.11ac, Dual Band, 2x2 Wi-Fi + Bluetooth 4.2
- Card Reader 6-in-1 (MMC/RSMHC/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 – Illuminate
- Touch Pad pointing device(2 buttons)with multi-gesture and scrolling function
- Finger Print Reader
- 1 HDMI Port
- 2 Mini DisplayPort 1.3 ports
- 1 Thunderbolt 3 /USB 3.1 Gen 2 Combo Port (Type C)
- 1 USB 3.1 Gen 2 Port (Type C)

- 3 USB 3.0 ports (USB 3.1 Gen1)(1 x powered USB powered port, AC/DC)



C1-7390/2020/FSL



b8cccf



		<ul style="list-style-type: none"> <li>• 1 USB 2.0 Port</li> <li>• 1 Headphone jack (2-in-1 Headphone/S/PDIF Optical)</li> <li>• 1 Microphone jack</li> <li>• 1 Line-In jack</li> <li>• 1 Line-out jack</li> <li>• 8 Cell Smart Lithium -Ion, 82WH Battery Pack</li> <li>• Kensington Lock Slot</li> <li>• Universal AC Adapter (100~240V AC 50/60hz)</li> </ul>
2.	RUGGED CASE FOR KIT	<ul style="list-style-type: none"> <li>• Above all Material should be skillfully packed in Pelican case with Lid Organiser</li> </ul>
3.	REMOTE FORENSIC ACCESS SOFTWARE	<ul style="list-style-type: none"> <li>• Software to provides direct, live, read-only access to the remote target computer's disks, volumes, and in certain cases physical memory. All access should be of the physical level with no file level locking, should give access to any and all content on the remote target, including protected system content (Registry files, Email PSTs, Database Files, etc)</li> <li>• Vendor Neutral Software to work on cross OS platforms with variety of Forensic Software Tools</li> <li>• Should support for AES 256-bit Encryption for connections</li> <li>• Should works with all RAID disks, physical drives, logical volumes, and physical memory</li> <li>• Dual dongle solution to place a licensing dongle in both the</li> </ul> <p>Forensic Machine and subject machine for secure remote write blocked access</p>
4.	WARRANTY	<ul style="list-style-type: none"> <li>• Product should carry 3 (Three) Year On-Site Warranty.</li> <li>• Any Software/ Firmware updates to be provided during the Warranty Period.</li> </ul>
5.	OEM	<ul style="list-style-type: none"> <li>• Tender Specific Authorisation Certificate from OEM is</li> </ul>

	AUTHORIZATION	Mandatory to participate in Tender in favour of Indian Distributor/ Reseller/ Bidder.
6.	TRAINING	<ul style="list-style-type: none"> <li>• One Day OEM Training with OEM Certification to be provided with each Machine to 1 Person at the time of Installation &amp; Training.</li> <li>• Training to be done by OEM Certified Engineer.</li> </ul>



C1-7390/2020/FSL



b8cccf

7.	PAST EXPERIENCE OF THE BIDDER	<ul style="list-style-type: none"> <li>• Bidder should have provided similar solution to at-least 3 Indian Government Organization in past.</li> <li>• Bidder should have 10 Years of experience working with Indian Government Organizations.</li> </ul>
----	-------------------------------	---

## 1. Forensic Tableau TX-1 Imager 3 YEAR WARRANTY

Forensic Imager should meet below specifications:

- High performance, reliable, and easy to use forensic duplicator - with a high resolution, touch screen User Interface (UI).
- It should support forensic imaging of SATA, USB 3, PCIe, SAS, FireWire 800, IDE, and network shares
- Outputs to SATA, USB 3, SAS, and network shares
- Supports up to two active forensic jobs at a time (simultaneous imaging)
- Supports up to four destinations per source with the ability to mix clone/image duplication and local/network destinations
- Job queuing option for efficiency and convenience
- Disk-to-File Duplication (Compressed .e01 & .ex01), Disk-to-Disk Duplication (Cloning), Compute Hash Values, Verify Hash Values, HPA/DCO Disable, Blank Check Drives, Format Drives, Wipe Drives, Display, Print, and Save Logs, Secure User Profiles
- High-resolution, color touch screen user interface, used to control and monitor ongoing operations. wizard driven UI uses simple touch gestures to select and initiate all functions
- Supports collecting data in a forensically sound (a.k.a. "write-blocked") manner.
- Network based forensic acquisitions, remote triage applications, or network based "write blocking",
- There are instances when central command may want or need to preview or collect data from a

storage device located thousands of miles away. When used as a network- based write blocker. View Drives and Collect Evidence as a Remote Write Blocker

- Imaging of all Mac Machines without the need to remove the Hard Drive from the mac machine.
- Kit should contain the below adapters & cables;
  - PCIe Card SSD Adapter
  - PCIe M.2 SSD Adapter
  - PCIe Apple SSD Adapter
  - mSATA and M.2 to SATA Adapter Kit
  - PCIe IDE Adapter Kit
  - Thunderbolt to Firewire Adapter for Mac Acquisition
  - USB C to USB Cable for Mac Acquisition
- All of content of the kit should be skilfully bundled in a rugged pelican waterproof case perfect for field or lab acquisition
- 3 years warranty



## 4. Access Data FTK Latest version WITH 3 YEAR LICENCE

•



Easy-to-use GUI with automated preprocessing of forensic data.

- The broadest OS support and analysis on the market.
- Advanced filtering and automated data categorization.
- Do it all. Preview, acquisition, mounting and analysis of live data.
- Flexibility. Available as a perpetual or subscription license.
- Native support for Volume Shadow Copy.
- Comprehensive volatile memory analysis.
- Add-on Cerberus for automated malware analysis and triage.
- Password cracking through PRTK/DNA.
- Visualization capabilities allow graphic analysis of file and email data.
- Integrated Computer Forensic Solution.
- Unmatched Processing.
- Handle massive data sets without crashing or losing work.
- Feature rich out of the box.



- Fast, Comprehensive index and Binary searching.
- File and Disk Encryption Support.
- Advanced gallery view for images and video with eid.
- Superior Email Analytics.
- Single-Node enterprise (Remote Investigation).
- Volatile and Memory Analytics.
- Internet Artifact Analytics.

## 5.Magnet Axiom with Magnet Cloud Module 3 YEAR LICENCE

- Should Support data acquisition from different devices and operating systems
- Should Support different drive types, including HDD, SSD, SD flash and USB
- Should Support Windows, OS X and Linux, iOS and Android
- Should Support acquisition from NTFS, HFS+, HFSX, EXT2, EXT3, EXT4, FAT32, EXFAT, YAFFS2, F2FS, APFS
- Ability to select different formats for the obtained image files, including .RAW,

.E01, .ZIP.

- Ability to select different types of image to be obtained, including physical image, logical image or targeted image.
- Ability to acquire all memory data from Windows system and Simplified expedite memory analysis with Volatility, which is fully integrated into the offered solution
- Support data acquisition from Android devices using ADB and more advanced methods.
- Ability to acquire the full image from LG devices using Download mode
- Ability to acquire the full image from Motorola devices using Bootloader Bypass methods
- Ability to acquire the full image from Samsung devices using Recovery images
- Support full image acquisition and password bypass from devices with MTK chipsets
- Support full image acquisition and password bypass from devices with Qualcomm Chipset using EDL mode
- Support data logical acquisition from Kindle devices
- Support data logical acquisition from iOS devices and save the image as .zip
- Ability to analyze data from forensic image file formats i.e. E01, Ex01, L01, Lx01, .AD1, .DD, .RAW, .BIN, .IMG, .DMG, .FLP, .VFD, .BIF, .VMDK, .VHD, .VDI,

.XVA, .ZIP, .TAR.

- [Computer] Ability to analyze memory dumps in the format of .RAW, .CRASH,

.VMSS, .HPAK, .ELF, .MEM, .DMP, .DD, .IMG, .IMA, .VFD, .FLP etc.



- 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.
- Multiple Device Queueing – Automatically process multiple devices in a row without the need for examiner-run separate process.
- End-to-end experience that brings together acquisition, processing and analysis, creating integration and a more navigable and manageable digital evidence database
- Support for a broad array of artifact types, and support for the latest versions of those apps and artifact types. Process and recover 1,000+ artifacts.
- Access to file system, registry and artifacts data and trace artifact evidence to its source data efficiently for a better verification process
- Filter stacking allows you to layer on several dimensions of filter criteria to pinpoint specific items in a large dataset.
- Ability to view SQLite database files using built-in SQLite viewer
- 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.
- ability to identify luring and sexual conversations as well as images that contain drugs, weapons, and nudity. machine learning technology, searches both text-based and media content to automatically identify nudity, weapons, drugs, and sexual conversations
- Support case dashboard that displays high level details about the case, evidence sources and summaries of processed results of multiple digital evidence in one screen.
- **Visualize connections between files, users, and devices.** Discover the full history of a file or artifact to build case and prove intent. Visualizes evidence

from disk and memory to show where files came from, who they are connected to, and where they're stored.

- Should also review text-based evidence to uncover potential sexual conversations. By automatically detecting these key pieces of evidence from an overwhelming amount of possibilities.
- 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.
- Add hash sets to either filter out non-relevant files to enhance search performance and reduce false positives or add hash sets that will specifically call out and identify known bad pictures and videos.
- Enhanced searching, sorting and filtering – search, sort and filter 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.
- Support multiple data views, including Column/Table view, Summary Row view, World Map view, Timeline view, Chat Threading view and Histogram view.
- Support to export & merge portable case and share with other stakeholders without the need for the software license or the need to install the software, the user can select different types of items to be included according to tags, comments and categories.
- Should have a feature to reduce overexposure to illicit/ disturbing content extracted to protect improve investigator wellness. These features are 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

- Should be capable to acquire evidence from the cloud, by sign in to an account with the target's user name and password.
- For twitter platform, it should be capable to acquire activity that is accessible to the public by using just twitter user name.
- Should be capable to acquire evidence from the following cloud platforms and services: Apple, Box.com, Dropbox, IMAP/POP Email, Facebook, Google, Instagram, Microsoft, Slack, Twitter, and WhatsApp
- Offered solution should come with OEM training for 02 days

## 6.Forensic Recovery of Evidence Device (FRED)

Processor 3.8/4.4 GHz, Intel i7-9800X, 8 Core, 16.55 MB Cache or higher Memory 64 GB PC4-21300 DDR4 2666 MHz

Software Microsoft Windows 10 Professional, 64-bit OpenSUSE Linux 64-bit Symantec Ghost

Graphics & Video Support Nvidia GTX 1050Ti, 4GB, 128-bit GDDR5, 768 CUDA cores Storage 512 GB NVMe PCIe SSD (OS)

512 GB SSD SATA III (Database/Cache/Temp) 4 TB SATA III 720 RPM HotSwap (Case/Data)

Extra Storage Slots 4 HotSwap Drive Bays 2.5"/3.5" SATA III (USB 3.1 connected)2

HotSwap Drive Bay 2.5"/3.5" SATA III (SATA connected) 1 NVMe SSD

Storage Controller Intel 6 Gb/s SATA (8) Intel M.2 x 4 PCIe Socket (2) RAID Controller 12 Channel PCIe 12 Gb/s SAS/SATA

Forensic Imaging & Write Blocking: UltraBay 4d hardware write blocked imaging of SATA, SAS, USB 3, IDE, Firewire and PCIe SSD devices

Single or multiple (concurrent) forensic imaging of storage devices

Convenient front panel write blocked or read/write switch for general drive management UltraBay 4d touch-screen user interface. Displays device details, display and manage LUNs and HDD protected regions. Examine file partitions.

Tableau Imager (TIM) pre-installed

DVD/CD/Blu-Ray BD-R/BD-RE/DVD±RW/CD±RW BluRay burner, dual-layer combo drive

Accessories: Forensic toolbox including adapters and cables: (SAS, SATA, IDE, microSATA, SATA LIF, MacBook Air Blade, PCIe SSD m.2 NVMe, PCIe SSD MacBook Pro (2013 and newer) and server class PCIe SSD

Precision electronics tool kit with assorted bits for opening enclosures

### **·Should be forensically sound and maintain the original evidence integrity.**

- **Should be the latest version at the time of supply**
- **1 year product warranty and onsite training should be provided**

#### 1. XRY Physical/Logical & XAMN (Mobile Device and Cloud Storage Analysis



C1-7390/2020/FSL



b8cccf

## **Software/Hardware kit) WITH 3 YEAR LICENCE**

All in one mobile forensic system designed for analysis of mobile phones & cloud storage should contain the following

Application Software for (logical extraction/physical extraction/Viewing, analysis & reconstruction of mobile phone and cloud data), Briefcase with Cable Organizer, Communication Unit, Mobile Phone Cable Kit, Photon Camera, SIM id-Cloner Device, Rewritable SIM id-Cloner Examination Cards, Write Protected Universal Memory Card Reader, Cleaning Brush & Accessories

### **Software should be capable of**

- Logical and Physical Extraction/Analysis and reconstruction of data in Mobile devices, Tablet & GPS Devices Examinations and Capable of integrating and using devices like Android PiDumper as future add-on when required.
- Photon option and camera, which supports mobile app that allows us to take screenshots and makes standard Android gestures like reading a chat by swiping over all messages.
- Memory Card Logical and Physical Examinations
- SIM Card Reading and Cloning
- Physical dump in Secure .XRY file format with forensic log
- Hash Algorithms
- File Signature Analysis
- Selective Extraction of Data
- Bypass or Recovery of Passcodes
- Reconstructed and Deleted Data
- Device Dump and Binary Importing
- Smartphone App Support
- Windows Based Software Solution
- Unique Help File for Every Device
- Easy Data Extraction
- HEX Analysis of Data
- Hash Algorithms
- Clone SIM Cards
- Convert Old XRY Files
- Geographic, Timeline, Chat and Connection View
- Bundled with 128 GB USB Flash Drive.

### **·Should be forensically sound and maintain the original evidence integrity.**

- **Should be the latest version at the time of supply**
- **3 year product warranty and onsite training should be provided**

#### **1. UFED 4PC Ultimate (3 Years license)**



C1-7390/2020/FSL



b8cccf

UFED 4PC Ultimate is enabling users to perform extraction, decoding, analysis and reporting on a single platform. It performs physical, logical, file system and password extraction of all data, including hidden and deleted, from the widest range of devices including legacy and feature phones, smart phones, tablets, phones manufactured with Chinese chipsets, portable GPS devices and memory cards.

UFED Device Adapter: It enables:

- Device Extraction via USB and RJ 45
- SIM Clone and extraction
- Extraction via embedded Bluetooth module

UFED 4PC Ultimate is a versatile solution that runs on existing hardware alongside other third-party software. It comes with a range of applications, invaluable for investigators to close cases faster:

- UFED Physical Analyzer – Powerful application for decoding, analysis and reporting
- UFED Phone Detective – Instant mobile phone identification. Also available as a mobile app for iOS and Android
- UFED Reader – Free application for report sharing with any authorized personnel

UFED 4PC Ultimate should operate with a USB software license dongle.

## 9. Encase Software- Latest version WITH 3 YEAR LICENCE

**Enhanced indexing engine:** Empowers investigators to conduct investigations with powerful processing speeds, advanced index searching, comprehensive language support and optimized performance

**Easy reporting:** Provides customizable templates to help examiners create compelling, easy to read, professional reports that can be shared for every case **Extensibility:** Offers extensibility through EnScripts, which are automated code commands that streamline and automate tasks and extend the capabilities of EnCase Forensic to help the examiners complete investigations more efficiently

**Workflow automation:** Delivers automated investigation workflows so examiners can easily navigate through EnCase Forensic to enhance how they uncover evidence

**Updated encryption support:** Provides encryption support for Microsoft® Windows® 10 Bit locker XTS-AES, Dell® Data Protection 8.17 and Symantec™ PGP v10.3; investigators can acquire encrypted evidence without worry about data corruption, damage or unnecessary delays

**Apple File System (APFS) support:** Supports APFS, the file system used in helping investigators conduct targeted data collections from APFS and send the output as an EnCase logical evidence file

**Volume shadow copy capabilities:** Examines Volume Shadow Snapshot (VSS) backups, also known as volume shadow copies, generated by Microsoft Windows,





allowing investigators to recover deleted or modified files, as well as full volumes and learn what may have taken place on a system before the investigation

**Apple T2 Security Bypass:** Acquires machines equipped with Apple T2 Security chips without additional hardware, drive partitions, or hassle. And if the user is logged in, no credentials are required

**Others:** EnCase software uniquely supports the imaging and analysis of RAID arrays, including hardware and software RAIDs. **It should provide Hardware Analysis, Recover Folders, Log and Event File Analysis, Symbolic Link Analysis, Compound Document and File Analysis, File Signature Analysis Built-in Registry Viewer, Proximity Search, Internet and Email Search,** Internet and Email investigation



C1-7390/2020/FSL



b8cccf

*J. Latha Devi*

Latha Devi M A  
Director



C1-7390/2020/FSL



b8cccf