

Electronics Corporation of India Limited
(A Government of India enterprise)
Antenna Products & Satcom Division
Hyderabad – 500062 (Telangana) India
Telephone: 91 40 2712 0017, 2718 2230
Fax: 91 40 2718 2373
E mail: apd_purchase@ecil.co.in


TENDER NO: ECIL: AP&SD: PUR: 14-5142

Date: 20-02-2017

TABLE OF CONTENTS OF THIS DOCUMENT

SL.No.	DOCUMENT DESCRIPTION	NO. OF PAGES.
1.	Table of Contents of Document	1 of 51
2.	Cover Page	2 of 51
3.	Tender Document	3 to 10 of 51
4.	Technical Document	11 to 51 of 51
	Total No. of Pages.	51

Cover page to the Tender Document

	<p align="center">ELECTRONICS CORPORATION OF INDIA LIMITED (A Government of India Enterprises) Antenna Products & Satcom Division , ECIL (PO), Hyderabad – 500 062</p>
---	---

Name of Organization	Electronics Corporation of India Limited, Hyderabad – 500 062 (Telangana) India		
Type of Organization	Public Sector Undertaking		
Tender Ref. No:	ECIL:AP&SD:PUR:14-5142		
Tender Title:	Supply of Cyber Forensics Tools and Equipment as per enclosed Tender Document		
Product Category:	Cyber Forensics Tools		
Document Cost:	Rs. 1000/- (Rupees One Thousand only)		
Tender Value:	EMD: Rs.2,00,000/-	Security Deposit: @10% of order value	
Tender type:	Buy		
Location:	Hyderabad (Telangana)		
Request for quote date:	On or before due date		
Last date for submission of bid:	06.03.2017 at 14.00 Hrs		
Opening date of part I	07.03.2017 at 14.00 Hrs		
Description of item:	Supply of Cyber Forensics Tools and Equipment	Quantity	
		1 Set	
Pre-Qualification:	<u>As per specifications given in the tender</u>		
Tender Document:	<u>View Tender Document *</u>		
Bid Document:	<u>View Price Bid Document *</u>		
Technical Document:	<u>View Technical Document*</u>		
Sector:	Electronics		
State:	Telangana		
For further Information contact: S r . DGM, IMM, AP&SD,ECIL			
E-Mail:	apd_purchase@ecil.co.in		
Phone:	+94 - 40 – 2712 0017 / 2718 2230		
Fax:	+91 -40 – 27182373		

Electronics Corporation of India Limited
(A Government of India enterprise)
Antenna Products & Satcom Division
Hyderabad – 500062 (Telangana) India
Telephone: 91 40 2712 0017, 2718 2230
Fax : 91 40 2718 2373
E mail: apd_purchase@ecil.co.in

Tender No: ECIL/AP&SD/PUR/14-5142

Tender Document

1. Invitation to Tender:

Electronics Corporation of India Limited, Antenna Products & Satcom Division (AP&SD) invites "Two part Bid" for as per details given below.

2. Important Dates :

Due date for submission of Two Part Bids : 06-03-2017 up to 14-00 Hrs.

Techno- commercial bid (part 1) will be **opened on 07-03-2017 at 14-00Hrs.** Interested vendors may be present with prior permission.

After evaluation of the techno commercial bids, qualified list of vendors will be finalized.

Price bid (part 2) of the qualified vendors will be opened at a later date, which will be communicated to the qualified vendors.

Clarifications can be obtained through mail.

3. Manner and method of submission of offers:

All pages of the tender shall be numbered and typed on the letter head of the vendor and be duly signed and stamped by company's authorized signatory. Hand written quotation will be summarily rejected. Corrections if any shall be duly authenticated with signature and seal of the company.

The quotation in prescribed form to this invitation shall be submitted in two parts and in different sealed envelopes super scribing tender number with due date. Quotations can be sent via email as password protected file. Password will be shared once technical evaluation is completed .

Part-I (Technical Bid); It shall comprise of two sections namely technical section and commercial section and both sections shall be submitted along with tender fee and EMD in a single sealed envelope. **This bid shall not contain any price details.**

Part-II (Price Bid): It shall comprise of price details and shall be summated in a sealed separate envelope.

The above two sealed envelopes of Part-I & Part II shall be put in a single sealed envelope and submitted to the attention of Senior Deputy General Manager / IMM, AP&SD, ECIL Post, Hyderabad - 500062, Telangana, India.

4. Cost of Tender Documents:

Tender fee of **Rs.1000/-** is to be remitted along with the techno commercial bid in the form of a crossed bank draft favoring Electronics Corporation of India Limited" from a nationalized bank payable at Hyderabad. The cost of tender document is non-refundable.

5. Earnest Money Deposit (EMD):

Earnest money deposit of Rs. 2,00,000/- shall be submitted along with the techno-commercial bid in the form of demand draft favoring Electronics Corporation of India Limited or a Bank Guarantee valid for a period of six months from a nationalized bank payable at Hyderabad. The EMD deposited by the unsuccessful bidders will be appropriated towards security deposit. The bids will not be considered in the absence of payment towards the cost of tender document and EMD.

6. Security deposit(SD):

The successful bidder will be required to remit a security deposit equivalent to 10% of the purchase order value exclusive of taxes and duties etc. after adjusting the EMD amount already remitted. SD is to be remitted along with the order acceptance in the form of a crossed bank draft favoring Electronics corporation of India limited or a Bank Guarantee from a nationalized bank payable at Hyderabad. The security deposit will be forfeited in the event of failure to execute the purchase order. The security deposit will be refunded without interest after the purchase order is successfully executed to the satisfaction of the purchaser.

7. Items tendered for:

SI No	DESCRIPTION	QUANTITY REQUIRED	
1.	Forensic Recovery Evidence Data Center (FRED C), make- Digital Intelligence	1	1 Set
	Network Printer	1	
	Forensic Analysis client workstations	5	
2.	IDE/SATA to USB 2.0/3.0 converters ,make - Digital Intelligence	1	
3.	UFED Touch Ultimate (Ruggedized Kit) with CHINEX with UFED Cloud Analyzer, make – Cellebrite		1 Set
4.	Forensic Falcon , make- Logicube	1	1 Set
	Evidence Disk Drives	19	
5.	Passware Kit Forensics Lab Edition 2016 v.4 , make – Passware	1	1 Set
	Password Kit Agents PCs	5	
6.	Forensic Tool Kit v6 Standalone – Perpetual License –make, Access Data –	1	1 Set
	Toolkit Server PC	1	
7.	Latest version of Digital Evidence Investigator, make – ADF Solutions.	1	
8.	e-mail Examiner v7.1, make – Paraben	1	
9.	Latest version of F-Response Consultant Edition	1	
10.	Latest version of Adroit Photo Forensics tool , make- Digital Assembly	1	
11.	Latest version of Stego Flash , make- Wet Stone	1	
12.	Network Email Examiner 4.1, make – Paraben	1	
13.	Latest version of Chat Examiner, make – Paraben	1	
14.	Latest version of SIM Clone Package (including blank SIM cards) , make – MOBILedit	5	Set
	BlankSIMCards	200	
15.	ESD safe Workstation desks/cubicles	4	Set
	ESD safe chairs	10	
	ESD Safe racks	3	
16.	Forensics Lab Information Management System (F-LIMS)	1	
17.	Biometric Access Control System	1	

Intending bidders who have not yet registered with ECIL are also requested to download “Suppliers Registration Form” from web [site www.ecil.co.in/tenders](http://www.ecil.co.in/tenders), fill it up and send the same along with the bids.

TENDER SUBMISSION FORMAT (PRICE BID DOCUMENT)

Tender No. : ECIL/AP&SD/PUR/14-5142

Date: 20-02-2017

I Vendor Particulars:

Name and address of the bidder	
Telephone, fax and e-mail	
Name and designation of the office representing vendor	

II Item tendered for:

SI No	DESCRIPTION	QUANTITY REQUIRED	
1.	Forensic Recovery Evidence Data Center (FRED C), make- Digital Intelligence	1	1 Set
	Network Printer	1	
	Forensic Analysis client workstations	5	
2.	IDE/SATA to USB 2.0/3.0 converters ,make - Digital Intelligence	1	
3.	UFED Touch Ultimate (Ruggedized Kit) with CHINEX with UFED Cloud Analyzer, make – Cellebrite		1 Set
4.	Forensic Falcon , make- Logicube	1	1 Set
	Evidence Disk Drives	19	
5.	Passware Kit Forensics Lab Edition 2016 v.4 , make – Passware	1	1 Set
	Password Kit Agents PCs	5	
6.	Forensic Tool Kit v6 Standalone – Perpetual License –make, Access Data –	1	1 Set
	Toolkit Server PC	1	
7.	Latest version of Digital Evidence Investigator, make – ADF Solutions.	1	
8.	e-mail Examiner v7.1, make – Paraben	1	
9.	Latest version of F-Response Consultant Edition	1	
10.	Latest version of Adroit Photo Forensics tool , make- Digital Assembly	1	
11.	Latest version of Stego Flash , make- Wet Stone	1	
12.	Network Email Examiner 4.1, make – Paraben	1	
13.	Latest version of Chat Examiner, make – Paraben	1	
14.	Latest version of SIM Clone Package (including blank SIM cards) , make – MOBILedit	5	Set
	BlankSIMCards	200	
15.	ESD safe Workstation desks/cubicles	4	Set
	ESD safe chairs	10	
	ESD Safe racks	3	
16.	Forensics Lab Information Management System (F-LIMS)	1	

17.	Biometric Access Control System	1
-----	---------------------------------	---

III **Terms and Conditions.**

1	Terms of price	
2	Payment terms (Please refer general Terms and Conditions of this tenders)	
3	Rate of Excise Duty, Service, and any other Taxes and duties applicable (in case Vendor imports any item directly Customs duty exemption will not provided by ECIL) Note: Vendor shall specifically mention applicability of all taxes and duties. In the absence of specific confirmation of Taxes and duties, the quotation is liable to be rejected.	
4	Preferred delivery period should not be more than 8 weeks	
5	Standard warranty of 3 years for all items except the ESD Safe Workstation desks/ cubicles, chairs and racks where in standard OEM warranty is acceptable	
6	Estimated Packing & forwarding charges.	
7	Validity of quotation (minimum 90 days)	
8	DD No. & Date for Cost of Tender Documents	
9	DD No. & Date for EMD	
10	CST Registration No.	
11	TIN No.	
12	Income Tax PAN No.	
13.	ISO – 9000 Certificate or any other Certification	
14.	SSI / NSI Registration No., if applicable.	
15.	Any other relevant information	

NOTE: The Vendor shall submit offer in the above format only. Against each instructions mentioned below the vendor shall give a comment complied (✓) or Not complied (x)

Instructions :

- a) No column shall be left blank in the format.
- b) Incomplete counter offer and deviation from the Terms and Conditions will be summarily rejected.
- c) Photostat copies of quote / offer will not be accepted. Only originals received within the time limit will be accepted.
- d) The vendor shall submit the certificate of registration under micro, small and medium enterprises development Act, 2006, in case of applicability.
- e) The offer shall meet point wise compliance to all points of Tender document, wherever non-compliance is there, suitable explanation needs to be provided.
- f) Technical proposal need not be restricted to the user requirements as given above. Any additional features may be added in the proposal to make it a professional package.
- g) Technical proposal may be as detailed as possible with functional block diagram where ever applicable.
- h) Foreign vendors shall offer bids directly or through their Indian Partners / Representatives.

General Criteria for acceptance of Tenders:

- 1. **Technical Specification:** Vendor shall comply with the Technical specification given in the Technical Document. The commercial offer of the Vendor who satisfies the technical requirement only will be opened -complied / not complied.
- 2. **Experience :** Vendor shall provide details with documentary evidence the experience in supply of similar systems - complied / not complied.
- 3. **Special Term:** Item wise L1 can be selected and ECIL has right to buy item wise. Suppliers not having products for all the items can submit the quote for their products/parts only.
- 4. **Warranty :** Standard warranty of 3 years for all items except the ESD Safe Workstation desks/ cubicles, chairs and racks where in standard OEM warranty is acceptable – complied / not complied.
- 5. **Foreign Vendors** shall have a Branch Office in India / Indian Partners / Representatives rendering support service – complied / not complied.
- 6. **Facilities :** Details of factory assembly and Testing facility shall be furnished. A committee of ECIL may visit to verify the facilities of the vendors for execution of Order if any .
- 7. **Service Centre :** Details of Service Centre location / Engineers working.
- 8. **Acceptance of Tenders :** No Tender will be accepted after due date. ECIL will not be responsible for postal / courier delay or lost in transit if any.

Note: Vendor shall provide documentary proof to prove his adherence to the qualifying criteria where ever necessary. Claims without support will not be considered.

GENERAL TERMS AND CONDITIONS

This Tender and any order resulting from this tender shall be governed by the following Terms and Conditions of the contract and the supplier quoting against this tender shall be deemed to have read and understood the same. In case counter terms and conditions of business have been offered by the supplier, ECIL shall not be deemed to be governed unless specific written acceptance thereof has been obtained from ECIL.

1. **Terms of Price** : Quotation shall be submitted on FOR Hyderabad or FOR destination basis including Transit insurance. In case of ex-works / Ex-godown / FOR dispatching station the approximate packing, forwarding and freight shall be indicated by the suppliers. Hyderabad suppliers shall arrange free delivery at our Stores.
2. **Validity of Quote** : The quotation shall remain valid for a minimum period of 90 days from tender opening date.
3. **Performance Bank Guarantee** : Vendor shall submit a performance bank Guarantee for 10% of Purchase order value covering standard free warranty period of 3 years from the date of acceptance of goods by ECIL.
4. **Payment** : For Item No. 15 (ESD Safe Workstation desks/ cubicles, chairs and racks) – 100% payment after delivery within 60days. For all other items except Item No. 15 - 90% payment within 60 days after the delivery and acceptance at ECIL and 10% after the completion of I&C.
5. **Insurance** : The supplier shall ensure goods for all transit risks if the payment terms is FOR Hyderabad or FOR destination unless otherwise stated specifically by the supplier in their quotation. The supplier shall ensure goods for all risks till acceptance of goods by End User.
6. **Liquidated Damages** : Delivery date is the essence of the contract. In the event of any delay in supply beyond the agreed delivery schedule, liquidated damages will be recovered @ 0.5% for week of delay or part thereof subject to maximum of 10% of the value of the order.
7. **Force majeure** : If the execution of Purchase Order is delayed beyond the period stipulated in the Purchase Order as a result of out break of hostilities, declaration of any embargo or blockage or fire, flood, acts of nature or any other contingency beyond the suppliers control due to act of God ,then ECIL may allow such additional time by extending the delivery period as justified by the circumstances of the case and its decision in this regard shall be final. Power failure will not be considered as a force majeure condition.
8. **Risk Purchase**: In case of failure to deliver the goods within the delivery date stipulated in the

purchase order unless prior extension of delivery period is obtained, ECIL will be at liberty to obtain such items as necessary from other source or cancel the order and in either case ECIL reserves the right to recover from the supplier the additional amount spent plus 10% to cover incidental expenses.

9. **Dispute resolution:** Any dispute arising out of purchase order or interpretation of any clause or terms and conditions hereof shall be settled through conciliation by both ECIL and the supplier, under the specific provision of arbitrational and conciliation act 1996. Only courts in Ranga Reddy district, state of Andhra Pradesh, India have exclusive jurisdiction over this order.
10. **Right to reject:** The purchase reserves the right to reject any or all offers wholly or in part without assigning any reason.
11. **Short closure:** ECIL has the right to short close the tender even after evaluating the quotations without assigning any reason.
12. **Bank details:** The supplier shall give along with the quotation name of their banker, account number and also income tax permanent (PAN).
13. **Jurisdiction:** All disputes arising in connection with executing the purchase order will be subject to jurisdiction of the courts in Hyderabad and Secunderabad only.

Technical Document

Latest version of ADF Digital Evidence Investigator

- Should accommodate the full investigative workflow from file and artifact acquisition, to data analysis, to comprehensive reporting
- Should be Highly configurable artifact and file collection, including internet and communication artifacts
- Should Rapidly search suspect media using large hash sets (>30 million), including Project VIC and CAID integration
- Should allow Powerful keyword and regular expression search capability to find relevant files and artifacts
- Should Display provenance, including comprehensive metadata, of all relevant files and artifacts
- Should allow Comprehensive video preview and frame extraction
- Should Recover images from unallocated drive space
- Should allow Unique timeline that combines files, actions and people into a single view
- Process NTFS, FAT, HFS+, and EXT file systems
- Provide powerful reporting capabilities (HTML and CSV)
- Access internal storage that cannot be easily removed from computer
- 64-bit architecture to deliver high performance and scalability
- Portable standalone viewer to easily share results with others
- Should be Single device to triage computers using Windows, Macintosh, or Linux platforms
- Should allow Viewing evidence immediately
- Should allow Powerful search capabilities
- Should allow Comprehensive reporting
- Should Scan multiple computers simultaneously with a single license
- Should scan suspect computers and prioritize cases for full forensic examinations.
- Should allow Live analysis of computers running Windows
- Should be Fully configurable collection of artifacts
- Should allow Reuse and share forensic intelligence
- Support Advanced image analysis
- Should be Forensically sound
- Should parse videos for immediate analysis
- Capable of integrating advanced search and image analysis capabilities to identify negative computers quickly.

➤ **Should at least support the following minimum requirements for Computer Architectures/ Operating Systems / File systems**

Operating system	Powered-OFF target computers	Powered- ON target computers
Windows XP	✓	✓
Windows Vista 32bit and 64bit	✓	✓
Windows 7 32bit and 64bit	✓	✓
Windows 8 32bit and 64bit	✓	✓
Windows Server 2003 32bit and 64bit	✓	✓
Windows Server 2008 32bit and 64bit	✓	✓
Ubuntu Linux (EXT2, EXT3, EXT4)	✓	

Red Hat Linux (EXT2, EXT3, EXT4)	✓	
Apple MAC with Intel Processor, Mac OSX, HFS, HFS+	✓	

- Should support system capture that scans a computer for known artifacts in known locations and can also carry out RAM dump on a live computer.

Should support following Search criteria for system captures -

SYSTEM CAPTURE	DESCRIPTION
Clipboard Dump	Create a dump of the clipboard on a Windows target system.
Cookie Information	List the website Cookies saved on Windows target system. Support for at least the following Web browsers -MS Explorer, Mozilla/Firefox, Safari, Opera, and Google Chrome.
Drive Encryption Status	Should collect information about encrypted drives and partitions. It should detect:
Installed Applications	Should collect the list of installed applications on a Windows target system.
Internet Browsing History	Should collect the list of all the cached URLs from Web browsers installed on Windows target system. Support for at least the following Web browsers - MS Explorer, Mozilla/Firefox, Safari Opera, and Google Chrome.
Internet Search History	Should be able to collect the search terms typed in Web browsers on Windows target systems. Support at least the following browsers - MS Explorer, Mozilla/Firefox, Safari, Opera, and Google Chrome. Support at least the following search engines - Google, Yahoo!, MSN/Bing, Facebook, Twitter, and MySpace.
Mapping Search History	Should be able to collect the maps and directions search history from Google Maps on Windows target system.
Network Information	Should be able to collect Network Information on a Windows target system. Information may be available after scanning a live computer.
Physical Memory Dump	Create a dump of the physical memory on a Windows target system.
Screenshot	Should be able to take a screenshot of all the screens on powered-ON Windows target
System Information	Should be able to collect information on the Operating System of the target computer.
USB Device History	Should be able to collect the history of all the USB devices plugged into a Windows target
User Profiling	Collects general the information about users detected on a Windows target System.
Visited Website Summary	Should be able to collect the list of unique websites visited from browsers installed on Windows system. Support at least the following browsers - MS Explorer, Mozilla/Firefox, Safari, Opera, and Google Chrome.

➤ **Should support following minimum user-defined Search Criteria**

File Collection	Searches for files by file properties as defined by the user
Keywords	Searches files for specified keywords
Regular Expressions	Searches files for strings matching a regular expression
MD5 Hash	Searches for known files by MD5 hash
Visual Similarity	Searches for picture files that are similar to a known set of pictures

It should be possible to refine the search criteria by detailed definitions of:

- File type – filename, file extension, file header, file size, file metadata (created, modified, accessed dates)
- File location by defining a) file paths using regular expressions, b) all allocated files, and c) deleted files.

➤ **Should support following minimum pre-configured criteria**

- Anti-Forensics – Keyword Search – Encryption Tools
- Anti-Forensics – Keyword Search – Wipers and other tools
- Chat – Windows Live Messenger – Contacts
- Chat – Windows Live Messenger – Saved Logs & Received Files
- Chat - Windows Live Messenger - Saved Logs - Non Standard Location
- Chat – Yahoo Messenger – Saved Chat Logs, Program Logs and Photo share
- Documents - Office - Collection
- Documents - Passport Numbers Regex - Collection
- G2 Users Files Collection All File Types
- Email – Outlook – All pst and ost files
- Email – Windows Mail & Windows Live Mail – Email, newsgroups, contacts
- Fast Picture Collection
- IPOC Hash set 1
- IPOC Hash set 2
- IPOC Keyword Search – File Content under1mb size – PART 1
- IPOC Keyword Search – Filename Only – PART 2
- IPOC Visual Search
- P2P Artifacts - Torrent Movies
- Pictures - Allocated Files Thorough - Collection
- Pictures - Fast - Collection
- Pictures - IE Temporary Internet Files - Collection
- Pictures - taken with Camera or Phone with EXIF data - Collection
- Video Files - Common Types - Collection
- Web Browsers - History Files - Collection
- Windows Artifacts - Desktop Items
- Windows Artifacts - Link Files
- Windows Artifacts - Registry Files - Collection
- Windows Artifacts - Vista W7 Thumb cache Files –Collection

- Windows Artifacts - Windows edb files
 - _Mac - Browser - Chrome Artifacts - Pictures Only
 - _Mac - Browser - Chrome Artifacts
 - _Mac - Browser - Firefox Artifacts - Pictures Only
 - _Mac - Browser - Firefox Artifacts
 - _Mac - Browser - Safari Artifacts - Part1
 - _Mac - Browser - Safari Artifacts - Part2
 - _Mac - Chat and Voice Communications -Skype Artifacts
 - _Mac - Desktop Items
 - _Mac - email - Apple Mail Part1
 - _Mac - email - Apple Mail Part2
 - _Mac - File Sharing and Cloud Storage -Dropbox
 - _Mac - Operating System Artifacts -iOS device Backups iPhone etc.
 - _Mac - Operating System Artifacts - Main List
 - _Mac - Operating System Artifacts - Print Jobs
 - _Mac - Operating System Artifacts - System Log
 - _Mac - Operating System Artifacts - Terminal log
 - _Mac - Operating System Artifacts - Trash
- The tool should be configurable to search for the most regular file types and users should be able to configure additional file types that can be defined by file name, file extension and/or file header. In addition, these files can be collected from within existing container files like zip or pst files.
- Users should be able to define the file locations in order to focus a search in known areas of a hard drive.
- Users should be able to search in the following areas.
- **Activity Sensor** (the 50 most recently modified folders),
 - **Preferred Paths** (user defined folders that are known to contain specific files or artifacts),
 - **All Allocated Files**, and
 - **Deleted Files** (files that have been deleted and removed from the Recycle Bin but still have an entry in the file system index).
- **Exported Reports**
- Users should be able to customize reports by selecting specific content by Search Types, File Types, System Logs, or individually tagged entries.
 - Output formats can include .csv, HTML, or MS Word.
 - Users should also have the option to include all original collected files with the exported report.
- **File Parsers**
- Should be possible to apply various file parsers to ensure that compressed and compound files are subjected to the full search criteria.
 - Support for the following minimum file formats should be available:
- Graphic Files**
- ✓ GEM Image (Bitmap)

- ✓ Graphics Interchange Format (GIF)
- ✓ JPEG
- ✓ JPEG2000
- ✓ Microsoft Windows Bitmap
- ✓ PC Paintbrush (PCX)
- ✓ Photoshop (PSD)
- ✓ Portable Network Graphics (PNG)
- ✓ TIFF

Office Documents

- ✓ Adobe PDF
- ✓ Microsoft Excel Charts
- ✓ Microsoft Excel for Macintosh
- ✓ Microsoft Excel for Windows
- ✓ Microsoft Word for DOS
- ✓ Microsoft Word for Macintosh
- ✓ Microsoft Word for Windows
- ✓ Microsoft WordPad
- ✓ Rich Text Format (RTF)
- ✓ Microsoft PowerPoint for Macintosh
- ✓ Microsoft PowerPoint for Windows

Email

- ✓ Microsoft Outlook PST

Archives

- ✓ 7zip
- ✓ gzip
- ✓ zip
- ✓ cram
- ✓ squash
- ✓ rar
- ✓ tar

Other Compound Files

- ✓ Windows thumbs. DB
- ✓ Windows thumb cache

➤ **For Video Files** - Should extract and displays frames from each video found in a scan and at least the following file types and codecs are to be supported.

Short name	Full name
✓ 3g2	3GP2 format
✓ 3gp	3GP format
✓ amr	3GPP AMR file format
✓ asf	ASF format
✓ avi	AVI format
✓ avm2	Flash 9 (AVM2) format
✓ avs	AVS format
✓ bink	Bink
✓ dts	raw DTS
✓ dv	DV video format

✓ dvd	MPEG-2 PS format (DVD VOB)
✓ flv	FLV format
✓ gif	GIF Animation
✓ h261	raw H.261
✓ h263	raw H.263
✓ h264	raw H.264 video format
✓ hls,applehttp	Apple HTTP Live Streaming format
✓ ipod	iPod H.264 MP4 format
✓ m4v	raw MPEG-4 video format
✓ mkv	Matroska file format
✓ matroska,webm	Matroska/WebM file format
✓ mov	MOV format
✓ mj2	Motion JPEG 2000 format
✓ mp4	MP4 format
✓ mpeg	MPEG-1 System format
✓ mpeg1video	raw MPEG-1 video
✓ mpeg2video	raw MPEG-2 video
✓ psp	PSP MP4 format
✓ swf	Flash format
✓ vcd	MPEG-1 System format (VCD)
✓ avs	AVS (Audio Video Standard) video
✓ binkvideo	Bink video
✓ flv	Flash Video (FLV) / Sorenson Spark /Sorenson H.263
✓ gif	GIF (Graphics Interchange Format)
✓ h261	H.261
✓ h263	H.263 / H.263-1996
✓ h263i	Intel H.263
✓ h263p	H.263+ / H.263-1998 / H.263version 2
✓ h264	H.264 / AVC / MPEG-4 AVC / MPEG-4 part 10
✓ mjpeg	MJPEG (Motion JPEG)
✓ mpeg1video	MPEG-1 video
✓ mpeg2video	MPEG-2 video
✓ mpeg4	MPEG-4 part 2
✓ mpegvideo	MPEG-1 video
✓ msmpeg4	MPEG-4 part 2 Microsoft variantversion 3
✓ msmpeg4v1	MPEG-4 part 2 Microsoft variantversion 1
✓ msmpeg4v2	MPEG-4 part 2 Microsoft variantversion 2
✓ theora	Theora
✓ wmv	Windows Media Video

- **Forensic Integrity should be maintained** - The tool should be forensically sound when the computer is booted from triage key or boot CD. Also, it should not alter file times and dates when used live on a running Windows computer.

Description	Powered OFF computer	Powered ON computer
Forensically sound	Yes	Yes
Change to file time stamps	No	No
USB key registry entry in standard mode	No	Yes

Other Recommended features:

- ✓ Run scans on live (on) computers
- ✓ Run scans on dead (off) computers
- ✓ Export basic reports
- ✓ Review Intel/evidence on suspect computer
- ✓ Keyword, hash, grep search capabilities
- ✓ File collection capability
- ✓ Scan NTFS, FAT, EXT, HFS systems
- ✓ Advanced image analysis search
- ✓ Add custom keywords prior to running scan
- ✓ Scan devices connected to suspect computer
- ✓ Bookmark evidence on suspect computer
- ✓ Run Scans with custom Search Profiles
- ✓ Customizable report templates
- ✓ Export HTML report formats
- ✓ Export CSV and MS Word report formats
- ✓ Create custom reports
- ✓ Create Search Profiles
- ✓ Image suspect drives
- ✓ Use external USB device for data collection
- ✓ Scan external devices from examiner's computer (USB, CD, DVD, SD cards, etc.)
- ✓ Scan drive images (dd, e01)
- ✓ Stealth Mode
- ✓ Deploy classified Search criteria (encryption)

Latest version of Adroit Photo Forensics tool

Should provide efficient Case Processing

- Should automatically generate case details based on selected evidence.
- Should allow options to balance between speed and recovery.
- Provide Built-in GUI to handle digital photo evidence.
- Provide option for batch processing to analyze multiple cases automatically.

Should provide comprehensive Evidence Support

- Should at least support Encase disk images (single and split)
- Support for RAW/DD images (single and split)
- Support for Logical/Physical drives

Maintain Forensic Integrity

- Provide ability to Generate MD5 and SHA1/SHA256 hashes of photos recovered.
- Provide ability to Generate reports with precise block range locations of photos.
- Provide ability to clearly identify partial photos and form of recovery for photos.
- Provide ability to Export hashes of photos recovered into FTK.
- Provide ability to Recoveries backed by scientifically proven techniques.

Support for Enhanced Recovery

- Provide Full Active Recovery support for NTFS/FAT/HFS/HFS+
- Carving Support for unallocated space and slack space between partitions.
- Ability to separate photos correctly carved and partially carved.

Enhanced Carving support

- Provide Validated sequential carving.
- Carving support to recover photos based on file system logs and validation.
- Carving support to recover fragmented photos automatically.
- Carving Support to recover fragmented photos manually.
- Embedded Carving support to recover photos from other files
- Size Carving support for recovery of BMPs, TIFFs, and RAW formats
- Support Windows Thumbnail Cache Recovery

Minimum Photo Format Support

- JPEG and camera RAW formats.
- PNG, GIF (active), and BMP.
- DNG and TIFF support

Photo Details Support for at least

- Complete File System Information of photos
- Complete Header Data information.
- Complete Metadata info (EXIF/IPTC).
- Embedded thumbnail identification.
- Block data linking for JPEGs.

Support for Photo Grouping/Filtering

- Photo specific grouping based on camera, EXIF Date stamps etc.
- Standard grouping based on File name, date, size etc.
- Enhanced Timeline grouping based on file modification/creation/access or EXIF dates.

Content Based Filtering support for at least

- Different Quality/Speed settings for Explicit Image Detection
- Child Explicit Image Detection.
- Face Detection.
- Thumbnail - Image mismatch detection.
- Duplicate photo using hash detection.

Advanced Categorization support for at least

- Create customized category profiles or use pre-existing
- Categorize from any screen with full hotkey support
- Automatically categorize based on Filter rules configured
- Categorize multiple selections or groups efficiently

BIOMETRIC ACCESS CONTROL

- **USB Numeric Keypad support** for Easy Command Input - to enroll users, delete users, or reset the terminal to its default settings.
- **Support Easy Data Management** using USB flash disk to transfer transaction logs to computer.
- **Provision for Built-In Alarm**
- Support for Enrollment with an administrator card. Just flash the card to enroll or delete a user.
- Should provide communication support via variety of voice commands combined with multi-colored LED signals.

➤ **Basic Minimum Requirements:**

SURFACE FINISHING	Acrylonitrile Butadiene Styrene (ABS)
TYPE OF SCANNER	Optical fingerprint scanner
MICROPROCESSOR	At least 300 MHz
MEMORY	Support at least 256 MB flash memory and 32 MB SDRAM
PRODUCT DIMENSION (L X W X H), mm	Preferably 78 x 50 x 150
STORAGE	
Fingerprint templates	Support for at least 1500 different templates
Card templates	Support for at least 10000 different templates
ENROLLMENT & VERIFICATION SUPPORT	
Methods	Support for at least Fingerprint & card
Recommended fingerprint per user ID	2
Fingerprint placement	Any angle
Verification time (sec)	< 1
FAR (%)	< 0.0001
FRR (%)	< 1
CARD TECHNOLOGY	RFID: 64-bit, 125kHz
COMMUNICATIONS TECHNOLOGY SUPPORT	
Method	Supports TCP/IP, RS485, USB disk
Baud rates	9600/19200/ 38400/ 57600/ 115200
Wiegand support	26-bit input/output
Power input	DC 12V 3A
Voice Support	Yes
ACCESS CONTROL FEATURE SUPPORT	
EM lock driving output	DC 12V 3A / Relay output
Alarm output	NO / NC
Support for Antipas back	Yes
VOICE LANGUAGE (TERMINAL)	English
SOFTWARE LANGUAGE	English
SOFTWARE	Preferably Ingress or equivalent

Latest version of Paraben Chat Examiner

- Support to parse out chat logs into readable data and analyse log files associated with different chat clients.
- **Support for at least following Chat Clients:**
 - Skype
 - Yahoo! Messenger
 - Windows Live Messenger (MSN)
 - ICQ
 - Trillian
 - Hello
 - Miranda
- Ability to perform advanced searches like keyword search, string search, regular expression search etc., and produce quality, detailed reports.
- Ability to open multiple chat logs in one workspace.
- Customizable filtering and searching capabilities.

Paraben e-mail Examiner V7.1

- Support email archive analysis and conversions.

Supported E-mail Types

- Microsoft Outlook (PST)
- Microsoft Outlook Offline Storage (OST)
- Thunderbird
- Outlook Express
- Eudora
- E-mail file (EML)
- Windows mail databases
- Plain Text mail
- America On-line (AOL)
- The Bat! (version 3.x and higher)
- Support for more than 750 MIME Types and related File Extensions

- **Should be able to export supported archives to at least the following:**

.PST, .EML, .MSG, .EMX

- Support to analyze Email Attachments
- Ability to recover Deleted Email from at least Outlook, Thunderbird, Eudora, and The Bat!
- Should provide Comprehensive Reporting abilities
- Supports Batch Exporting With Advanced Filtering
- Customizable filtering and searching capabilities.

Digital Intelligence Forensic Recovery Evidence Data Center (FRED C)

Sno.	Description	Quantity
	Forensic Recovery of Evidence Data Center (FREDC) consisting of:	1
	Forensic File Server (4U) <ul style="list-style-type: none"> ❑ Dual(2) Intel® Xeon® E5-2620 v3 CPU, (Hex Core)2.4 GHz, 15MB Cache, 8.0 GT/s Intel® QPI [T1330] ❑ 64 GB(PC4-17000 DDR4 2133 MHz ECC Memory[T2317] ❑ 60 TB Internal RAID6 Array - (10 X 6 TB Drives) ❑ 1 x 500 GB 7200 RPM SATA Hard Drive in removable drive bay – Disaster Recovery Drive ❑ 1 x Dual Port 10 Gigabit Ethernet Converged Network Adapter [T6232] ❑ 4 port (16 channel) SAS controller card Detailed System Specifications: <ul style="list-style-type: none"> ❑ 4U Rackmount Enclosure (10 Bays) ❑ 1100 Watt Modular Power Supply ❑ Dual Intel® Socket 2011-3 Motherboard for Xeon® processor E5-2600 v3 Product Family ❑ Intel C612 Chipset ❑ 16 DIMM Slots supporting DDR4 1600/1666/2133 Registered ECC memory, Maximum up to 512 GB ❑ 6 PCI-Express 3.0(x4/x8/x16)Slots ❑ 10 ports Intel 6.0 Gb/s SATA Controller ❑ 1 Serial Port Header ❑ 1 RJ-45 port for iKVM (ASMB8 card) ❑ 1 PS/2 Port (Keyboard/Mouse) ❑ 2 RJ45 ports - 10/100/1000 MB/s Gigabit Intel® ❑ i350-AM2 Ethernet Controller ❑ 4 USB 2.0 Ports – 2 Back Mounted, 2 Front Mounted ❑ 5 USB 3.0 Ports – 2 Back Mounted, 3 Front Mounted ❑ Aspeed AST2400 32MB VRAM Graphics Controller ❑ 4 x 2.5" SATA Drive Chassis with external access ❑ 2 x RAID Chassis with 5 removable drive bays each (10total) ❑ BD-R/BD-RE/DVD±RW/CD±RW Blu-ray Burner Dual-Layer Combo Drive Software: <ul style="list-style-type: none"> · Suse Linux Enterprise Server Software · Yosemite Backup Software 	1
	96.0 Terabyte RAID Array Module(84 Terabyte RAID-6) (3U) <ul style="list-style-type: none"> ❑ 16-Bay, 3U Rack mount RAID Enclosure (Multilane SAS Attached) ❑ 16 x 6.0 TB, 7200 RPM Hard Drives in Hot swap removable drive trays 	1
	LTO-6 Ultrium Robotic Tape Library (2U) <ul style="list-style-type: none"> · LTO-6 Ultrium Drive, 16 Slot Library, 2.5 TB(Uncompressed)/ 6.25 TB (Compressed) per tape, Up to100 TB Total Online Backup Capacity, SAS interface 	1
	LTO-6 Media Set <ul style="list-style-type: none"> · Qty 15 x Data Media (2.5 TB/6.25 TB capacity) · Qty 1 x Cleaning Media 	1
	10 Gigabit (Copper) Network Switch <ul style="list-style-type: none"> ❑ Qty 1 x Fully managed, line-rate 10G Copper 'Base-T' rack mount switch. ❑ Supports up to 24 10GBase-T (RJ45) and 4 SFP+ ports. 	1

	1 Gigabit (Copper) Network Switch · 48 Port Gigabit Ethernet (10/100/1000 MB/S) rack mount Network Switch	1
	24 Port Rack mount Cat 5e Patch Panel (2U)	1
	24 Port Rack mount Cat 6A Patch Panel (2U)	1
	Rack mount 19 inch LCD Display with integrated Keyboard/Track Pad (1U)	1
	8 port KVM Switch KVM with IP Remote Access	1
	12 Outlet 15A Rack mount Power Strip	2
	3000 VA Rack mount Uninterruptable Power Supply(UPS) (2U)	1
	42U Rack mount Enclosure w/doors and Ventilation Fans -23.5"(w) x 36"(d) x 84"(h)	1
	<p>Forensic Recovery of Evidence Device –Rack Mount (FRED-RM) (4U)</p> <ul style="list-style-type: none"> · Intel® Core™ i7-5820K CPU (Hex Core Processor), 3.3 GHz, 15MB Intel® Smart Cache [T1046] · 32 GB (4x8GB)PC3-17000 DDR4 2133 MHz Memory[T2010] · 1 x 256 GB Solid State SATA III Drive – OS Drive[T3047] · 1 x 128 GB Solid State SATA III Drive –Temp/Cache/DB Drive [T3300] · 1 x 2.0 TB 7200 RPM SATA III Hard Drive – Data · Drive installed in HotSwap Bay1 [T3007] · 1 x Single Port 10 Gigabit Ethernet Converged · Network Adapter [T6231] · 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 [T0016] <p>Windows 10 Professional (64 bit) [T0018] Other Operating Systems to be included:</p> <ul style="list-style-type: none"> • SUSE Professional Linux (64 bit) <p>System Restore Media – Bootable Blu-ray disc containing restore environment and factory configured operating system images</p> <p>Hardware Write Blocking: Digital Intelligence UltraBay 3d Hardware Write-Blocker with touch screen display:</p> <ul style="list-style-type: none"> · 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 · Digital Intelligence Integrated Forensic Media Card Reader Read-Only and Read/Write switchable <p>Detailed System Specifications:</p> <ul style="list-style-type: none"> · 4U Rack mount Enclosure (10 Bays) · 1100 Watt Modular power supply · i7 Motherboard with Intel® X99 Chipset · 7 PCI-Express 3.0(x16)Slots · 8 ports Intel® 6 Gb/s SATA Controller · 1 port Intel® SATA Express Controller (or 2 x SATA 6Gb/s ports) · 1 port ASMedia® SATA Express Controller (or 2 xSATA Gb/s ports) · 8 Channel High Definition Audio CODEC featuringCrystal Sound 2 · 2 RJ45 LAN ports (Intel® I210-AT, 1 x Gigabit LAN 	1

	<ul style="list-style-type: none"> · Intel® I218LM, 1 x Gigabit LAN Controllers) · 2 eSATA 6 Gb/s ports - AS Media® controller · 14 USB 3.0/2.0 ports - 11 Back Mounted, 3 Front Mounted · 2 USB 3.1 ports – 2 Back Mounted · 1 Write Blocked USB 3.0/2.0 port - Front Mounted · 2 FireWire IEEE 1394b (800 MB/s) ports – 1 Back Mounted, 1 Front Mounted(Write Blocked) · 4 x 2.5" SATA Drive Chassis with external access · 1 x Shock Mounted SATA Removable Hard Drive Bays(IDE Capable) · 1 x Hot Swap Shock Mounted Universal (IDE/SATAcompatible) Removable Hard Drive Bays · BD-R/BD-RE/DVD±RW/CD±RW Blu-ray Burner Dual-Layer Combo Drive · Extendable/Retractable Imaging Work shelf with integrated ventilation · Other Software included: Symantec Ghost, CDAuthoring Software, DRIVESPY, IMAGE, PDWIPE,PART, and PDBLOCK · Toolbox containing: Adapters, Cables, Digital Camera, Security Screwdriver Set and OEM Documents 	
	Network Color printer	1
	Analysis Client Workstations <ul style="list-style-type: none"> <input type="checkbox"/> 3.6 GHzIntel Core i7-4790 , 1600 MHz, 7200 RPM <input type="checkbox"/> 8MB Cache <input type="checkbox"/> 8GB DDR3 RAM <input type="checkbox"/> Intel Z87 Chipset <input type="checkbox"/> (SSD/HDD) - HDDUpto2TB <input type="checkbox"/> NVIDIA GeForce GTX 745, 4GB <input type="checkbox"/> Windows 8.1 or higher <input type="checkbox"/> Peripherals <ul style="list-style-type: none"> o Wireless Keyboard o Wireless Optical Mouse <input type="checkbox"/> USB 2.0 4 <input type="checkbox"/> USB 3.0 6 <input type="checkbox"/> Power Supply (Watts) 500W <input type="checkbox"/> Dimension (W x D x H) 174.1 x 428.6 x 413.6 mm <input type="checkbox"/> Weight 10.01 Kg <input type="checkbox"/> 22" Monitor 	5
	3 years hardware warranty, lifetime technical support (telephone, email, online support ticket system)	1
	International INDIA Onsite Installation, Configuration, and Equipment Orientation	1

Forensics Lab Information Management System (F-LIMS)

- Should work seamlessly across crime scene, lab, and property unit modules.
- Support Pre-logging of evidence and documenting the crime scene, to laboratory analysis and property storage and disposition, F-LIMS should streamline the process
- Compliance with ISO 17025, ASCLD-LAB, CALEA and other accreditation standards.
- Should allow Set up of new sites, lab units, analyses, workflows and examiner report templates, and review processes through easy-to-use workflow settings.
- Should maintain electronic chain-of-custody via user name and password or signature pads.
- Provision for Configurable workflows for any of the analytical units.
- Ability to Store and track highly sensitive crime scene evidence and other property.
- Ability to accurately document every movement and account for every item, from receipt to disposition, with real-time barcoded tracking.
- Availability of Option for Field Responders to pre-log evidence directly from their mobile field kit.
- Support complete case management, from central reception to disposition
- Supervisors should be able to manage analyst caseload, and examiners should be able to assign tests and enter results for items of evidence.
- Provision to generate examiner reports in at least Microsoft Word or Crystal Reports.
- Provision to Pre-populate results and headers based on unit templates.
- Provision to Produce statistical reports on evidence throughput, turnaround times, backlogs, workload and more, for resource management and submission.
- Ability to create dashboards that display key performance indicators with Advanced Analytics.
- Support Complete document management system that links documents to required quality standards, with version control and maintenance of retired materials.
- Ability to Perform quality audits within the LIMS, track proficiency testing and training, document equipment and quality checks.
- Support for QA Compilation Application to prepare for assessments and year-end quality report
- Ability to store key information in an Excel spreadsheet when offline, then import directly back into the system once online
- Support for vehicle and body processing templates to streamline note taking, easily store and annotate photos, record the results of presumptive tests, collect evidence and start the chain- of-custody immediately.
- Should Receive alerts for misfiled or misplaced evidence and reminders when evidence is overdue.
- Should be able to send disposition requests to officers and document the response.
- Should be able to generate return to owner documents and evidence inventory reconciliation reports.

ACCESS DATA Forensic Tool Kit v6 Standalone – Perpetual License

Sno	Description	Quantity
	Forensic Toolkit	1
a)	<ul style="list-style-type: none"> Should allow users to create images, process a wide range of data types from forensic images to email archives and mobile devices, analyze the registry, crack passwords, and build reports—all within a single solution Should have KFF hash library with 45 million hashes. Should provide Advanced, automated analysis without the scripting. True multi-threaded / multi-core support Should be Database driven - One Shared Case Database. The components are compartmentalized allowing the processing workers to continue processing data without interruption. Deduplication support - Gain a more complete understanding of data sooner with enhanced interoperability between FTK and Summation. Support Shared FTK & Summation Audit Log - Any updates to the audit log mean documents viewed in the FTK viewer will be displayed in the Summation audit log and vice versa. Support Wizard-driven processing to ensure no data is missed. <ul style="list-style-type: none"> Cancel/Pause/Resume functionality Real-time processing status CPU resource throttling Email notification upon processing completion Pre- and post-processing refinement support Advanced data carving engine support to allow specifying criteria, such as file size, data type and pixel size to reduce the amount of irrelevant data carved while increasing overall thoroughness. Intuitive interface, support for email analysis customizable data views, high processing speeds and stability Support for shared index file, eliminating the need to recreate or duplicate the file. Single node enterprise support <ul style="list-style-type: none"> Should be able to install a persistent agent on a single computer to enable the remote machine analysis and incident response capabilities Should be able to preview, acquire and analyze hard drive data, peripheral device data, and volatile/memory data on Windows®, Apple® OS, UNIX® and Linux® machines. Should have capability to uninstall the agent at any time, and push it out to a different computer for multi-machine analysis. Should be easy, wizard-driven agent deployment. Should have secure remote device mounting capability using the Pico agent. Advance Volatile/Memory Analysis support <ul style="list-style-type: none"> Should support 32-bit and 64-bit Windows® OS Should have comprehensive analysis of volatile data Should be able to do static RAM analysis from an image or against a live system Should enumerate all running processes, including those hidden by rootkits, and display associated DLLs, network sockets and handles in context. Should dump a process and associated DLLs for further analysis in third party tools. Should be able to do memory string search to allow examiner to identify hits in memory and automatically map them back to a given process, DLL or piece of unallocated space and dump the corresponding item. Should be able to provide VAD tree analysis and exposes registry artifacts in memory and parse and display handle information from memory. 	

	<ul style="list-style-type: none"> • MAC features support <ul style="list-style-type: none"> ◦ Should be able to process B-Trees attributes for metadata ◦ Should support PLIST support ◦ Should have SQLite database support ◦ Should have apple DMG and DD_DMG disk image support ◦ Should have JSON file support • Should support regular expression in index searching to allow examiner to search for advanced combinations of characters within indexed data. • Broad file system, file type and email support <ul style="list-style-type: none"> ◦ Should have support for 700+ image, archive and file types ◦ Should have support for Notes NSF, Outlook PST/OST, Exchange EDB, Outlook Express DBX, Eudora, EML (Microsoft Internet Mail, EarthLink, Thunderbird, Quick mail, etc.), Netscape, AOL and RFC 833 ◦ Should be able to analyze DMG (compressed and uncompressed), Ext4, exFAT, VxFS (Veritas File System), Microsoft VHD (Microsoft Virtual Hard Disk), Blackberry IPD backup files, Android YAFFS / YAFFS 2 and many more. ◦ Should be able to create and process • Advanced Forensic Format (AFF) images. • Visualization Support <ul style="list-style-type: none"> ◦ Automatically construct timelines and graphically illustrate relationships among parties of interest in a case. ◦ Support Email, Social and File Visualization views. The data in multiple display formats, including timelines, cluster graphs, pie charts, geolocations and more, to help determine relationships and find key pieces of information. ◦ Social Analyzer to allow viewing email communications at the domain level and drill down to the custodian level to see communications among specific individuals. • Internet Browser and Web-Based Email Evidence support • Support to Unlock files with decryption password cracking and recovery and recover passwords from over different applications • Should automatically decrypt (with proper credentials) Credant, Safe Boot, Utimaco, Safeguard Enterprise and Easy, EFS, PGP, Guardian Edge, Point sec and S/MIME. • Should be able to identify encrypted PDFs. • Supports Explicit Image Detection (EID) for auto- identification of potentially pornographic images. recognizes flesh tones and auto-identifies more than 30,000 potentially pornographic images. • Should be able to generate detailed reports in native format, HTML, PDF, XML, RTF, and more - with links back to the original evidence. • Should be able to define Registry Supplemental Reports (RSR) during pre-processing or additional analysis. • Should have capability to see which files could not be processed or indexed with the Processing Exception/Case Info report. • Should be able to create a CSV of processed files that can be imported into Excel or a database application. • Should be able to export MSGs for all supported email types. • Should be able to identify PDF files through the PDF file system. • Should highlight index search hit for PDF files in the natural view. • Support for an OCR engine - Optical Character Recognition (OCR) - Expand to other languages with the ability to choose which language before converting images to readable text. 	
--	---	--

	<ul style="list-style-type: none"> • Should allow the user to send registry files to Registry Viewer from FTK even if the files have not yet been identified. • Provision to Create, import and export reusable processing profiles with pre-defined processing options for different investigative needs • Log2timeline CVS Support • Comprehensive Index & Binary Searching support • Single-node Remote Investigations support • Microsoft® PhotoDNA® Integration support • Volume Shadow Copy (VSC) file review support • Automated Language Identification support • Internet And Chat Analysis support • Exceptional Apple® iOS® Analysis support • Rich Reporting support • Provision for FTK Web Viewer, Powered by Summation – Should be able to conduct case with real-time collaboration. • Support for instant access to case data as it's being identified in FTK while incident responders are in the field or performing on-site collections. • Multi-Case Search in Web Viewer • Support Volume Shadow Copy - Quickly identify and extract information from the Windows® shadow system files or set up directly within FTK • Compatibility should allow users the ability to view Cellebrite UFD, UFR and UFDX Images within FTK. • Includes the latest enhancements for compatibility with Windows 10. 	
	Toolkit Server PC	1
b)	<p>Minimum Requirements :</p> <ul style="list-style-type: none"> • 23 3/4" High, 8 3/8" Wide, 25 1/4" Deep - 80 lbs • Intel Core i7-6800K CPU (Hex Core Processor), 3.4 GHz, 15MB Intel Smart Cache • 32 GB (2x16GB)PC3-17000 DDR4 2133 MHz Memory • 1 x 256 GB Solid State SATA III Drive - OS Drive • 1 x 256 GB Solid State SATA III Drive - Temp/Cache/DB Drive • 1 x 2.0 TB 7200 RPM SATA III Hard Drive - Data • Drive installed in Hot Swap Bay1 • NVidia GTX 750Ti 2GB 128 bit DDR5 PCI-Express Video Card with 1 VGA (D-Dub), 1 HDMI, and 2 DVI orts • 22" Widescreen LCD Monitor with Built-in Speakers • Windows 10 Professional (64 bit) Single RAID Chassis <p>Option 12 Channel PCIe 6 Gb/s SAS/SATA RAID Controller – 1 RAID Chassis with 5 removable drive bays</p> <p>RAID Set #1</p> <ul style="list-style-type: none"> • 2 TB 7200 RPM SATA III Hard Drive Set (Set of 5 Drives) • Hardware Write Blocking: <ul style="list-style-type: none"> ◦ 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 PCIe Write Blocker • Write-Block and Read/Write visibility via Lock/Unlock LEDs • Read and write mode capabilities for all device ports controlled via LCD Menu • Allows simultaneous imaging of 2 attached devices • Media Card Reader - Read-Only and Read/Write switchable 	

Latest version of F-Response Consultant Edition

- Should connect to a virtually limitless number of remote target machines.
- Should allow the examiner to obtain completely vendor neutral, write protected access to remote physical disks, logical volumes, and physical memory.
- Should be a GUI based Application.
- **Should provide Full Live Read-Only Access, No File Level Locking –**
 - ✓ Provide direct, live, read-only access to the remote target computer's disks, volumes, and physical memory.
 - ✓ All access should be at the physical level so no file level locking is to be involved.
 - ✓ Should give access to all content on the remote target, including protected system content (Registry files, Email PSTs, Database Files, etc.).
- **Should be an Executable and Software –**
 - ✓ Should function as a single executable ("exe") on the remote target computer that requires no drivers or installation components, as well as no reboot when deployed and started.
 - ✓ Should use minimal resources and be highly portable, requiring only the minimum resources necessary to run Windows XP or higher.
- **Should provide Web based Disk Access Support**
 - ✓ Provide web based disk access and representation.
 - ✓ Should use standard web technologies (HTTPS/REST) to provide direct access to the remote target machines, Logical and Physical targets in both raw and logical format.
 - ✓ Can be accessed and used from any modern web browser and also exposes a feature rich and Extensible application programming interface (API) accessible from any system capable of making and interpreting web queries and JSON.
- **Should provide at least following Targets and Platform Support**
 - ✓ Should work with all RAID disks, physical drives, logical volumes, and physical memory (32 & 64 bit Windows). Should include target executable for most of the modern operating system environments, including exotic hardware such as IBM AIX and HPUNIX.
 - ✓ Should work with all Computer Forensics, eDiscovery and Data Recovery software packages.
- **Provide Scripting and Programming**
 - ✓ Should include access to a fully scriptable COM Object capable of automating many of the Management Console tasks from any programming environment that supports COM.
- **Should at least satisfy the following Minimum Hardware Requirements (Examiner Computer)**
 - ✓ Pentium 233-megahertz (MHz) processor or faster
 - ✓ At least 2000 megabytes (MB) of RAM (8 GB is recommended)
 - ✓ At least 500GB of Disk Space.
- **Platform Support (Minimum)**

- ✓ Should support at least the following remote target platforms:
 - Windows 2000, XP, 2003, Vista, 2008, 7, 8, 2012, 32 and 64bit, Physical memory supported on both 32bit and 64bit Windows
 - OSX 10.3, 10.4, 10.5, 10.6, 10.7, 10.8 Universal Binary, Intel Apple OSX
 - Linux distributions build on Glibc 2.3.5 and higher, Android on ARM, and Embedded Linux (NetgearReadyNAS)
 - Solaris 8, 9, & 10 on SPARC and Open Solaris on Intel
 - IBM AIX 5.1, 5.2, 5.3, 6.1 on the Power processor
 - HP_UX11iv2, 11iv3 on the Itanium processor
 - FreeBSD 7 on the Intel/i386 processor
 - SCO Open Server 6 and UnixWare 7 on the Intel/i386 processor

IDE/SATA to USB 2.0/3.0 converters – Digital Intelligence

- Should allow converting 2.5"/3.5" Serial ATA, HDD, and other Serial ATA Devices into USB 3.0 / 2.0 interfaces.
- Should include USB 3.0 To IDE/ Serial ATA Multifunctional External Cable.
- Interface.
 - ✓ Serial ATA; IDE; USB 3.0.
- Minimum Data Transfer Rate.
 - ✓ Transfer rate available for 480Mb/s. Suitability. 2.5", 3.5", 5.25" Devices.
- Should be Plug-play and Hot-plug
- Should include Power/Adapter (AC 100~240V, 50~60Hz; DC 12V 4Amp)
- Should include Power adapter for 3.5"/ Bus-Power for 2.5" HDD
- At least Support the following hard drives
 - ✓ IDE Hard drives from 20GB up to 4000GB (4TB)
 - ✓ SATA or SATA II/ SATA III Hard Drives from 80GB up to 4,000GB
 - ✓ IDE/PATA or SATA I /II or III Drives, SSD or Magnetic Storage
- Should include at least one USB 3.0 to IDE+SATA Cable Adapter for 40pin IDE Drives &44 Pin IDE Drives and 22 Pin SATA Power + Signal Connector.
- OS Support:
 - ✓ Should support Windows 8/ Windows 7 Vista/2003/ XP/ 2000
 - ✓ Should support Linux and Mac OS.X

Logicube Forensic Falcon

Sno	Description	Quantity
1	Forensic Falcon	1
	<ul style="list-style-type: none"> • Should support Imaging and verification to multiple image formats: Support at least native copy, dd image, e01, ex01 and file-based copy. • Should provide compressions for at least E01/Ex01 formats. • Support at least SHA1, SHA256, MD5 and dual-hash (MD5+SHA1) authentication. • Should provide at least 4 Source and 5 Destination ports. • Should include at least 2 SAS/SATA, 1 USB 3.0, 1 FireWire Write-blocked source ports and 2 SAS/SATA, 2 USB 3.0 and 1 FireWire Destination ports. • Should have at least one Gigabit Ethernet port for network connectivity. • Provision for USB source and destination to be converted to SATA using a USB to SATA converter. • Built-in support for SAS/SATA/USB/FireWire storage devices. • Should include adapters to support at least 1.8"/2.5"/3.5" IDE and 1.8" ZIF and MicroSATA drive interfaces. • Provide support for 1 SCSI source and 1 destination drive. • Provide Support for M.2 PCIe and M.2 NVMe type SSDs and mini-PCIe and PCIe express cards using an express card adapter along with specific interface adapters. • Should be able to Image to or from a network location. Should be able to image to a network location using CIFS protocol and/or image from a network location using iSCSI. • Should be able to Image to an external storage device (such as a NAS) using the Gigabit Ethernet, USB 3.0 or SAS/SATA connection • Provision for users to disable various network services (such as HTTP, SSH, Telnet, CIFS/NETBIOS, iSCSI, Iperf and Ping) for security purposes. • Should provide Write-blocked preview/triage hard drive contents. • Should be able to Preview the drive contents directly on the unit. • The Unit should be able to be used as a write-blocker. Should include file browser feature to provide logical write blocked access to source or destination drives connected to Unit. • Should allow users to view the drive's partitions and contents, and view text files, jpeg, PDF, XML, HTML files. • Should support other files types (such as .doc and .xls) to be viewed by connecting unit to a network and via a PC, for download and view. • The unit should also allow to preview suspect/source drives or destination drives using the USB connection from the unit to a computer, or by using the SMB protocol. • Should allow users to use the iSCSI protocol to preview source drives. 	

	<ul style="list-style-type: none"> • Support use of a web browser to manage all operations remotely, easily connect to a networked unit from laptop or desktop using a web browser. • Should support automatic page scaling for ipad type devices. • Should support Image from a desktop or laptop PC without removing the hard drive. • Should allow creating a forensic bootable USB flash drive that allows the user to image a source drive from a computer on the same network without booting the computer's native operating system. • Should support Image from a MAC™: Should support Imaging from a MAC™ system booted in "target disk mode" using the write blocked FireWire port on the unit. The MAC's internal drive should be shown as a "source" drive. • Ability to wipe at least one destination drive while simultaneously imaging to another, or image from multiple source drives to multiple destinations. • Should be able to perform up to at least five tasks concurrently. • Should support Parallel Imaging. Should be able to perform multiple imaging tasks from the same source drive to multiple destinations using different imaging formats. • Should be able to clone to a network location or a destination drive in mirror copy format while simultaneously imaging in e01 or dd format to a different destination drive • Should support Concurrent Image+Verify. • Unit should be able to perform a forensic, filter-based file copy : Filter and then image specific file types by file extension such as .PDF, .doc, .jpeg, .mov, etc. • Should be able to Secure sensitive evidence data with whole drive AES 256 bit Encryption. Decryption should be able to be performed using the unit or by using open source software programs such as FreeOTFE, True Crypt, Vera Crypt • Should support Multi-pass wipe(DoD specifications) or use secure erase to wipe drives, supporting wipe at speeds of up to 27GB/min. • Should allow the user to push evidence files from destination drives connected to the unit or from the unit repository, to a network location. • Should also perform an MD5 or SHA hash during the push process, and a log file to be generated for each push process. • Should support Image restore feature. Should provide File to drive mode to restore DD, E01, EX01 images created by the Unit to another drive • Should support setting specific tasks to be performed sequentially, for example, first wipe the destination drive then hash the source drive then image the source drive. • Should include an internal, removable storage drive that stores O/S and audit trail/logs. 	
--	--	--

- Should provide Audit Trail/Log files for detailed information on each operation.
- Provision to log files on the unit or via a web browser, exported to XML, HTML or PDF format to a USB enclosure.
- Should allow users to print the log files directly from their PC when connected to unit via a web browser.

Additional features

- Should include HPA/DCO capture, drive “trim” feature to manipulates the DCO and HPA areas of destination drives,
- The ability to set password-protected user profiles and save Configurations
- Provision for a drive “time-out” feature to automatically put drives in stand-by mode after a specified idle time,
- Audible beep to notify user when tasks have completed, blank disk check, drive spanning
- At least 7” color touch screen display, two USB 2.0 host ports for keyboard, mouse or printer connectivity, and an HDMI port to connect a projector or monitor.

Power Requirements	12 VDC 12Amp
Power Consumption	< 140W with drives
Operating Temperature	0 to 40°C (32 to 104°F)
Relative Humidity	20% to 80%
Net Weight	2.0lbs/1.0k
Dimensions	7.6”W X 5.5”D X 2.6”H (19.0cm X 13.9cm X 6.6cm)
Agency Approvals	RoHs compliant FCC Part 15 Class A CE

	Power supply & power cord	1
	Fire wire cable	1
	Standard CAT6 network cable (100 mts)	1
	SAS/SATA cables	4
	USB 3.0 type A cable	1
	USB 3.0 device cable	1
	1.8" microSATA adapter	1
	1.8" IDE ZIF to SATA adapter	1
	2.5"/3.5" IDE to SATA adapter	1
	1.8" IDE to SATA adapter	1
	6-pin SATA power plugs	4
	USB A female to USB mini-B 5 pin male adapter	1
	USB A female to micro B male converter coupler adapter	1
	CD-ROM with Users' Manual	1
	Carrying case	1
2	Hard Disk Drives (Evidence Disks)	
	2TB SATA 6.0 Gb/S 3.5inch	2
	1TB SATA Internal Desktop Hard drive	2
	500 GB SATA 7200 RPM Internal Hard Disk for Laptop	2
	Internal 2.5 inch Mobile 500GB SATA Hard Disk Drive	2
	2TB Desktop internal SATA Drive 2.5"	2
	4TB Internal Hard Drive	1
	120 GB SATA III Internal Solid state Drive	1
	500gb SSD internal Drive	1
	2TB wired External Hard Disk Drive	2
	1TB wired External Hard Disk Drive	4

Paraben Network E-mail Examiner 4.1

- An advanced network email archive analysis and conversion tool.
- Support for computer forensic examinations, eDiscovery, email de-duplication, or conversion to various email formats such as PST or EML.

Should support at least following Network E-mail Archives

Microsoft Exchange	5.0, 5.5, 2000, Exchange 2003, 2007, & 2010 (.EDB)
Lotus Notes	4.0, 5.0, 6.0, 8.0, 8.5 (SB 41 & 4), .0 (.NSF)
GroupWise	Information stores up to version 8.0

Exports Supported Archives To:

.PST, .EML, .MSG, .EMX

- Should be able to analyse Email Attachments
- Should be able to recover Deleted Email from at least Exchange (EDB), Lotus Notes (NSF), and GroupWise
- Support for Comprehensive Reporting
- Provision for Batch Exporting with Advanced Filtering possibilities
- Customized Searching & Filtering capabilities.

Pass ware Kit Forensics Lab Edition 2016 V.4– Password Recovery Software

Sno.	Description	Quantity
	Passware Kit Forensics	1
	<ul style="list-style-type: none"> • Should be able to report all password-protected items on a computer and decrypt them. • Must be able to acquire and analyze live memory images, decrypt hard disks and smart phone data, and get administrative access to Windows and Mac computers. • The software should recognize at least the following protected file types to (even in batch mode) recovering their passwords. <ul style="list-style-type: none"> ✚ Acrobat 3.0, Acrobat 4.0, Acrobat 5.0, Acrobat 6.0, Acrobat 7.0, Acrobat 8.0, ✚ Acrobat 9.0, Acrobat 10.0, Acrobat 11.0 ✚ Symantec ACT! 2.0, Symantec ACT! 3.0, Symantec ACT! 4.0, Symantec ACT! 2000, ACT! by Sage 2005, ACT! By Sage 2006, ACT! By Sage 2007, ACT! by Sage 2008, ACT! by Sage 2009 ✚ Android Backup 4.4 or earlier, Android Image 4.4 or earlier, Apple Disk Image, Apple iCloud Token, Apple iTunes Backup / iOS 4.x - 10.x, Best Crypt 6.0, Best Crypt 7.0, Best Crypt 8.0 ✚ FileMaker Pro 3.x – 14.x, Google Chrome Website, ICQ 2000 - 2003 ✚ ICQ 99a, ICQ Lite, KeePass ✚ Lotus 1-2-3 1.1+, Lotus Notes 4.x, Lotus Notes 6.x, Lotus Notes 7.x ✚ Lotus Notes 8.x, (RC2, AES encryption), Lotus Organizer 1.0, Lotus Organizer 2.0, Lotus Organizer 3.0, Lotus Organizer 4.0, Lotus Organizer 5.0, Lotus Organizer 6.0, Lotus Word Pro 96 – 99 ✚ LUKS Disk Image, Mac OS / FileVault2, Mac OS X Keychain, Mac OS X User / Hash, Mac OS X 10.8 - 10.10 User / Hash, Mozilla Firefox Website ✚ MS Access 2.0, MS Access 95, MS Access 97, MS Access 2000, MS Access 2002, MS Access 2003, MS Access 2007, MS Access 2010 ✚ MS Access 2013, MS Access 2.0 System Database, MS Access 97 System Database, MS Access 2000 System Database, MS Access VBA ✚ MS Backup, MS Excel 4.0, MS Excel 5.0, MS Excel 95, MS Excel 97 ✚ MS Excel 2000, MS Excel 2002, MS Excel 2003, MS Excel 2007, MS Excel 2010, MS Excel 2013, MS Excel 2016, MS Pocket Excel, MS Excel VBA, MS Internet Explorer Website, MS Internet Explorer Web form ✚ MS Internet Explorer Content Advisor, MS Mail, MS Money 99 or earlier ✚ MS Money 2000 – 2001, MS Money 2002, MS Money 2003 - 2004 ✚ MS Money 2005 – 2007, MS One Drive, MS OneNote 2003 Section ✚ MS OneNote 2007 Section, MS OneNote 2010 Section, MS OneNote 2013 Section, MS Outlook 2000/2003/2007/2010/2013 Email Accounts, MS Outlook 2000/2003/2007/2010/2013 Form Template 	

	<ul style="list-style-type: none"> ✚ MS Outlook 2000/2003/2007/2010/2013 Personal Storage, MS Outlook Express Accounts, MS Outlook Express Identities, MS PowerPoint 2002, MS PowerPoint 2003, MS PowerPoint 2007, MS PowerPoint 2010 ✚ MS PowerPoint 2013, MS PowerPoint VBA, MS Project 95, MS Project 98 ✚ MS Project 2000, MS Project 2002, MS Project 2003 ✚ MS SQL 2000, MS SQL 2005, MS SQL 2008 ✚ MS Windows NT User / Secure Boot Option, MS Windows 2000 User / Secure Boot Option, MS Windows 2000 Server User / Secure Boot Option, MS Windows 2000 Server Active Directory Administrator, ✚ MS Windows XP User / Secure Boot Option, MS Windows 2003 Server User / Secure Boot Option, MS Windows 2003 Server Active Directory Administrator, MS Windows 2003 SBS User / Secure Boot Option, MS Windows 2003 SBS Active Directory Administrator, MS Windows Vista User / Secure Boot Option, MS Windows Vista / BitLocker, MS Windows 2008 Server User / Secure Boot Option, MS Windows 2008 Server Active Directory Administrator, MS Windows 2008 Server / BitLocker, MS Windows 7 User / Secure Boot Option, MS Windows 7 / BitLocker, MS Windows 2012 Server User / Secure Boot Option, MS Windows 2012 Server Active Directory Administrator, MS Windows 2012 Server / BitLocker, MS Windows 8 - 8.1 User / Secure Boot Option, MS Windows 8 - 8.1 / BitLocker, MS Windows 10 User / Secure Boot Option, MS Windows 10 / BitLocker, MS Windows Domain Administrator, MS Windows Live ID Account, MS Windows NTLM/LANMAN Hash, MS Windows Phone, MS Windows User / UPEK ✚ MS Word 1.0, MS Word 2.0, MS Word 3.0, MS Word 4.0, MS Word 5.0, ✚ MS Word 6.0, MS Word 95, MS Word 97, MS Word 2000, MS Word 2002, MS Word 2003, MS Word 2007, MS Word 2010, MS Word 2013 ✚ MS Word 2016, MS Word VBA, MYOB earlier than 2004, MYOB 2004 ✚ MYOB 2005, MYOB 2006, MYOB 2007, MYOB 2008, MYOB 2009, MYOB 2010, Network Connection, Norton Backup, Open Document, Paradox Database, Peachtree 2002 – 2006, Peachtree 2007, Peachtree 2008 ✚ Peachtree 2010, Peachtree 2013, PGP Desktop 9.x - 10.x Zip ✚ PGP Desktop 9.x - 10.x Private Key ring, PGP Desktop 9.x - 10.x Virtual Disk, PGP Desktop 9.x - 10.x Self-Decrypting Archive, PGP WDE 	
--	---	--

	<ul style="list-style-type: none"> • GnuPG Private key ring, Quattro Pro 5 – 6, Quattro Pro 7 – 8, Quattro Pro 9 - 12, X3, X4, QuickBooks 3.x - 4.x, QuickBooks 5.x, QuickBooks 6.x - 8.x, QuickBooks 99, QuickBooks 2000, QuickBooks 2001, QuickBooks 2002, QuickBooks 2003, QuickBooks 2004, QuickBooks 2005, QuickBooks 2006, QuickBooks 2007, QuickBooks 2008, QuickBooks 2009, QuickBooks 2010, QuickBooks 2011, QuickBooks 2012, QuickBooks 2013, QuickBooks 2014, QuickBooks for Mac 2013 • QuickBooks for Mac 2014, QuickBooks Backup, Quicken 95/6.0, Quicken 98, Quicken 99, Quicken 2000, Quicken 2001, Quicken 2002, Quicken 2003, Quicken 2004, Quicken 2005, Quicken 2006, Quicken 2007, Quicken 2008, Quicken 2009, Quicken 2010, Quicken 2011, Quicken 2012, Quicken 2013, Quicken 2014 • RAR 2.0 Archive, RAR 2.9 - 4.x (AES Encryption) Archive, RAR 5.x Archive, Remote Desktop Connection, Safari 5.0 - 5.1 Website • Schedule+ 1.0, Schedule+ 7.x, True Crypt Non-System Partition/Volume 5.0 or later, True Crypt System Partition/Volume 5.0 or later, True Crypt Whole Disk 5.0 or later, True Crypt Hidden Partition 6.0 or later, True Crypt Hidden OS 6.0 or later • Unix OS User Hash, Vera Crypt, WordPerfect 5.x, WordPerfect 6.0 • WordPerfect 6.1, WordPerfect 7 - 12, X3, X4, WinZip 8.0 or earlier • Yandex Browser Website, Zip Archive, 7-Zip Archive • Should allow instant decryption, password recovery with Dictionary and Brute-force methods. • Provision for GPU acceleration and distributed computing (both for Windows and Linux) for password recovery • Should support password recovery for Open Office files • Support for shared dictionaries • Support Instant reset of Windows 10 Live ID passwords • Support for RT12 tables for hashed passwords • Should support at least 100 Passware Kit Agents for distributed password recovery on up to 100 computers including both Windows and Linux platforms • Passware Kit Agent for Linux should allow running a portable Passware Kit Agent from a bootable Linux USB drive on any system without installation • Should scan computers for encrypted evidence • Should detect all the encrypted files & hard disk images, report encryption type and decryption complexity • Should support 64-bit version for improved performance while processing simultaneously larger dictionary files • Should support Batch processing - Run password recovery for groups of files without manual intervention • Should support Mobile Forensics - Recovers Passwords for Apple iPhone/iPad and Android backups, as well as Android images. Should be able to extract data from Windows Phones' images. • Should support Integration with Oxygen Forensic Suite • Live Memory Analysis support - Analyze live memory images and hibernation files and extract encryption keys for hard disks, logins for Windows & Mac users, and passwords for files and websites • Should be able to Decrypt FDE <ul style="list-style-type: none"> ▪ Encrypts or recovers passwords for Bit Locker, True Crypt, LUKS, FileVault2, Apple DMG, and PGP disk images ▪ Should be able to integrate with Guidance Encase ▪ One-click password recovery directly from Encase v7 and higher • Support accelerated password recovery with multiple computers, NVIDIA & AMD GPUs, Tableau Password Recovery & TACC, and Rainbow Tables • Support for an unlimited number of GPU cards for hardware acceleration • Should Include Passware Kit Forensic - 1-User License (Server) 	
--	---	--

	Password Kit Agents	5
	<p>Minimum Requirements :</p> <ul style="list-style-type: none"> • Processor - Intel® 4th generation Core™ i5 Quad Core • Operating System - Windows 8 64-bit/ Windows 8 Pro 64-bit/ Windows • 7 Home Premium SP1 32 bit/ Windows 7 Home Premium SP1 64 bit/ Windows 7 Professional SP1 32 bit/ Windows 7 Professional SP1 64 bit/ Windows 7 Ultimate SP1 32 bit/ Windows 7 Ultimate SP1 64 bit/ Ubuntu® • DIMM slots; Non-ECC dual-channel 1600MHz DDR3 SDRAM, supports up to 16GB Hard Drive • Hard Disk Drives: 1TB or higher • Supports Hybrid and Hybrid Opal SED FIPS • Integrated Intel® HD Graphics 4600 (with select CPUs) / discrete graphics solutions from AMD • Optical Drive : Support for optical disc drives and media card reader options • Security : Trusted Platform Module4 (TPM) 1.2,DataProtection SecurityTools, Encryption, Chassis lock slot support, Chassis Intrusion Switch, Setup/BIOS Password, I/O Interface Security, Smart Card keyboards, Intel® Trusted Execution Technology, Intel® Identity Protection Technology, Intel® Anti-Theft Technology, KACE Security, BIOS support for Computrace • Systems Management : Support Out of Band Systems Management • Ports <ul style="list-style-type: none"> ○ 2 external USB 3.0 Ports ○ 6 external USB 2.0 Ports ○ Serial Port ○ PS/2 port ○ RJ-45 Network Connector ○ VGA port • Connectivity Integrated Realtek® RTL8151GD Ethernet LAN 10/100/1000; support for PCIe 10/100/1000 network card, wireless 802.11n card support • USB KBD 7 Mouse • 22" Wide Screen LCD Monitor with Built-in Speakers 	

Latest version of Mobil Edit SIM Clone Package (including blank SIM cards)

- Should provide a SIM Card Reader/Writer application with at blank Rewritable SIM Cloning Cards
- Should provide both Clone and copy function for the SIM
- Should be able to modify the SIM details (ICCID, IMSI)
- Should be able to create custom SIM (ICCID, IMSI)
- Support format of SIM for data removal
- Support for connection of multiple readers

Cellebrite UFED Touch Ultimate (Ruggedized Kit) with UFED CHINEX, cables and accessories

Must be capable of both logical and physical mobile data extraction for different of mobile phones / smartphones with different operating system or chipset.

The collection of the mobile data extracted should be done through a standalone portable handheld device without requiring to connect to any computer devices.

- Should instantly provide mobile phone identification.
- Shall be able to perform physical, logical and file system extractions from Mobile phone handsets.
- Shall be able to do complete extraction of existing, hidden, and deleted phone data, including call history, text messages, contacts, images, GPS fixes and geotags
- Shall be able to perform enhanced decoding - enabling support for multiple data types such as:
 - SMS, contacts, chat, email, web history, SIM data, cookies, MMS, GPS location fixes, call logs, calendar, contacts and more
- Should support password protected, jail broken, non-jail broken, encrypted and non-encrypted iOS devices.
- Shall be able to perform Physical data extraction and password recovery from iOS devices: iPhone , iPad , iPod Touch 3G/4G
- Shall be able to do Tom Tom trip-log decryption and physical data extraction from other portable GPS devices.
- Should support decoding of JTAG physical extractions from a rich set of data
- Shall be able to bypass PIN/Pattern/Passcode lock from selected Android devices running any version.
- Shall allow identification of mobile device by various visual elements selections
- Shall be able to extract location information (such as Wi-Fi, cell tower and navigation applications) from iPhone, Blackberry and Android devices
- Should provide comprehensive analysis capabilities via Physical Analyzer including timeline, project analytics, malware detection, and watch list
- Shall be able to generate reports in PDF, HTML, XML, Excel with header and footer customization feature.
- Shall be able to generate at least MD5 & SHA256 hash signatures for data authentication.
- Shall be able to edit fields such as case name/number, examiner's name and more
- Shall be able to perform advanced physical extraction from iOS devices for encrypted and password protected devices
- Shall be able to perform Instant search – diving into the decoded data instantly allowing users to locate strings in the phone memory and directing them to the content's source
- Should be a complete field-ready mobile operational kit – compact tip connectors with at least 4 master cables for extraction and charging during usage
- Must be able to perform physical extraction of Blackberry devices running BB OS 4,5,6,7, from all available partitions (User and system)
- Must be able to decode physical extraction of Blackberry devices for recovering deleted data including deleted and group BBM messages
- Provides a specialized pin-out scanning solution to allow extraction from non-standard, Chinese made phones.

- Must be able to perform physical extraction from locked Nokia Symbian based (BB5 series) devices
- Must be able to decode physical extraction of Nokia Symbian based and BB5 based devices
- Must allow physical extraction from locked android phones.
- Must allow bypassing of password in order to perform physical extraction from locked android phones without having to have ADB enabled.
- Support extraction of devices running BADA OS – Physical extraction, password extraction and password removal.
- Support Forensic cloning of SIM ID to isolate the phone from network activity during analysis
- Support Logical and file system extraction of Apple devices running iOS 7.1/7.0.6/6.1.6
- Physical extraction and advanced decoding, via USB debugging, for ALL Android OS Versions including Android 4.X (Ice Cream Sandwich)
- 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, V Kontakte and more
- Should translate foreign-language content from extractions using an offline translation solution
- Support decoding of device and network timestamps for SMS and MMS from Motorola Android devices.
- Support decoding of Bluetooth MAC address and factory serial number from Samsung Galaxy S4 a
- Support enhanced locations decoding from file system and physical extraction from iPhone 4 running iOS 7.x
- Support enhanced decoding of application permission to include location service permissions.
- Support enhanced decoding of contact list, call log, calendar, tasks from Windows Mobile 6/6.5 physical extractions.
- Support enhanced email decoding from BlackBerry backup.
- Support enhanced decoding of WhatsApp including attachments and account information
- Support enhanced decoding of Facebook including users profile pictures, search strings and web history
- Support enhanced Decoding of Gmail app including deleted emails and support for new app versions of WeChat, Badoo, BlackBerry Messenger, Silent Phone
- Support decoding of existing and deleted data from these devices.
- Should be able to monitor events in a single chronological view
- Shall have advanced image carving capability
- Shall have Powerful feature used to recover deleted image files and fragments when only remnants are available
- Shall have ability to highlight information based on predefined list of values
- Shall have entities and hex bookmarking capability
- Allow viewing communications between sources in date and time order.
- Shall be able to do user password extraction.

- Shall allow viewing, searching, and exporting tables and content (including deleted data) from SQLite database files.
- Shall have Python scripting facility to enhance decoding and add customized decoding functions according to specific needs
- Solution shall provide analytical reports of decoded data, presenting statistical information of communication performed to/from the device
- Solution shall provide the ability to display a timeline of all decoded data with filtering capabilities by available fields
- Solution shall allow advance search capabilities in the HEX image, for strings, SMS, passwords, numbers, patterns, dates and more
- Should support Hexadecimal view of the extracted data enabling advanced search based on multiple parameters (regular expressions and more). Highlight the exact position for each decoded content entry, enabling full tractability between the analyzed data and the Hex.
- Solution shall allow user the flexibility to define or customize the decoding process.
- **Support Simplified workflow** for user to select the device and only then to select the action applicable for the device. The application should notify the user about the new workflow and instructions.
- **Support User authentication** – To enable the administrator to manage user accounts, and grant access to users with username and password. User authentication should ensure that only users with the right credentials can access the unit. Access rights should further be enforced by defining permission levels per profile.
- **Support Permission management-** To enable the administrator to create profiles that define the access permissions for the users, including access rights per extraction type, content types and more. A single profile can be assigned to multiple users. The users and profiles can be exported into an encrypted permission management file, which can be imported into multiple units.
- **Support Enhanced AutoDetect** – automatic AutoDetect upon device connection, which enables streamlined operational flow.
- **Support transaction counter** – Counting the number of transactions performed on the unit to monitor device usage. Transactions should include all extractions per type and device tool actions. The counters should be managed locally and can also be reset.
- Support to enable static IP setting through a setting interface.
- **Support Physical data Extraction from Phones manufactured with Chinese Chipsets**
 - ✓ Provide Physical extraction of existing, hidden and deleted data
 - ✓ Provide State-of-the-art decoding and reporting of data: Call logs, SMS, MMS, videos, images, apps data, deleted data, GPS fixes and much more
 - ✓ Provide User password extraction
 - ✓ Provide Automatic pin-out recognition
 - ✓ Provide Ability to bypass and decode the user lock from the extraction
- Should be able to access private-user cloud data utilizing login information extracted from the mobile device.
- Should be able to login to private-user cloud data using usernames and passwords provided by the investigated subject, retrieved from personal files, contacts or via other discovery

means.

- Extract information from cloud data sources while logging and tracing the entire process to maintain data authenticity.
- Should be able to normalize different cloud services in a unified format and view in Timeline, File Thumbnails, Contacts or Maps format.
- Provide Powerful decoding, analysis and reporting functions with its intuitive user interface, instant search, advanced highlights engine, superb hex viewer, report generator.

UFED ruggedized edition kit content

Part	Quantity
UFED Touch Device	1
UFED Solid Protector case	1
UFED Touch Leather case	1
Tip & Cable Set (Ultimate)	1
Tip & Cable Organizer	1
Ruggedized Carrying case	1
Case Embedded work surface	1
Faraday bag	1
UFED memory card reader	1
Micro SIM adapter	1
SIM ID cloning cards	5
Micro SIM ID cloning cards	5
UFED power supply	1
UFED external hard drive – 500 GB	1
UFED Lock scissors	1
Car power adaptor	1
UFED to PC cable	1
Phone power up cable	1
Current 5v To 6v adapter	1

Cleaning brush for phone connectors	1
UFED phone charger	1
Tip Velcro strap	1
Spare tips cartridge	1
UFED Chinex Kit	1
UFED Cloud Analyzer	1

KIT Weight & Dimensions (Recommended)

Weight & Dimensions	
Case Dimension (cm)	48.7 (L) x 38.6 (W) x 18.5 (H)
Weight	< = 10 Kg

UFED Touch HW Specifications: General Specification (Recommended)

Part	Description
Display	7" WVGA (800x480) TFT Touch LCD, 280 NITS LED
Operation System	Microsoft Window XP embedded or higher
Processor	Intel ATOM Z510 1.1GHz
Chipset	Intel Poulsbo US15W Premium chipset
System Memory	1GB DDR2, 333MHz (667 DDR2 Data Rate)
Storage	PSSD MLC NAND Flash: 64GB capacity
Power Supply	Input: AC 100-240V, 50/60Hz. Output: DC 12V, 4.16A (50w max)
Unit dimensions	237mm (W) x 127mm (D) x 39mm (H)
Weight	1Kg

Batteries

Part	Description
Type	Lithium Polymer, 7.4V, 3850mA.
Discharge time	While being used: 5 \pm 1 hr.
Recharge time	~3 hours

Network

Part	Description
Bluetooth	Wi2Wi – W2CBW003 (Integrated WLAN-B.T Sip), Bluetooth Specification V2.0 + EDR
Wi-Fi	Wi2Wi – W2CBW003 (Integrated WLAN-B.T Sip), 802.11 b/g (up to 54 Mbps data rate)

I/O Interfaces

Part	Description
USB ports	4 x USB 2.0 ports, 1 x Mini USB port
Serial Ports	RJ-45 for device and storage connectivity
SIM Card reader	Integrated SD card reader
Microphone & Speaker	Intel High Definition Audio , integrated microphone and speakers
Audio output	1 x Headphone jack
Video Output	1 x VGA Port

Latest version of Wet Stone Stego Flash

- Support Rapid identification of known steganography programs
- Should be able to detect suspicious files through blind anomaly-based approach
- Should Easily identify image artifacts and image characteristics
- Should support State-of-the-art image analysis with advanced image filters
- Should provide State-of-the-art audio analyzer
- Should be able to Crack and extract payloads from carrier files with a simple point and click interface.
- Should allow scan of different kinds of audio files, JPG, BMP, GIF, PNG and more
- Should be able to quickly, accurately and easily detect steganography programs as a first look in the investigation process by scanning for different data hiding applications using Fibonacci search methods or any other equivalent algorithms.
- Generate case specific reports for management or court presentations.
- Should be able to flag the suspected carrier types (program artifacts, program signatures, statistical anomalies). Once suspected carrier files are found, it should be able to automatically scan the entire file system and bring back results in an easy to read interface with suspected files flagged.
- Capability to scan forensic images of other popular forensic tools such as Encase, FTK, dd, Raw, ISO and safe back images.
- Provision for operational discovery modes (directory, drive, archives, drive image, network path)
- Provide anomaly based steganography detection tool.
- Files flagged should be detected with a blind detection technique looking for artifacts within those scanned media files and then displayed with a threat association and notification of any artifacts found.
- No prior knowledge of steganography programs should be necessary for operation.
- Provide a full featured imaging and analysis tool allowing investigators to search for visual clues that steganography has in fact been utilized in both image and audio files.
- Provide deep analysis for detected images and audio files
- Provide a built in utility to obtain the pass phrase that has been used on a file found to contain steganography.
- Should support a file viewing panel which displays the individual file image or audio wave and the file attributes including image details, DCT coefficients, color pairs etc.
- Should include filter options that transform the images into one of three different presentations: Intensity, Saturation or Hue. Other filter options should display only selected Least Significant Bits (LSBs) of specific colors.
- Should include popular password dictionaries in order to execute a dictionary attack and ability to bring in other dictionaries or if password is revealed through suspect questioning, can run that password against the detected image or audio files.
- Should quickly and easily crack and extract payloads from carrier files with a simple point and click interface.

ESD safe Workstation desks/cubicles

- Floating top designs with veneer/laminate/plywood , scratch and stain resistant work surfaces
- LHS/RHS styled desks for cabin layout
- Optimal usage of dead spaces for storage with flex boxes / side units/ sliding partitions or doors/in-built shelves / pullout trays
- Wire management using access flaps with wire carriers

ESD safe chairs

- Pneumatic height control with adjustable tension and lockout feature
- Swivel capability, Adjustable headrest, caster(s) included, ANSI/BIFMA certified, adjustable seat height, Armrests included, padded armrests, reclining, Locking tilt control with adjustable tilt tension control, Eco leather seating , built-in Lumbar support

ESD Safe racks

- 1No. Solid back stationery cabinets with at least 3 adjustable shelves and 3 point locking
- 2No. Mobile pedestal (with lock and pencil tray) –3 Drawer cabinet

List of Deliverables:

SI No	DESCRIPTION	QUANTITY REQUIRED	
18.	Forensic Recovery Evidence Data Center (FRED C), make- Digital Intelligence	1	1 Set
	Network Printer	1	
	Forensic Analysis client workstations	5	
19.	IDE/SATA to USB 2.0/3.0 converters ,make - Digital Intelligence	1	
20.	UFED Touch Ultimate (Ruggedized Kit) with CHINEX with UFED Cloud Analyzer, make – Cellebrite		1 Set
21.	Forensic Falcon , make- Logicube	1	1 Set
	Evidence Disk Drives	19	
22.	Passware Kit Forensics Lab Edition 2016 v.4 , make – Passware	1	1 Set
	Password Kit Agents PCs	5	
23.	Forensic Tool Kit v6 Standalone – Perpetual License –make, Access Data –	1	1 Set
	Toolkit Server PC	1	
24.	Latest version of Digital Evidence Investigator, make – ADF Solutions.	1	
25.	e-mail Examiner v7.1, make – Paraben	1	
26.	Latest version of F-Response Consultant Edition	1	
27.	Latest version of Adroit Photo Forensics tool , make- Digital Assembly	1	
28.	Latest version of Stego Flash , make- Wet Stone	1	
29.	Network Email Examiner 4.1, make – Paraben	1	
30.	Latest version of Chat Examiner, make – Paraben	1	

31.	Latest version of SIM Clone Package (including blank SIM cards) , make – MOBILedit	5	Set
	BlankSIMCards	200	
32.	ESD safe Workstation desks/cubicles	4	Set
	ESD safe chairs	10	
	ESD Safe racks	3	
33.	Forensics Lab Information Management System (F-LIMS)	1	
34.	Biometric Access Control System	1	