

ज्ञापांक. 1312/401835/आपूर्ति

92-1-3-2018

पुलिस महानिदेशक का कार्यालय, बिहार, पटना

पटना, दिनांक-17/12/18

सेवा में,

निदेशक,
सूचना एवं जनसम्पर्क विभाग,
बिहार, पटना।

विषय- निविदा आमंत्रण सूचना सं०-18/2018-19 के प्रकाशन के संबंध में।

निदेशानुसार उपर्युक्त विषय के संबंध में निविदा आमंत्रण सूचना सं०-18/2018-19 की प्रतियाँ भेजते हुए अनुरोध है कि इसे राज्य एवं राज्य से बाहर के प्रमुख समाचार पत्रों में (अंग्रेजी एवं हिन्दी) के अगले दो संस्करणों में प्रकाशित कराने की कृपा की जाय साथ ही पी०आर०डी० वेबसाईट पर भी प्रसारित करने की कृपा की जाय।

इस निविदा आमंत्रण सूचना का प्रकाशन किन-किन समाचार पत्रों में किया गया इसकी सूचना देने की कृपा की जाय।

अनु०-यथोपरि।

h
17/12

पुलिस महानिरीक्षक के सहायक (क्यू०),
बिहार, पटना

प्रतिलिपि:-

1. आई०टी० मैनेजर, पुलिस महानिदेशक का कार्यालय, बिहार, पटना को कृपया सूचनार्थ। कृपया इसे आज ही वेबसाईट पर अपलोड किया जाय। साथ ही Indian Trade Journal, Kolkata के अंक में प्रकाशन हेतु Government of India, the Controller of Publications, Civil Lines, Delhi : 110 054, (Tel No. 011-23812527, FAX : 011-23817846), Email Id- sk.mondal.dgcis@nic.in के पतेपर भी अनिवार्य रूप से भेजा जाय।
2. Government of India, the Controller of Publications, Civil Lines, Delhi : 110 054, (Tel No. 011-23812527, FAX : 011-23817846), Email Id- sk.mondal.dgcis@nic.in को कृपया सूचनार्थ एवं आवश्यक क्रियार्थ प्रेषित। अनुरोध है कि उक्त निविदा का प्रकाशन Indian Trade Journal, Kolkata के अंक में करने की कृपा की जाय।

h
17/12

पुलिस महानिरीक्षक के सहायक (क्यू०),
बिहार, पटना

182

Police Headquarters, Bihar, Patna
Notice Inviting Tender No.-18/2018-19

1. Name of the Department: Office of Director General of Police, Bihar, Patna.
2. Date & Time for Pre-Bid Meeting : 31 /12/2018 At 11:00 AM
3. Last date & time for the acceptance of the tender : 21 /01 /2019, Till 02:00 PM
4. Date & time fixed for the opening of the tender : 21 /01 /2019, At 04:00 PM
5. Place fixed for receiving & opening the tender : Office of Director General of Police, Bihar, Patna.

6. Details of Job:

S.N.	Item name	Quantity
1	Desktop	30
2	Laptop	12
3	Hard Disk 6 TB	05
4	CAT 6 Cable Bundle with Crimping Tool	03
5	UPS	03
6	Software for Data Extraction of Mobile, GPS, PDA, Tablet, Chinese Phones with Cloud Based Data Extraction.	01
7	Portable Investigator Tool	01
8	Software for Forensic Extraction of Mobile, PDA, GPS, Drone, Tablets Data with Simultaneous Extraction Option.	01
9	Disk Forensic Analysis Software.	01
10	Forensic Video Analysis Tools.	01
11	Forensic Video Acquisition Tool Kit.	01
12	Network Miner	01
13	Social Media Workstation.	02
14	High End Forensic Workstation with Inbuilt Write Blocker and Duplicator.	02
15	Write Blocker Kit with High End Forensic Duplicator.	01
16	Comprehensive Drive Extraction and Internet Artifacts Analysis Tool.	01
17	Social Media Analysis Tool.	01
18	Disk Forensic Tool Kit with Malware Analysis Tool.	02
19	Multiple GPU Based Password Recovery/Cracking Solution.	01
20	First Responder Portable Field Kit.	01
21	MAC Acquisition & Analysis Tool.	01
22	CD/DVD/Examiner.	01
23	Web Server & Data Base Server.	01
24	E3 Universal with Chat Stick and Porn Stick.	01
25	Managed Switch 8 Port.	04
26	Mini Screw Driver Tool Set.	02

27	Blower	01
28	Colour Network Printer.	01
29	Offline Colour Laser Printer.	02
30	Hardware Firewall.	01
31	KVM Switch-8 Port.	02
32	26-U Rack.	02
33	GIGA BIT Ethernet Switch 24 Ports.	01
34	Powered Portable HDD-10 TB	02
35	BIG Size Touch Screen LED.	01
36	LED Display Screen.	01
37	4-Channel PIP Split-Screen Video.	01
38	Visualiser.	01
39	Podium with I-Panel.	01
40	Table Microphone for Podium.	01
41	Collar Microphone.	02
42	Cordless Microphone.	02
43	Audio System.	01
44	Video Camera.	01
45	Network Switch.	03

Specifications and other terms & conditions of the tender may be obtained in person from this office or may be downloaded from the website www.prdbihar.gov.in or www.biharpolice.bih.nic.in.

h
17/12/18

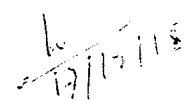
AIG (Q)
Bihar, Patna

Terms & Conditions of Tender No.-18/2018-19

180

1. The tender should be submitted in two parts: (i) Technical Bid and (ii) Financial Bid, duly sealed in two separate envelopes super-scribed as "Technical Bid" and "Financial Bid".
2. All relevant papers/ E.M.D./certificates/specifications etc. of items should be enclosed in the Technical Bid.
3. The rates of the items shall be quoted in the Financial Bid only.
4. All charges like IGST/CGST/SGST etc. shall be clearly mentioned in the Financial Bid and the net rate (in figures and words) including all taxes and duties must also be quoted. Vague offers like indicating taxes "as applicable" will not be accepted.
5. The rates of the items shall be quoted in the Financial Bid in two parts :
(i) With AMC (Annual Maintenance Contract) and (ii) Without AMC
6. There should be no cutting, over writing or correction on the rates.
7. The technical and financial bids for each item should be submitted separately in separate envelopes. The technical and financial bids for more than one items submitted together in the same envelope shall not be accepted.
8. If the financial bid is submitted in the same envelope containing the technical bid then also it shall be summarily rejected.
9. The technical and financial bids should be put in two separate sealed envelopes and the envelopes should be marked Tender No-18/2018-19 (Technical Bid) and Tender No-18/2018-19 (Financial Bid) along with the name and address of the firm. The sealed envelopes containing the technical and the financial bids should be sent in another sealed envelope which should be marked as Tender No-18/2018-19. This envelope should not bear the name and address of the firm.
10. Income Tax Returns of last three years, a photocopy of GST registration number of the participating firm and turn-over of any two of the previous three financial years should be submitted with the technical bid. It should be specifically mentioned whether IT return has been filed manually or electronically.
11. The turnover of the firm for the last reported financial year should be at least equal to the amount of the supply order which is being issued. A copy of the profit and loss Account of the firm for any two of the previous three financial years, certified by a Chartered Accountant should be submitted along with the tender. If the tenderer is authorized dealer or authorized supplier of manufacturing firm, then the certified details of the turnover of authorizing firm may be accepted. Tender specific authorization from the OEM must be submitted, but in certain cases where authorization from OEM is not required, the Technical-cum-User committee (T.U.C.) shall decide about exemption (if any) on a case-by-case basis; citing appropriate reasons for the same.
12. If there is some discount in the price of any item, it should be deducted from price itself and such discounts should not be quoted separately.
13. If the product is available on DGS & D rate contract, then a copy of the contract must be attached and pricing be done including all taxes.
14. A copy of the test report for the product issued by any established and recognized private Laboratory or by agency accredited by the Government should be attached with the technical bid. However if required, the Technical-cum-User committee (T.U.C.) can take decision regarding exemptions/relaxations (if any), citing appropriate reasons.
15. In case of Bullet Proof/Bullet Resistant items, test report of TBRL or any Government Approved/Recognized Laboratory is compulsory.

16. Firms participating in this tender shall also submit duly sworn affidavit to the effect that " this firm has not been black listed/debarred by any Government or Semi Government or Private Agency and no sister concern of this firm is participating in this tender."
17. Firms participating in this tender shall also submit the self attested list of users of its equipments.
18. All items shall be received at Central Clothing Store, Patna; therefore price should be quoted FOR Central Clothing Store, Phulwari Sharif, Patna.
19. Firms will have to deposit a sum of Rs.50,000/- (Fifty Thousand) only as an earnest money deposit in the form of Bank Draft duly pledged in favor of the undersigned along with the quotations. The small scale units located in Bihar shall not be liable to deposit earnest money. Exemption from submitting E.M.D. will also be available to those who are registered with the Central Purchase Organization/State Purchase Organization and National Small Industries Corporation (NSIC).
20. Technical Bids will be opened on scheduled date and time in the office chamber of Police Headquarter. Representatives of the firms competing in the tender may remain present at the time of opening of the technical bid.
21. The technical bids will be opened first and placed before the Technical Committee of the Police Headquarters, Bihar. If the technical bids are found satisfactory as per tender conditions, it will be put before Central Purchase Committee of the Police Headquarters, Bihar. The firms may be required to participate in the demonstrations of the quoted product and discussions with this committee.
22. Any paper/document will not be accepted after opening the tender.
23. Successful firm will have to enter into an agreement after depositing a sum of 5% of the total value of the order as security money in the form of Bank Guarantee duly pledged in favor of undersigned.
24. The firm will be required to provide satisfactory after-sales service after the delivery of the product.
25. The firm will be required to supply all the items within the stipulated time frame as mentioned in the purchase order.
26. Payment for the delivered items will be made only after the acceptance report of the Inspection Committee of the Police Headquarters, Bihar.
27. The firm whose quotation is approved by the Central Purchase Committee of the Police Headquarters, Bihar, shall be invited to enter into an agreement with the undersigned.
28. It is expected to submit the duly filled chart attached herewith, along with the technical bid if not the tender shall be summarily rejected.
29. Indexing of the requisite documents must be done and submitted along with the technical bid.
30. Hands on training for 3 weeks of the equipment must be imparted to the user group by the firm after successful installation.
31. Director General of Police Bihar, Patna reserves the right to reject any or all the quotations partially or fully, without assigning any reason thereof.
32. The Quantity indicated may increase or decrease at the time of issuing purchase order.
33. The bids must be include the data sheet of individual item.


A I G (Q)
Bihar, Police.

Description of item	Description	
<u>Desktop</u>	Specification	
	Processor	
	Processor Make	Intel
	Processor Generation	7th
	Processor	Intel Core i7-7700 (3.6 GHz, 8 MB Cache, 4 Cores)
	Chipset	Intel B250
	Graphics Type	Integrated
	Graphic Memory	2 GB
	Operating System (Pre-Loaded)	Windows 10 Professional
	Type of RAM	DDR 4
	RAM Size (GB)	8
	RAM Expandability upto (GB)	32
	RAM Speed (MHz)	2400
	Hard Disk (GB)	1000
	Cabinet	Tower
	Cabinet Volume (Litres)	14.8
	Internal Bays	2
	External Bays (Number)	1
	DIMM Slots (Number)	2
	USB Port 2.0 (Number)	4
	USB Port 3.0 (Number)	4
	Monitor Size (INCHES)	21.5
	Monitor Resolution (PIXELS)	1920x1080
	Mouse	Optical
	Keyboard	Standard
Optical Drive	DVD R/W	
Internal Speaker	Yes	
On Site OEM Warranty (Year)	3	

LAPTOP

Specification

Processor Make	Intel
Processor Generation	8 th
Processor	Intel Core i7 8550U (1.8 GHz, 8 MB Cache, 4 cores)
Graphics Type	Dedicated
Graphics Card Description	NVIDIA® GeForce® 940MX 4 GB DDR3
Graphics Memory (GB)	4
Type of RAM	DDR 4
RAM Size (GB)	8
RAM Expandable upto (in GB) using spare DIMM Slot on Mother Board	32
RAM Speed (MHz)	2400
Type of Hard Disk Drive	SATA
Hard Disk Drive Size(GB)	2000 gigabyte
Hard Disk Drive Speed (rpm)	5400
Operating System	Windows 10 Home
Network Connectivity	Ethernet Gigabit 10/100/1000
Wi-fi Connectivity	802.11 a/b/g/n
Bluetooth	4.0 or higher
Display Size (Inch)	15.6
Display Resolution (Pixel)	1920 x 1080
Optical Drive	Yes
Keyboard	Backlit
Battery Type (Li-Ion/Li-Polymer)	Removable
Battery Back-up (Hours)	9
Battery Warranty (Year)	1
On Site OEM Warranty (Year)	1

HARD DISK 6 TB

Specification

Type	External Portable
Connectivity	Wired
Digital Storage Capacity (TB)	6
Speed (rpm)	7200
Data Transfer Rate (Gb/sec)	160 MB/s

	OS Compatibility	Windows® 10 / Windows 8.1 / Windows 8 / Windows® 7 / Mac
	Dimension (W x H x D) (mm x mm x mm)	4.646 x 1.614 x 7.799" / 118.0 x 40.99 x 198.1 mm
	Standard Accessories to be supplied with the Hard Disk	Power Adapter, 4.0' / 1.2 m USB 3.0 Cable
	Operating Temperature Range (Degree C)	0-45
	Operating Humidity (% RH)	90
	On Site OEM Warranty (Years)	2
CAT-6 CABLE BUNDLE	Specification	
	Conductor diameter Nominal (Range) (mm)	0.5
	Number of pair (Number)	4
	Lenght of cable in a bundle (Mtrs)	305
	Conductor Materail	Copper
	Insulation	PVC
	Minimum Diameter over insulation (mm)	305
	Overall diameter of cable (mm)	0.5
CRIMPING TOOL	Specification	
	Length of Hand Tool in mm	165
	Weight of hand tools in Grams	185
	Width of hand tools in mm	4 millimeter
	Jaw length of Hand tool in mm	4 millimeter
	Jaw Thickness of Hand tool in mm	4 millimeter
UPS 10 KVA	Specification	
	Rating in KVA (KVA)	10.0 KVA
	Input Power	single phase 160V - 260V sinewave,50Hz
	Output power	Single phase 230V +/-1% sinewave 50 Hz
	Backup time (Minutes)	120

	<table border="1"> <tr> <td>Warranty for UPS (Years)</td> <td>3</td> </tr> <tr> <td>Movable trolley for Batteries</td> <td>With trolley or with rack</td> </tr> <tr> <td>Warranty for battery</td> <td>2</td> </tr> <tr> <td>Installation and Commissioning</td> <td>Yes</td> </tr> </table>	Warranty for UPS (Years)	3	Movable trolley for Batteries	With trolley or with rack	Warranty for battery	2	Installation and Commissioning	Yes														
Warranty for UPS (Years)	3																						
Movable trolley for Batteries	With trolley or with rack																						
Warranty for battery	2																						
Installation and Commissioning	Yes																						
UPS 5 KVA	<table border="1"> <thead> <tr> <th colspan="2">Specification</th> </tr> </thead> <tbody> <tr> <td>Online UPS should support for critical infrastructures such as Data Centres, Network operating centres, Security operation centres, State and District centres, Command and Control centre etc., across the Country to provide impetus to the e-Governance services e.g. Public food distribution, e Way bill, Counseling, e-Office, IVFRT etc., services under Digital India Programme</td> <td>Yes</td> </tr> <tr> <td>On Line UPS Capacity/Battery back up time at full load/Minimum VAH</td> <td>5 KVA/60 Minutes/8193 VAH</td> </tr> <tr> <td>Inverter Technology</td> <td>PWM with IGBT, double conversion</td> </tr> <tr> <td>Noise level (1 meter distance from UPS)</td> <td><= 55 dB</td> </tr> <tr> <td>UPS shall be supplied with required rated power cable (Copper)</td> <td>5 Meters</td> </tr> <tr> <td>Battery recharge time (after complete discharge to 90% charge) and charge rating: Battery recharge time to 90% charge after 100% DoD</td> <td>8 to 10 hours</td> </tr> <tr> <td>Battery cutoff voltage during back up</td> <td>Not less than 10.5 V</td> </tr> <tr> <td>Batteries shall supply with</td> <td>With trolley or With rack</td> </tr> <tr> <td>Warranty for UPS (on site comprehensive warranty) (in years)</td> <td>4</td> </tr> <tr> <td>Warranty for battery (replacement warranty) (in years)</td> <td>2</td> </tr> </tbody> </table>	Specification		Online UPS should support for critical infrastructures such as Data Centres, Network operating centres, Security operation centres, State and District centres, Command and Control centre etc., across the Country to provide impetus to the e-Governance services e.g. Public food distribution, e Way bill, Counseling, e-Office, IVFRT etc., services under Digital India Programme	Yes	On Line UPS Capacity/Battery back up time at full load/Minimum VAH	5 KVA/60 Minutes/8193 VAH	Inverter Technology	PWM with IGBT, double conversion	Noise level (1 meter distance from UPS)	<= 55 dB	UPS shall be supplied with required rated power cable (Copper)	5 Meters	Battery recharge time (after complete discharge to 90% charge) and charge rating: Battery recharge time to 90% charge after 100% DoD	8 to 10 hours	Battery cutoff voltage during back up	Not less than 10.5 V	Batteries shall supply with	With trolley or With rack	Warranty for UPS (on site comprehensive warranty) (in years)	4	Warranty for battery (replacement warranty) (in years)	2
Specification																							
Online UPS should support for critical infrastructures such as Data Centres, Network operating centres, Security operation centres, State and District centres, Command and Control centre etc., across the Country to provide impetus to the e-Governance services e.g. Public food distribution, e Way bill, Counseling, e-Office, IVFRT etc., services under Digital India Programme	Yes																						
On Line UPS Capacity/Battery back up time at full load/Minimum VAH	5 KVA/60 Minutes/8193 VAH																						
Inverter Technology	PWM with IGBT, double conversion																						
Noise level (1 meter distance from UPS)	<= 55 dB																						
UPS shall be supplied with required rated power cable (Copper)	5 Meters																						
Battery recharge time (after complete discharge to 90% charge) and charge rating: Battery recharge time to 90% charge after 100% DoD	8 to 10 hours																						
Battery cutoff voltage during back up	Not less than 10.5 V																						
Batteries shall supply with	With trolley or With rack																						
Warranty for UPS (on site comprehensive warranty) (in years)	4																						
Warranty for battery (replacement warranty) (in years)	2																						
SOFTWARE FOR DATA EXTRACTION OF	<ul style="list-style-type: none"> • All-in-one mobile forensic Software solution adding flexibility and convenience to investigations • Trusted technology providing users with all physical, file system and logical 																						

**MOBILE, GPS,
PDA, TABLET,
CHINESE
PHONES WITH
CLOUD BASED
DATA
EXTRACTION**

- extraction capabilities
- Should come with specialized adaptor to connect mobile handset to mitigate driver issues for various mobile handset.
 - Physical extraction and decoding while bypassing pattern lock / password / PIN from Android devices including HTC, LG, Motorola, Samsung Galaxy S family (including Galaxy SIII and S4), i phone and more
 - Widest support for extraction and decoding from Apple devices running iOS3+
 - Physical extraction from BlackBerry® devices running OS 4-7. Exclusive decoding: BBM data, apps, emails, Bluetooth and more.
 - Physical extraction and decoding from locked Nokia, BB5, Apple devices – password extraction from selected devices
 - Shall be able to generate MD5 & SHA256 hash signatures for data authentication
 - Shall be able to generate Reports with the organization logo.
 - Shall have advanced image carving capability
 - Shall have entities and hex bookmarking capability
 - Shall have Python scripting facility to enhance decoding and add customized decoding functions according to specific needs
 - File system extraction from any device running Windows phone 7.5 and 8 including Samsung, Nokia, HTC, Huawei and ZTE
 - Should recover physical data from phones with Chinese chipsets. Enables the physical extraction of evidentiary data and passwords from phones manufactured with Chinese chipsets, such as MTK, Spreadtrum and Infineon using specialized proprietary tips at least 25+ tips for Chinese phones and connectors and alligator clips.
 - TomTom® trip-log decryption, and data extraction from other portable GPS devices
 - Rich set of decoding: application data, passwords, emails, call history, SMS, contacts, calendar, media –files, location information etc.
 - Generate and customize easy-to-read reports and customize reports in different formats e. g. PDF, HTML, XML and Excel
 - Deploys custom boot loaders to ensure forensically sound extractions

	<ul style="list-style-type: none"> • Frequent updates to ensure compatibility with new phones as they enter the market • Exhibits multiple locations of a suspect on a single map • Unique evidence verification engine enables validation of recovered artifacts • User-friendly UI • Camera Kit to Add image categories and descriptions in the UFED to generate reports, Capture images/videos of the device as evidence, even when data is not extractable • Access private-user cloud data utilizing login information extracted from the mobile device • 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. • Case containing specialized Tip Set inbuilt with boot loaders & Proprietary Cable Set, SIM ID Cloning Cards, Micro SIM ID Cloning Cards, Nano SIM ID Cloning Cards, Multi SIM Card Adapter, Memory Card Reader.
<p>PORTABLE INVESTIGATOR TOOL</p>	<ul style="list-style-type: none"> • Customizable System Information Gathering for live system acquisition • Should have ability to be run on systems without a valid operating system. • Index and Search within the file contents of Office, Acrobat documents, image files and more • Search through email archives from Outlook, ThunderBird, Mozilla and more • Uncover recent activity of website visits, downloads and logins • Collect detailed system information • Password recovery from web browsers, decryption of office documents • Discover and reveal hidden areas in your hard disk • Browse Volume Shadow copies to see past versions of files • Verify and match files with MD5, SHA-1 and SHA-256 hashes • Find misnamed files where the contents don't match their extension • Create and compare drive signatures to identify differences • Timeline viewer provides a visual representation of system activity over time • File viewer that can display streams, hex, text, images and meta data

- Email viewer that can display messages directly from the archive
- Registry viewer to allow easy access to Windows registry hive files
- File system browser for explorer-like navigation of supported file systems on physical drives, volumes and images
- Raw disk viewer to navigate and search through the raw disk bytes on physical drives, volumes and images
- Web browser to browse and capture online content for offline evidence management
- ThumbCache viewer to browse the Windows thumbnail cache database for evidence of images/files that may have once been in the system
- SQLite database browser to view the and analyze the contents of SQLite database files
- ESEDB viewer to view and analyze the contents of ESE DB (.edb) database files, a common storage format used by various Microsoft applications
- Prefetch viewer to identify the time and frequency of applications that been running on the system, and thus recorded by the O/S's Prefetcher
- Plist viewer to view the contents of Plist files commonly used by MacOS, OSX, and iOS to store settings
- UsnJrnl viewer to view the entries stored in the USN Journal which is used by NTFS to track changes to the volume
- Case management enables you to aggregate and organize results and case items
- HTML case reports provide a summary of all results and items you have associated with a case
- Centralized management of storage devices for convenient access across all OSForensics' functionality
- Drive imaging for creating/restoring an exact copy of a storage device
- Rebuild RAID arrays from individual disk images
- Install OSForensics on a USB flash drive for more portability
- Maintain a secure log of the exact activities carried out during the course of the investigation
- Sort image files by colour

	<ul style="list-style-type: none"> • Disk indexing and searching not restricted to a fixed number of files • No watermark on web captures • Multi-core acceleration for file decryption • View NTFS directory \$I30 entries to identify potential hidden/deleted files
<p>SOFTWARE FOR FORENSIC EXTRACTION OF MOBILE, PDA, GPS, DRONE, TABLETS DATA WITH SIMULTANEOUS EXTRACTION OPTION</p>	<ul style="list-style-type: none"> • Should be all in one mobile forensic system • Should combine both mobile phone logical and physical solution in one package • Should allow investigator full access to all the possible method to recover data from a mobile device • Should built software based solution ,complete with all necessary hardware for recovering data from mobile device in a secure manner and go deeper in to a mobile device to recover vital data • Should have a combination of logical and physical analysis tool available for supported device • Should produce a combine report containing both live and deleted data from the same handset • Should Perform simultaneous operations like extraction, decoding and analysis, on a single platform • Should includes multiple mobile phone extraction capability simultaneously atleastuptothree(3) devices. • Should be able to recover deleted data e.g. contacts, image, SMS, emails, VOIP Call Data, video, GPS locations etc. • Should be able to decode mobile Apps such as Viber, Whatsapp, Skype, Facebook, messenger, QQ, etc, • Extraction should supports acquisition of internal memory and removable media. • Should generate hex-dumps from the phone memory, typically by bypassing the device operating system • Physical extraction allows users to generate hash values of the memory image, as well as individually decoded files. • Should support GPS Device Physical extraction and Examinations • Should have Triage Mode • Should allow search of data either by specific parameters or open text

	<ul style="list-style-type: none"> • Should able to clone card Mini/Micro/Nano • Should have Write Protected Universal Memory Card Reader and you can analysis the same. • It should automatically generates an audit trail of the forensic process for peer review • It should recover VOIP call data, GPS mapping information and instant messaging logs • Should have Report Generator to generate and customize reports in different formats e. g. PDF, HTML, XML and Excel • Extract data from non-standard mobile devices • The device must come with a add on Kit which should support maximum number Chinese mobile phones having mother boards with Chinese chipsets (Pin Point) • Should support Chinese chipsets.
<p>DISK FORENSIC ANALYSIS SOFTWARE</p>	<p>The industry-standard technology solution for capturing, analyzing and reporting on digital evidence. Powerful filters and scripts enable investigators to build a case based on forensically sound evidence. Investigators can collect actionable intelligence from Internet activity, chat sessions, email, documents, graphics, address books and over two hundred additional file formats. They can recover digital evidence residing in deleted files, reformatted disks, swap and slack space, hidden files, print spools and more. In addition, EnCase Forensic helps investigators review data that other tools cannot access, including system files and encrypted data.</p>
<p>FORENSIC VIDEO ANALYSIS TOOLS</p>	<ul style="list-style-type: none"> • Import video, image and audio files quickly and easily. • Batch import video sequences from VMSeS like Milestone and numerous directly supported proprietary files • Convert analogue to digital • Connect to an IP camera to stream video into your investigation • Rapidly decode video using a unique combination of Windows codecs • Capture from proprietary player using specially designed capture tool • Automatically analysis codec and encoding of a file type. • Import multiple different sources of video simultaneously • Add evidential metadata to you video like source, exhibit reference etc.

	<ul style="list-style-type: none"> • Correct time anomalies by offsetting the time to the speaking clock. • Utilize advanced video analytics to filter events • Search video automatically by Directional i.e. movement right, left, straight etc. • Search video automatically by Object colours • Search video automatically by Region i.e. partial view of recording • Review key events frame by frame • Speed up video playback for rapid reviewing • Jump from event to event automatically by playing all events • Zoom in on key areas of the video to see objects clearer • Bookmark key persons of interest and events quickly using tagging features • Export your viewing log to excel, word or pdf • Use frame by frame editing functions to create precise evidential packages • Clarify images and video using contrast and brightness • Apply multiple layered clarification techniques including Brightness & Contrast, Crop, Histogram Stretch, Histogram Equalize, Rotate, Mirror, Contrast stretch, Deinterlace, Noise removal, Sharpen, Scale filters • Layer enhancement filters and view step by step the approaches taken •
<p>FORENSIC VIDEO ACQUISITION TOOL KIT</p>	<ul style="list-style-type: none"> • directly, Offered Tool should be able to bypass any system passwords and recover data from non-functioning systems. • Tool should be able to identify the proprietary DVR filesystem used by the surveillance system, which means you do not need to know the make or model of the DVR. • Tool should scan the hard drive to identify recoverable clips. Users can easily sort or filter the clip list to identify the video you need. • Easily watch the DVR video within Tool, eliminating any need for external DVR Players. • Tool should offer a forensically safe option for surveillance DVR data recovery. Queue exports of native or open video and save time with the included export report. • Tool should make it easy to view, analyze, and categorize videos in the integrated

video player.

- Tool should overlay critical (and correct) metadata into the preview for Examiner.
- Should be able to easily save a still image or an openly playable video clip.
- Use tags to easily mark and locate video clips based on information that is important to the case.
- Tool should have Motion Analytics Engine enabling to easily identify which clips to review first based on motion activity.
- Receive a list of motion events and easily jump to the video that matters.
- Filter and sort video using the identified level of motion in each clip to highlight which video clips have the most action.
- Should have motion score to identify which clips have more motion activity relative to other clips.
- Tool should have feature to recover video that is no longer accessible to the DVR. This allows Examiner to recover formatted, deleted, or partially overwritten video.
- Tool should have ability to overlay critical metadata such as Channel and Date/Time during preview, allowing you to easily develop a timeline of events.
- Tool should identify the type of recording for a given video clip. This allows to easily identify clips that were triggered by motion or recorded on schedule.
- Tool should recover the system defined channel name, giving insight into the area or view for each video clip.
- Tool should have feature to recover recorded audio from the DVR.
- By accessing the DVR hard drive (or forensic image) directly, Tool should identify and recover video significantly faster than manually exporting individual clips from the DVR itself.
- Easily multi-task Tool should also Queue up multiple exports, view multiple previews at the same time, and begin reviewing video while the scan is still progressing.
- Should be able to export both playable AVIs and native files
- Tool should provide any necessary player to review the native exports.
- Support for **100+ DVR Proprietary File Systems** including NVP_3000P filesystem, new variant of the STLfilesystem, UWARE_264filesystem, NAFS_264, Mirage_HiSi

	<p>and Mirage_IVNET filesystems</p> <ul style="list-style-type: none"> • Tool should support <u>1000+ DVR's</u> • Tool should have facility to add Profiler of the unsupported DVR within the Software to add its support from OEM in future releases • Offered Tool should have continuous filesystem updates feature to download latest filesystems just like any Anti-Virus program • Tool should also come with IDE/ SATA Write Blocker Device for protecting Original DVR Hard Disks from tampering. Write Blocker should be able to connect with any standard Laptop/ Desktop using USB3 connection. Write Blocker should be Read-write and read-only switchable • <u>Precession Tool Kit : for opening various DVR's</u>
<p>NETWORK MINER</p>	<ul style="list-style-type: none"> • Software for geographically distant consulting or E-Discovery teams needing direct access to a wide array of potential target machines. • Should connect to a virtually limitless number of remote target machines and allows the examiner to obtain completely vendor neutral, write protected access to remote physical disks, logical volumes, and in some cases physical memory from over ten different remote operating system environments • Should provide direct, live, read-only access to the remote target computer's disks, volumes, and in certain cases physical memory. Since all access is at the physical level there is no file level locking, giving access to any and all content on the remote target, including protected system content (Registry files, Email PSTs, Database Files, etc). • 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. In addition, it should be designed to use minimal resources and is highly portable, requiring only the minimum resources necessary to run Windows XP. • Should support the largest array of remote target platforms including the following: <ul style="list-style-type: none"> - Windows Includes Windows 2000, XP, 2003, Vista, 2008, 7, 8, 10, 2012, 32 and 64bit, Physical memory only supported on 32bit and 64bit Windows

	<ul style="list-style-type: none"> - Apple OSX Includes OSX 10.3 to 10.11 Universal Binary (Field Kit only supports Intel Apple OSX) - Linux includes most Linux distributions build on Glibc 2.3.5 and higher, Android on ARM, and Embedded Linux (NetgearReadyNAS) - Solaris includes Solaris 8, 9, & 10 on SPARC and OpenSolaris on Intel - IBM AIX includes AIX 5.1, 5.2, 5.3, 6.1 on the Power processor - HPUX includes HP_UX11iv2,11iv3 on the Itanium processor - FreeBSD includes FreeBSD 7 on the Intel/i386 processor - SCO includes SCOOpenServer 6 and Unixware 7 on the Intel/i386 processor
<p>SOCIAL MEDIA WORKSTATION</p>	<p>Processor: Intel Core 7th Generation i7-7700 Processor RAM: 32GB Windows: 10 Pro (64 Bit) HDD: 1TB Graphics: 4GB With wifi card Monitor: 22" LED KeyBoard Mouse (wired) Should be Branded</p>
<p>HIGH END FORENSIC WORKSTATION WITH INBUILT WRITE BLOCKER AND DUPLICATOR</p>	<ul style="list-style-type: none"> • 2.1 GHz, Dual Intel Xeon E5-2640 v4, 10 Core, 20 MB Cache (10 core) • RAM 64GB (DDR5 or above) • 1x512NVMeSSD -OS Drive • 1x512GB SolidStateSATA III Drive- Cache • 1x512GBSolidStateSATA IIIDrive pro series-Temp • 1x10TB7200 RPMSATAHardDrive-DataDrive • 128 BIT GDDR5, 768 CUDA CORE 4GBDedicated Graphics card • 27"WideScreenLED Monitor • Windows10Professional (64bit)or latest • Licensed Linux (64 bit) • AnIntegratedWrite-Blocker toensureforensically soundaccesstoalltypesofmediainterfaces. <ul style="list-style-type: none"> ➤ Direct support for USB 3.0, SATA, FireWire800/400, IDE, SAS, PCIe drive interface ➤ touch-screen user interface. Displays device details, display and manage

	<p>LUNs and HDD protected regions. Examine file partitions.</p> <ul style="list-style-type: none"> ➤ Write-Block and Read/Write visibility via Lock/Unlock LEDs ➤ Read and write mode capabilities for all device ports controlled via LCD Menu ➤ Integrated support on the write blocker to Allow simultaneous imaging of 2 attached devices without any software manipulation <ul style="list-style-type: none"> • 1100WattModularpowersupply • Motherboardwith Intel®C612 PCH Chipsetorhigher • Integrated Forensic Media Card Reader - Read-Only or Read-Write mode capable • Integrated Retractable imaging shelf (fully retracts into the system when not in use) with Dual fans for maximum cooling and surface coverage and Slotted, cushioned, non-conductive, non-skid, surface to place the evidence when connected to the Write Blocker and supports all popular drives IDE/SATA/SAS/USB • 2 x Shock Mounted SATA Removable Hard Drive Bays (IDE Capable) • 4 x HotSwap Shock Mounted Universal (IDE and SATA compatible) Removable Hard Drive Bays • BD-R/BD-RE/DVD±RW/CD±RW Blu-ray Burner Dual-Layer Combo Drive • RJ45 LAN ports (2 X 1 Gigabit) • USB 3.1 (Minimum 3 ports) • USB 3.1 type C (Minimum 1 port) • USB 3.0 (Minimum 11 ports) • USB 2.0 (Minimum 2 ports) • Keyboard and Mouse Combo • Esata 6 Gb/S (Minimum 2 ports) • Tool box containing: <ul style="list-style-type: none"> ➤ CD Case: Containing system restore media. ➤ System Keys: For removeable hard drive bays and front case bezel. ➤ Adapters and Cables: Cables and adapters to image and process internal/ external drives including SAS, SATA, IDE, microSATA, SATALIF, MacBook Air Blade Type SSDs, mini/micro SSD cards, 1.8 inch IDE (iPod), 2.5 inch IDE (laptop), PCIeSSDm.2NVMe, PCIeSSD MacBook Pro and Server Class
--	--

	<p>PCIe SSD</p> <ul style="list-style-type: none"> ➤ Digital Camera: Useful to document your suspects environment and hardware. ➤ Security Screwdriver Set: A varied assortment of popular security bits for opening computer enclosures that may have been locked down in a corporate environment
<p>WRITE BLOCKER KIT WITH HIGH-END FORENSIC DUPLICATOR</p>	<ul style="list-style-type: none"> • Portable kit which contains a complete family of hardware write blockers along with adapters and connectors • Should include separate Portable Write Blockers with following connection: IDE/ SATA SAS USB3 FireWire PCIe • All connectivity on Host side should be USB3 or better • Should also contain Forensic Memory Card Reader • Forensic Memory Card Reader should be switchable from Read-Only to Read-Write operation • Should have USB3 Read Only/Read Write switchable External Hard Drive Chassis with Power Supply • Should contain suitable Power Supplies, Cables and Adapters • Should have minimum below adapters in the a Kit: <ul style="list-style-type: none"> a) mSATA / M.2 to SATA Adapter Kit b) Blade Type SSD Adapter c) SATA LIF Adapter d) microSATA e) 1.8" IDE Laptop Adapter f) 2.5" IDE Laptop Adapter g) ZIF IDE Adapter h) PCIe Card SSD Adapter i) PCIe M.2 SSD Adapter

	<p>j) PCIe Apple SSD Adapter</p> <p>Forensic Imager should meet below specifications:</p> <ul style="list-style-type: none"> • 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. • All of content of the kit should be skilfully bundled in a rugged pelican waterproof case perfect for field or lab acquisition
<p>COMPREHENSIVE DRIVE</p>	<ul style="list-style-type: none"> • Ability to automatically queue multiple acquisition and processing actions – to increase efficiencies and save time

**EXTRACTION
AND INTERNET
ARTIFACTS
ANALYSIS TOOL**

- End-to-end experience that brings together acquisition, processing and analysis, creating integration and a more navigable and manageable digital evidence database
- Ability to discover the full history of a file or artifact to build a case and prove intent. Utility to visualizes where files came from, who they are connected to, and where they're stored.
- 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.
- automation utility to queue multiple devices and device types for image acquisition.
- Support for a broad array of artifact types, and support for the latest versions of those apps and artifact types
- Access to file system, registry and artifacts data and trace artifact evidence to its source data efficiently for a better verification process
- The ability to present findings in a customizable way that fits their report needs and parameters.
- Acquire images from any iOS or Android device, hard drives, and removable media
- Recovers evidence from 300+ types of Internet Artifacts from Windows and Mac computers.
- Recovers 165+ types of Smartphone Artifacts from iOS, Android, and Windows Phone powered smartphones and tablets.
- Get to relevant evidence faster using filters. Isolate evidence from a specific date or time range, or create filters to narrow results based on field values for any supported artifact type. Filter stacking allows you to layer on several dimensions of filter criteria to pinpoint specific items in a large dataset.
- Create and manage a number of different tags to help you narrow down the results quickly and begin to see patterns in an individual's activity. Using the comments function, identify and share your thoughts with other key stakeholders. You can also create profiles that are associated with an individual and then associate other

	<p>identifiers (email addresses, phone numbers, etc) with the profile, so that you can filter evidence to show only the evidence associated with the individual.</p> <ul style="list-style-type: none"> • Create your own custom artifact definitions to find more artifact data or have Evidence Analyzer's Dynamic App Finder automatically identify new apps and create artifact definitions which can then be saved for future use. • 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. • Should be capable of machine learning technology, searching both text-based and media content to automatically identify nudity, weapons, drugs, and sexual conversations. • Should support multiple instances of memory analysis (RAM Analysis) • 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. • Explore file systems and registry hives for greater insights • Process and recover 500+ types of artifacts • Automate all acquisition and processing tasks required to prepare evidence for analysis. • Explore file systems and registry hives for greater insights • Trace artifact evidence back to its source data in seconds • built on the analysis capabilities allowing you to recover hundreds of types of digital forensic artifacts • Retrieve data from services including Facebook, Office 365, Google apps, iCloud, Instagram, Twitter, YouTube, Dropbox, Box, Outlook and more. • Should extract and ingest third-party tokens and keychains from mobile devices, allowing investigators to access cloud and social media accounts without requiring a password for supported accounts.
<p>SOCIAL MEDIA ANALYSIS TOOL</p>	<ul style="list-style-type: none"> • It should have ability to collect and index data from social media streams, linked content and websites through APIs, webmail connectors and direct web

	<p>navigation. Tool should aggregate data from these multiple sources in real time, in a highly scalable and case-centric manner.</p> <ul style="list-style-type: none"> (i) Facebook (ii) Twitter (iii) Instagram (iv) You Tube (v) Tumblr (vi) Web pages & Websites (vii) Gmail (viii) Yahoo Mail (ix) Outlook.com (x) AOL Mail (xi) Internet Message Access Protocol (IMAP) <ul style="list-style-type: none"> • Should perform broad, unified searches across multiple accounts, social media streams and websites from a single interface. Linked content is automatically indexed and searched through the tool fast-as user types search from one user interface. Results are aggregated for sorting, tagging and export consistent with standard e-Discovery, or investigative, workflow. • MD5 hash values of individual items are calculated upon capture and maintained through export. Automated logging and reports generated. Key metadata unique to social media & web streams are captured through deep integration with APIs provided by the publisher. The metadata is important to establishing chain of custody and also provides key evidence relevant to the substantive case as well as authentication. • Should maintain data in a searchable native format from collection through production, uniquely providing a complete platform to address social media in the same manner as devices, e-mail and e- documents. Deliver collected email in PST format while maintaining hierarchical structural.
<p>DISK FORENSIC TOOL KIT WITH MALWARE</p>	<ul style="list-style-type: none"> • Create images, process a wide range of data types from forensic images to email archives, analyse the registry, conduct an investigation, decrypt files, crack passwords, and build a report all with a single solution.

ANALYSIS TOOL

- database driven so that work associated with memory-based tools is not lost in the event of a GUI crash. Compartmentalized components allowing the processing workers to continue processing data without interruption.
- Recover passwords from 100+ applications.
- KFF hash library with 45 million hashes.
- Advanced, automated analysis without the scripting.
- True multi-threaded / multi-core support.
- Wizard-driven processing ensures no data is missed.
- Cancel/Pause/Resume functionality
- Real-time processing status
- CPU resource throttling
- Email notification upon processing completion
- Pre- and post-processing refinement
- Advanced data carving engine allows you to specify criteria, such as file size, data type and pixel size to reduce the amount of irrelevant data carved while increasing overall thoroughness.
- Create, import and export reusable processing profiles with pre-defined processing options for different investigative needs.
- Support for 700+ image, archive and file types
- Notes NSF, Outlook PST/OST, Exchange EDB, Outlook Express DBX, Eudora, EML (Microsoft Internet Mail, Earthlink, Thunderbird, Quickmail, etc.), Netscape, AOL and RFC 833
- Process and 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.
- Create and process Advanced Forensic Format (AFF) images.
- Supports Windows® (32- and 64-bit), Apple®, UNIX® and Linux® operating systems
- Comprehensive analysis of volatile data
- Static RAM analysis from an image or against a live system
- Enumerate all running processes, including those hidden by rootkits, and display

	<p>associated DLLs, network sockets and handles in context.</p> <ul style="list-style-type: none"> • Dump a process and associated DLLs for further analysis in third-party tools. • Memory string search allows you 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. • Provides VAD tree analysis and exposes registry artifacts in memory and will parse and display handle information from memory. • Internet / Chat tab • Advanced Google Chrome analysis • 50+ Internet, Chat, P2P and online game carvers to automatically expose this critical evidence during processing • Video thumbnails • Explicit Image Detection auto-identifies potentially pornographic images by analysing shapes, orientation and flesh tones. • Automated malware triage platform solution, empowering organizations to proactively identify compromised systems. first layer of defense against the risk of imaging unknown devices and allows one to identify infected files and avoid exporting them after processing your data
<p>MULTIPLE GPU BASED PASSWORD RECOVERY/ CRACKING SOLUTION</p>	<ul style="list-style-type: none"> • Multiple GPU (Graphics Processing Unit) based Password Recovery/ Cracking Solution required for massive parallel processing and computation. • Product Offered should be expandable and scalabe as per User requirement in future • Offered Product should have at-least 4 CUDA enabled Graphics Card (GTX 1080 or higher/ better) with minimum 2000 CUDA Core each • GPU Machine and Host Machines offered in the solution should be Rack-mountable and all components of the Offered solution should be fitted in suitable size Rack • Host Machine (Branded and Reputed) should have minimum below configuration with other standard configuration: <ul style="list-style-type: none"> ➤ Rack Mount

- 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 HotSwap Bay1
- 22" WideScreen LCD Monitor with Built-in Speakers
- Windows 10 Professional (64 bit)
- Hardware Write Blocking:
 - 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
 - Solution should have all Networking, Monitor, KVM, Cables, Power Supplies available to run the Machine
 - Number of GPU Machines and Host Machines should be as per requirement to accommodate at-least 8 CUDA enabled GPU Cards in rack
 - Offered Product should have sufficient Air/ Liquid Cooling so that all components including GPU Cards should function without heating up.
 - Product should also include PASSWARE KIT FORENSIC (with minimum 5 Agents) Decryption Software utilizing CUDA for Password Recovery
 - Offered Product should give minimum below speed of Password Breaking using Brute Force attack:
 - a) MS Office 2007 DOC file with Microsoft enhanced RSA and AES Cryptographic

	<p>provider, 128 bit 5,00,000 passwords/second</p> <p>b) MS Office 2010 DOCX file with AES 128 bit Encryption. 2,00,000 passwords/second</p> <p>c) MS Office 2016 DOCX file with AES 256 bit Encryption 7,000 passwords/second</p> <p>Similar/ corresponding speed should be available for other Files and Algorithms</p> <ul style="list-style-type: none"> • Product including all GPU Cards will be continuously working for multiple Weeks/ Months • Standard 230 V Server Level Power Supply will be provided by the Purchaser with Air-conditioning temperature/ environment of 16 deg C • Product Offered should be of International Repute & Brand and should not be assembled Machine. • Bidder should be OEM or direct Authorized Distributor or Reseller in India. In case of Distributor/ Reseller; OEM/ Manufacturer's Authorization for Supply and Service should be attached with the Tender. • Bidder should have past experience of installing at-least 3 units of the offered product in different Central or State Government Organizations in India. Past Order copies to be attached for supporting the same. • Bidder should have OEM trained Manpower for Product Installation and support, Supporting document for the same to be attached. • Offered Product should have Proven Track record of selling in India • Product Offered should be demonstrated at our Location or any other Indian Government Location, Cost of conducting Demonstration will be borne by Bidder • Demonstration to be provided with at-least 1 setup of Machines having minimum 4 GPU Cards and proof of concept of scaling up
<p>FIRST RESPONDER PORTABLE FIELD KIT</p>	<ul style="list-style-type: none"> ➤ Intel Core i7-8700K 6 Core Processor ➤ 64 GB PC4-19200 DDR4 2400 Memory ➤ 1TB NVMe Solid State Internal SATA Drive (OS Drive) ➤ 512 GB NVMe Solid State Internal SATA Drive (Temp Drive)

- 4 TBGB Internal SATA Drive (DATA Drive)
- 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 8260 - 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 - Illuminated
- 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
- 1 USB 2.0 Port
- 1 Headphone jack (2-in-1 Headphone/S/PDIF Optical)
- 1 Microphone jack
- 1 Line-In jack
- 1 Line-out jack
- 8 Cell Smart Lithium -Ion, 82WH Battery Pack
- Kensington Lock Slot
- Universal AC Adapter (100~240V AC 50/60hz)
- Dimensions: 15.20 x 10.32 x 1.41 (inch)
- Weight: 7.5 lbs (complete system + battery)
- Windows 10 Professional (64 bit)/ Other Operating Systems included: SUSE Professional Linux (64 bit)
- System Restore Media - Bootable Blu-ray disc containing restore environment and

factory configured operating system images

- **KIT SHOULD CONTAIN PROTABLE FORENSIC WRITE BLOCKER WITH THE FOLLOWING INTERFACE;**

- USB 3.0 - IDE/SATA, SAS, USB 3.0, Firewire, USB 3.0 Forensic Card Reader and Writer has been designed specifically for forensic use and incorporates SuperSpeed USB3 (5Gb/s) technology.
- Universal Power Supply and Power Adapter cables, Standard Cables and Adapters

- **KIT SHOUD CONTAIN LATEST FORENSIC DUPLICATOR WITH FOLLOWING CONFIGURATION;**

- Should have a Forensic Duplicator with capabilities to support Greater than 2TB HARD DRIVES
- Image a 2TB HDD (2000GB)
- Clone HDDs with no size limit
- Forensically duplicates HDD 's faster than ever - up to 15 GB/min with hashing
- Standard features include Disk-to-Disk (clone) and Disk-to-File (image) duplication, Format, Wipe, Hash (MD5 or SHA-1), HPA / DCO detection and removal, and Blank Disk Check.
- Make one (1:1), two (1:2), or three (1:3) copies of evidence drives.
- Acquisitions of USB 3.0, SATA, and IDE/PATA devices can be directed to either USB 3.0 or SATA output devices.
- Option to acquire SAS drives with additional modules
- outputs to raw DD, .e01 (compressed), .ex01 (compressed), or .dmg formats
- USB 3.0 convenience and speed built in
- extensive log files is easy to view and save
- Built-in, user-selectable MD5 and SHA256 verification
- Hash re-verification on read from destination(s) – user-selectable
- Colour LCD user interface

- **EXTERNAL DEVICES AND ENCLOSURES**

- USB3 Read Only/Read Write switchable External Hard Drive Chassis with Power Supply
- Digital Intelligence Integrated Forensic Media Card Reader - Read-Only and Read/Write Switchable

- **EXTRAS**

- Hard Drive Adapter 2.5 Inch
- Hard Drive Adapter 1.8 Inch
- TDA5-ZIF ZIF HD Adapter w/case
- TDA3-1 Micro SATA HD Adapter
- SATA LIF Adapter
- Blade Type SSD Adapter
- FireWire Adapter 9pin to 4pin
- FireWire Adapter 9pin to 6pin
- Micro/Mini SD to SD Adaptor Kit
- 2 TB SATA Hard Drive
- Precision Electronic Tool Kit
- Power Strip - 120v/240v Compatible
- Universal Power Adapter
-

- **PELICAN CASE**

- Hard-sided with Padded Laptop Insert
- Watertight / Airtight
- High Impact
- Custom Foam Lined
- Custom Lid Organizer for Cables and Adapters

	<ul style="list-style-type: none"> ➤ 24" x 20" x 14" - 58lbs • SOFTWARE <ul style="list-style-type: none"> ➤ Microsoft Windows 10 Professional 64 bit (Configured & Pre-Installed) ➤ Microsoft Office 2016 ➤ Suse Linux Professional (Pre-Configured) ➤ Symantec GHOST ➤ DVD/CD Authoring Software ➤ MOBILE EDIT FORENSIC EXPRESS SOFTWARE ➤ HARD DRIVE ANALYSIS SOFTWARE: software with advanced sorting, filtering, keyword searching, previewing and scripting technology with Live Boot virtualization to boot windows, linux and mac system in a native environment, Shadow Copy, Meta extraction, Carving, Hash Sets, Index and Keyword search, Bookmarking and more. ➤ EMAIL ANALYSIS SOFTWARE: to analyze message headers, bodies, and attachments and recover email in the deleted folders; it recovers email deleted from deleted items (deleted/deleted). Should provides support for over a dozen email archive types, all with easy-to-use options and automated deleted data recovery
<p>MAC ACQUISITION & ANALYSIS TOOL</p>	<ul style="list-style-type: none"> ➤ Should Target and forensically acquire files, folders, and user directories while avoiding known system files and other unneeded data ➤ Preserve valuable metadata by maintaining its association with the original file ➤ Authenticate collected data using any or all MD5, SHA-1, or SHA-256 hash functions ➤ Thoroughly log data acquisitions and source device attributes throughout the collection process ➤ Selectively acquire email, chat, address book, Calendar, and other data on a per-user, per-volume basis ➤ Capture important live data such as Internet, chat, and multimedia files in real time ➤ Soundly acquire and save volatile Random Access Memory (RAM) contents to a

destination device

- Choose from 26 unique system data collection options, including active system processes, current system state, and print queue status
- Extensively log live data acquisition information throughout the collection process
- automatically recognizes a combined volume from a Fusion Drive and presents it for imaging
- If File Vault 2 exists, the examiner can, with use of the password, Keychain file or recovery key, mount the volume in a read-only fashion, allowing for either a triage or collection of the files
- Use the source machine's own system to create a forensic image by booting from USB dongle
- Write-protect source devices while maintaining read-write access on destination devices
- Should allows examiners to view various data points that can be attributed to a user's actions. Traces of potentially important user activity from many disparate locations are organized for practical, efficient examination. Elements include:
 - Windows Registry artifacts - recently executed files and programs, link files, jumplists, Prefetch and Superfetch data
 - Device connection data for all devices previously connected to the system, including USB device connection dates/times and the associated user account
 - iOS device backups
 - Recent file downloads
 - Trash (for Mac OS X volumes) and Recycle Bin (for Windows volumes)
 - Current and deleted user account info
 - All the above components must be neatly packed in a Highly ruggedized watertight/ airtight case.
 - Should Analyze several types of memory files, including raw dumps, Hibernation files (Windows Vista to Windows 10), pagefile.sys, and crash dumps (full, from Windows Vista or 7)
 - Performs file carving and bulk extraction content searches (for numerous items such as URLs, addresses, phone numbers, etc.)

- Features a Memory subview for analyzing processes, libraries, sockets, handles, and drivers
- Processes memory files many times faster than traditional open-source forensic tools
- Should include signature **File Filter** view includes examiner-defined filter options to quickly pinpoint relevant data within large data sets
- Should allow Examiners to apply any number of filters or inverse filters to quickly isolate important data from system files or base application files. Should come with several pre-set file filters, including those that filter by file type, file attribute, geolocation coordinates, and source device type.
- **Media** view has built-in support for all commonly used picture and video file types, and it includes several helpful and examiner-oriented analysis features
- Built-in GPS Mapping
- Proprietary Skin Tone Analysis Algorithm
- Video Frame Analysis
- Communication view allows examiners to see a full log of calls, voicemail, social media activity, and more. Most importantly, examiners can view messaging threads in list view or in their native format
- designed to make reporting incredibly flexible. Examiners may export large data sets in an easily readable format, and can export reports in a variety of formats to enable easy information sharing with all interested third parties.
- Should come with following workstation :

Display:

- 5K Retina display
- 27-inch (diagonal) Retina 5K display
- 5120x2880 resolution with support for one billion colours
- 500 nits brightness
- Wide colour (P3)

Processor 8-Core, 3.2GHz Intel Xeon W , Turbo Boost up to 4.2GHz , 19MB cache

Graphics:

	<ul style="list-style-type: none"> • Vega 56 • Radeon Pro Vega 56 graphics processor with 8GB of HBM2 memory • 56 compute units • 3584 stream processors • 9 teraflops single precision • 18 teraflops half precision <p>Memory:</p> <ul style="list-style-type: none"> • 32GB of 2666MHz DDR4 ECC memory • Quad-channel memory controller <p>Storage: 1TB SSD</p> <p>Video Support and Camera</p> <ul style="list-style-type: none"> • 1080p FaceTime HD camera • Simultaneously supports full native resolution on the built-in display at 1 billion colours and: • Two 5120x2880 (5K) external displays at 60Hz with support for 1 billion colours, or • Four 3840x2160 (4K UHD) external displays at 60Hz with support for 1 billion colours, or • Four 4096x2304 (4K) external displays at 60Hz with support for millions of colours • Support for extended desktop and video mirroring modes • Thunderbolt 3 digital video output • Native DisplayPort output over USB-C • Thunderbolt 2, HDMI, DVI and VGA output supported using adapters (sold separately)
<p>CD/DVD EXAMINER</p>	<ul style="list-style-type: none"> • Reports can be produced for print, HTML, text file or CSV output with over 50 different data items selectable. An unlimited number of user-defined reports can be created. Additionally, should have "timeline" report showing every timestamp on the disc. • Put up to 300 discs at once in one of the supported Robotic Loader systems and it will automatically collect all content from every disc. Flexible reporting for each disc processed. Import the results directly into EnCase or FTK. Optionally

	<p>photograph each disc as it is processed.</p> <ul style="list-style-type: none"> • Discs can be automatically collected to an image file in either ISO+CUE format or an InfinaDyne format. The ISO+CUE format works for all DVD-type (DVD+, DVD-, BD, BD-R, BD-RE) discs and CDs containing only data (no audio or video) • Transfer data collected to EnCase, FTK, etc. • "Inaccessible" discs files can be searched using scan specification syntax, including regular expressions. • This tool identifies files containing graphic content (ART, BMP, GIF, JPEG, PNG, PSD, TIFF, etc.) independent of the file extension. • Supports RAW images from over 600 different digital cameras. • Low-level sector examination and scanning • Allows direct examination of the contents of files on the disc from the main window. • This feature eliminates lengthy re-discovery of the disc's contents. • Locates data on discs that has been dropped from the file system, either because of software glitches, deletion or user action. This is now done for all format discs. • Permits users to select the level of automatic retries performed whenever a data error is encountered. This can make otherwise unreadable data sectors readable again. This allows the user to balance examination speed with thoroughness. • CD Text, ISRC and RID Audio Disc Display.
<p>WEB SERVER & DATA BASE SERVER</p>	<p>Processor core available : 6 Processor cache : 20 MB L3 Processor : Intel® Xeon® E5-2643 v4 (6 core, 3.4 GHz, 20 MB, 135W) Processor number : 1 Processor speed : 3.4 GHz Maximum memory : 3.0TB Memory slots : 24 DIMM slots Memory type : HPE DDR4 Smart Memory Memory, standard : 32 GB (2x 16 GB) RDIMM Included hard drives : None included, 8 SFF drives supported Optical drive type : None included Infrastructure management : Standard: HPE iLO Management with Intelligent Provisioning</p>

	<p>Optional: HPE iLO Advanced, HPE Insight Control, and HPE OneView Power supply type : 2 HPE 500W Flex Slot Platinum power supplies Expansion slots : 2 PCIe 3.0, 1 full-height/three-quarter length and 1 low profile Network controller : 1 embedded HPE 1 Gb Ethernet 4-port 331i adapter Storage controller : HPE Flexible Smart Array P440ar/2 GB plus Smart Storage Battery System fan features : 5 standard hot plug fans, redundant</p>
E3 UNIVERSAL WITH CHAT STICK AND PORN STICK	<ul style="list-style-type: none"> • Chat stick is a thumb drive device that will search your entire computer, scan it for chat logs from Yahoo, MSN 6.1, 6.2, 7.0, & 7.5, ICQ 1999-2003b, Trillian, Skype, Hello, & Miranda and create are port in an easy to read format so you can see what your kids or employees are saying to people online. • The Porn Detection stick is designed to scan all images and video sony our computer for illicit images. It's nearly impossible to keep any computer connected to the internet clean from pornography, even with programs that are designed to prevent access to porn. The Porn detection stick will not only scan your system for pornography, it will securely wipe any found images and videos so it's gone forever. The porn detection stick will scan through files, deleted date, internet history, and zip files so there's no hiding improper activity.
MANAGED SWITCH 8 PORT	08 Port 10/100/1000 M
MINI SCREW DRIVER TOOL SET	The precision electronics tool kit is s a complete comprehensive standard in precision screwdriver bit sets, featuring 30 pct of selected bits and 10 pcs of essential repair tools.
BLOWER	Bosch GBL-800E 820-Watt Vari-Speed Air Blower.
COLOUR NETWORK PRINTER	<p>Key Features</p> <ul style="list-style-type: none"> • Heavy duty laser jet with throughput of >35 pages per minute • Resolution :- $\geq 600 \times 600$ dpi • RAM :- 2 GB • Speed: At least >35 pages (A4) per minutes • Page type support:- A3, A4, Legal • Connectivity : USB • Self-Diagnostic: Self-test print out & configuration etc. • Paper Feed: >2000 A4 sheets • Warranty: 3 years on site

	<ul style="list-style-type: none"> • Spare Cartridges: Two numbers of spares cartridges should be provided. <p>Scanner: The printer should have a scanner built in.</p>
OFFLINE COLOUR LASER PRINTER	<ul style="list-style-type: none"> • Laser jet with throughput of >25 pages per minute with best Resolution. • RAM :- 1 GB or higher • Page type support:- A4 and Legal • Both Side printing • Connectivity : USB & LAN interface • Self-Diagnostic: Self-test print out & configuration etc. • Paper Feed: A4/ Legal sheets • Spare Cartridges: Two numbers of spares cartridges should be provided.
HARDWARE FIREWALL	<p>Architecture and Performance:</p> <ul style="list-style-type: none"> • Appliance based Next Generation Firewall. • Firewall throughput at least 8 Gbps or better • Firewall should have at least 1 Gbps UTM throughput. • Should support New sessions/second 80K or more • Should support at least 2000K Concurrent Sessions • Should have redundant power supply. • Should have at least 200GB internal Storage. • Should be rack mountable. <p>Ports:</p> <ul style="list-style-type: none"> •The security appliance should have at least 10 x 1Gbe Ethernet ports Configurable as Internal/DMZ/WAN Ports. •Should support multiple WAN IPs. •Should have at least 1x Console Ports (Rj45), 2 x USB Ports etc. <p>High Availability Support:</p> <ul style="list-style-type: none"> •State full failover to prevent session Losses. •On power up the platform should use built-in system monitoring & diagnostics before going online to detect failure of hardware. •Online software reconfiguration to ensure that changes made to a platform configuration take place with immediate Effect. •Functionality to upgrade the software of the appliance without disrupting the Services. <p>Feature:</p>

•Should have inbuilt Next Generation Firewall features like State full Firewall, IPS, Anti-Virus, Anti-malware, Anti-spyware, Anti-spam, Web filtering, Application Filtering, Web Application firewall, SSL Inspection, Application Control Bandwidth management etc.

•Stateful Inspection Firewall

i) Multiple Security Zones

ii) Location-aware and Device-aware Identity-based Access Control Policy

iii) Access Control Criteria (ACC): User-Identity, Source and Destination Zone, MAC and IP address, Service

iv) Country-based Traffic Control

v) Access Scheduling - Policy based Source and Destination NAT, Gateway Specific NAT Policy.

vi) DoS and DDoS attack prevention.

vii) MAC and IP-MAC filtering.

viii) Spoof Prevention.

• Virtual Private Network.

i. IPSec, L2TP, PPTP

ii. IPSec NAT Traversal

iii. Dead peer detection

iv. External Certificate Authority support

v. Domain name support for tunnel end points

• SSL VPN

i. TCP & UDP Tunneling

ii .Authentication - Active Directory, LDAP, RADIUS

iii Multi-layered Client Authentication - Certificate, Username/Password - User & Group policy enforcement

ivNetwork access - Split and Full tunneling.

• User Authentication

i. Internal database

ii. External LDAP/LDAPS/RADIUS

database Integration

	<p>iii. 2-factor authentication: should support 3rd party solution</p> <p>Management:</p> <ul style="list-style-type: none"> • Should be configurable using CLI, GUI and central management software. • Should support local access on on-board console/serial interfaces and SSHv2. • Should support AAA features through RADIUS & 802.1x. • Should support multiple levels of administration roles to manage and monitor the device. • Should support Network Time Protocol. • Should support management through SNMP. • Should be able to send and receive Syslog and SNMP traps to and from devices. <p>The GUI management interface should provide real-time system and traffic profiling, Syslog monitoring, real-time device monitoring, event logs collection, analysis & reporting facilities.</p> <p>Certification:</p> <ul style="list-style-type: none"> • At least EAL 4 or equivalent certified. <p>Industry Standards: EMC: FCC Part 15, Safety Approvals EN 60950, IEC 60950-1, CE marking</p>
KVM SWITCH - 8 PORT	Eight Ports KVM switch with standard make.
26-U RACK	26-U Rack with all Power Supply Facility and Sufficient No's of Power plug slots of Standard Measures and Make.
GIGA BIT ETHERNAL SWITCH 24 PORTS	24 Ports switch of Standard Make
POWERED PORTABLE HDD- 10 TB	10 TB Rack mountable Powered NAS with HDD – with Standard Make.
BIG SIZE TOUCH SCREEN LED	<p>Screen Size:85 inch or above diagonally</p> <p>Source:VGA, RGB, DVI, HDMI, USB</p> <p>Resolution: 1920 x1080 Native or better</p> <p>Brightness:450 Nits</p> <p>Contrast ratio:Min 3,000:1</p> <p>Colors: 281 trillion</p>

	<p>Hor. viewing angle: 120° Vert. viewing angle: +/-60° Refresh rate: 60 Hz Touch: Min four simultaneous touches:</p> <ul style="list-style-type: none"> • Standard Features: Variable width line, highlighter, eraser etc. functions. • Spot Light, Curtain, Zoom. • Screen Capture and audio recording. • Transparency level of screen can be varied. • Import Picture. • Handwriting reorganization. • Save, Print, Export image Text annotations. <p>OS Support: Should support all the latest available OS. Speaker: 15 W + 15 W @ 8 ohm Lifetime: 100,000 hours (@50% brightness)</p>
<p>LED DISPLAY SCREEN</p>	<p>Screen Size: 80 inch or above diagonally or higher Pixel pitch:Min 1 mm Brightness: Min 280cd/m² Resolution: Min 3840 x 2160 Contrast ratio: Min 3,500:1 Hor. viewing angle: 120 degrees(min 50% brightness) Lifetime: 100,000 hours (@50% brightness) Vert. viewing angle: +/-60° (min 50% brightness) Colors: More than 1 billion Source compatibility: VGA, RGB, DVI, HDMI, USB Tile/tile Z-alignment: +/-0.5mm Stand: Suitable to carry the weight of screen</p>
<p>4- CHANNEL PIP SPLIT-SCREEN VIDEO</p>	<ul style="list-style-type: none"> • HD Video Inputs: HDMI female x 4 • HD Video Output: HDMI female x 1 • HDMI Cable Distance: Up to 15m or 60 ft for 1080p at 12 bits • HDMI Input Cable Distance: Up to 15m or 60 ft for 1080p at 8 bits • Video Bandwidth: 225MHz/6.75Gbps

	<ul style="list-style-type: none"> • Digital Audio Sampling Rate Support: 32Khz to 192Khz • Operation Control: IR remote, Front Panel, Web Panel, RS232, Telnet • HDMI DVI Input Resolution Support: • 640x480 pixels at 60/72/75/85Hz, 800x600 pixels at 56/60/72/75/85Hz • 1024x768 pixels,1280x720,1280x1024 pixels • 1280x1024,1360x768,1440x900 • 1600x900,1600x1200,1680x1050 • 1920x1080, 1920x1200 • 480p, 576P • 720p at 50/60Hz • 1080i at 50/60Hz • 1080p at 24/25/30/50/60Hz • HDMI Output Resolution Support: • 1024x768, 1280x800, 1280x1024, 1366x768, 1440x900 • 1600x900, 1600x1200, 1680x1050, 1920x1200, NATIVE • 480p, 576p, 720p at 50/60Hz, 1080p at 24/25/30/50/60Hz • I/O Format Support: RGB 4:4:4, YUV 4:4:4 and YUV 4:2:2 • Color Space Support:8-bit, 10-bit and 12-bit • Size: 436mm x 247mm x 44mm or 17.2" x 9.72" x 1.73" (WxDxH) • Power Supply: AC input of 100-240V with DC 12V 3A output • Power Consumption: 18W •
VISUALISER	<p>Image Sensor:1/3" Color CMOS/CCD, 800,000 pixels or better</p> <p>Zoom: Min 192X zoom (optical and digital)</p> <p>Focus: Powered (Auto Focus / Manual)</p> <p>Iris: Auto</p> <p>Illumination System: With main unit and light box.</p> <p>light source:Base & Upper</p> <p>Frame rate: 30 frames/sec</p> <p>VGA Out: 1024 x 768(XGA) or better(preferably 1920 x1080)</p> <p>Image Options: Color with auto/manual white balance</p> <p>Output Selection:One touch button for presenter to select Camera or Input VGA/PC.</p>
PODIUM WITH	Dimension: Standard Height. Length and width to be decided based on

<p>I – PANEL</p>	<p>Dimension on housing equipment. Housing space: Suitable space for mounting following items.</p> <ul style="list-style-type: none"> i) PC ii) Keyboard iii) I Panel iv) Visualizer v) Microphone vi) Table Lamp vii) Power strip for above equipment viii) Storage space (for laser pointer, presenter, pen, remote etc) <p>Table Top space: Space for</p> <ul style="list-style-type: none"> i) I Panel ii) Space for Presenter Laptop iii) Suitable assembly for Table Lamp and Microphone. <p>Design: Design to be proposed by bidder and approved by purchaser before delivery.</p> <p>I-Panel</p> <p>Screen Type: 15" interactive touch Screen</p> <p>Platform Support: Should support all latest operating system.</p> <p>Screen Size: Minimum 15" Diagonal</p> <p>Resolution: Minimum 1024 x 768 (XGA)</p> <p>Active Area: 12" x 9" (304 mm x 228 mm)</p> <p>Response Time: 30 ms or better</p> <p>Accuracy: +/-0.5 mm</p> <p>Pixel Pitch: 0.012" x 0.012" (0.297 mm x 0.297 mm)</p> <p>Incline: 20° to 80°</p> <p>Number of Colours: Minimum 16.7 Million</p> <p>Contrast Ratio: Minimum 300:1</p> <p>I/O Connectors: DC Power In VGA 15-Pin D-Sub (IN/OUT) USB Connector</p>
<p>TABLE MICROPHONE FOR PODIUM</p>	<p>Output Impedance @ 1,000 Hz: To be matched with the audio system</p> <p>Dynamic Range: >90 dB</p> <p>Mute Switch Attenuation: 50.0 dB minimum</p> <p>Column length: Min 1feet or to be proposed as per design of podium</p>

COLLAR MICROPHONE	Carrier Frequencies: UHF (minimum 4-channels) Modulation: Frequency modulation Dynamic Range: > 90 dB Signal / Noise: 90dB Working Range (average conditions): Sufficient to cover the Training Room Size (45' x 18') Mobile transmitter Power source: Rechargeable Battery
CORDLESS MICROPHONE	RF Carrier Frequency Range: UHF (minimum 4-channels) Working Range (average conditions): Sufficient to cover the Training Room Size(45' x 18') Dynamic Range: >90 dB Signal / Noise: 90dB Mobile transmitter Power source: Rechargeable Battery
AUDIO SYSTEM	<ul style="list-style-type: none"> • Suitable audio system with Audio Mixer, Audio Amplifier, Ceiling Speaker & Audio Woofer to be considered which suits the acoustic of the training Room. • This audio system should be fully compatible with Microphones.
VIDEO CAMERA	<ul style="list-style-type: none"> • Connectable to HD TVI and analog cameras • Connectable to Coaxitron camera with long transmission distance • Connectable to network cameras • Encoding at up to 720P resolution • HDMI Output and VGA output at up to 1920x1080P resolution • New GUI supports starting record with one key • Instant playback for assigned camera during multi-channel live view mode • Supports up to 8-ch synchronous playback; and reverse playback for multi-channel • Smart playback to go through less effective information • Manual video quality diagnostics • Customization of tags, searching and playing by tags • Locking and unlocking record files • Provide 1 SATA interface for HDD with up to 6TB capacity • 1 self-adaptive 10M/100 M network interface • Support axis by EZVIZ Cloud P2P

	<ul style="list-style-type: none"> • Support Hikvision DDNS (Dynamic Domain Name System) • Network Detection Function
NETWORK SWITCH	<p>Ports: (32) QSFP+ 40GbE ports</p> <p>Memory and processor: 1 GB flash Packet buffer size: 12.2 MB 4 GB SDRAM</p> <p>Latency: 10 Gbps Latency: < 1 μs</p> <p>Throughput: up to 1429 Mpps</p> <p>Routing/switching capacity: 2560 Gbps</p> <p>Management features:</p> <ul style="list-style-type: none"> • IMC - Intelligent Management Center • Command-line interface • Out-of-band management • SNMP manager • Telnet • FTP

Note- All Softwares/ hardwares should have three years warranty and additional updates.