ANNEXURE - A

1- Network Monitoring and Device Tracking Solutions

S. No.	Name of Hardware/Software	Product Specifications
01	Network Monitoring and Device Tracking Solutions	• Should be a good search engine for Internet-connected devices. • Should be able to keep track of all your devices that are directly accessible from the Internet. • Should provide up to 20 million results per month • Should scan up to 65,536 IPs per month • Should provide Network Monitoring for 65,536 IPs • Should provide Access to most filters • Should allow paging through search results • Should provide basic access to the Streaming API • Tool should be used for commercial Use • Product should be used through CLI and the website • Should be able to see what you currently have connected to the Internet within your network range • Should be able to set up with real-time notifications when something unexpected shows up. • Should be able to Discover Trends on the Internet • Should provide Private firehose feature • Should provide IP lookups and batch IP lookups

2- Digital Data Extraction and Analysis Software

S. No.	Name of Hardware/Software	Product Specifications
01	Digital Data Extraction and Analysis Software	• An adaptable platform designed for thorough data extraction and analysis, accommodating a diverse range of sources such as real-time data acquisition, memory analysis, computers, cloud resources, mobile devices, and vehicle data. • Customized workflows tailored for Windows, MacOS, and Linux environments, ensuring seamless integration and efficient performance across different operating systems. • Capable of retrieving data from Android devices and performing logical acquisition from iOS devices, Windows phones, MTP devices, SIM cards, and Kindles. • Compatibility extends to popular Linux distributions such as Ubuntu, Debian, Red Hat, Kali, and more, catering to a wide array of systems. • Enables data export in the .ivo file format, empowering users to consolidate vehicle forensic data with other sources within a single case, streamlining the analysis of waypoints, routes, velocity logs, contacts, call logs, attached devices, and more. • Additionally provides support for various file systems, including YAFFS2, NTFS, HFS+, HFSX, EXT2, EXT3, EXT4, FAT32, and EXFAT.Targeted image for Windows includes Event Logs, Windows Registry Hives, Pagefile, Hibernation File, Master File Table, , USN Journal, , Setup API Logs, , LNK Files, User Profiles, Prefetch Files. • It must possess the capability to facilitate the capture of Physical Memory (RAM Dump), enabling the examination of crucial artifacts often exclusively contained in memory. • The tool should include the functionality to capture memory from individual running processes. This

		feature becomes invaluable when time constraints exist or specific processes are of particular interest, as it permits focused retrieval, reducing data fragmentation and improving the recovery of larger data types. • The platform should offer both GUI and Command Line options for memory acquisition, ensuring minimal disruption to the suspect system. • A command-line utility should be provided for swift and non-intrusive inspection of suspect computer systems to detect encrypted volumes during incident response.Ability to analyze data from forensic image file formats i.e. E01, Ex01, L01, Lx01,.AFF .AD1, .DD, .RAW, .BIN, .IMG, .DMG, .FLP, .VFD, .BIF, .VMDK, .VHD, .VDI, .XVA, .ZIP, .TAR. • Ability to analyse memory dumps in the format of .RAW, .CR*ASH*, .VMSS, .HPAK, .ELF, .MEM, .DMP, .DD, .IMG, .IMA, .VFD, .FLP etc. • Support Full Drive Decryption, with the integrated capability, can detect and decrypt TrueCrypt, BitLocker, McAfee, VeraCrypt and FileValut2 with known password or using brutal force attack. • Should have a utility for determining and retrieving user passwords based on keywords from a case file significantly reducing the time involved in trying to brute-force this password manually • Multiple Device Queueing – Automatically process multiple devices in a row without the need for examiner-run separate process. • Filter stacking allows you to layer on several dimensions of filter criteria to pinpoint specific items in a large dataset. • Ability to view SQLite database files using built-in SQLite viewer • Should support OCR support for extraction of text from PDF documents (including text in scanned documents and text from pictures in PDF documents) and from picture artifacts for Keyword Searching.

		• Should support search for keywords on both recovered artifact and sector level content both prior to processing the case as well as after processing the complete case with an option to select all added evidence sources or any particular evidence source. • Should allow users to tag or exclude artifact evidence from case data during processing based on a keyword list. case examiner should be able to load the list of keywords and choose to either tag or exclude artifacts containing those keywords. This can be helpful where a manual review process is utilized to remove the content, or in scenarios where it must automatically be excluded. • Recovers more artifacts from both allocated and unallocated space by extracting data from full files or carving for deleted data and traces of data elements/fragments left behind by apps and websites, presenting it in an organized and easy to read format. • Ability to identify luring and sexual conversations. 15+ AI Categories to automatically identify and bifurcate images related to drugs, weapons, nudity, weapons, militants, vehicles, screen captures, documents, ID Cards, Human Faces, License Plates, Building, Child Abuse, Tattoos, Invoices, etc • identify and categorize handwritten documents automatically with AI. • support CSAM investigations with AI technology, and help you uncover key evidence even more quickly Including new AI technology from Thorn to identify illicit content leveraging their CSAM Image Classifier to improve the detection of CSAM across picture and video artifacts. • • Inbuilt Support for finding similar pictures by building picture comparison for identifying any similar pictures from the extracted images or external images using CBIR (Content Based Image Retrieval) feature

		• Should have advance option to analyse media file using dedicated Media explorer to view, sort, and filter media evidence using criteria that are specific to pictures and videos. The Media explorer should stacks copies of the same picture or video that were found in different source locations. • ability to hover over image/video, which should provide a larger, higher resolution preview of the image or video. Users can also zoom and pan around an image within the preview. For videos, investigator should be able to use the mouse to quickly scroll through the contents of the video. • Should allow investigator to filter media files by Investigation leads, including attributes such as camera serial numbers, Exif created dates, camera make & model, Items with Geolocation data, Deleted source, items matching social media platforms, Lens model & Serial Number, file extension, VICS attributes, media attributes, video attributes, and file attributes. The date / time filter is also available in the Filters bar. • Should allow investigator to Sort by option to organize the evidence in ascending or descending order based on attributes such as skin tone, media size. • Should allow investigator to filter video files with attributes such as video files within carving limit, media duration etc • Should have utility which can be installed on any number of Windows Tablet or Laptop to empower frontline officers to collect and report on fleeting digital evidence. The tool should be capable to Maintain privacy and build trust with the public while capturing crucial but fleeting digital evidence from consenting victims and witnesses. • Quickly get Photo, video evidence with an external or internal camera or by connecting to the victim or witness’s mobile phone, or memory card. • Support case dashboard that displays high level details about the case, evidence sources and summaries of

		processed results of multiple digital evidence in one screen. • **Visualize connections between files, users, and devices.** Discover the full history of a file or artifact to build case and prove intent. visualizes evidence from disk and memory to show where files came from, who they are connected to, and where they're stored. • Should support pre-processing date filters which gives investigators the option of setting a date and time range for the artifacts that will be added to a case. This feature allows to limit the artifact data being collected in order to comply with warrant restrictions around the applicable dates for the investigation. • Should support parse and carve and parse selected artifact option to save time on a case if carving is not necessary for investigation. • Should have Timeline explorer to consolidate all the timestamps from files and artifacts in a single view, with colours and tags to differentiate timestamp categorizes. • Ability to automatically find potential chat databases along with other valuable evidence from non-chat apps that aren't yet supported in an artifact. users can then easily create an XML or Python artifact to be searched for in future cases. • Capability for parsing unsupported database using custom artifacts or Python Scripts for popular local applications like Tally, Airbnb, ccleaner, FakeGPS, Linkedin, onion browser bookmarks etc. • Should have a GUI/Wizard-driven utility, so no coding experience required to build custom artifacts CSV/Delimited files (tab-separated, space-separated, or custom delimiters) and SQLite databases to bring data into the offered tool from other sources without needing to know XML/Python or API. • Should have a platform that allows forensics professionals access to repository of Custom artifacts and option to upload custom scripts that they have

		built, and help their peers with their cases, or download artifacts others have built to help with their own cases. • Add hash sets to either filter out non-relevant files to enhance search performance and reduce false positives or add hash sets that will specifically call out and identify known bad pictures and videos. • Enhanced searching, sorting and filtering – search, sort and filter artifact data for relevant keywords, time/date stamps, tags or comments, or layer filter criteria to pinpoint items in a powerful and intuitive, but natural interface. Support filter stacking for multiple filters. • Should capture web pages as they are at a specific point in time for situations where the web pages need to be displayed in an environment where Internet access is not available (such as a court room). • Support multiple data views, including Column/Table view, Summary Row view, World Map view, Timeline view, Chat Threading view and Histogram view. • Support to export & merge portable case and share with other stakeholders without the need for the software license or the need to install the software, the user can select different types of items to be included according to tags, comments and categories. • Should support a fast and intuitive option to create custom digital forensic reports, combining forensic data from case files and all other external data sources using versatile word processing tools to quickly build comprehensive reports for a range of audiences. • The custom report feature should have an intuitive drag-and-drop functionality to let the examiner place artifact details directly into report, maintaining the forensic integrity of the data while integrating elements like visual previews for media-based artifacts and evidence device summary details to provide stakeholders with straightforward and efficient reports. • Should have a feature to reduce overexposure to illicit/ disturbing content extracted to protect improve investigator wellness. This f**e**atures should be

		configurable and optional, allowing examiners to work the way that they want. Blur or block media thumbnails, Mute audio on videos, Set timer reminders to take breaks or alerts to stop grading,View grading progress and set goals for amount of media graded • Should support Dark mode to help investigators work long hours staring at the screen. • Should be capable to acquire evidence from the cloud, by sign in to an account with the target's user name and password, or—for some platforms—an authentication token that the tool discovers during a search or creates itself. • Should support cloud based Data acquisition from popular Cloud services, including iCloud,MS Office365, POP/IMAP emails, Facebook, Twitter, Google, Slack, Instagram, Box, Dropbox, Microsoft Teams, Uber, Lyft, Mega etc. • Should have ability to acquire public data from Twitter and Instagram without knowing the targeted user’s credential. • Should Support ingesting the downloaded user data package from Facebook, Google and Slack. • Should Support analysis of warrant return from Google, Facebook, Instagram, Snapshot and iCloud. • Should have option to save cloud acquisitions to AFF4-L containers. • The platform offers a preprogrammed, plug-and-play turnkey solution incorporating unique technology, including Neula, which empowers non-technical stakeholders to use it confidently. Its ultra-simple approach prioritizes user-friendliness. • The platform supports investigators in detecting various illicit content, including CSAM, cryptocurrency, dark web applications, and anti-forensic software, among others, on Windows and Mac computers, external drives, unlocked Android and IOS devices. • Investigators can swiftly assess potential evidence sources using the platform, allowing for efficient

		prioritization of investigations. By default, it can scan a 500 GB drive in under 5 minutes. • The platform enables non-intrusive consent based triage of Mac and Windows computers, external drives, Android and IOS devices , allowing investigators to identify and prioritize potentially relevant evidence sources.. • The platform can quickly detect encrypted volumes, such as TrueCrypt, PGP®, VeraCrypt, SafeBoot, or Bitlocker® encrypted volumes. • The capability to extract the recovery key for mounted BitLocker drives within 10 seconds of scanning should be available, which would enable investigators to bypass the creation of images at the crime scene and save a significant amount of time. • Allow investigators to create predefined templates to guide non-technical users in scanning evidence.