



# CENTRAL FORENSIC SCIENCE LABORATORY

Directorate of Forensic Science Services  
Ministry of Home Affairs, Government of India

Ramanthapur, Hyderabad-500013, Telangana State

Phone: 91-40-2703 8429 : Fax: 91-40-2703 9281

(An ISO/IEC 17025:2005 laboratory accredited by NABL)

Notified 'Examiner of Electronic Evidence' under Sec.79A of I.T.Act-2000



No. 1(425)/CFSL(H)/2018/

Dated: 10/05/2019

## TO WHOMSOEVER IT MAY CONCERN

Please find enclosed herewith the generalized specifications of the following:

1. Software and hardware tools for the proposed four units
2. Forensic Smart Server
3. Digital Forensic Platform

required for the National Cyber Forensic Laboratory for Evidentiary Purpose (NCFL-E) at CFSL, Hyderabad for review and suggestions.

The suggestions may please be sent to the Director on or before 24/05/2019 positively by way of post or e-mail at the following mail ID.

- [Director.cfsl-hyd@nic.in](mailto:Director.cfsl-hyd@nic.in)

  
Director  
10/5/19  
Central Forensic Science Laboratory  
HYDERABAD

**Broad Based Specifications of Vehicle for Scene of Crime Unit of  
National Cyber Forensic Laboratory for Evidentiary purpose**

S. No.	Name of the Tool	Specifications
2.	Digital Forensic Triage Tool Kit	<ol style="list-style-type: none"> <li>Support collection of data from file systems including NTFS, FAT (12, 16 &amp; 32 bit), EXFAT, HFS+, XFS, APFS, EXT2, EXT3 &amp; EXT4.</li> <li>Support collection of data from both UEFI and BIOS based systems.</li> <li>Support Profile configuration based on case.</li> <li>Support digital forensic triage from powered off computers (Desktops, Laptops, Servers aka windows/linux/iOS)and running Windows computers(NTFS/FAT).</li> <li>Support capture of volatile data/memory (RAM capture)</li> <li>Support collection of Files from Removable Media (e.g. USB Drives)</li> <li>Support collection of Files from Forensic Images (E01, DD etc.)</li> <li>Support collection of files from Devices with Internal Memory Storage E.g. Digital Cameras.</li> <li>Support physical backup to be supported by popular digital forensic tools.</li> <li>Support extraction of data from Customised Locations.</li> <li>Support data collection from mounted encrypted partitions.</li> <li>Support automated analysis and report generation in PDF/HTML/DOCX of files collected from a target device.</li> <li>Support automatic Logging (Device, Processing &amp; User Interaction) of activities.</li> <li>Support filter of data by Criteria to Target Specific Results.</li> <li>Support Identify, Process and Display Browser History, Display Contents of E-Mail, Chat, Social Media Artefacts.</li> <li>Support automatic indexing and tagging of hash and keyword matches.</li> <li>Support time lining.</li> <li>Solution in a ruggedized portable system with suitable processing and configuration as below: <ol style="list-style-type: none"> <li>Processor family – intel core i7 or better</li> <li>RAM – 16GB DDR3 or more.</li> <li>SSD hard disk with 01TB capacity.</li> <li>Front integrated camera.</li> <li>11.6” FHD (1920x1080) 16:9 Direct-View outdoor-readable display.</li> <li>3 x USB 3.0, 1 x USB 3.1 (Type USB-C) Gen 1 supports power and display Micro Serial Port, Universal Audio Jack</li> <li>Intel Integrated HD Graphics</li> <li>Inbuilt supportive OS with dual boot to Windows 10.</li> <li>Lithium ion 2 cell primary as well as secondary battery along with suitable 3-prong AC adaptor.</li> </ol> </li> <li>Perpetual Licensing with 01 year warranty and Service Maintenance Support (SMS) with update/upgrade for a period of 02 years after warranty.</li> </ol>

		20. Desirable: Solution should include certified training for 03 Experts from OEM with-in India or at OEM location.
--	--	--

**Broad Based Specifications of the Faraday Bags for Scene of Crime Unit of  
National Cyber Forensic Laboratory for Evidentiary purpose**

S. No.	Name of the Item	Specifications
6.	Faraday Bags	<ol style="list-style-type: none"><li>1. Should be able to isolate all types of RF connectivity i.e., Wi-Fi, Bluetooth, 2G, 3G, 4G LTE, GPS.</li><li>2. Should have sizes as below to suit various devices like laptops, notebooks, iPads, Mobiles, Drones etc.,:<ol style="list-style-type: none"><li>a. Width – 62 cm x height – 49cm</li><li>b. Width – 46 cm x height – 32cm</li><li>c. Width – 32 cm x height – 42cm</li><li>d. Width – 22 cm x height – 28cm</li><li>e. Width – 11.5 cm x height – 19cm</li><li>f. Width – 17.5 cm x height – 24.5cm</li><li>g. Width – 12.5 cm x height – 22cm</li><li>h. Width – 125 cm x height – 60cm</li></ol></li></ol>

**Broad Based Specifications of the S/w and H/w Tools for Scene of Crime Unit of  
National Cyber Forensic Laboratory for Evidentiary purpose**

S. No.	Name of the Tool	Specifications
7.	Imaging and write blocking device.	<ol style="list-style-type: none"> <li>1. Capable to acquire/clone data from one-to-one, two-to-two, one-to-two and two-to-one destinations media.</li> <li>2. Capable to acquire/clone data at the rate of 50 GB/Min or higher.</li> <li>3. Capable to acquire/clone data in Drive to Drive and Drive to file/s format to support analysis in various forensic analysis tools.</li> <li>4. Capable to cross copy support for various hard disk interfaces, USB interfaces.</li> <li>5. Capable to authenticate the data with multiple hashing algorithms.</li> <li>6. Capable to identify and acquire HPA and DCO areas of the suspect media.</li> <li>7. Capable to acquire data directly from the live system with support for content-based image.</li> <li>8. Capable to boot/mount the suspect media virtually in a write protected environment for preview of live data.</li> <li>9. Capable to acquire data from suspect RAID (all RAID configurations) drives.</li> <li>10. Capable to acquire data over a network.</li> <li>11. Capable to generate the log of the processes.</li> <li>12. Capable to search for the key words in the suspected media.</li> <li>13. Include data and power interfaces to support all interfaces i.e., SATA, IDE, Fire wire, USB2, USB3, e-SATA, Micro-SATA, combine-SATA, SSDs and ZIF etc., along with their respective connecting cables.</li> <li>14. Preloaded operating software.</li> <li>15. Perpetual Licensing with 01 year warranty and Service Maintenance Support (SMS) with update/upgrade for a period of 02 years after warranty.</li> <li>16. Desirable: Solution should include certified training for 03 Experts from OEM with in India or at OEM location.</li> </ol>

**Broad Based Specifications of the S/w and H/w Tools for Digital Storage Media Examination Unit of  
National Cyber Forensic Laboratory for Evidentiary purpose**

S. No.	Name of the Tool	Specifications
1.	Hardware Forensic Imaging Device.	<ol style="list-style-type: none"> <li>1. Capable to acquire/clone data from one-to-one, two-to-two, one-to-two and two-to-one destinations media.</li> <li>2. Capable to acquire/clone data at the rate of 50 GB/Min or higher.</li> <li>3. Capable to acquire/clone data in Drive to Drive and Drive to file/s format to support analysis in various forensic analysis tools.</li> <li>4. Capable to cross copy support for various hard disk data interfaces, USB interfaces.</li> <li>5. Capable to authenticate the data with multiple hashing algorithms.</li> <li>6. Capable to identify and acquire HPA and DCO areas of the suspect media.</li> <li>7. Capable to acquire data directly from the live system with support for content-based image.</li> <li>8. Capable to boot/mount the suspect media virtually in a write protected environment for preview of live data.</li> <li>9. Capable to acquire data from suspect RAID (all RAID configurations) drives.</li> <li>10. Capable to acquire data over a network.</li> <li>11. Capable to generate the log of the processes.</li> <li>12. Capable to search for the key words in the suspected media.</li> <li>13. Include data and power interfaces to support all interfaces i.e., SATA, IDE, Fire wire, USB2, USB3, e-SATA, Micro-SATA, combine-SATA, SSDs and ZIF etc., along with their respective connecting cables.</li> <li>14. Preloaded operating software.</li> <li>15. Perpetual Licensing with 01 year warranty and Service Maintenance Support (SMS) with update/upgrade for a period of 02 years after warranty.</li> <li>16. Desirable: <ul style="list-style-type: none"> <li>○ Solution should include certified training for 03 Experts from OEM with in India or at OEM location.</li> </ul> </li> </ol>

**Broad Based Specifications of the S/w and H/w Tools for Digital Storage Media Examination Unit of  
National Cyber Forensic Laboratory for Evidentiary purpose**

S. No.	Name of the Tool	Specifications
2.	Hardware write Blocker Kit	<ol style="list-style-type: none"><li>1. The kit should have Separate write-blocker devices to support vivid data interfaces i.e., SATA, IDE, Fire wire, USB2, USB3, e-SATA, Micro-SATA, combine-SATA, SSDs and ZIF etc., along with their respective connecting cables.</li><li>2. Perpetual Licensing with 01 year warranty and Service Maintenance Support (SMS) with update/upgrade for a period of 02 years after warranty.</li></ol>

**Broad Based Specifications of the S/w and H/w Tools for Digital Storage Media Examination Unit of  
National Cyber Forensic Laboratory for Evidentiary purpose**

S. No.	Name of the Tool	Specifications
3.	Tool for acquisition of Data from HDDs, Smart Phones, Cloud and VSCs and automated processing and analysis of data specific criteria to internet and social media artefacts.	<ol style="list-style-type: none"> <li>1. Support Acquisition of various devices like HDDs, Androids, iPhones, Cloud etc.,</li> <li>2. Support analysis of data in an automated way by recovery, analysis and presentation of various artefacts from windows, iOS, mobiles.</li> <li>3. Support acquisition and analysis of volume shadow copies.</li> <li>4. Support analysis of various Mobile logical and physical backups.</li> <li>5. Support analysis of various artefacts from Windows, MAC, Unix based OSs.</li> <li>6. Support automated parsing of various internet artefacts, social networking app, instant messages and peer to peer data parsing.</li> <li>7. Support creation of portable cases for review purpose.</li> <li>8. Support APFS, NTFS, iOS, FAT, EXT based file systems.</li> <li>9. Support linkage analysis among files, users and devices.</li> <li>10. Support time line analysis.</li> <li>11. Support Data Analytics.</li> <li>12. Support auto identification of password protected/encrypted containers and decrypting them with inbuilt or add-on module.</li> <li>13. Support analysis of data basing on AI processing</li> <li>14. Supports creation of customized reports.</li> <li>15. Perpetual Licensing with 01 year warranty and Service Maintenance Support (SMS) with update/upgrade for a period of 02 years after warranty.</li> <li>16. Desirable: <ul style="list-style-type: none"> <li>○ Solution should include certified training for 03 Experts from OEM with in India or at OEM location.</li> </ul> </li> </ol>



**Broad Based Specifications of the S/w and H/w Tools for Digital Storage Media Examination Unit of  
National Cyber Forensic Laboratory for Evidentiary purpose**

S. No.	Name of the Tool	Specifications
4.	Tool for digital evidence processing and analysis.	<ol style="list-style-type: none"> <li>1. Support acquire, search, analyse, store and share digital evidence found inside computer and mobile devices, RAM and cloud.</li> <li>2. Support extract digital evidence from multiple sources by analysing hard drives, drive images, cloud, memory dumps, iOS, Blackberry and Android backups, GrayKey, UFED, OFB, Elcomsoft, JTAG and chip-off dumps.</li> <li>3. Support Windows (all versions, including Windows 10), macOS, Unix-based systems (Linux, FreeBSD, etc.), iOS (iPhone/iPad), Android, Windows Phone 8/8.1, Blackberry.</li> <li>4. Support EnCase, L01/Lx01, FTK, DD, SMART, X-Ways, Atola, DMG, tar and zip files, Mobile backups, UFED and OFB images, GrayKey and Elcomsoft iOS images, chip-off dumps, JTAG dumps.</li> <li>5. Support VMWare, Virtual PC/Hyper-V, VirtualBox, XenServer.</li> <li>6. Support APFS, FAT, exFAT, NTFS, HFS, HFS+, ext2, ext3, ext4, YAFFS, YAFFS2 file systems.</li> <li>7. Support Various Cloud Artefacts parsing and analysis.</li> <li>8. Support analysis of Photos with included module of Photo manipulation.</li> <li>9. Support parsing analysis of emails from various email clients.</li> <li>10. Support extraction, parsing and analysis of various browser artefacts.</li> <li>11. Support extraction, parsing and analysis of various mobile apps.</li> <li>12. Support extraction, parsing and analysis of peer to peer, social networking apps, encrypted containers.</li> <li>13. Support inbuilt SQLite Viewer, Hex Viewer, Registry Viewer, PList Viewer.</li> <li>14. Support both lab and field level investigations with flexible licencing via portable mode through an USB without installation and electronic dongle based with installation on any desired workstation.</li> <li>15. Perpetual Licensing with 01 year warranty and Service Maintenance Support (SMS) with update/upgrade for a period of 02 years after warranty.</li> <li>16. Desirable: <ul style="list-style-type: none"> <li>○ Solution should include certified training for 03 Experts from OEM with in India or at OEM location.</li> </ul> </li> </ol>

**Broad Based Specifications of the S/w and H/w Tools for Digital Storage Media Examination Unit of  
National Cyber Forensic Laboratory for Evidentiary purpose**

S. No.	Name of the Tool	Specifications
5.	Software for the forensic previewing, Imaging and analysis of Digital Media and Smart Phones.	<ol style="list-style-type: none"> <li>1. Should support Preview of suspect media.</li> <li>2. Should support acquire data from various types of storage media.</li> <li>3. Should support acquiring data in multisession.</li> <li>4. Should support various operating systems viz., Windows, Linux, UNIX, Sun Solaris, Macintosh, Apple's iOS, Android OS, Blackberry OS, HP's Palrn OS, Nokia Symbian, Windows Mobile OS etc.</li> <li>5. Should support automated processing of evidence with capability to indexing, auto de-NISTing, file signature analysis, hash analysis, Protected File Analysis, Expand compound files, File parser for Email (PST, NSF, DBX, EDB, AOL, MBOX), extract internet artefacts, time line analysis, System Info Parser, I M Parser (AOL, N4SN, Yahoo), File Carver, Windows Event Log Parser, Windows Artefact Parser, Unix Login, Linux Syslog Parser, etc.</li> <li>6. Should support decryption of disks, volumes, folders and files of the suspected media having various types of encryption.</li> <li>7. Should support custom programmes for processing of data.</li> <li>8. Should support various file formats for viewing the data.</li> <li>9. Should support iOS Physical image analysis.</li> <li>10. Perpetual Licensing with 01 year warranty and Service Maintenance Support (SMS) with update/upgrade for a period of 02 years after warranty.</li> <li>11. Desirable: <ul style="list-style-type: none"> <li>○ Solution should include certified training for 03 Experts from OEM with in India or at OEM location.</li> </ul> </li> </ol>

**Broad Based Specifications of the S/w and H/w Tools for Digital Storage Media Examination Unit of  
National Cyber Forensic Laboratory for Evidentiary purpose**

S. No.	Name of the Tool	Specifications
6.	Integrated Computer Forensics Software	<p>The tool should have the following capabilities:</p> <ol style="list-style-type: none"> <li>1. Disk cloning and imaging</li> <li>2. Ability to read partitions and file system structures inside raw (.dd) image files, ISO, VHD and VMDK images</li> <li>3. Built-in interpretation of JBOD, RAID 0, RAID 5, RAID 5EE, and RAID 6 systems, Linux software RAIDs, Windows dynamic disks, and LVM2</li> <li>4. Native support for FAT12, FAT16, FAT32, exFAT, TFAT, NTFS, Ext2, Ext3, Ext4, Next3, CDFS/ISO9660/Joliet, UDF and additional support file systems HFS, HFS+/HFSJ/HFSX, ReiserFS, Reiser4, XFS, many variants of UFS1 and UFS2, many data structures of APFS.</li> <li>5. Analysis of file system data structures, including \$LogFile in NTFS, .journal in Ext3/Ext4</li> <li>6. Superimposition of sectors, e.g. with corrected partition tables or file system data structures to parse file systems completely despite data corruption, without altering the original disk or image</li> <li>7. Ability to create skeleton images, cleansed images, and snippet images</li> <li>8. Various data recovery techniques, and powerful file carving</li> <li>9. Viewing and editing binary data structures using templates</li> <li>10. Gathering slack space, free space, inter-partition space, and generic text from drives and images.</li> <li>11. File and directory catalog creation for all computer media</li> <li>12. Easy detection of and access to NTFS alternate data streams (ADS)</li> <li>13. Mass hash calculation for files.</li> <li>14. Viewer for Windows event log files (.evt, .evtx), Windows shortcut (.lnk) files, Windows Prefetch files, \$LogFile, \$UsnJrnl, restore point change.log, Windows Task Scheduler (.job), \$EFS LUS, INFO2, wtmp/utmp/btmp log-in records, MacOS X kcpasssword, AOL-PFC, Outlook NK2 auto-complete, Outlook WAB address book, Internet Explorer travellog (a.k.a. RecoveryStore), Internet Explorer index.dat history and browser cache databases, SQLite databases such as Firefox history, Firefox downloads, Firefox form history, Firefox sign-ons, Chrome cookies, Chrome archived history, Chrome history, Chrome log-in data, Chrome web data, Safari cache, Safari feeds, Skype's main.db database with contacts and file transfers.</li> <li>15. Powerful physical and logical search capabilities for many search terms at the same time.</li> <li>16. Recursive view of all existing and deleted files in all subdirectories.</li> <li>17. Automatic coloring for the structure of FILE records in NTFS.</li> <li>18. Ability to analyze remote computers in conjunction with included add-on module.</li> </ol>

**Broad Based Specifications of the S/w and H/w Tools for Digital Storage Media Examination Unit of  
National Cyber Forensic Laboratory for Evidentiary purpose**

		<p>19. Perpetual Licensing with 01 year warranty and Service Maintenance Support (SMS) with update/upgrade for a period of 02 years after warranty.</p> <p>20. Desirable:</p> <ul style="list-style-type: none"><li>○ Solution should include certified training for 03 Experts from OEM with in India or at OEM location.</li></ul>
--	--	--

**Broad Based Specifications of the S/w and H/w Tools for Digital Storage Media Examination Unit of  
National Cyber Forensic Laboratory for Evidentiary purpose**

S. No.	Name of the Tool	Specifications
7.	Software for the image mounting, password cracking and forensic analysis of Digital Media.	<ol style="list-style-type: none"> <li>1. Should support Windows, Apple, UNIX and Linux operating systems for analysis of the media.</li> <li>2. Should support RAM analysis.</li> <li>3. Should support PLIST, SQLite database, Apple DMG and DD_DMG disk image and JSON file, etc.</li> <li>4. Should support automated processing of evidence with capability to indexing, auto de-NISTing, recover files and partitions, detect deleted files, file signature analysis, hash analysis, Recover Folders, Expand compound files, parse Email databases, extract Internet artefacts, time line analysis, System Info Parser, IM Parser (AOL, MSN, Yahoo), File Carver, Windows Event Log Parser, Windows Artefact Parser, etc.,</li> <li>5. Should support the registry log analysis.</li> <li>6. Should support auto detection of password protected files, decryption of various types of encrypted files.</li> <li>7. Should support generation of csv based reports for time line analysis.</li> <li>8. Should support automated explicit image identification Skin tone analysis.</li> <li>9. Should support automated tile indexing and statistical report generation for each file type.</li> <li>10. Should support auto carving of files and adding the carved files to the file tree structure.</li> <li>11. Should support Password cracking.</li> <li>12. Should include all supported modules.</li> <li>13. Perpetual Licensing with 01 year warranty and Service Maintenance Support (SMS) with update/upgrade for a period of 02 years after warranty.</li> <li>14. Desirable: <ul style="list-style-type: none"> <li>○ Solution should include certified training for 03 Experts from OEM with in India or at OEM location.</li> </ul> </li> </ol>

**Broad Based Specifications of the S/w and H/w Tools for Digital Storage Media Examination Unit of  
National Cyber Forensic Laboratory for Evidentiary purpose**

S. No.	Name of the Tool	Specifications
8.	MAC Forensic Toolkit along with MAC Work Station	<p><b>1. Specification for MAC Forensic Tool Kit:</b></p> <ul style="list-style-type: none"> <li>a. Should have a Software Write-Blocker, Imager and Analysis.</li> <li>b. Support imaging of RAM capture Volatile Data from MAC machines.</li> <li>c. Should have Built-in Live Imaging.</li> <li>d. Should support acquisition and analysis of latest MAC OSX.</li> <li>e. Support Processing of forensic images or live Macs.</li> <li>f. Should have support for iTunes backups, Time Machine Folder Hard Links Backup, File Vault Analysis.</li> <li>g. Support Advanced Timeline Analysis.</li> <li>h. Support full log of social media activity parsing.</li> <li>i. Support Image mounting supporting popular forensic image formats and Fusion drives.</li> <li>j. Automatic identification of Spoliation artefacts.</li> <li>k. Supports creation of customized reports – PDF, HTML, CSV and XML.</li> <li>l. Perpetual Licensing with 01 year warranty and Service Maintenance Support (SMS) with update/upgrade for a period of 02 years after warranty.</li> <li>m. Desirable: <ul style="list-style-type: none"> <li>o Solution should include certified training for 03 Experts from OEM with in India or at OEM location.</li> </ul> </li> </ul> <p><b>2. Specification for MAC Workstation:</b></p> <ul style="list-style-type: none"> <li>a. Latest Mac OS</li> <li>b. 3.1 GHz 6-Core Intel Xeon E5 or higher</li> <li>c. 16 GB 1866 MHz DDR3 or higher</li> <li>d. 1000 GB HDD or higher or support for multiple HDDs</li> <li>e. 1680 x 1050 or higher screen resolution</li> </ul>

**Broad Based Specifications of the S/w and H/w Tools for Digital Storage Media Examination Unit of  
National Cyber Forensic Laboratory for Evidentiary purpose**

S. No.	Name of the Tool	Specifications
9.	e-Mail Parsing and Analysis tool	<ol style="list-style-type: none"><li>1. Should support extraction of e-Mail archives from live systems, Forensic Disk Images.</li><li>2. Should support identification, parsing and analysis of mails from various e-Mail clients like Exchange Offline Storage, Microsoft Outlook, IBM Notes (Lotus Notes), Exchange Server, Gmail, Yahoo, IMAP, Hotmail etc.,</li><li>3. Should support web-based mail containers.</li><li>4. Should support link analysis and time line analysis.</li><li>5. Perpetual Licensing with 01 year warranty and Service Maintenance Support (SMS) with update/upgrade for a period of 02 years after warranty.</li><li>6. Desirable:<ul style="list-style-type: none"><li>o Solution should include certified training for 03 Experts from OEM with in India or at OEM location.</li></ul></li></ol>

**Broad Based Specifications of the S/w and H/w Tools for Digital Storage Media Examination Unit of  
National Cyber Forensic Laboratory for Evidentiary purpose**

S. No.	Name of the Tool	Specifications
10.	High End Forensic Work Station	<ol style="list-style-type: none"> <li>1. Processor – intel dual XEON silver CPU 10 core with total threads 40 and 2.2 GHZ 13.75 MB cache or better RAM – Minimum 64 GB ECC MEMORY PC4 21300 DDR 4 or more.</li> <li>2. OS drive - 1 X 512GB M.2 NVMe PCIe Solid State</li> <li>3. Temp/Cache/DB Drive - 1 x 512 GB SATA Solid State Drive.</li> <li>4. DATA DRIVE - 1 x 10 TB 7200 RPM SATA.</li> <li>5. GPU - GTX 1050Ti 4GB 128-bit GDDR5, 768 CUDA CORES, PCI-Express Video Card</li> <li>6. Display – Minimum 24” LCD/ LED Monitor with FHD or better.</li> <li>7. Operating System – preloaded and pre activated Windows 10 Professional with recovery media.</li> <li>8. Integrated write blocking with support for USB 3/2/1.1, PCIe, SATA, Firewire 800/400, IDE, SAS etc., with features like Touch screen interface, Write-Block and Read/Write visibility via Lock/Unlock, Read and write mode capabilities for all device ports, controlled via LCD Menu.</li> <li>9. Should allow simultaneous imaging of 2 attached devices on the integrated write blocker</li> <li>10. Capable to perform forensic imaging of 6 SATA Drives simultaneously.</li> <li>11. Dock with cooling system for Evidence Hard Drive</li> <li>12. Integrated Forensic Media Card Reader - Read-Only or Read-Write mode capable.</li> <li>13. Integrated Retractable imaging shelf (fully retracts into the system when not in use).</li> <li>14. Dual fans for maximum cooling and surface coverage for IDE/SATA/SAS/USB Drives</li> <li>15. Auto On/Off switch when shelf is opened or closed.</li> <li>16. Slotted, cushioned, non-conductive, non-skid, surface supports all popular drive sizes (3-1/2", 2-1/2", 1.8", etc).</li> <li>17. 2 x Shock Mounted SATA Removable Hard Drive Bays (IDE Capable)</li> <li>18. 4 x Hot Swap Shock Mounted Universal (IDE and SATA compatible) Removable Hard Drive Bays. Read-Only or Read-Write mode capable.</li> <li>19. RJ45 LAN ports (2 X 1Gigabit), 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, E-sata 6 Gb/S (Minimum 2 ports),</li> <li>20. System Keys: For removable hard drive bays and front case bezel.</li> <li>21. Adapters and Cables: Cables and adapters to image and process internal/external drives including SAS, SATA, IDE, microSATA, SATA LIF, MacBook Air Blade Type SSDs, mini/micro SSD cards, 1.8 inch IDE (iPod), 2.5 inch IDE (laptop), PCIe SSD m.2 NVMe, PCIe SSD MacBook Pro and Server Class PCIe SSD</li> </ol>



**Broad Based Specifications of the S/w and H/w Tools for Digital Storage Media Examination Unit of  
National Cyber Forensic Laboratory for Evidentiary purpose**

		<p>22. 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> <p>23. BD-R/BD-RE/DVD±RW/CD±RW Blu-ray Burner Dual-Layer Combo Drive</p> <p>24. Perpetual Licensing with 01 year warranty and Service Maintenance Support (SMS) with update/upgrade for a period of 02 years after warranty.</p>
--	--	--

**Broad Based Specifications of the S/w and H/w Tools for Mobile Phone and Embedded System Examination Unit of  
National Cyber Forensic Laboratory for Evidentiary purpose**

S. No.	Name of the Tool	Specifications
1.	Mobile Phone Forensic Examination Lab Kit	<ol style="list-style-type: none"> <li>Software based suit to support Logical, File System and Physical level analysis of various Mobile phones running on Android, iOS, RIM, Windows and custom build OSs.</li> <li>Support bypassing/unlocking of security locks for mobile phones.</li> <li>Support super user/administrative privilege access to popular mobile Oss with various device profiles and support bit-by-bit physical extraction.</li> <li>Support bit-by-bit physical extraction of data from mobile phones based on various chip sets while maintaining the integrity of the data.</li> <li>Support analysis and parsing of data from various mobile artefacts.</li> <li>Support data acquisition and analysis from SIM and USIM cards with various form factors.</li> <li>Support data acquisition and analysis from GPS devices.</li> <li>Support data acquisition and analysis from satellite phones.</li> <li>Support data acquisition and analysis from expandable memory of mobile phones.</li> <li>Support pulling the data from remote cloud resources through cloud login keys extracted from Mobile device.</li> <li>Support extraction of WhatsApp &amp; Viber cloud backup from iCloud and Google Drive.</li> <li>Support data acquisition and analysis from UAVs.</li> <li>Support data acquisition and analysis from Satellite phones.</li> <li>Solution should include specialised data extraction capabilities from <ol style="list-style-type: none"> <li>Locked iPhones later to 4S and</li> <li>Locked Androids with OS later to 6.0 and Security Patch later to October 2016.</li> <li>Solution should support unlocking of minimum 100 mobile phones per annum.</li> </ol> </li> <li>Support data analytics with capability to perform text analytics, image analytics.</li> <li>Support extractionof images using Optical Character Recognition and categorize it as documents or screen shots.</li> <li>Support with various data cables for various mobile phones.</li> <li>Support data acquisition and analysis from popular chipset manufacturers.</li> <li>Supports creation of customized reports.</li> <li>Perpetual Licensing through USB Dongle with 01 year warranty and Service Maintenance Support (SMS) with update/upgrade for a period of 02 years after warranty.</li> <li>Desirable: Solution should include certified training for 03 Experts from OEM with in India or at OEM location.</li> </ol>

**Broad Based Specifications of the S/w and H/w Tools for Mobile Phone and Embedded System Examination Unit of  
National Cyber Forensic Laboratory for Evidentiary purpose**

S. No.	Name of the Tool	Specifications
2.	Software Based solution for Mobile Devices and CDR Analysis.	<ol style="list-style-type: none"> <li>1. Software based solution for the analysis of various Mobile phones running on Android, iOS, Windows and custom build OSs.</li> <li>2. Supports lock screen bypass and Screen Lock disabler with acquisition of locked phones.</li> <li>3. Support data acquisition and analysis from drones.</li> <li>4. Support non- encrypted and encrypted backup parsing.</li> <li>5. Support data acquisition and analysis from SIM cards.</li> <li>6. Support data acquisition and analysis from expandable memory of mobile phones.</li> <li>7. Support pulling the data from cloud resources of mobile phones and analysis.</li> <li>8. Support Call Data Record (CDR) Analysis.</li> <li>9. Support with various data cables for various mobile phones.</li> <li>10. Support data acquisition and analysis from popular chipset manufacturers.</li> <li>11. Supports creation of customized reports.</li> <li>12. Perpetual Licensing through USB Dongle.</li> <li>13. Perpetual Licensing with 01 year warranty and Service Maintenance Support (SMS) with update/upgrade for a period of 02 years after warranty.</li> <li>14. Desirable: <ul style="list-style-type: none"> <li>○ Solution should include certified training for 03 Experts from OEM with in India or at OEM location.</li> </ul> </li> </ol>

**Broad Based Specifications of the S/w and H/w Tools for Mobile Phone and Embedded System Examination Unit of  
National Cyber Forensic Laboratory for Evidentiary purpose**

S. No.	Name of the Tool	Specifications
3.	Solution for Mobile Phone Forensics and Photo recogniser.	<ol style="list-style-type: none"> <li>1. Should support enhanced logical level analysis of Mobile Phones.</li> <li>2. Should support Physical data analysis of Mobile Phone data extracted from other utilities.</li> <li>3. Should support advanced application data analysis.</li> <li>4. Should support Password cracking.</li> <li>5. Should support identify which images present on the analysed phone were taken by the phone's camera using a sensor fingerprint.</li> <li>6. Should support recognition of Photos.</li> <li>7. Should support data extraction from Apple Cloud.</li> <li>8. Should support integrating with other tools like Oxygen Phone Detective, UFED etc.,</li> <li>9. Support bypass of iOS Phones via locked down files extracted from Systems.</li> <li>10. Support for live view of data before actual extraction.</li> <li>11. Support by-passing PIN via SIM cloning.</li> <li>12. Support deleted data recovery.</li> <li>13. Support concurrent extractions.</li> <li>14. Support for Photo Matcher.</li> <li>15. Should include cable tool kit with all adopters.</li> <li>16. Perpetual Licensing with 01 year warranty and Service Maintenance Support (SMS) with update/upgrade for a period of 02 years after warranty.</li> <li>17. Desirable: <ol style="list-style-type: none"> <li>o Solution should include certified training for 03 Experts from OEM with in India or at OEM location.</li> </ol> </li> </ol>

**Broad Based Specifications of the S/w and H/w Tools for Mobile Phone and Embedded System Examination Unit of  
National Cyber Forensic Laboratory for Evidentiary purpose**

S. No.	Name of the Tool	Specifications
4.	Solution for Conducting CHIP level analysis of Mobile Phones.	<ol style="list-style-type: none"> <li>1. Support Extraction of chip-off memory, JTAG board, ISP</li> <li>2. Support Physical/Logical extraction of mobile device</li> <li>3. Support Extraction of selected partition</li> <li>4. Support Data preview during extraction</li> <li>5. Support Write protection and evidence integrity</li> <li>6. Supports feature phones and smartphones.</li> <li>7. Supports iOS, Android, Windows, Tizen, Samsung, LG, Pantech, Apple, Microsoft, Nokia, Motorola Global, Chinese, Japanese, Indian mobile phones.</li> <li>8. Support for various Mobile File Systems viz., FAT12/16/32, exFAT, NTFS, EXT3/4, HFS+, EFS, YAFFS, FSR, XSR</li> <li>9. General memory chip reader</li> <li>10. Heat blower for the general disassemble work</li> <li>11. BGA Reballing kit</li> <li>12. Hot plate for reballing</li> <li>13. Microscope - Zoom Stereo, 3.5X~180X</li> <li>14. Rework station</li> <li>15. Mobile phone dryer</li> <li>16. The JTAG Toolkit should include the below equipment: <ol style="list-style-type: none"> <li>○ RIFF 2 JTAG box</li> <li>○ Z3X Easy JTAG box</li> <li>○ JPIN JTAG Connectors</li> <li>○ Digital Multi-meter</li> <li>○ DC Power Supply</li> <li>○ Banana Plug</li> <li>○ Minigrabber</li> <li>○ Precision Repair Toolkit</li> <li>○ Soldering Station</li> <li>○ Chisel and Sharp Soldering Tips</li> <li>○ Solder Supplies</li> <li>○ LED Magnification Visor</li> <li>○ Safety Glasses</li> <li>○ Wire Stripper</li> <li>○ PCB Board</li> <li>○ Toolkit Case</li> <li>○ Additional JTAG-specific tools and supplies</li> </ol> </li> <li>17. The Chip off Toolkit should at least include the below equipment: <ol style="list-style-type: none"> <li>○ Z3X Easy JTAG box</li> <li>○ Digital Multi-meter</li> <li>○ Precision Repair Toolkit</li> <li>○ Soldering Station</li> <li>○ Solder Supplies</li> <li>○ Pin Probe Test Socket Adapters</li> <li>○ Milling Machine</li> <li>○ Chip-off Heat Station</li> <li>○ Reflow Oven</li> <li>○ Hotair Rework Station</li> </ol> </li> </ol>

**Broad Based Specifications of the S/w and H/w Tools for Mobile Phone and Embedded System Examination Unit of  
National Cyber Forensic Laboratory for Evidentiary purpose**

		<ul style="list-style-type: none"> <li>○ LED Magnification Visor</li> <li>○ Safety Glasses</li> <li>○ PCB Holder</li> <li>○ Microscope for Electronics</li> <li>○ eMMC and UFS Programming Tools</li> <li>○ Toolkit case</li> <li>○ Additional chip-ff specific tools and supplies</li> </ul> <p>18. The Software and the Hardware related apps preloaded on to a system which is part of the suite with the following specs:</p> <ul style="list-style-type: none"> <li>○ OS: Windows 10</li> <li>○ CPU: i7</li> <li>○ RAM: 64GB or more</li> <li>○ HDD: 2TB or more</li> <li>○ Display: 1024x768 or above</li> <li>○ USB: USB 2.0 port 4 or higher</li> </ul> <p>19. Perpetual Licensing through USB Dongle with 01 year warranty and Service Maintenance Support (SMS) with update/upgrade for a period of 02 years after warranty.</p> <p>20. Desirable:</p> <ul style="list-style-type: none"> <li>○ Solution should include certified training for 03 Experts from OEM with in India or at OEM location.</li> </ul>
--	--	---

**Broad Based Specifications of the S/w and H/w Tools for Mobile Phone and Embedded System Examination Unit of  
National Cyber Forensic Laboratory for Evidentiary purpose**

S. No.	Name of the Tool	Specifications
5.	Mobile Phone Forensic Examination Field Kit	<ol style="list-style-type: none"> <li>1. Field solution to the Logical, File System and Physical level analysis of various Mobile phones running on Android, iOS, Windows and custom build OSs.</li> <li>2. Support bypassing/unlocking of security locks for mobile phones.</li> <li>3. Support super user/administrative privilege access to popular mobile OSs.</li> <li>4. Support analysis and parsing of data from various mobile artefacts.</li> <li>5. Support data acquisition and analysis from SIM cards with various form factors.</li> <li>6. Support data acquisition and analysis from GPS devices.</li> <li>7. Support data acquisition and analysis from satellite phones.</li> <li>8. Support data acquisition and analysis from expandable memory of mobile phones.</li> <li>9. Support pulling the data from cloud resources of mobile phones and analysis.</li> <li>21. Support pulling the data from remote cloud resources through cloud login keys extracted from Mobile device.</li> <li>10. Support extraction of WhatsApp &amp; Viber cloud backup from iCloud and Google Drive.</li> <li>11. Support data acquisition from UAVs.</li> <li>12. Support link analysis and time line analysis also data analytics.</li> <li>13. Support with various data cables for various mobile phones.</li> <li>14. Support data acquisition and analysis from popular chipset manufacturers.</li> <li>15. Supports creation of customized reports.</li> <li>16. Perpetual Licensing through USB Dongle.</li> <li>17. Perpetual Licensing with 01 year warranty and Service Maintenance Support (SMS) with update/upgrade for a period of 02 years after warranty.</li> <li>18. Desirable: <ul style="list-style-type: none"> <li>o Solution should include certified training for 03 Experts from OEM with in India or at OEM location.</li> </ul> </li> </ol>

**Broad Based Specifications of the S/w and H/w Tools for Mobile Phone and Embedded System Examination Unit of  
National Cyber Forensic Laboratory for Evidentiary purpose**

S. No.	Name of the Tool	Specifications
6.	Forensic Data extractor tool for Mobile Communication devices.	<ol style="list-style-type: none"> <li>1. <b>Should be windows-based software solution.</b></li> <li>2. Automated and manual mode of data extraction of data from cloud sources.</li> <li>3. Should support getting actionable intelligence on flight paths, launch locations, images, video, operational logs and other critical data from Drones.</li> <li>4. Support extract and decode data from non-standard mobile devices.</li> <li>5. Support raw method of analysis via camera attachment.</li> <li>6. Support wide range of mobile devices with various OSs like Android, iOS, Windows, Blackberry, Bada.</li> <li>7. Support HEX view of data.</li> <li>8. Support deleted data recovery.</li> <li>9. Should support device dump and binary data analysis.</li> <li>10. Should support</li> <li>11. Perpetual Licensing with 01 year warranty and Service Maintenance Support (SMS) with update/upgrade for a period of 02 years after warranty.</li> <li>12. Desirable: <ul style="list-style-type: none"> <li>○ Solution should include certified training for 03 Experts from OEM with in India or at OEM location.</li> </ul> </li> </ol>



**Broad Based Specifications of the S/w and H/w Tools for Mobile Phone and Embedded System Examination Unit of  
National Cyber Forensic Laboratory for Evidentiary purpose**

S. No.	Name of the Tool	Specifications
7.	High End Forensic Work Station	<ol style="list-style-type: none"> <li>1. Processor – intel dual XEON silver CPU 10 core with total threads 40 and 2.2 GHZ 13.75 MB cache or better RAM – Minimum 64 GB ECC MEMORY PC4 21300 DDR 4 or more.</li> <li>2. OS drive - 1 X 512GB M.2 NVMe PCIe Solid State</li> <li>3. Temp/Cache/DB Drive - 1 x 512 GB SATA Solid State Drive.</li> <li>4. DATA DRIVE - 1 x 10 TB 7200 RPM SATA.</li> <li>5. GPU - GTX 1050Ti 4GB 128-bit GDDR5, 768 CUDA CORES, PCI-Express Video Card</li> <li>6. Display – Minimum 24” LCD/ LED Monitor with FHD or better.</li> <li>7. Operating System – preloaded and pre activated Windows 10 Professional with recovery media.</li> <li>8. Integrated write blocking with support for USB 3/2/1.1, PCIe, SATA, Firewire 800/400, IDE, SAS etc., with features like Touch screen interface, Write-Block and Read/Write visibility via Lock/Unlock, Read and write mode capabilities for all device ports, controlled via LCD Menu.</li> <li>9. Should allow simultaneous imaging of 2 attached devices on the integrated write blocker</li> <li>10. Capable to perform forensic imaging of 6 SATA Drives simultaneously.</li> <li>11. Dock with cooling system for Evidence Hard Drive</li> <li>12. Integrated Forensic Media Card Reader - Read-Only or Read-Write mode capable.</li> <li>13. Integrated Retractable imaging shelf (fully retracts into the system when not in use).</li> <li>14. Dual fans for maximum cooling and surface coverage for IDE/SATA/SAS/USB Drives</li> <li>15. Auto On/Off switch when shelf is opened or closed.</li> <li>16. Slotted, cushioned, non-conductive, non-skid, surface supports all popular drive sizes (3-1/2", 2-1/2", 1.8", etc).</li> <li>17. 2 x Shock Mounted SATA Removable Hard Drive Bays (IDE Capable)</li> <li>18. 4 x Hot Swap Shock Mounted Universal (IDE and SATA compatible) Removable Hard Drive Bays. Read-Only or Read-Write mode capable.</li> <li>19. RJ45 LAN ports (2 X 1Gigabit), 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, E-sata 6 Gb/S (Minimum 2 ports),</li> <li>20. System Keys: For removable hard drive bays and front case bezel.</li> <li>21. Adapters and Cables: Cables and adapters to image and process internal/external drives including SAS, SATA, IDE, microSATA, SATA LIF, MacBook Air Blade Type SSDs, mini/micro SSD cards, 1.8 inch IDE (iPod), 2.5 inch IDE (laptop), PCIe SSD m.2 NVMe, PCIe SSD MacBook Pro and Server Class PCIe SSD</li> <li>22. Security Screwdriver Set: A varied assortment of popular security bits for opening computer enclosures that may have been locked down in a corporate environment</li> <li>23. BD-R/BD-RE/DVD±RW/CD±RW Blu-ray Burner Dual-Layer Combo Drive</li> <li>24. Perpetual Licensing with 01 year warranty and Service Maintenance Support (SMS) with update/upgrade for a period of 02 years after warranty.</li> </ol>

**Broad Based Specifications of the S/w and H/w Tools for Advanced Digital Forensic Examination Unit of  
National Cyber Forensic Laboratory for Evidentiary purpose**

S. No.	Name of the Tool	Specifications
1.	Damaged Media Analysis suite	<ol style="list-style-type: none"> <li>1. Hardware-Software solution for diagnosis, repair and recovery of data from</li> <li>2. Damaged HDDs based on               <ul style="list-style-type: none"> <li>○ SATA (Serial ATA) ,IDE interfaces for various manufacturers(Seagate, Western Digital, Fujitsu, Samsung, Maxtor, Quantum, IBM (HGST), HITACHI, TOSHIBA,etc)of various capacities with support for all the file systems (i.e. FAT, exFAT, NTFS, EXT2/3/4, HFS+, UFS1/2, XFS, ReiserFS, VMFS and virtual images VMDK, and VHD etc.) and various form factors: 3.5" - desktop drives, 2.5", 1.8" - laptop drivesetc.</li> </ul> </li> <li>3. Damaged RAID arrays based on               <ul style="list-style-type: none"> <li>○ SATA, IDE interfaces with different configurations like Stripe, Mirror, JBOD, 1E Offset, 1E Adjacent, 4, 5, 5E, 5EE, 6, 6 Adaptec and any combinations of RAID etc.</li> </ul> </li> <li>4. Damaged SSDs with SATA, PATA, mSATA, and M.2 (NGFF) interfaces and of various capacities produced by different manufacturers(such as OCZ, Corsair, Crucial, RunCore, A-DATA, G.Skill, Micron, Plextor, Intel, Samsung, Seagate, SanDisk, Kingston and others.)</li> <li>5. All NAND based devices where there is no access through the authorized drive interface:               <ul style="list-style-type: none"> <li>○ UFD (USB Flash Drive), SD (Secure Digital Card), CF (Compact Flash), micro SD (micro Secure Digital Card), MS (Memory Stick), xD, Monolithic Flash Devices, MMC (Multi Media Card), Voice Recorder (dictaphone), mobile phones with various generations having different operations systems.</li> </ul> </li> <li>6. The solution should include creation of clean room facility of 100 sft. for disassembling/reassembling the media with all required anti-dusting and vacuum cleaning capabilities.</li> <li>7. The solution should provide all required drive library with regular updates/upgrades for a period of 03 years.</li> <li>8. The suit should include features of Disk Diagnostics and automatically diagnose hard disk electronics, motor, heads, media surface, firmware, file systems, and provide a clean and easy to read report.</li> <li>9. Should support identification of damage in the areas - Circuit Board (PCB), Motor, Heads (status of each head is displayed), Media Surface, Firmware Area, Partitions and File System.</li> <li>10. Should support imaging the damaged disk by way of Multi-pass imaging with different timeouts for each pass, Reducing read block size to a very small value, Utilizing PHY reset and interface reset feature, Imaging data from good heads only, Bad sector recovery.</li> <li>11. Support selective head imaging.</li> <li>12. Support artefact finding basing on predefined criteria.</li> <li>13. Support disk password removal.</li> <li>14. Support segment hashing.</li> <li>15. Support bad sector recovery, file recovery, firmware recovery.</li> <li>16. Support various disk utilities like, drive comparison, sanitisation, HPA detection, SSD Trim, Disk editor, etc.,</li> <li>17. Perpetual Licensing with 01 year warranty and Service Maintenance Support (SMS) with update/upgrade for a period of 02 years after</li> </ol>

**Broad Based Specifications of the S/w and H/w Tools for Advanced Digital Forensic Examination Unit of  
National Cyber Forensic Laboratory for Evidentiary purpose**

		<p>warranty.</p> <p>18. Desirable:</p> <ul style="list-style-type: none"><li>○ Solution should include certified training for 03 Experts from OEM within India or at OEM location.</li></ul>
--	--	--

**Broad Based Specifications of the S/w and H/w Tools for Advanced Digital Forensic Examination Unit of  
National Cyber Forensic Laboratory for Evidentiary purpose**

S. No.	Name of the Tool	Specifications
2.	Password Recovery solution.	<ol style="list-style-type: none"> <li>1. Able to crack password of vivid files with dictionary/brute-force/custom attacks.</li> <li>2. Able to decrypt encrypted disks/volumes/folders/files with white box and black box attacks with the assistance of memory/RAM dumps.</li> <li>3. Able to bypass/crack windows boot passwords, SAM, NTLM Hashes.</li> <li>4. Able to bypass/crack passwords of smart phones.</li> <li>5. Support advanced Password Recovery for archives compressed with various methods.</li> <li>6. Support decryption of EFS-Encrypted Files and FDE Volumes/Disks, MAC OS Keychain and File Vaults.</li> <li>7. Support recovery of Passwords for various Instant Messages and various Intuit Documents.</li> <li>8. Support recovery of Passwords of files created by various word processing applications.</li> <li>9. Support recovery of Passwords of POP3 and IMAP email clients and extraction of Passwords from the auto complete locations of various Web Browsers.</li> <li>10. Support decryption of Encrypted SQL databases.</li> <li>11. Support decryption of Sage PeachTree Accounting Passwords, Protected ACT! Documents, PeachTree Accounting Passwords</li> <li>12. Support Distributed Password Recovery with support minimum of 15 Clients.</li> <li>13. Support Extraction of data from Blackberry Backups i.e. IPD and BBB and Mobile Phone Backups.</li> <li>14. Support Decryption of WhataApp Databases from Androids and iTunes Backups along with other chat applications.</li> <li>15. Support recovery of password from Windows User account Salts.</li> <li>16. Support decryption of Bitcoin Vaults.</li> <li>17. Perpetual Licensing with 01 year warranty and Service Maintenance Support (SMS) with update/upgrade for a period of 02 years after warranty.</li> <li>18. Desirable: <ul style="list-style-type: none"> <li>○ Solution should include certified training for 03 Experts from OEM within India or at OEM location.</li> </ul> </li> </ol>

**Broad Based Specifications of the S/w and H/w Tools for Advanced Digital Forensic Examination Unit of  
National Cyber Forensic Laboratory for Evidentiary purpose**

S. No.	Name of the Tool	Specifications
3.	Virtual Machine Creation and Management Tool.	<ol style="list-style-type: none"> <li>1. Able to Create New VMs, Create Large VMs (such as 16CPU, 64GB RAM, 3GB VRAM) with support to various Guest OSs.</li> <li>2. Support for latest Windows 10 as Guest and Host.</li> <li>3. Support for macOS Mojave Host and Guest</li> <li>4. Support for Mass Deployment, Host/Guest Integration, Host/Guest File Sharing</li> <li>5. Support running VMs with Different View Modes, 3D Graphics with DX10.1 and OpenGL 3.3 Support, Drag-able Tabbed Interface, One-Click SSH to Linux VM</li> <li>6. Device Support, 4K / Retina Display Support, Support a Wide Range of Virtual Devices, USB Smart Card Reader Support, USB 3.0 Device Support, Works with Assistive Devices (Section 508 Compliant), Multi-Language Keyboard Support</li> <li>7. Able to run BootCamp as VM, Import/Convert BootCamp into VM</li> <li>8. Microsoft Virtualization Based Security (Guest) Support, Virtual Trusted Platform Module (vTPM)</li> <li>9. UEFI Boot Support, UEFI Secure Boot Support</li> <li>10. Create/Manage Encrypted VM</li> <li>11. Virtual Network Rename</li> <li>12. Run Managed/Restricted Desktop</li> <li>13. REST API Control</li> <li>14. vCenter Server Appliance Effortless Deploy</li> <li>15. Command Line Operation</li> <li>16. Snapshots, Run Multiple VMs at Once, Run Encrypted VM</li> <li>17. Virtual Network Customization, Virtual Network Simulation (packet loss, latency), Virtual Machine Cloning</li> <li>18. Share Virtual Machine (Workstation Server)</li> <li>19. Perpetual Licensing with 01 year warranty and Service Maintenance Support (SMS) with update/upgrade for a period of 02 years after warranty.</li> <li>20. Desirable: <ul style="list-style-type: none"> <li>o Solution should include certified training for 03 Experts from OEM within India or at OEM location.</li> </ul> </li> </ol>

**Broad Based Specifications of the S/w and H/w Tools for Advanced Digital Forensic Examination Unit of  
National Cyber Forensic Laboratory for Evidentiary purpose**

S. No.	Name of the Tool	Specifications
4.	Disassembler coupled Debugger with hex editor.	<p>Should support</p> <ol style="list-style-type: none"> <li>1. RAM editor e.g. for debugging purposes (programming), for examining/manipulating any running program and computer games (cheating).</li> <li>2. Analyzing files e.g. to determine the type of data recovered as lost cluster chains by ScanDisk or chkdsk.</li> <li>3. ASCII - EBCDIC conversion to Allow exchange text between mainframe computers and the PC in both directions.</li> <li>4. Edit   Convert Binary, Hex ASCII, Intel Hex, and Motorola S conversion.</li> <li>5. Conveniently editing data structure using custom templates. Download a tutorial.</li> <li>6. Splitting files that do not fit on a disk</li> <li>7. Finding interesting values (e.g. the number of lives, ammunition, etc.) in saved game files using the Combined Search or using the File Comparison utility.</li> <li>8. Manipulating text Viewing and manipulating files that usually cannot be edited as they are protected by Windows (e.g. the swap file, temporary files of the Internet Explorer), using the disk editor.</li> <li>9. Viewing, editing, and repairing system areas such as the Master Boot Record with its partition table and boot sectors.</li> <li>10. Automated file editing using scripts</li> <li>11. Interactive, programmable, multi-processor disassembler coupled to a local and remote debugger and augmented by a complete plugin programming environment.</li> <li>12. Support explore binary programs, for which source code isn't always available, to create maps of their execution.</li> <li>13. Support debugging the various 32-bit and 64-bit MS Windows executables, MS Windows, Linux, Mac OS X both locally and remotely.</li> <li>14. Perpetual Licensing with 01 year warranty and Service Maintenance Support (SMS) with update/upgrade for a period of 02 years after warranty.</li> <li>15. Desirable: <ul style="list-style-type: none"> <li>o Solution should include certified training for 03 Experts from OEM within India or at OEM location.</li> </ul> </li> </ol>

**Broad Based Specifications of the S/w and H/w Tools for Advanced Digital Forensic Examination Unit of  
National Cyber Forensic Laboratory for Evidentiary purpose**

S. No.	Name of the Tool	Specifications
5.	Visual Resource Editor.	<ol style="list-style-type: none"> <li>1. Should support Working with 32- and 64-bit executable files such as .EXE, .DLL, binary .RES, ActiveX Controls (.OCX), Borland Libraries (.DPL and .BPL), XP Visual Styles (.MSSTYLES), Control Panel Extensions (.CPL), Screen Savers (.SCR) and any other win32 executables.</li> <li>2. Resource optimizing, error checking and repairing automatically.</li> <li>3. Support for insert the manifest resource in existing applications</li> <li>4. Automatic UPX unpacking.</li> <li>5. Support for custom plug-ins to perform any start-up processing.</li> <li>6. Saving multiple resources at once.</li> <li>7. Navigate easily through the Delphi forms, RCData, and objects, and view their contents (Image Lists, Strings List, Glyphs, Bitmaps).</li> <li>8. Perpetual Licensing with 01 year warranty and Service Maintenance Support (SMS) with update/upgrade for a period of 02 years after warranty.</li> <li>9. Desirable: <ul style="list-style-type: none"> <li>o Solution should include certified training for 03 Experts from OEM within India or at OEM location.</li> </ul> </li> </ol>

**Broad Based Specifications of the S/w and H/w Tools for Advanced Digital Forensic Examination Unit of  
National Cyber Forensic Laboratory for Evidentiary purpose**

S. No.	Name of the Tool	Specifications
6.	Advanced 2 and 3-way file comparison merging and folder synchronization tool.	<p>The tool should have the following capabilities:</p> <ol style="list-style-type: none"><li>1. Text comparison and merging</li><li>2. Compare text from common office file formats</li><li>3. Image and binary file comparison</li><li>4. Three-way comparison and automatic merging</li><li>5. Folder hierarchy comparison and synchronization</li><li>6. Archive comparison.</li><li>7. Direct access to configuration management (version control) systems, Time Machine and FTP sites</li><li>8. Perpetual Licensing with 01 year warranty and Service Maintenance Support (SMS) with update/upgrade for a period of 02 years after warranty.</li><li>9. Desirable:<ul style="list-style-type: none"><li>o Solution should include certified training for 03 Experts from OEM within India or at OEM location.</li></ul></li></ol>



**Broad Based Specifications of the S/w and H/w Tools for Advanced Digital Forensic Examination Unit of  
National Cyber Forensic Laboratory for Evidentiary purpose**

S. No.	Name of the Tool	Specifications
7.	SQL Database Comparator.	<ol style="list-style-type: none"> <li>1. Should support SQL Server 2005, 2008, 2012, 2014, 2016, 2017, SQL Azure, &amp; SQL Server on Amazon RDS databases.</li> <li>2. Support to take Snapshots of the schema for audit and roll-back purposes.</li> <li>3. Capable to               <ul style="list-style-type: none"> <li>○ Backup files (both native SQL Server &amp; Redgate SQL Backup Pro)</li> <li>○ Compare and deploy changes to SQL Server database schemas (from dev, to test, to production)</li> <li>○ Compare two SQL Server databases (Small and Large), synchronize, and deploy from within SSMS</li> <li>○ Automatically create error-free deployment, synchronization scripts</li> <li>○ Generate T-SQL scripts that update one SQL Server database to match the schema of another</li> <li>○ Migrate individual schema differences, a selection of them, or all of them</li> <li>○ Support for reading encrypted database objects</li> <li>○ Troubleshoot database differences and explore schema changes to see what's going on in development</li> <li>○ Support for Temporal Tables, Retention Tables, Azure Active Directory authentication, SQL Graph, save database and server login details, connections to SQL Server instances on Linux, Run deployments from the command line</li> </ul> </li> <li>4. Should include all supported modules.</li> <li>5. Perpetual Licensing with 01 year warranty and Service Maintenance Support (SMS) with update/upgrade for a period of 02 years after warranty.</li> <li>6. Desirable:               <ul style="list-style-type: none"> <li>○ Solution should include certified training for 03 Experts from OEM within India or at OEM location.</li> </ul> </li> </ol>

**Broad Based Specifications of the S/w and H/w Tools for Advanced Digital Forensic Examination Unit of  
National Cyber Forensic Laboratory for Evidentiary purpose**

S. No.	Name of the Tool	Specifications
8.	Forensic Log Analysis tool	<ol style="list-style-type: none"><li>1. Support GUI based automated SQL query access to any system log or text-based data including Web Server Logs (IIS, Apache, W3C, SharePoint, MS Exchange, FTP, etc), Windows System Events and application log files (generated with log4net, Nlog, SeriLog, etc.).</li><li>2. Perpetual Licensing with 01 year warranty and Service Maintenance Support (SMS) with update/upgrade for a period of 02 years after warranty.</li><li>3. Desirable:<ul style="list-style-type: none"><li>o Solution should include certified training for 03 Experts from OEM within India or at OEM location.</li></ul></li></ol>

**Broad Based Specifications of the S/w and H/w Tools for Advanced Digital Forensic Examination Unit of  
National Cyber Forensic Laboratory for Evidentiary purpose**

S. No.	Name of the Tool	Specifications
9.	Forensic Data Mining through OSINT architecture.	<ol style="list-style-type: none"> <li>1. Should provide a platform for data mining from open web resources.</li> <li>2. Should include All APIs to perform search of the online resources.</li> <li>3. Should include subscription for access to Kaspersky full Threat Intelligence.</li> <li>4. Query Threat Grid's database of threat intelligence.</li> <li>5. The set of transforms to retrieve data from Facebook, Instagram, Foursquare, LinkedIn, Twitter, Google+, V Kontakte. Search queries to Google, Bing, Baidu, Yandex, Yahoo, Google Images, Youtube. Search for documents, companies, offshores, aliases. Identify Facebook, Skype, Gravatar profiles by email.</li> <li>6. Query the ThreatConnect Platform for your indicators, groups, and other information.</li> <li>7. Query Flashpoint's Deep and Dark Web intelligence datasets..</li> <li>8. Query the Intel 471 API to obtain attribution and additional data around indicators and threat actors.</li> <li>9. Query the CrowdStrike Intelligence API to obtain attribution and additional data for indicators.</li> <li>10. Query the CrowdStrike ThreatGraph API to interact with CrowdStrike Falcon data.</li> <li>11. SocialNet maps social media connections with data from 70+ social networks using 700+ transforms. Query by email address, aliases, phone numbers, or names to visualize 1 to 1 correlations, multiple relationships and networks into the thousands of records.</li> <li>12. Transforms for monitoring and analyzing news from different sources.</li> <li>13. Query the Digital Shadows cyber threat intelligence database.</li> <li>14. Visualize threat data, identify connections and correlate campaigns in minutes using 30+ transforms.</li> <li>15. Search and visualize relationships between phishing attacks and their payloads.</li> <li>16. Query FireEye iSIGHT Intelligence holdings.</li> <li>17. Investigate cybercrime with DomainTools historic and reverse datasets.</li> <li>18. Threat Intelligence transforms from Silobreaker.</li> <li>19. Visualize ZeroFOX social media threat intelligence and custom alerts.</li> <li>20. Query ThreatCrowd for Malware, Passive DNS, historical Whois data and Maxmind Precision Services.</li> <li>21. Use PhoneSearch to verify phone numbers, providing real names, addresses, social media links and related persons.</li> <li>22. Investigate and pivot domains, identities, IPs, &amp; more with DomainTools Iris.</li> <li>23. Should support in-house installation and function and strictly no data sharing.</li> <li>24. Should support code analysis by way of multi core processing, distributed processing.</li> <li>25. Perpetual Licensing with 01 year warranty and Service Maintenance Support (SMS) with update/upgrade for a period of 02 years after warranty.</li> <li>26. Desirable: <ul style="list-style-type: none"> <li>○ Solution should include certified training for 03 Experts from OEM within India or at OEM location.</li> </ul> </li> </ol>

**Broad Based Specifications of the S/w and H/w Tools for Advanced Digital Forensic Examination Unit of  
National Cyber Forensic Laboratory for Evidentiary purpose**

S. No.	Name of the Tool	Specifications
10.	High End Forensic Work Station	<ol style="list-style-type: none"> <li>1. Processor – intel dual XEON silver CPU 10 core with total threads 40 and 2.2 GHZ 13.75 MB cache or better</li> <li>2. RAM – Minimum 64 GB ECC MEMORY PC4 21300 DDR 4 or more.</li> <li>3. OS drive - 1 X 512GB M.2 NVMe PCIe Solid State</li> <li>4. Temp/Cache/DB Drive - 1 x 512 GB SATA Solid State Drive.</li> <li>5. DATA DRIVE - 1 x 10 TB 7200 RPM SATA.</li> <li>6. GPU - GTX 1050Ti 4GB 128-bit GDDR5, 768 CUDA CORES, PCI-Express Video Card</li> <li>7. Display – Minimum 24” LCD/ LED Monitor with FHD or better.</li> <li>8. Operating System – preloaded and pre activated Windows 10 Professional with recovery media.</li> <li>9. Integrated write blocking with support for USB 3/2/1.1, PCIe, SATA, Firewire 800/400, IDE, SAS etc., with features like Touch screen interface, Write-Block and Read/Write visibility via Lock/Unlock, Read and write mode capabilities for all device ports, controlled via LCD Menu.</li> <li>10. Should allow simultaneous imaging of 2 attached devices on the integrated write blocker</li> <li>11. Capable to perform forensic imaging of 6 SATA Drives simultaneously.</li> <li>12. Dock with cooling system for Evidence Hard Drive</li> <li>13. Integrated Forensic Media Card Reader - Read-Only or Read-Write mode capable.</li> <li>14. Integrated Retractable imaging shelf (fully retracts into the system when not in use).</li> <li>15. Dual fans for maximum cooling and surface coverage for IDE/SATA/SAS/USB Drives</li> <li>16. Auto On/Off switch when shelf is opened or closed.</li> <li>17. Slotted, cushioned, non-conductive, non-skid, surface supports all popular drive sizes (3-1/2", 2-1/2", 1.8", etc).</li> <li>18. 2 x Shock Mounted SATA Removable Hard Drive Bays (IDE Capable)</li> <li>19. 4 x Hot Swap Shock Mounted Universal (IDE and SATA compatible) Removable Hard Drive Bays. Read-Only or Read-Write mode capable.</li> <li>20. RJ45 LAN ports (2 X 1Gigabit), 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, E-sata 6 Gb/S (Minimum 2 ports),</li> <li>21. System Keys: For removable hard drive bays and front case bezel.</li> <li>22. Adapters and Cables: Cables and adapters to image and process internal/external drives including SAS, SATA, IDE, microSATA, SATA LIF, MacBook Air Blade Type SSDs, mini/micro SSD cards, 1.8 inch IDE (iPod), 2.5 inch IDE (laptop), PCIe SSD m.2 NVMe, PCIe SSD MacBook Pro and Server Class PCIe SSD</li> <li>23. Security Screwdriver Set: A varied assortment of popular security bits for opening computer enclosures that may have been locked down in a corporate environment</li> </ol>

**Broad Based Specifications of the S/w and H/w Tools for Advanced Digital Forensic Examination Unit of  
National Cyber Forensic Laboratory for Evidentiary purpose**

		24. BD-R/BD-RE/DVD±RW/CD±RW Blu-ray Burner Dual-Layer Combo Drive 25. Perpetual Licensing with 01 year warranty and Service Maintenance Support (SMS) with update/upgrade for a period of 02 years after warranty.
--	--	---

**Broad Based Specifications for Forensic Smart Server for  
National Cyber Forensic Laboratory for Evidentiary purpose**

**Technical Specification for Integrated Smart racks and its components**

The laboratory of CFSL, Hyderabad intends to establish a Forensic Smart Server on a turn-key solution basis of design, built, operate, maintain and handover basis. The Server should be handled/maintained for one year on-site and thereafter on AMC basis if CFSL personnel not in a position to maintain on their own.

**1. SCOPE:**

- 1.1 This specification covers intelligent integrated/inbuilt infrastructure, standalone system design, engineering, manufacture, assembly, testing at manufacturer's works, supply, delivery at site, unloading, handling, proper storage at site, erection, testing and commissioning at site of complete infrastructure for the proposed **High End Forensic Server** to be installed by CFSL at Hyderabad as detailed in the specification, complete with all accessories required for efficient and trouble free operations.
- 2 The detail specifications of the intelligent integrated/inbuilt infrastructure, standalone system shall be composed of dual active power and cooling distribution paths, with redundant components.
- 3 The Intelligent Integrated Infrastructure essentially includes internal redundant or backup power supplies, environmental controls (e.g., rack mount air conditioning, smoke detection, Water leak detection, temperature & humidity sensor, door status sensor etc), security devices etc. Critical systems like UPS and Rack mount Air-conditioning system will have N+N topology respectively.
- 4 The Intelligent integrated infrastructure shall be having foot print approximately 18 Sq.Ft which shall have min 42 U usable space (2 rack), to accommodate IT and network equipment & devices.
- 5 The Intelligent integrated infrastructure would provide many functionality and some of the key functionalities are Cold Contained Front Aisle & Rear Contained Hot Aisle, insulation, remote management and single point of service and should manufacture and maintain the spare parts in India. All critical components Like PAC, UPS, Racks & environment monitoring system shall be from Single OEM.
- 6 The Intelligent integrated Infrastructure shall have following components:-
  - 6.1 Rack Mount Air conditioner with digital scroll compressor, of capacity 7 kW 02 nos. to cater IT load approximately 7 kW for total 2 racks.

**Broad Based Specifications for Forensic Smart Server for  
National Cyber Forensic Laboratory for Evidentiary purpose**

- 6.2 2 x 7 KVA – rack mount UPS with P.F. up to 0.9 & efficiency up to 92.5%. There should be 20 minutes battery back-up. UPS should be mounted inside the cabinet only. Batteries should be mounted on a stand, placed adjacent to the rack in a closed cabinet.
- 6.3 Smoke detectors, water leaks detection system, temperature & humidity sensor, door sensor, and alarm beacon. 1 set
- 6.4 42 U racks of dimension 800 mm x 1000 mm, 2 numbers ; Front glass door & rear plain door for both racks.
- 6.5 Monitoring system – capable for Email alerts
- 6.6 Optional Pin type / Biometric access control system which should be control by access control panel. 1 set
- 6.7 Optional ,Novec 1230 Gas based fire suppression system as per NFPA guidelines
- 6.8 42U Vertical Rack mount PDU of type IEC C13 x 12 sockets & IEC C19 x 4 sockets combination, each rack shall have two such PDU's.
- 6.9 All critical components like PAC, UPS, Racks & Environment monitoring system should be from a single OEM.
- 6.10 OEM should have Manufacturing Units In India and should maintain spare parts.
- 6.11 Electrical system with essential MCB for UPS & Cooling unit input supply.

**DETAILED SPECS OF COMPONENTS**

**2. Uninterrupted Power Supply (UPS) System**

**Configuration: 2 x 7 kVA (N+N Redundancy)**

**General Description:**

Supply, install, test and commissioning of two numbers of true online, double conversion, high efficiency, high power factor Uninterruptible Power Systems (UPS) rated at 2 x 7 kVA with battery backup support for 20 minutes on full load. The backup batteries should be supplied with the necessary arrangements to mount outside rack in a closed cabinet.

## **Broad Based Specifications for Forensic Smart Server for National Cyber Forensic Laboratory for Evidentiary purpose**

### **Scope:**

- The scope include design, supply, installation, testing and commissioning of the complete UPS system and related accessories including:
- All Server racks will get power feed from two independent 2 x 7 KVA UPS systems to ensure redundancy.
- All systems should be tested in factory as per the manufactures recommended procedure for all operating parameters and the test results should be provided during the installation.
- Delivery at site, unloading, handling, installation of complete system including interconnection from the UPS system to batteries and to input / output panels switches. All interconnections shall be done using multi-strand Flexible Copper conductor cables of appropriate sizes.
- Scope includes battery bank connections and providing safety barriers for all bus bars and cable connection leads on battery racks.
- Energizing of UPS and Battery bank commissioning.
- UPS control parameters setting and complete testing of system on load.-
- Service backup by engineer till system is fully operational and subsequently training is to be provided to the concerned persons of the Institute.
- Any upgrade of the system hardware and associated other software during the warranty period should be supplied at free of charge.
- Acceptance tests will be carried out after installation and the systems will be taken over only after successful completion of the acceptance tests.
- Operation and service manuals of the systems containing technical / Electronic drawings / circuit diagrams complete in all respects should be supplied.

### **Specification / features of the Each UPS system are as follows:**

- i. Widest input range.
- ii. Double conversion and IGBT technology.
- iii. Full IGBT Rectifier / Battery charger.
- iv. IGBT based Inverter.
- v. Batteries to support 20 minutes full load backup.
- vi. Facility for remote viewing
- vii. Easy to expand in a cost effective way



**Broad Based Specifications for Forensic Smart Server for  
National Cyber Forensic Laboratory for Evidentiary purpose**

**7KVA UPS other Technical Specification:**

7 kVA UPS Technical Specifications	
OUTPUT PARAMETERS	
Capacity	07 kVA / 9 KW
Power Factor	0.9
Configuration	1 Ph 3 wire or 3 Ph 4wire
Nominal Voltage	220Vac
Voltage Precision	3 %
O/P Voltage THD	<=3% - Linear load <=5% - Non linear load
Output Frequency	50 Hz / 60 Hz
Frequency Precision	0.25 %
Load Crest Factor	3:1 comply with 62040-3
Over load Performance	105%-125%; 5 mins, 125%-150% ; 1 min
AC-AC Efficiency	>92.5%
Switching time	0 milli second
INPUT PARAMETERS	
Rectifier Type	IGBT Rectifier
Rated Voltage	230/400 Vac single phase 3 wire/3 phase 4 wire
Input Voltage Range	Single Phase 120 to 288 Vac;
Input Frequency range- Hz	45 - 65 Hz
Input Power Factor	>=0.99 for 1Ø / 0.95 for 3Ø
BATTERY PARAMETERS	
Type	SMF/12V
ENVIRONMENTAL PARAMETERS	

**Broad Based Specifications for Forensic Smart Server for  
National Cyber Forensic Laboratory for Evidentiary purpose**

Operating temperature	0 to 40 deg. centigrade
Relative Humidity	5-95% without Condensation
Max. Altitude	<1500 meters
<b>SYSTEM PARAMETERS &amp; STANDARDS</b>	
Conversion Type	Online Double Conversion
Installation Mode	Rack / Tower Convertible
Noise level	>5 dB
Safety	IEC/EN62040-1-1
Electromagnetic Compatibility	IEC/EN62040-2, IEC/EN61000-3-11, IEC/EN61000-3-12, YD/T1095-2008
Surge Protection	IEC EN62040-2/meeting IEC EN61000-4-5
Protection level	IP20
Dimension (mm)	430x640x85 (2U)
<b>COMMUNICATION &amp; MANAGEMENT</b>	
Interface Type	USB/ Intelligent slot/(Dry Contact Card/Modbus card/RS 485 card)

**Installation:**

- (i) The entire system shall be installed as per manufacturer's recommendations & instructions including all interconnections for supply & control circuits.
- (ii) All components shall be clearly identified using labels including battery cells individually.
- (iii) Services of authorized representative or manufacturer for supervision of installation, connections, testing, & adjustments shall be provided.

**Testing& Commissioning:**

- (i) Under supervision of manufacturer's representative all system functions, operations, protective features shall be checked & preset to ensure compliance or specifications.
- (ii) Test the system as per recommendations & test listed bellow using pre-calibrated instruments.

**Broad Based Specifications for Forensic Smart Server for  
National Cyber Forensic Laboratory for Evidentiary purpose**

1. Load simulation.
2. Simulation of malfunctions to verify protective device operations.
3. Duration of supply on emergency. Low battery voltage alarm & shutdown, transfer & restoration of normal supply.
4. Remote status & alarm tests.

In case of test any shortfalls / faults, the same shall be rectified & test procedure shall be again repeated to establish satisfactory performance.

**Cleaning:**

On completion of installation, testing of the system all components, cabinets etc. shall be cleaned & unwanted material, debris shall be removed from site. Scratches dents if any shall be cleaned & touched up to match the original finish.

**Drawings & Manuals for UPS**

Following drawings & manuals / information shall be submitted in at least THREE copies at appropriate stages & for handing over the system.

- i Manufacturer's data for product, features, components & performance along with the offer.
- ii Operation & maintenance manual with;
  1. List of recommended spares & replacement components.
  2. Detail operating instructions covering operations in normal & abnormal conditions.
  3. Shop drawings showing detail fabrication, assembly of components, internal & interconnecting wiring, dimensions, plans & views, installation details access & clearance etc for approval.
  4. Product certificates for Brought out items.
  5. Factory test certificates & Inspection report.
  6. Field test reports.

3. **Rack Mount Air Conditioning System**

**b. Configuration:**

- i. Supply, installation, testing and commissioning of 7 kW rack cooling Type Air-conditioning Units designed specifically for high sensible heat ratio with cooling techniques to match the low latent loads of systems to be installed in the integrated cabinet for effective and uniform distribution of cooling.
- ii. The cooling unit will have digital scroll compressor which modulates the cooling capacity as per heat load requirement inside the IT Rack.
- iii. Cold air will be supplied to the cold aisle containment of the integrated cabinet and the hot air will be taken from the hot aisle containment of the cabinet.

**Broad Based Specifications for Forensic Smart Server for  
National Cyber Forensic Laboratory for Evidentiary purpose**

**7 kW Cooling Unit Technical Specification:**

<b>Specification</b>
High sensible cooling unit with 100% duty cycle
Cooling capacity of 7 kW with capacity modulation
Split indoor & Outdoor unit design
Cooling Unit integrated in rack, 19" mountable not more than 9U
Digital Scroll compressor for capacity modulation
Digital Scroll compressor for high reliability
Electronically commutated centrifugal evaporator fan for high energy efficiency
Air flow suitable to rack equipment from bottom to top discharge in vertical direction
Thermal insulation on indoor unit
Under voltage and Overvoltage protection for equipment safety
High Pressure & Low Pressure protection for safe operation
Washable filter with 80% efficiency down to 20 micron rating and HDPE media
Flare type Thermostatic Expansion Valve for easy serviceability
Refrigerant R 410 A compatible
Hydrophilic evaporator coil
Individual breakers at indoor and outdoor unit for protection
Flexible Cu piping for easy indoor to outdoor connection at rack level
ON/OFF switch at indoor unit for emergency purpose

**Scope of work:**

- a. Mounting of RCU (02 nos.) in a rack space (9U + 9U)
- b. Laying gas pipe line & water drainage line.
- c. Outdoor unit location will be provided by customer outside room.
- d. Powering the device for indoor as well as outdoor unit along with necessary cable connectivity & insulation material
- e. Installation, refrigerant charging, testing & commission under vendor scope.

**Broad Based Specifications for Forensic Smart Server for  
National Cyber Forensic Laboratory for Evidentiary purpose**

#### **4. Rack & Accessories**

Supply and installation of high density IT Rack with containment, having 42U as standard, complete with keyboard tray, cable manager & blanking panels with basic PDU and rack accessories.

**Rack & Accessories Technical Specification:**

- a. Rack is 42 U 19" mounting type with 2000 (Height) x 800 (Width) x 1000 (Depth).
- b. Rack design is sturdy frame section, corners are stiffened with welded MS die cast.
- c. Rack frame is, scalable and modular with safe load carrying capacity of 1400 Kg on enclosure frame and 1000 Kg on 19" mounting angles.
- d. Base plinth with 100 mm height
- e. Cut outs with rubber grommet on top and bottom plate for cable entry.
- f. Cable entry provision from top & bottom both.
- g. Vertical Cable manager on both LHS & RHS on rear side.
- h. Front Glass door for complete 42U height visibility and rear plane door with stiffener for strength.
- i. Thermally insulated cold aisle chamber.
- j. Blanking panels to prevent air mixing.

#### **5. Monitoring**

Supply and installation of Liebert RDU system which, continuously collects critical information from network connected devices, temperature, humidity, door sensors and other dry contact monitoring. Based on pre-set parameters, automated email alerts are sent to the intended recipients.

**Monitoring Technical Specification:**

- a. Intelligent Rack environment remote monitoring.
- b. Modbus 485 Communications
- c. SNMP Communication.
- d. Single window for monitoring all sensors.
- e. Data and logs of historical information of alarms and notification.
- f. Temperature & Humidity Sensor, with LCD display and RJ45 connector.

**Broad Based Specifications for Forensic Smart Server for  
National Cyber Forensic Laboratory for Evidentiary purpose**

- g. Door opening sensor with RJ 45 connector.
- h. Water leak detection sensor with RJ45 connector.
- i. Smoke detection sensor with RJ45 connector.
- j. Alarm device with LED flash and sound option.

**6. Rack Power Distribution Unit (Socket Strip)**

Supply and installation of vertical rack mount power distribution unit (zero U).

- a. Each rack shall have two vertical PDU's having IEC C13 x 12 nos. C-19 x 04 nos. Sockets with 32 Amp MCB with indicator.

**7. Electrical System (POD Device):**

Supply and installation of electrical distribution system.

- a. 19" rack mountable Power Output Device with essential breakers to be mounted in the rack. Consumes only 3U space of rack height.
- b. Main Incomer- 80 Amp 4 Pole MCB with suitable provision of terminal blocks for connections.
- c. UPS I/P - 2 nos. of 50 Amp SP MCB for UPS Supply.
- d. Cooling I/P - 2 nos. of 16 Amp 4P MCB for Cooling Unit Supply.
- e. Spares -1 no. of 32 Amp MCB for spares.
- f. All input supply cables from POD unit to equipments are connected with industrial socket (male - female) with suitable rating.

**Broad Based Specifications for Forensic Smart Server for  
National Cyber Forensic Laboratory for Evidentiary purpose**

**SERVER AND SERVER SOFTWARE**

S. No.	Components	Description
1	Form factor	The Server should be 2U form factor with platinum efficiency, rack mount.
2	Architecture & processor	The server should be Intel based architecture- Two nos. of x86 64bit processors. The processor should be latest available, reliable series. Each Processor should have 24 cores or higher.
3	Memory	The server should have loaded with 512 GB latest DDR Memory using 32GB DIMMS with scalability option upto 1 TB.
4	Storage - HDD	The server should have loaded with 2 x 400GB SSD drives in RAID1 or higher SSD drives.
5	RAID Controller	The server should have loaded with 12Gb/s SAS Raid Controller supporting RAID 0, 1 & 5 .
6	Network	The server Should have 2 x 1 Gb E embedded LAN on Motherboard for network connectivity
		The server Should have 2 x 10G SFP+ Network Adaptor with necessary transceivers
		The server Should have 2 x 16 Gbps Fibre Channel HBA card with necessary transceivers
7	Ports	The server Should have 1 serial port, 2 USB ports, 1 VGA video port for server connectivity
8	I/O Slots	The server should have minimum 6 PCIe 3.0 slots plus 1 dedicated 12-Gbps RAID controller slot and 1 dedicated mLOM slot
9	Management	The server should have Integrated Remote Management card for monitoring, Server Health logging, out-of-band management, alerting, trouble shooting (via secure web GUI, telnet), Remote virtual media with required license, OS deployment etc.
10	Power supply	The server should have N+N redundant power supply. The power supply modules shall be hot swappable.
11	Cooling Fans	The server should have Redundant hot swappable fully populated cooling fans.
12	Operating System Compatibility, Certification	Certification for latest Server version of Windows and minimum two Linux flavours. The Server should support latest versions of Microsoft Hyper-V, VMWare Vsphere 6.5 or above, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, Microsoft Windows Server 2012 onwards.

**Broad Based Specifications for Forensic Smart Server for  
National Cyber Forensic Laboratory for Evidentiary purpose**

13	Accessories	Rack mount Rail Kits , IEC Power Cord 15A 14AWG C14 to C13, 3-Feet- 2 Numbers and Portable USB DVD Drive for installation
14	Warranty	5 Years on-site comprehensive OEM Warranty with 24 x 7 Support.
15	Other features	Should support Standard Virtualization Software.
16	Drivers / Software utilities	All required device drivers for OS installation, system configuration and server management.



**Broad Based Specifications for Forensic Smart Server for  
National Cyber Forensic Laboratory for Evidentiary purpose**

**SERVER SOFTWARE WITH VIRTUALISATION**

Sl. No.	Components	Description
1	Operating System	Microsoft Windows Server 2019 (Standard) with 24 licenses with virtualization support to create number of virtual machines on the servers.

Sl. No.	Specifications for Access Switch
<b>A</b>	<b>Hardware Feature</b>
1	The switch should have minimum 48 * 10/100/1000T ports with 4 x 1GE SFP ports
2	The switch should support stacking using dedicated stacking ports separate from above mentioned uplink ports with support for minimum 8 switches in a single stack for high availability and quick resiliency
3	The switch should support a stacking bandwidth of minimum 80 Gbps
4	The switch should have 2 GB or more RAM
5	The switch should have 4 GB or more Flash
6	The switch have Forwarding rate of minimum 260 mpps and switching bandwidth of 170 Gbps
7	The switch should have 2 10G MM SFP+ modules.
8	All the SFP module from same OEM
<b>B</b>	<b>Software Feature</b>
1	Should support 1000 VLANs
2	Shall support all the Layer 3 routing protocols like Static route, RIP, OSPF v3 and Policy based routing.
3	Shall support 1000 multicast routes
4	The switch should support 15K MAC address
5	The switch should support total 3K IPv4 routes.
6	The switch should support total 1K IPv6 routes.

**Broad Based Specifications for Forensic Smart Server for  
National Cyber Forensic Laboratory for Evidentiary purpose**

<b>C</b>	<b>Security Feature</b>
1	The switch should have Loop Detection and Loop protection mechanism
2	The switch should support DHCP snooping
3	The switch should support MAC address filtering
4	The switch should support Private VLANs provide security and port isolation
5	The switch should support Strong password security and encryption
6	The switch should support flexible & multiple authentication mechanism, including 802.1X, MAC authentication bypass
7	Shall Support Simplified segmentation and micro-segmentation, with predictable performance and scalability
<b>D</b>	<b>Management Feature</b>
1	The switch should support SNMPv1, v2c and v3
2	The switch should support sFlow/Netflow/Jflow to monitoring traffic in switched and Routed networks
3	The switch should support TFTP , NTP and Syslog
4	Should support Unidirectional Link Detection Protocol (UDLD) that allows detection of unidirectional links caused by incorrect fiber-optic wiring or port faults
5	<b>Warranty, Safety, compliance and support</b>
6	The switch must have ROHS compliant
7	The switch must have UL,EN, IEC compliant
8	The switch should come with 5 year on-site comprehensive OEM warranty with 24 x 7 support and SI should share the support contract certificate.
<b>E</b>	<b>Others</b>
1	Switch should be a current model from the OEM .Bidder should not propose any model for which End of sale/End of support date had been already announced.
2	Proposed switch should be from the same OEM as the access switches proposed
3	The OEM must be in Gartner Magic Quadrant of leaders for Wired and Wireless LAN as on the day of publication of this RFP

**Broad Based Specifications for Forensic Smart Server for  
National Cyber Forensic Laboratory for Evidentiary purpose**

**Firewall**

<b>Sl. No.</b>	<b>Specifications for Firewall</b>
1	The NGFW firewall should be appliance based security platform and should be capable of providing firewall, URL Filtering, application filtering, VPN and IPS functionality
2	The appliance should have minimum 8x1GbE Copper interface.
3	The NGFW firewall should support 1 RJ45 management interface and mini USB console.
4	The NGFW firewall should support minimum 4 GB RAM and 8 GB flash memory from day one.
5	The NGFW firewall should support minimum 50 GB SSD drive for log porpose.
6	The NGFW Firewall should support stateful failover of sessions in Active/Standby
7	The NGFW firewall Should have maximum Firewall throughput of 740 Mbps and FW+AVC+IPS throughput of 120 Mbps and it should include all Protocol.
8	Firewall Should support DES, 3DES/ AES IPsec VPN throughput of minimum 90 Mbps. Should support minimum 7500 Static IPsec VPN.
9	The firewall should support 45K maximum concurrent sessions with Application Visibility and Control
10	Firewall should support minimum 4.5K new connections per second with Application Visibility and Control
11	The firewall should supporting more than 3000 applications, as well as geolocations, users, and websites
12	The firewall should support more then 80 number of URL category
13	The firewall should be SNMP manageable with support for SNMP Version 1, 2 and 3.
14	The firewall should support SSH Version-2 for Command Line Management.

**Broad Based Specifications for Forensic Smart Server for  
National Cyber Forensic Laboratory for Evidentiary purpose**

15	The Firewall OEM must be in Gartner Magic Quadrant of leaders for Enterprise Network Firewalls as on the day of publication of this RFP
16	The NGFW firewall should support 0 to 40 degree temprature
17	The firewall shall conform to UL 60950-1 and EN 60950-1
18	The firewall should come with 5 year on-site comprehensive OEM warranty with 24x7 support and SI should share the support contract certificate.

**Broad Based Specifications for Forensic Smart Server for  
National Cyber Forensic Laboratory for Evidentiary purpose**

S. No.	Specifications for Core Switch
<b>A</b>	<b>Hardware Feature</b>
1	The switch should have minimum 24 number of 1G/10G multigigabit ports. 16 No of 1G and 8 No's of 10G SFP+ to be supplied as per the requirement of the servers specification.
2	The switch should have dual power supply
3	The switch should support 2 * 40G QSFP port for future expansion
4	The total aggregate switching capacity shall be 600 Gbps or more
5	The total forwarding capacity shall be 150 Mpps
6	The switch should have 450 Gbps of stacking bandwidth
7	The switch should have 6 GB or more RAM
8	The switch should have 15 GB or more Flash
<b>B</b>	<b>Software Feature</b>
1	The switch should support total MAC address 32K
2	The switch should support 22K IPv4 routes.
3	The switch should support 15K IPv6 routes.
4	The switch should support 7500 IPv4 multicast routes
5	The switch should support 1000 IPv6 multicast routes
6	The switch should support total 60K netflow entry
7	The switch should support 30 MB or more packet buffer
8	The Switch should support non-blocking Layer 2 switching and Layer 3 routing.
9	Switch should be SNMP manageable with support for SNMP Version 1, 2 and 3.
10	Switch should support console, TELNET and SSH Version-2 for Command Line Management.
11	Jumbo Frames support up to 9K Bytes on 1G/10G Ports
12	Should support port, subnet based 802.1Q VLANs. The switch should support 4000 vlans. The switch must support Private VLAN or equivalent.
13	The switch should support IEEE 802.1d, 802.1w and 802.1Q
14	The switch should support Protocol-Independent Multicast (PIM) for IP multicast routing, including PIM Sparse Mode (PIM SM), bidirectional PIM and Source-Specific Multicast (SSM)

**Broad Based Specifications for Forensic Smart Server for  
National Cyber Forensic Laboratory for Evidentiary purpose**

<b>C</b>	<b>Warranty, Safety, compliance and support</b>
1	The switch shall conform to EN 55022 Class A/B or CISPR24 Class A/B or CE Class A/B or FCC Class A/B Standards for EMC (Electro Magnetic Compatibility) requirements
2	The switch should come with 5 year on-site comprehensive OEM warranty with 24 x 7 support and SI should share the support contract certificate.
<b>D</b>	<b>Others</b>
1	Switch should be a current model from the OEM .Bidder should not propose any model for which End of sale/End of support date had been already announced.
2	Proposed switch should be from the same OEM as the access switches proposed
3	The OEM must be in Gartner Magic Quadrant of leaders for Wired and Wireless LAN as on the day of publication of this RFP

**Broad Based Specifications for Forensic Smart Server for  
National Cyber Forensic Laboratory for Evidentiary purpose**

**Storage system with 200TB usable capacity**

<b>S. No.</b>	<b>Feature</b>	<b>Description</b>
<b>1</b>	<b>Storage Capacity</b>	
1.1	Support	The storage shall support SSD, SAS and SATA/NL SAS based disks simultaneously.
1.2	Capacity	The storage should be provided with 100TB usable capacity on RAID5 with SAS drives & 100TB usable capacity on RAID6 with NL-SAS drives.
1.3	Scalability	The storage should be scalable to at least 192 dual ported disk drives with a combination of Flash/SSD, SAS and NL-SAS drives within the same array
<b>2</b>	<b>Storage Controller</b>	
2.1	Availability	The Storage system must have at least two controllers running in an active-active mode with automatic failover to each other in case of one controller fails for both NAS(CIFS, NFS) and SAN(iSCSI & FCP). The storage array should provide with data consistency and integrity in all circumstances.
2.2	Scalability & Upgrade Options	The proposed system should be field upgradeable to a higher model through data-in-place upgrades.
<b>3</b>	<b>Cache</b>	
3.1	Scalability	Proposed solution should be scalable to 128GB of cache without addition of controllers. Cache shall be on controller and not SSD/PCIe.
3.2	Cache utilization	The storage array Cache should be Global Single Image, Write Mirrored Cache capable of mirroring all writes and keeping a single cached copy of read data thereby eliminating wastage for mirrored reads and optimal utilization of cache resources. OEMs mirroring both read and write should provide additional cache equal to read % considered in for read/write ratio taken for calculation.

**Broad Based Specifications for Forensic Smart Server for  
National Cyber Forensic Laboratory for Evidentiary purpose**

3.3	Feature	The storage array should be able to provide online cache partitioning to ensure dedicated cache resources to critical workloads as opposed to common cache resources across all workloads / application so as to avoid any situation where-in the behaviour of the certain workloads impact the performance of the critical workloads / applications
3.4	Protection	Storage should have ability to protect data in cache in case of controller failures. The cache on the storage should have 72hrs or more battery backup.
<b>4</b>	<b>Protocols</b>	
4.1	Availability	The storage should be configured with FCP, iSCSI, NFS and CIFS protocols for use with different applications. Any hardware/software required for this functionality shall be supplied along with it in No Single Point Of Failure mode.
4.2	Architecture	The proposed Storage system must be of an architecture able to support Block(SAN) without controller upgrade i.e FC protocol and iSCSI
<b>5</b>	<b>RAID</b>	
5.1	Support	The system should support RAID 5, RAID1+0/RAID6 or equivalent RAID technologies.
5.2	Diversity	Multiple RAID configurations to be configured in the proposed solution. RAID implementation should be hardware based and optimized for writes.
5.3	Scalability	The proposed storage system must allow creation of LUN/Volume across a pool that spans across 3 Tiers or Disk/RAID and be automatically optimized through SUB-LUN tiering.
<b>6</b>	<b>Interface</b>	
6.1	Provisioning	Proposed Storage should be configured with minimum 4 numbers of 10Gbps Ports and 4 numbers of 16Gbps FC ports.
6.2	Scalability	Ports should be scalable to 8 nos of 16Gbps FC & 8 nos of 10Gbps iSCSI.



**Broad Based Specifications for Forensic Smart Server for  
National Cyber Forensic Laboratory for Evidentiary purpose**

6.3	Back end	Proposed Storage should be configured with 12Gbps backend SAS Links.
7	<b>Storage Functionality</b>	
7.1	Features	The storage shall have the ability to expand LUNS/Volumes on the storage online and instantly.
7.2		The storage shall have the ability to create logical volumes without physical capacity being available or in other words system should allow over-provisioning of the capacity. The license required for the same shall be supplied for the maximum supported capacity of the offered storage model.
7.3		The storage should be configured with Quality of Service feature. Should have capability to define IOPS and MB/s per volume/LUN.
7.4	Data Protection and Security	System should have redundant hot swappable components like controllers, disks, power supplies, fans etc.
7.5		The LUN security & masking software to be provided to protect LUNs configured to Heterogeneous OS Hosts connected on the same FC ports.
7.6		The storage array should be able to support hardware based non-invasive, media agnostic data encryption executed at the Storage back-end controller level / in disk level with no performance impact on the storage.
7.7		The storage should have the requisite licenses to create point-in-time snapshots. The storage should support minimum 1024 snapshots per volume/LUN. The license proposed should be for the complete supported capacity of the system.
7.8		Storage should have licenses to create full clones and space efficient clones.
7.9		Storage should have licenses to vault the snapshots to next tier in the same storage or to a different storage (secondary storage).
7.10		Proposed Storage Array should have capability to create point in time volume copies for a production volume across external storage (SAN Attached third party storages) using storage virtualization.

**Broad Based Specifications for Forensic Smart Server for  
National Cyber Forensic Laboratory for Evidentiary purpose**

7.11	Provisioning and Data Tiering	Offered Storage array shall provide heterogeneous storage virtualization either natively or using external appliances for vendors like, but not limited to, EMC, HP, IBM, Hitachi, Netapp etc. The necessary hardware and software should be quoted for entire proposed capacity.
7.12		The storage shall support logical partitioning of controllers, such that each partition appears as a separate storage in itself.
7.13		The storage array should support Dynamic & Automatic Data Tiering capability to Dynamically move highly accessed data using either Policy based tiering or automated tiering to Fastest Disk tier in order to Enhance data performance without any interruptions to the business applications.
7.14		Proposed Storage should have capability to leverage external storage (SAN Attached third party storages) to be consumed as 3rd tier in dynamically tiered storage pool.
7.15	Disaster Recovery Support	The solution shall support replication on it for the full supported capacity of the system for both SAN and NAS data.
7.16		The solution shall support replication in cascade, one to many and many-to-one mode.
7.17		The replication solution on storage shall support failover to BCP/DR storage and failback as and when required.
7.18		The array should support Replication topologies using a Synchronous and/or Asynchronous Storage replication.
7.19		Storage family should have native support for Active-Active sites across primary and near line storages to achieve Zero RTO.
7.2	Management	The Storage Management Software shall be GUI based and shall be able to discover and monitor storage system. It shall provide pro-active intelligence by monitoring performance of Storage Infrastructure.

**Broad Based Specifications for Forensic Smart Server for  
National Cyber Forensic Laboratory for Evidentiary purpose**

7.21		Storage should have performance monitoring software which is an automated, intelligent and path-aware storage resource management tool that maps, monitors, analyzes and measures storage network resources and performance from the application to the device. By monitoring all storage network resources, including hosts, file systems, databases, SAN switches and storage systems, performance monitoring software should provide the necessary visibility for complete performance management of the entire storage environment including replication setup.
7.22		Storage should have the logical partitioning of ports, cache and disk (parity groups) into independently managed virtual machines. The virtual private storage machine would be an allocation of specific ports, cache and disks or parity groups within a partition. Storage should have facility to administer individual partition and that administrator would then be able to use any of the storage management tools and business continuity software within his or her partition, but only to be able to impact the storage and resources within that partition. These partitions can be allocated dynamically to utilize resources based on changes in business requirements.
7.23		Should be provided with Easy to use GUI based and web enabled administration interface for configuration, storage management and current and historic performance analysis
7.24	Investment Protection	Should be able to visualize, use external storage capacity as an internal tier to proposed storage thereby improving greater scalability and protect existing investment.
7.25	OS support	Support for industry-leading Operating System platforms including: LINUX , Microsoft Windows, HP-UX, SUN Solaris, IBM-AIX, etc. It shall support connecting hosts over iSCSI and shall be supplied with any Multipathing software if required with the solution.
7.26	Secure Multi tenancy	Storage to support multiple domain consolidation into a single box

**Broad Based Specifications for Forensic Smart Server for  
National Cyber Forensic Laboratory for Evidentiary purpose**

7.27	Warranty & SLA	The Hardware and software quoted should have 5 years onsite comprehensive OEM warranty with 24X7 support alongwith upgrade and updates. Support with proactive care
7.28	Storage Evaluation	Storage must be in Leaders quadrant of gartner (general purpose Disk arrays) atleast for 2 years
7.3	Resilience	High Availability with Active-Active controller Design, Industry standard RAID 5 & RAID 6 support for protection, Hot Swappable components, Non-Disruptive Upgrades for Capacity, interface and Performance, support for multi-site data replication (in future), Support for resource partitioning/multi tenancy, Cache with battery backup and de-stage protection, Native proactive system components failure identification and alert, Performance monitoring with trend analysis.
7.31	Data Services	Support for Thin Provisioning, Space Efficient Snaps and Clones, Pattern Removal/page reclamation, Always on Encryption with no performance impact, Native QoS and SLA configuration with monitoring,
7.32	Cables	should be supplied with number of fibre channel cables as per the requirement to connect to the servers
8	<b>Certification</b>	
8.1	Certification	Proposed storage has to be certified by Indian Agencies for standardization (like BIS etc)

**Broad Based Specifications for Forensic Smart Server for  
National Cyber Forensic Laboratory for Evidentiary purpose**

**BACKUP SOFTWARE**

S. No.	Description
	<b>Backup software with capacity based license.</b>
1	Backup Software Solution must have Wizard-driven configuration and modifications for backup, restoration and devices.
2	The Solution should bring the power and flexibility you need to ensure Availability for all your physical and virtual servers
3	Solution should comply with Application-aware processing
4	Solution should comply with File indexing and search capabilities
5	Solution should comply with Instant Recovery of virtual machines, files and folders
6	Solution shall have in-built frequency and calendar-based scheduling system.
7	Solution should comply with Server-specific scheduling and retention
8	Should have in-built calendar based scheduling system and also support check-point restart able backups for file systems. It should support various level of backups including full, incremental, differential, synthetic and virtual synthetic backups
9	Solution should comply Transaction log backup for databases

**Broad Based Specifications for Forensic Smart Server for  
National Cyber Forensic Laboratory for Evidentiary purpose**

10	Solution should comply with changed data blocks since the last backup cycle for Incremental backups.
11	Solution should support Source-side encryption
12	Solution should provide recovery from physical servers, Virtual and image level recovery.
13	Solution should let you restore items and objects from the following applications: Microsoft Active Directory, Microsoft Exchange, Microsoft SQL Server & Oracle.
14	Solution should provide backup agent software with licenses.
15	Warranty: 5 Years on-site comprehensive OEM Warranty with 24 x 7 Support.

**Broad Based Specifications for Forensic Smart Server for  
National Cyber Forensic Laboratory for Evidentiary purpose**

**TAPE LIBRARY**

<b>Specifications for Tape Library</b>		
1	Tape library	1 No of LTO 7 Tape Library with minimum 3 drives and extra 3 drives for future scalability.
2	Capacity	<ol style="list-style-type: none"> <li>1. Shall support Native data capacity of 140TB (uncompressed) expandable to 350TB (2.5:1compressed) using LTO-7 technology or better</li> <li>2. Shall be offered with LTO-7 FC tape drive and minimum of 24 cartridge slots or more. Shall support encryption.</li> <li>3. Should populate minimum of 200 TB usable Data Cartridge</li> </ol>
3	Tape Drive Architecture	<ol style="list-style-type: none"> <li>1. Offered LTO-7 drive in the Library shall conform to the Data rate matching technique for higher reliability</li> <li>2. Tape Drive Architecture in the Library shall conform to the INCITS/T10 SCSI-3 standard or newer standards.</li> </ol>
4	Speed	Offered LTO-7 drive shall support 300MB/sec in Native mode.
6	Encryption device	Offered Library shall be provided with a hardware device like USB key, separate appliance etc. to keep all the encrypted keys in a redundant fashion.
7	Connectivity	Offered Tape Library shall provide 16/ 8 Gbps native FC connectivity to switches.
8	Management	Tape Library shall provide web based remote management.
9	Barcode Reader and Mail slots	Tape library shall support Barcode reader and mail slot.
10	Other Features	<ol style="list-style-type: none"> <li>1. Tape Library shall have GUI Panel</li> <li>2. Shall be rack mountable</li> <li>3. Tape Library shall be supplied with software which can predict and prevent failures through early warning and shall also suggest the required service action</li> <li>4. Offered Software shall also have the capability to determine when to retire the tape cartridges and what compression ratio is being achieved</li> </ol>
11	Warranty	5 years on-site comprehensive OEM warranty with 24x7 support.

**Broad Based Specifications for Digital Forensic Platform for  
National Cyber Forensic Laboratory for Evidentiary purpose**

S. No.	Name of the Tool	Specifications
1.	The integrated Forensic Platform for sharing the Digital Forensic tools with suitable APIs.	<ul style="list-style-type: none"> <li>• Integrated platform that enables centralized case management and web-based access to various digital forensic tools.</li> <li>• Interface to distribute processing support, Role Assignment, Password Cracking and Recovery, Wizard-Driven Multi-Machine, Customizable Processing.</li> <li>• Integrated Simultaneous access through centralised management console via web interface.</li> <li>• Automate email notifications regarding case state.</li> <li>• Should integrate the following tools not limited, to provide tool accessibility remotely               <ol style="list-style-type: none"> <li>1. Software for the image mounting, password cracking and forensic analysis of Digital Media.</li> <li>2. Tool for acquisition of Data from HDDs, Smart Phones, Cloud and VSCs and automated processing and analysis of data specific criteria to internet and social media artefacts.</li> <li>3. MAC Forensic Toolkit.</li> <li>4. Tool for digital evidence processing and analysis.</li> <li>5. Digital Forensic Triage Tool Kit</li> <li>6. Solution for Mobile Phone Forensics and Photo recogniser.</li> <li>7. Automated Malware Analysis tool.</li> </ol> </li> <li>• The solution should be deployed/operated on the in house server at CFSL, Hyderabad. The required server hardware and software components for the Integrated API are the responsibility of the solution provider.</li> <li>• The platform should be flexible enough to accommodate more number digital forensic tools and licences as per the need in future.</li> <li>• The solution should have a web user interface for the seamless and smooth management of the users as well as tools</li> <li>• The solution should have the required open APIs to integrate the above digital forensic tools and make them available via LAN and WAN.</li> </ul>



		<ul style="list-style-type: none"> <li>• Perpetual Licensing for the platform including the forensic tools with 01 year warranty with Service Maintenance Support (SMS) for updates/upgrades up to 02 years after expiry of warranty.</li> <li>• Desirable: <ul style="list-style-type: none"> <li>○ Solution should include certified training for 03 Experts from OEM with in India or at OEM location.</li> </ul> </li> </ul>
<p>NOTE:</p> <ol style="list-style-type: none"> <li>1. The generalised specification for the tools mentioned at 1, 2, 3, 4 are given at S/N. 7, 3, 8 and 4 respectively of Annexure – B</li> <li>2. The generalised specification for the tool mentioned at 5 is given at S/N. 2 of Annexure – A</li> <li>3. The generalised specification for the tool mentioned at 6 is given at S/N. 3 of Annexure – C</li> </ol>		