FUNDACIÓN INTERNACIONAL Y PARA IBEROAMÉRICA DE ADMINISTRACIÓN Y POLÍTICAS PÚBLICAS

TECHNICAL SPECIFICATIONS DOCUMENT FOR A MIXED CONTRACT IN LOTS, FOR THE SUPPLY, ON A PURCHASE BASIS, OF HARDWARE AND SOFTWARE EQUIPMENT FOR FORENSIC SOLUTIONS, AND THE PROVISION OF INSTALLATION, CONFIGURATION AND TRAINING SERVICES IN THE FRAMEWORK OF THE EUROPEAN COMMISSION PROJECT "ACT - ADVANCE COUNTER TERRORISM FOR LEBANON SECURITY PROJECT".

File Number: SPD-2023-045

Title: TECHNICAL SPECIFICATIONS DOCUMENT FOR A MIXED CONTRACT IN LOTS, FOR THE SUPPLY, ON A PURCHASE BASIS, OF HARDWARE AND SOFTWARE EQUIPMENT FOR FORENSIC SOLUTIONS, AND THE PROVISION OF INSTALLATION, CONFIGURATION AND TRAINING SERVICES IN THE FRAMEWORK OF THE EUROPEAN COMMISSION PROJECT "ACT - ADVANCE COUNTER TERRORISM FOR LEBANON SECURITY PROJECT".

Processing: RESTRICTED

Procedure treatment: ORDINARY

1. BACKGROUND

FIIAPP F.S.P. is a non-profit state public sector foundation whose activities, characterised by the pursuit of the general interest, fall within the framework of international cooperation aimed at modernising institutions, reforming Public Administrations, and strengthening democratic governance.

A continuous dialogue between the European Union and Lebanon has been focusing, for several years, on security and counterterrorism. Aligned with the European Neighbourhood Policy and the European Union Global Strategy on Foreign and Security Policy, an agreed roadmap addresses the areas of counterterrorism, justice and law enforcement, countering terrorism financing and violent extremism, among others. In this context, the project "ACT - Advance Counter Terrorism for Lebanon security" is implemented by the European Consortium led by FIIAPP with the collaboration of CIVIPOL and the Carabinieri.

The project aims at contributing to improved citizens security against terrorism based on rule of law and human rights. Three specific objectives are pursued:

SO 1: Improved national response against terrorism in line with international standards
SO 2: Improved cyber-security and protection and response against cyber-terrorism
SO 3: Improved application of rights-based approach to Counter Terrorism (CT)/ Violent Extremism (VE) cases by law enforcement officials and Courts.

In the framework of the second component, a refined assessment of Lebanese Law Enforcement Agencies' (LEAs) needs in digital forensic equipment has been carried out in November 2022, following a preliminary assessment conducted in October 2021. The revision has led to identify the minimal and top priority needs of digital forensic investigations based on several criteria including laboratory status, its workload, its efficiency, its contribution to the Lebanese judicial authorities and the number of operational qualified experts. This equipment needs to be available for the Lebanese digital forensic experts for each of the four LEAs (Lebanese Armed Forces, Internal Security Forces, General Security Forces, State Security Forces) as soon as possible to upgrade their current digital investigation capabilities and to become sufficiently functional to benefit from further training that the project intends to provide in the fight against terrorism and organised crime.

2. CONTRACT SUBJECT

The subject of the mixed contract in lots, is the supply, on a purchase basis, of hardware and software equipment for forensic solutions, and the provision of installation, configuration, and training service in the framework of the European commission project "ACT - Advance counter terrorism for Lebanon security project".

The contractual purpose is then the procurement of digital forensic solutions for the various digital forensic laboratories of the **end users**: the Lebanese LEAs (Lebanese Armed Forces - LAF, Internal Security Forces – ISF, General Directorate of General Security - GDGS, General Directorate of State Security – GDSS) as detailed in this document and annexes.

These digital forensic solutions should allow the lawful (e.g. Lebanese law 81) acquisition, analysis and examination of digital evidence (computers, mobile phones and other digital devices) without compromising the chain of custody and the integrity of collected digital evidence. Such investigation activities may be performed:

- Using special-purpose IT hardware and software tools for logs collection, acquisition of data, imaging of data, examination of digital evidence, analysis of digital evidence, correlation of digital evidence, presentation of digital evidence, preservation, and lawful archiving of digital evidence;
- Using Laboratory Equipment for the recovery of data from defective / broken / destroyed devices.

The requested Digital Forensic equipment fall under these lots and categories:

- **Lot 1: Digital Forensic IT Hardware** (Digital Storage Solutions - for Digital Evidence data, Digital Forensic Workstations and Laptops);
- **Lot 2: Digital Forensic Hardware Tools** (Data Recovery Hardware tools, Chip tools)
- **Lot 3: Digital Forensic Software Tools** (Data Recovery Software tools, Smartphone Forensic Investigation Software tools, Computer Forensic Investigation Software tools, Computer Forensic Investigation Software - Password Recovery Kit) and **Training** (Training on Smartphone Forensic Investigation Software, Training on Computer Forensic Investigation Software)

Lot #	Category	Sub-category
1	1.1 Digital Forensic IT Hardware	1.1.1. Digital Storage Solutions - for Digital Evidence data 1.1.2 Digital Forensic Workstations and Laptops
2	2.1 Digital Forensic Hardware Tools	2.1.1 Data Recovery Hardware tools 2.1.2 Chip tools
3	3.1 Digital Forensic Software Tools 3.2 Training	3.1.1 Data Recovery Software tools 3.1.2 Smartphone Forensic Investigation Software tools

Lot #	Category	Sub-category
		3.1.3 Computer Forensic Investigation Software tools 3.1.4 Computer Forensic Investigation Software - Password Recovery Kit 3.2.1 Training on Smartphone Forensic Investigation Software 3.2.2 Training on Computer Forensic Investigation Software

3. DESCRIPTION OF THE EQUIPMENT AND SERVICES TO BE PROVIDED

The supplies and services to be procured, and complementary related information, are detailed in Annexes 1,2, 3 and 4. The place of delivery shall be the sites of the various end users (Lebanese LEAs) in and around Beirut, Lebanon. They must comply with the following:
- Bids shall include all technical specifications detailed for each item and complete the details asked for each element in the annexes below, as well as the documents indicated below, such as the training plan and the initial draft project management plan.
- All supplies must have the warranty specified in the annexes, subject to extension as an award criterion.
- The supplies must be in full compliance with the European Commission's regulations, in relation to the products requested.
- Transport to the place of delivery is included in the price of the supplies. The contractor assumes all risk of deterioration, loss, or misplacement until delivery in accordance with the specifications in the annexes below.

Goods manufactured in a country shall be excluded if as a matter of Lebanese law or official local regulation, the Lebanese Government prohibits commercial relations with that Country.

Explanatory note on the training required:
There are two types of training required:
- Basic digital forensic hardware training that is directly associated with the delivery of equipment/hardware and your installation of the equipment (not a specific item delivery). This type of training is the one included in Lot 1 for the digital forensics workstation/laptop course;
- Advanced and specific training for digital forensic software: These are specific training sessions the days following the delivery, this is the type of training included in lot 3 and these are specific items to be delivered.

The bidder shall comply with the following Digital Forensic Solutions requirements:

- **Export license requirements**: The bidder must obtain any export licenses required for the delivery of the requested solutions to the end-users as listed in the present document.
- **Bill of quantity**: The bidder must submit a completed bill of quantity in line with the template provided in the present document. The country of origin of all items/items will be included in the submitted bill of quantity.
- **Software Licenses**: All the procured software must include appropriate number of genuine licenses (wherever applicable) under the name of beneficiary end-users.
- **Evidence integrity**: The solutions shall allow the collection of evidence in a manner that protects chain of custody. The solutions shall allow the collection of digital evidence in a manner that shows impartiality and consistency of investigations.

The bidder's responsibilities shall include:

- Project planning and management;
- Installation planning and preparation;
- Delivery, installation and configuration;
- User training;
- System testing and transition to operations;
- Warranty, support and maintenance services.

The bidder therefore:

- should be a trusted specialised Digital Forensic Solution provider or System Integrator (SI), or a representative of such a company.
- shall have the capabilities to offer all required services regarding the submitted items: delivery, installation, and configuration.
- shall have the capabilities to offer sustainable after sales services covering warranty, support and maintenance.
- shall have the capabilities to offer training and a full transfer of know-how on for the proposed solutions.

4. ANNEXES

ANNEX 1 – REQUIREMENTS AND TECHNICAL SPECIFICATIONS

LOT 1: DIGITAL FORENSIC IT HARDWARE (DIGITAL STORAGE SOLUTIONS - FOR DIGITAL EVIDENCE DATA, DIGITAL FORENSIC WORKSTATIONS AND LAPTOPS)

DIGITAL FORENSIC SOLUTIONS

Network Attached Storage: NAS – Configuration A

The requested "NAS – Configuration A" shall comply with the following requirements:

NAS – Configuration A requirements		
Requirement #	**Category**	**Description**
NAS-A.1	Make & Model	<< to be specified by bidder>>
NAS-A.2	Form Factor	Rack mountable
NAS-A.3	Processor	Intel Xeon E-2236 6-core/12-thread 3.4 GHz or better
NAS-A.4	Memory	128 GB DDR4
NAS-A.5	Flash memory	2 x 1TB SSD (Dual boot OS protection)
NAS-A.6	Operating System	<< to be specified by bidder>>
NAS-A.7	Drive compatibility	- 3.5-inch SATA 6Gbps/3Gbps hard disk drives - 2.5-inch SATA 6Gbps/3Gbps hard disk drives - 2.5-inch SATA SSD (Solid State Drives)
NAS-A.8	Hot swappable	Yes
NAS-A.9	SSD Cache Acceleration Support	Yes
NAS-A.10	RAID	RAID 50/60
NAS-A.11	Storage capacity	72 x 16TB Hard Disk Drive 512e/4Kn SATA 6Gb/s Enterprise
NAS-A.12	SATA	6 Gb/s
NAS-A.13	Storage Controller	- 1 x Quad M.2 PCIe SSD expansion card (supports up to four M.2 2280 formfactor M.2 PCIe (Gen3 x4) SSDs); - PCIe Gen3 x 8 host interface - 6 Gb/s SATA
NAS-A.14	Expansion enclosures	- Form factor: rackmount; - Quantity: as required to accommodate the required number of HDD;

NAS – Configuration A requirements		
Requirement #	**Category**	**Description**
		- Drive compatibility: 2.5"/3.5" SAS 12Gbps & SAS/SATA 6Gbps drives; - 4 x SFF-8644 Mini-SAS HD ports or equivalent - PSU: redundant;
NAS-A.15	Storage Expansion cards	- Quantity: as required to accommodate the required number of expansion enclosures - Interface: dual port SAS 12Gb/s or equivalent
NAS-A.16	10 Gigabit Ethernet Port	2 x 10GbE SFP+ SmartNIC port
NAS-A.17	Gigabit Ethernet Port (RJ45)	2 x 10GBase-T port Gigabit Ethernet Port: 4 x Gigabit RJ-45 Ethernet port.
NAS-A.18	SFP + Optical Module for 10GBASE-SR	Two pairs are required.
NAS-A.19	USB 3.2 Gen 2 (10Gbps) Port	2 x USB 3.2 Gen 2 10Gbps or better
NAS-A.20	I/O ports	- USB / RJ45 - Optional: VGA or HDMI
NAS-A.21	System Monitoring	- Monitors temperature for CPU and memory - Monitors Voltage for CPU, memory, chipset and power supply - Over-temperature warning indicator - Fan and PSU fail LED indicator
NAS-A.22	Server Management	- IPMI 2.0 compliant - iKVM feature
NAS-A.23	Real Time Replication	Required
NAS-A.24	Power Supply	Redundancy 1+1; Voltage: 200-240VAC; Frequency: 50Hz-60Hz
NAS-A.25	Regulation and compliance	CE; RoHS 6/6 Compliant
NAS-A.26	Support and Warranty	5-years support and warranty

Network Attached Storage: NAS – Configuration B

The requested "NAS – Configuration B" shall comply with the following requirements:

NAS – Configuration B requirements		
Requirement #	**Category**	**Description**
NAS-B.1	Make & Model	<< to be specified by bidder>>
NAS-B.2	Form Factor	Rack mountable
NAS-B.3	Processor	Intel Xeon E-2236 6-core/12-thread 3.4 GHz or better
NAS-B.4	Memory	128 GB DDR4
NAS-B.5	Flash memory	2 x 1TB SSD (Dual boot OS protection)
NAS-B.6	Operating System	<< to be specified by bidder>>
NAS-B.7	Drive compatibility	- 3.5-inch SATA 6Gbps/3Gbps hard disk drives - 2.5-inch SATA 6Gbps/3Gbps hard disk drives - 2.5-inch SATA SSD (Solid State Drives)
NAS-B.8	Hot swappable	Yes
NAS-B.9	SSD Cache Acceleration Support	Yes
NAS-B.10	RAID	RAID 50/60
NAS-B.11	Storage capacity	56 x 16TB Hard Disk Drive 512e/4Kn SATA 6Gb/s Enterprise
NAS-B.12	SATA	6 Gb/s
NAS-B.13	Storage Controller	- Quad M.2 PCIe SSD expansion card (supports up to four M.2 2280 formfactor M.2 PCIe (Gen3 x4) SSDs); - PCIe Gen3 x 8 host interface - 6 Gb/s SATA
NAS-B.14	Expansion enclosures	- Form factor: rackmount; - Quantity: as required to accommodate the required number of HDD; - Drive compatibility: 2.5"/3.5" SAS 12Gbps & SAS/SATA 6Gbps drives; - 4 x SFF-8644 Mini-SAS HD ports or better - PSU: redundant;
NAS-B.15	Storage Expansion cards	- Quantity: as required to accommodate the required number of expansion enclosures - Interface: dual port SAS 12Gb/s (SFF-8644)
NAS-B.15-1	10 Gigabit Ethernet Port	2 x 10GbE SFP+ SmartNIC port
NAS-B.16	Gigabit Ethernet Port (RJ45)	2 x 10GBase-T port Gigabit Ethernet Port: 4 x Gigabit RJ-45 Ethernet port.
NAS-B.17	SFP+ Optical Module for 10GBASE-SR	Two pairs required.
NAS-B.18	USB 3.2 Gen 2 (10Gbps) Port	2 x USB 3.2 Gen 2 10Gbps or better
NAS-B.19	I/O ports	- USB / RJ45

NAS – Configuration B requirements		
Requirement #	**Category**	**Description**
		- Optional: VGA or HDMI
NAS-B.20	System Monitoring	- Monitors temperature for CPU and memory - Monitors Voltage for CPU, memory, chipset and power supply - Over-temperature warning indicator - Fan and PSU fail LED indicator
NAS-B.21	Server Management	- IPMI 2.0 compliant - iKVM feature
NAS-B.22	Real Time Replication	Required
NAS-B.23	Power Supply	Redundancy 1+1; Voltage: 200-240VAC; Frequency: 50Hz-60Hz
NAS-B.24	Regulation and compliance	CE; RoHS 6/6 Compliant
NAS-B.25	Support and Warranty	3-years support and warranty

Network Attached Storage: NAS – Configuration C

The requested "NAS – Configuration C" shall comply with the following requirements:

NAS – Configuration C requirements		
Requirement #	**Category**	**Description**
NAS-C.1	Make & Model	<< to be specified by bidder>>
NAS-C.2	Form Factor	Rack mountable
NAS-C.3	Processor	Intel Xeon E-2236 6-core/12-thread 3.4 GHz or better
NAS-C.4	Memory	128 GB DDR4
NAS-C.5	Flash memory	2 x 1TB SSD (Dual boot OS protection)
NAS-C.6	Operating System	<< to be specified by bidder>>
NAS-C.7	Drive compatibility	- 2.5-inch SATA 6Gbps/3Gbps hard disk drives - 2.5-inch SATA SSD (Solid State Drives)
NAS-C.8	Hot swappable	Yes
NAS-C.9	SSD Cache Acceleration Support	Yes
NAS-C.10	RAID	RAID 5/6
NAS-C.11	Storage capacity	24 x 2TB SSD

NAS – Configuration C requirements		
Requirement #	**Category**	**Description**
NAS-C.12	SATA	6 Gb/s
NAS-C.13	Storage controller	Quad PCIe SSD
NAS-C.14	10 Gigabit Ethernet Port	2 x 10GbE SFP+ SmartNIC port
NAS-C.15	Gigabit Ethernet Port (RJ45)	2 x 10GBase-T port Gigabit Ethernet Port: 4 x Gigabit RJ-45 Ethernet port.
NAS-C.16	SFP+ Optical Module for 10GBASE-SR	Two pairs required.
NAS-C.17	USB 3.2 Gen 2 (10Gbps) Port	2 x USB 3.2 Gen 2 10Gbps or better
NAS-C.18	I/O ports	- USB / RJ45 - Optional: VGA or HDMI
NAS-C.19	System Monitoring	- Monitors temperature for CPU and memory - Monitors Voltage for CPU, memory, chipset and power supply - Over-temperature warning indicator - Fan and PSU fail LED indicator
NAS-C.20	Server Management	- IPMI 2.0 compliant - iKVM feature
NAS-C.21	Real Time Replication	Required
NAS-C.22	Power Supply	Redundancy 1+1; Voltage: 200-240VAC; Frequency: 50Hz-60Hz
NAS-C.23	Regulation and compliance	CE; RoHS 6/6 Compliant
NAS-C.24	Support and Warranty	3-years support and warranty

Switch for "NAS – Configuration C"

An additional 24 ports switch shall be provided. It shall comply with the following requirements:

Switch for "NAS – Configuration C" requirements		
Requirement #	**Category**	**Description**
NAS-C-S.1	Make & Model	<< to be specified by bidder>>
NAS-C-S.2	Form Factor	Rack mountable
NAS-C-S.3	Number of ports	24 Gigabit Ethernet ports with line-rate forwarding performance

Switch for "NAS – Configuration C" requirements		
Requirement #	**Category**	**Description**
NAS-C-S.4	Uplinks	Four Gigabit Small Form-Factor Pluggable (SFP/SFP+)

Tape storage

The requested "Tape Storage" shall comply with the following requirements:

Tape storage requirements		
Requirement #	**Category**	**Description**
TAPS.1	Make & Model	<< to be specified by bidder>>
TAPS.2	Form Factor	Rack-mountable or standalone
TAPS.3	LTO compliance	- LTO Generation 8 tape drive native data transfer rate up to 300 MBps - LTO Generation 8 media specification tape cartridge compressed capacity of up to 30 TB with 2.5 to 1 compression - Encryption on LTO Ultrium 8 and Ultrium 7 tape drives - Support for media partitioning and self-describing tape - Adherence to LTO specifications
TAPS.4	Tape drives	2 x LTO Ultrium 8 half-high 6 Gb SAS Or 2 x LTO 8 Gb Fiber Channel drives (one option to be maintained)
TAPS.5	Cartridge capacity	24 tape cartridges
TAPS.6	Standard barcode reader	Required
TAPS.7	I/O station	single-cartridge I/O station
TAPS.8	Cartridge magazines	2
TAPS.9	Cables for the tape storage attachment	Required up to the number of tape drives installed. Note: At least one SAS cable should be specified to attach a TS3100 or TS3200 to the server SAS host bus adapter (HBA). Note 2: We can add SAS interposers to attach using several SAS cables Note 3: In case of Fiber, Features for specifying Fibre Channel cables and their respective lengths must be specified.

Tape storage requirements		
Requirement #	**Category**	**Description**
TAPS.10	Expansion card for the host server	2 x PCIe cards SAS or Fiber
TAPS.11	Data cartridges	100 x LTO Ultrium 8 Data Cartridge 12TB Native / 30TB Compressed
TAPS.12	Removable cartridge magazines	5 x compatible cartridge magazines
TAPS.13	Supported Operating Systems	It must be possible to attach the tape storage to Linux and Windows servers.
TAPS.14	Management software	- The management software must allow for direct, intuitive, and graphical access to data stored in tape drives and libraries. - Tape-stored data must be accessed as if it were on disk or flash storage. - The management software must allow the users of tape library systems to inventory cartridges and read, write, and search data on any cartridge, enabling writing of metadata and tagging of individual files for easy and fast access to files stored on cartridges.
TAPS.15	Power Supply	Redundancy 1+1; Voltage: 200-240VAC; Frequency: 50Hz-60Hz
TAPS.16	Regulation and compliance	CE; RoHS 6/6 Compliant
TAPS.17	Support and Warranty	3-years support and warranty

DIGITAL FORENSICS WORKSTATIONS AND LAPTOPS

Digital Forensics Workstations – Configuration A

The requested "Digital Forensics Workstations – Configuration A" shall comply with the following requirements:

Digital Forensics Workstations – Configuration A requirements		
Requirement #	**Category**	**Description**
DFW-A.1	Make & Model	<< to be specified by bidder>>
DFW-A.2	Form Factor	Desktop

Digital Forensics Workstations – Configuration A requirements		
Requirement #	**Category**	**Description**
DFW-A.3	Motherboard chipset	<< to be specified by bidder>>
DFW-A.4	Processor	2 x Xeon 16core CPU 2.2 GHz or better (Q1-23 or newer)
DFW-A.5	Memory	512 GB DDR5
DFW-A.6	Graphics	16 GB VGA GDDR6 or better
DFW-A.7	Operating System	Microsoft Windows 11 Professional, 64-bit
DFW-A.8	Storage	- 2 x 10TB SATA III 720 RPM HDD - 2TB (NVMe PCIe SSD) - 2TB (NVMe PCIe SSD) - 2TB (NVMe PCIe SSD)
DFW-A.9	Extra Storage Slots	- 3 HotSwap Drive Bays 2.5”/3.5” SATA III (USB 3.1 connected) - 2 HotSwap Drive Bay 2.5”/3.5” SATA III (SATA connected) - 2 Internal M.2 NVMe SSD
DFW-A.10	Storage Controller	- 6 Gb/s SATA (8) - M.2 x 4 PCIe Socket (1) - 6 Gb/s SATA (2)
DFW-A.11	RAID Controllers	16 Channel PCIe 12 Gb/s SAS/SATA
DFW-A.12	RAID Capacity	- Three (3) x Five (5) bay RAID chassis (15 drives total). - Five 2 TB (8 TB RAID5). - RAID capacity up to 210 TB using 14 TB drives.
DFW-A.13	Network	10 Gigabit Network Card - 1 port CAT6A Copper
DFW-A.13	Drive Bays	- Native SATA, shock-mounted, removable (2) - Hot-swap, USB 3.1 connected SATA III, shock-mounted, read only or read write selectable, removable (3)
DFW-A.14	Drive Bay Ecosystem	- Hot-swappable, interchangeable USB 3.1 connected drive trays - 2.5" / 3.5" SATA drive tray, user selectable read/write or read only (write blocked) modes - Forensic card reader tray for flash memory access, user selectable read / write or read only (write blocked) modes - M.2 / NVMe PCIe SSD and M.2 SATA drive tray, user selectable read/write or read only (write blocked) modes - USB 3.1 hub tray, with several external USB3.1 port connections.
DFW-A.15	Forensic Imaging & Write Blocking	The digital forensic workstation must have hardware based write blockers with the following features and capabilities:

Digital Forensics Workstations – Configuration A requirements		
Requirement #	**Category**	**Description**
		- Hardware write blocked imaging of SATA, SAS, USB, IDE, Firewire and PCIe SSD devices - Single or multiple (concurrent) forensic imaging of storage devices - Convenient front panel write blocked or read/write switch for general drive management - Touch-screen user interface. Displays device details, display and manage LUNs and HDD protected regions. Examine file partitions. - Tableau Imager (TIM) or equivalent pre-installed
DFW-A.16	Media Card Reader	The digital forensic workstation must integrate forensic card reader Switchable between Read-Only and Read-Write operation: - Forensic Card Reader or equivalent - User selectable write blocked or read/write
DFW-A.17	External Connections & Expansion	The system must have front accessible USB ports (USB 3.1 and USB 2.0)
DFW-A.18	Audio	8-channel high-definition audio CODEC
DFW-A.19	Optical Drive	DVD/CD/Blu-Ray: BD-R/BD-RE/DVD±RW/CD±RW BluRay burner, dual-layer combo drive
DFW-A.20	Display	- 22inch LED Screen or better - Monitor Resolution: 1920 x 1080 full HD
DFW-A.21	Peripherals	QWERTY desktop keyboard and optical mouse
DFW-A.22	Power Supply	Line voltage: 100-240 VAC; Frequency: 50-60 Hz
DFW-A.23	Accessories	- Forensic toolbox containing drive adapters and power / signal cables (SAS, SATA, IDE, microSATA, SATA LIF, MacBook Air, Blade SSD) - PCIe SSD drive adapters (PCIe SSD m.2 NVMe, 2013 or newer MacBook Pro SSD, and server class PCIe SSD) - All specific tools that might be required for opening enclosures
DFW-A.24	Warranty	3-years warranty must be included

Digital Forensics Workstations – Configuration B

The requested "Digital Forensics Workstations – Configuration B" shall comply with the following requirements:

Digital Forensics Workstations – Configuration B requirements		
Requirement #	**Category**	**Description**
DFW-B.1	Make & Model	<< to be specified by bidder>>
DFW-B.2	Form Factor	Desktop
DFW-B.3	Motherboard chipset	<< to be specified by bidder>>
DFW-B.4	Processor	Intel i9 18core CPU 3 GHz or better
DFW-B.5	Memory	128 GB DDR4
DFW-B.6	Graphics	8 GB VGA or better
DFW-B.7	Operating System	Microsoft Windows 10 Professional, 64-bit
DFW-B.8	Storage	- 1TB NVMe PCIe SSD (OS) - 1TB NVMe PCIe SSD (SWAP/Cache/Temp) - 2TB NVMe PCIe SSD (Database) - 8 x 6 TB SATA III 720 RPM HDD (Case/Data)
DFW-B.9	RAID	One (1) High End RAID Controller Cards with 12 Gb/s Processing
DFW-B.10	Drive bay ecosystem	- One (1) 2.5" Hot Swap Bay with Four (4) Removable Trays - One (1) 3.5" Hot Swap Bay with Five (5) Removable Trays
DFW-B.11	Network	10 Gigabit Network Card - 1 port CAT6A Copper
DFW-B.12	Forensic Imaging & Write Blocking	The digital forensic workstation must have hardware based write blockers with the following features and capabilities: - Front Panel Forensic Card Reader - Tableau T3iu Forensic Bridge or similar
DFW-B.13	External Connections & Expansion	The system must have front accessible USB ports (USB 3.0 and USB 2.0)
DFW-B.14	Audio	8-channel high-definition audio CODEC
DFW-B.15	Optical Drive	DVD/CD/Blu-Ray: BD-R/BD-RE/DVD±RW/CD±RW BluRay burner, dual-layer combo drive
DFW-B.16	Display	- 22inch LED Screen (or better - Monitor Resolution: 1920 x 1080 full HD
DFW-B.17	Peripherals	QWERTY desktop keyboard and optical mouse
DFW-B.18	Power Supply	Line voltage: 100-240 VAC; Frequency: 50-60 Hz
DFW-B.19	Warranty	3-years warranty must be included

Digital Forensics Workstations – Configuration C

The requested "Digital Forensics Workstations – Configuration C" shall comply with the following requirements:

Digital Forensics Workstations – Configuration C requirements		
Requirement #	**Category**	**Description**
DFW-C.1	Make & Model	<< to be specified by bidder>>
DFW-C.2	Form Factor	Desktop
DFW-C.3	Motherboard chipset	<< to be specified by bidder>>
DFW-C.4	Processor	2 x Xeon 12core CPU 2.2 GHz or better
DFW-C.5	Memory	64 GB DDR4
DFW-C.6	Graphics	4 GB VGA GDDR5 or better
DFW-C.7	Operating System	Microsoft Windows 11 Professional, 64-bit
DFW-C.8	Storage	- 1TB NVMe PCIe SSD (OS) - 2 TB SSD SATA III (Database/Cache/Temp) - 2 TB SATA III 720 RPM HotSwap (Case/Data)
DFW-C.9	Extra Storage Slots	- 3 HotSwap Drive Bays 2.5"/3.5" SATA III (USB 3.1 connected) - 2 HotSwap Drive Bay 2.5"/3.5" SATA III (SATA connected)
DFW-C.10	Storage Controller	- NVMe SSD controller - 6 Gb/s SATA (8) - M.2 x 4 PCIe Socket (2)
DFW-C.11	RAID Controllers	12 Channel PCIe 12 Gb/s SAS/SATA
DFW-C.12	RAID Capacity	5 Drive RAID Chassis Up to 8 TB configured as RAID5
DFW-C.13	Network	10 Gigabit Network Card - 1 port CAT6A Copper
DFW-C.14	Drive Bays	- Native SATA, shock-mounted, removable (2) - Hot-swap, USB 3.1 connected SATA III, shock-mounted, read only or read write selectable, removable (3)
DFW-C.15	Drive Bay Ecosystem	- Hot-swappable, interchangeable USB 3.1 connected drive trays - 2.5" / 3.5" SATA drive tray, user selectable read/write or read only (write blocked) modes - Forensic card reader tray for flash memory access, user selectable read / write or read only (write blocked) modes - M.2 / NVMe PCIe SSD and M.2 SATA drive tray, user selectable read/write or read only (write blocked) modes - USB 3.1 hub tray, with several external USB3.1 port connections.

Digital Forensics Workstations – Configuration C requirements		
Requirement #	**Category**	**Description**
DFW-C.16	Forensic Imaging & Write Blocking	The digital forensic workstation must have hardware based write blockers with the following features and capabilities: - Hardware write blocked imaging of SATA, SAS, USB 3, IDE, Firewire and PCIe SSD devices - Single or multiple (concurrent) forensic imaging of storage devices - Convenient front panel write blocked or read/write switch for general drive management - Touch-screen user interface. Displays device details, display and manage LUNs and HDD protected regions. Examine file partitions. - Tableau Imager (TIM) or equivalent pre-installed
DFW-C.17	Media Card Reader	The digital forensic workstation must integrate forensic card reader Switchable between Read-Only and Read-Write operation: - Forensic Card Reader or equivalent - User selectable write blocked or read/write
DFW-C.18	External Connections & Expansion	The system must have front accessible USB ports (USB 3.1 and USB 2.0)
DFW-C.19	Audio	8-channel high-definition audio CODEC
DFW-C.20	Optical Drive	DVD/CD/Blu-Ray: BD-R/BD-RE/DVD±RW/CD±RW BluRay burner, dual-layer combo drive
DFW-C.21	Display	- 22inch LED Screen or better - Monitor Resolution: 1920 x 1080 full HD
DFW-C.22	Peripherals	QWERTY desktop keyboard and optical mouse
DFW-C.23	Power Supply	Line voltage: 100-240 VAC; Frequency: 50-60 Hz
DFW-C.24	Accessories	- Forensic toolbox containing drive adapters and power / signal cables (SAS, SATA, IDE, microSATA, SATA LIF, MacBook Air, Blade SSD) - PCIe SSD drive adapters (PCIe SSD m.2 NVMe, 2013 or newer MacBook Pro SSD, and server class PCIe SSD) - All tools required for opening enclosures
DFW-C.25	Warranty	3-years warranty must be included

Digital Forensics Workstations – Configuration D

The requested "Digital Forensics Workstations – Configuration D" shall comply with the following requirements:

Digital Forensics Workstations – Configuration D requirements		
Requirement #	**Category**	**Description**
DFW-D.1	Make & Model	<< to be specified by bidder>>
DFW-D.2	Form Factor	Desktop
DFW-D.3	Motherboard chipset	<< to be specified by bidder>>
DFW-D.4	Processor	Intel i9 CPU 16 (8P+8E) cores up to 5.2 GHz or better
DFW-D.5	Memory	32 GB RAM DDR4
DFW-D.6	Graphics	4 GB VGA GDDR5 or better
DFW-D.7	Operating System	Microsoft Windows 11 Professional, 64-bit
DFW-D.8	Storage	1TB M.2 NVMe PCIe SSD (OS)
DFW-D.9	Network	10 Gigabit Network Card - 1 port CAT6A Copper
DFW-D.10	External Connections & Expansion	The system must have front accessible USB ports (USB 3.0 and USB 2.0)
DFW-D.11	Audio	8-channel high-definition audio CODEC
DFW-D.12	Optical Drive	DVD/CD/Blu-Ray: BD-R/BD-RE/DVD±RW/CD±RW BluRay burner, dual-layer combo drive
DFW-D.13	Display	- 24inch LED Screen or better - Monitor Resolution: 1920 x 1080 full HD
DFW-D.14	Peripherals	- QWERTY desktop keyboard and optical mouse - Gaming Headset with Detachable Microphone for PC
DFW-D.15	Power Supply	Line voltage: 100-240 VAC; Frequency: 50-60 Hz
DFW-D.16	Warranty	3-years warranty must be included

Digital Forensics Laptop – Configuration A

The requested "Digital Forensics Laptop – Configuration A" shall comply with the following requirements:

Digital Forensics Laptop – Configuration A requirements		
Requirement #	**Category**	**Description**
DFL-A.1	Make & Model	<< to be specified by bidder>>
DFL-A.2	Form Factor	Laptop
DFL-A.3	Motherboard chipset	<< to be specified by bidder>>

Digital Forensics Laptop – Configuration A requirements		
Requirement #	**Category**	**Description**
DFL-A.4	Power Supply	200-240VAC ; 50Hz
DFL-A.5	Processor	Intel i9 16core CPU 2.1 GHz or better (Q1-23 or newer)
DFL-A.6	RAM	64 GB DDR5
DFL-A.7	Graphics	8 GB VGA GDDR6 or better
DFL-A.8	Operating System	Microsoft Windows 11 Professional, 64-bit
DFL-A.9	Storage	- 2TB M.2 NVMe PCIe SSD - 2TB M.2 NVMe PCIe SSD - 8TB SATA SSD
DFL-A.10	Network	- 10/100/1000 Mbps gigabit Ethernet adapter - Dual Band Wireless Wi-Fi 6E AX211 + Bluetooth Module
DFL-A.11	USB	USB 3.1 (2 or more)
DFL-A.12	Optical Drive	USB BR-RE / CDRW / DVDWR
DFL-A.13	Display	- 15inch LCD Screen or better - Monitor Resolution: 1920 x 1080 full HD
DFL-A.14	Keyboard and mouse	Built-in QWERTY keyboard and built-in mouse
DFL-A.15	Peripherals	- Optical mouse - Hard sided case with padded laptop insert - USB 3.1 External 3.5" Hard Drive Enclosure - 1 x 2 TB SATA Hard Drive
DFL-A.16	Forensic Imaging & Write Blocking	The digital forensic workstation must have hardware based write blockers with the following features and capabilities: - Tableau Imager (TIM) or equivalent pre-installed - Set of forensic hardware write blocker (USB3.0 to IDE/SATA, PCIe, and USB3.0) including interface cables, SATA III to m.2 and mSATA SSD adapter, PCIe m.2 SSD adapter, and power supplies in a watertight/airtight case - Forensic Media Card Reader – Read-Only and Read/Write switchable or equivalent
DFL-A.17	Power Supply	Line voltage: 100-240 VAC; Frequency: 50-60 Hz
DFL-A.18	Warranty	3-years warranty must be included

Digital Forensics Laptop – Configuration B

The requested "Digital Forensics Laptop – Configuration B" shall comply with the following requirements:

Digital Forensics Laptop – Configuration B requirements		
Requirement #	**Category**	**Description**
DFL-B.1	Make & Model	<< to be specified by bidder>>
DFL-B.2	Form Factor	Laptop
DFL-B.3	Moterboard chipset	<< to be specified by bidder>>
DFL-B.4	Processor	Intel Core i7 6 P-core & 8 E-core 2.3 GHz or better
DFL-B.5	RAM	64 GB DDR4
DFL-B.6	Graphics	8 GB VGA GDDR6 or better
DFL-B.7	Operating System	Microsoft Windows 11 Professional, 64-bit
DFL-B.8	Storage	- (1) 1TB M.2 NVMe SSD for the Operating System - (1) 2TB M.2 NVMe SSD for Database / Evidence Files
DFL-B.9	Network	- 10/100/1000 Mbps gigabit Ethernet adapter - Dual Band Wireless Wi-Fi 6E AX211 + Bluetooth Module
DFL-B.10	USB	USB 3.1 (2 or more)
DFL-B.11	Display	- 15.6inch LCD Screen or better - Monitor Resolution: 1920 x 1080 full HD
DFL-B.12	Keyboard and mouse	Built-in QWERTY keyboard and built-in mouse
DFL-B.13	Peripherals	Optical mouse
DFL-B.14	Power Supply	Line voltage: 100-240 VAC; Frequency: 50-60 Hz
DFL-B.15	Warranty	3-years warranty must be included

Training on Digital Forensics Workstation / Laptop

The following table summarizes the requirements regarding the training program on Digital Forensics Workstation.

Digital Forensics Workstation / Laptop Training requirements		
Requirement #	**Category**	**Description**
DFTWL.1	Training Module Goals	After the installation of the Digital Forensics Workstation is completed, the end-users shall be trained on the utilization of the Digital Forensics Workstation features.
DFTWL.2	Details of the training module / curriculum	- General introduction on the Digital Forensics Workstation environment (software and hardware). - Familiarization with the common work procedures and investigations techniques and procedures - Developing workflows for the use cases

Digital Forensics Workstation / Laptop Training requirements		
Requirement #	**Category**	**Description**
		- Automation of data and meta-data extraction. - Administration tasks
DFTWL.3	Module Duration	2 days; Up to 10 participants
DFTWL.4	Place of Execution	Client Facility in Beirut
DFTWL.5	Qualification / Expertise required to the trainees	- Technicians with basic knowledge of PCs and the windows operational system - Technicians with basic knowledge of Digital Forensics investigations

LOT 2: DIGITAL FORENSIC HARDWARE TOOLS (DATA RECOVERY HARDWARE TOOLS, CHIP TOOLS)

Data Recovery Hardware Tools

PCI express card for workstation

The requested Data Recovery Tool – PC Systems shall comply with the following requirements:

Data recovery Tool – PC Systems requirements		
Requirement #	**Category**	**Description**
DRHT-A.1	Make & Model	<< to be specified by bidder>>
DRHT-A.2	Hardware form factor	PCI express card
DRHT-A.3	Main features	The tool should enable repair and data recovery from damaged SATA HDD. The tool should support the following features: - Diagnose a drive - Ability to access HDD firmware area and perform firmware repair, cloning and mount - Ability to change drive's configuration (head map, to boot from firmware copies, to adapt a donor PCB, to manually load firmware modules in RAM) - Copy by using hardware direct control over the disk - Access to data area in case of bad translator/defect lists - Ability to deactivate failed heads or scratched surfaces - Ability to bypass, view or clean ATA password - Ability to access PCB ROM infos - Ability to copy HDD with bad sectors or damaged surfaces

Data recovery Tool – PC Systems requirements		
Requirement #	**Category**	**Description**
		- Ability to create ISO image for forensic use (sector by sector) - Ability to to manage the data recovery process from diagnosis till drive restoration and copy to a new drive or file image
DRHT-A.4	Supported HDD brands	- Seagate; Western Digital; TOSHIBA; HITACHI / IBM (HGST); Samsung; Fujitsu; Maxtor; Quantum
DRHT-A.5	File system	- FAT, exFAT, NTFS, ReFS, HFS+, APFS, EXT2/3/4, XFS, F2FS, ReiserFS, BtrFS, VMFS, UFS1/2, ZFS, DHF4.1, WFS0.x and virtual machine images
DRHT-A.6	Accessories	- Adapters to allow practical attachment and communication with the drive - Power adapters - Media with client Software for PC - Cables
DRHT-A.7	Performances	The tool must ensure greater stability and a top speed of 6 Gb/sec in cloning operations
DRHT-A.8	Standards	AHCI SATA3 standard with 64bit drivers
DRHT-A.9	Power Supply	200-240VAC ; 50Hz
DRHT-A.10	Warranty	3-years warranty must be included

Portable data recovery system for SATA HDD/SDD

The requested Data recovery Tool – Portable Systems shall comply with the following requirements:

Data recovery Tool – Portable Systems requirements		
Requirement #	**Category**	**Description**
DRHT-B.1	Make & Model	<< to be specified by bidder>>
DRHT-B.2	Hardware form factor	External device
DRHT-B.3	Main functionalities	The tool should enable repair and data recovery from damaged SATA HDD and SSD. The tool should support the following features: - Diagnose a drive - Ability to access HDD firmware area and perform firmware repair, cloning and mount

Data recovery Tool – Portable Systems requirements		
Requirement #	**Category**	**Description**
		- Ability to change drive's configuration (head map, to boot from firmware copies, to adapt a donor PCB, to manually load firmware modules in RAM) - Copy by using hardware direct control over the disk - Access to data area in case of bad translator/defect lists - Ability to deactivate failed heads or scratched surfaces - Ability to bypass, view or clean ATA password - Ability to access PCB ROM infos - Ability to copy HDD with bad sectors or damaged surfaces - Ability to create ISO image for forensic use (sector by sector) - Ability to manage the data recovery process from diagnosis till drive restoration and copy to a new drive or file image
DRHT-B.4	Supported HDD / SSD brands	- Seagate; Western Digital; TOSHIBA; HITACHI / IBM (HGST); Samsung; Fujitsu; Maxtor; Quantum
DRHT-B.5	Supported USB Flash brands	- A-DATA, Apacer, Corsair, Goodram, Kingston, Lexar, Samsung, Sandisk, Silicon Power, Smartbuy, Toshiba, Transcend, Verbatim.
DRHT-B.6	Supported SSD vendors	- OCZ, Corsair, Crucial, RunCore, A-DATA, G.Skill, Micron, Plextor, Intel, Samsung, Seagate, SanDisk, Kingston, Smartbuy, Silicon Power, PNY, AMD, Lexar, Transcend, Patriot, GoodRam, Kingspec, Toshiba.
DRHT-B.7	Interfaces	- SATA (Serial ATA) and USB devices compliant with the Mass Storage Device specification, i.e. external USB 2.0/3.0 HDD and USB Flash drives with logical issues (File System corruption, deleted data). - SSHD (Solid State Hybrid Drive). - PATA (IDE) - SAS (Serial Attached SCSI) - M.2 PCIe NVMe and M.2 (NGFF) - mSATA - Micro SATA, PATA, LIF, ZIF, Apple proprietary interface - PCIe x1-x16 - SD/MicroSD Memory Cards
DRHT-B.8	RAID	Support of virtual RAID levels
DRHT-B.9	File system	- FAT, exFAT, NTFS, ReFS, HFS+, APFS, EXT2/3/4, XFS, F2FS, ReiserFS, BtrFS, VMFS, UFS1/2, ZFS, DHF4.1, WFS0.x, and virtual machine images
DRHT-B.10	Accessories	- SAS adapter - PC SATA-PATA adapter - M.2 PCIe NVMe SSD/M.2 SATA SSD adapter - SATA-mSATA adapter

Data recovery Tool – Portable Systems requirements		
Requirement #	**Category**	**Description**
		- Micro SATA, PATA, LIF, ZIF, Apple proprietary interface adapters - PCIe x16 SSD Adapter - 2-in-1 Card Reader Adapter - Power adapters - Media with client Software for PC - Cables - Hard case
DRHT-B.11	Performances	The tool must ensure greater stability and a top speed of 6 Gb/sec in cloning operations
DRHT-B.12	Power Supply	200-240VAC ; 50Hz
DRHT-B.13	Warranty	3-years warranty must be included

Mobile data recovery systems

The requested Data recovery Tool – Mobile Systems shall comply with the following requirements:

Data recovery Tool – Mobile Systems requirements		
Requirement #	**Category**	**Description**
DRHT-C.1	Make & Model	<< to be specified by bidder>>
DRHT-C.2	Hardware form factor	External device
DRHT-C.3	Main functionalities	The tool must allow low-level access to mobile devices and tablets with the help of a USB cable to recover data even when the device is operating using its minimum operating conditions.
DRHT-C.4	Software	- Extract data through the standard ports of the devices with the help of low-level protocols and software methods (Low-level Access) - Parse and analyze the data that has been extracted using Low-level Access or with the Chip-off Method - Extract deleted data - Export data in formats compatible with 3d party tools
DRHT-C.5	Analysis capabilities	Get the access to the phone contacts, calendar, SMS, WhatsApp, mediafiles, general phone information, the list of Wi-Fi networks, and accounts information.

Data recovery Tool – Mobile Systems requirements		
Requirement #	**Category**	**Description**
DRHT-C.6	Diagnostic ports	- USB 2.0 / 3.0 - eMMC Port (SD/eMMC/eMCP), - SD/microSD Port (SD/eMMC/eMCP/microSD) - Write protect switchers for SD / MMC Ports
DRHT-C.7	File system	FAT12/16/32, NTFS, Ext2/3/4, HFS+, exFAT, F2FS, etc.
DRHT-C.8	Accessories	- Cables - USB adapters - Micro USB adapters - SD/MMC adapters - Power adapters - Media with client Software for PC - Cables - Hard case
DRHT-C.9	Power Supply	200-240VAC ; 50Hz
DRHT-C.10	Warranty	3-years warranty must be included

Portable Write blockers for data recovery

The requested Data recovery Tool – Mobile Systems shall comply with the following requirements:

Data recovery Tool – Portable Write blocker requirements		
Requirement #	**Category**	**Description**
DRHT-D.1	Make & Model	<< to be specified by bidder>>
DRHT-D.2	Hardware form factor	Portable device
DRHT-D.3	Main functionalities	The portable devices(s) must provide write-blocker(s) that enable forensic acquisition of data
DRHT-D.4	Interfaces	- SATA/IDE Bridge - PCIe Bridge - USB 3.0 Bridge
DRHT-D.5	SATA/IDE Bridge	- Must enable forensic acquisition of SATA and IDE solid-state-drives - IDE media detection ○ IDE Device: Parallel ATA hard disk devices with Logical Block Addressing (LBA) support - SATA media detection ○ SATA Device: SATA 1 or SATA 2 hard disk devices - Write-block status, and activity

Data recovery Tool – Portable Write blocker requirements		
Requirement #	**Category**	**Description**
		- Read/write mode capability via switch
DRHT-D.6	PCIe Bridge	- PCIe devices that comply with the AHCI standard or NVMe 1.0 specification must be supported - Write-block status, and activity - Read/write mode capability via switch
DRHT-D.7	USB 3.0 Bridge	- Must enable forensic acquisition of USB 3.0 devices and older devices that conform to the USB Mass Storage class specification and support the Bulk Only Interface Protocol - Must enable imaging speeds up to 340 MB/second - Write-block status, and activity - Read/write mode capability via switch
DRHT-D.8	Host connection	USB 3.0 host computer connection
DRHT-D.9	Accessories	- Power adapters - Media Reader - PCIe Adapters ○ PCIe Card SSD Adapter ○ 4x PCIe M.2 SSD Adapters ○ PCIe adapter cable (4 inch) - Cables ○ One SATA cable ○ Three Unified SAS cable ○ 2x IDE cable ○ 2x 3M to Molex power cables ○ 2x 3M to SATA power cables ○ 2x USB 3.0 Type A to Type B - Hard case
DRHT-D.10	Warranty	3-years warranty must be included

Portable PCIe HDD Duplicator

The requested Data recovery Tool – PCIe HDD Cloning shall comply with the following requirements:

Data recovery Tool – PCIe HDD Duplicator requirements		
Requirement #	**Category**	**Description**
DRHT-E.1	Make & Model	<< to be specified by bidder>>
DRHT-E.2	Hardware form factor	Portable device

Data recovery Tool – PCIe HDD Duplicator requirements		
Requirement #	**Category**	**Description**
DRHT-E.3	Main functionalities	The portable devices must provide PCIe hard drive duplicator
DRHT-E.4	Cloning capabilities	- The device must support up to 4 master drives to 4 target drives - The device must support cloning to/from PCIe M.2, AHCI and NVMe type drives and PCIe express cards (using optional PCIe adapters is allowed)
DRHT-E.5	Write-protection	Write-blocked functionality must be available to prevent any alteration to sensitive data on the master drive.
DRHT-E.6	Wipe mode	Must meet NIST 800-88 guidelines
DRHT-E.7	I/O ports	- 1 PCIe, 2 SATA (SAS included) and 1 USB 3.0, 1 FireWire master port - 1 PCIe, 2 SATA (SAS included), and 1 USB 3.0, 1 FireWire target port.
DRHT-E.8	Accessories	- IDE, ZIF, mSATA, microSATA, eSATA drives and compact flash media adapters - IDE to SATA adapters - Power adapters - Cables
DRHT-E.9	Warranty	3-years warranty must be included

Chip tools

Cold Chip-off Station

The requested "Cold Chip off station" shall comply with the following requirements:

Cold Chip off Tools requirements		
Requirement #	**Category**	**Description**
CTCO.1	Make & Model	<< to be specified by bidder>>
CTCO.2	Main functionality	Cold Chip-off station should feature a programmable milling cutter to perform cold chip off operations through precision sawing, milling and flat grinding.
CTCO.3	Milling operations	- The station shall be equipped with motorized X, Y and theta controls - The milling operations shall be controllable remotely through software

Cold Chip off Tools requirements		
Requirement #	**Category**	**Description**
CTCO.4	Vision system	- The station shall feature a high-resolution colour vision system. - The colour optical system should be equipped with split vision, zoom, micro-adjust, auto-focus and software operation camera functionalities.
CTCO.5	Boards and components	The system should fit boards up to 25 inches and places components from 1 millimeter to 120 millimeters.
CTCO.6	Power Supply	200-240VAC ; 50Hz
CTCO.7	Warranty	3-years warranty must be included

Desoldering Station

The requested “desoldering station” shall comply with the following requirements:

Desoldering Station requirements		
Requirement #	**Category**	**Description**
CTDS.1	Make & Model	<< to be specified by bidder>>
CTDS.2	Main purpose	The device must allow reworking of circuit boards by replacing defective BGA and FINEPITCH components, and for the assembly of circuit boards in a laboratory context.
CTDS.3	Camera and split optical unit	- 2.0 megapixel CMOS USB 2.0 camera with zoom lens - Split optical unit for precise and controlled alignment of component with respect to PCB - Two coloured LED lights to provide a contrasted image of the circuit board and an image of the component's contact surface
CTDS.4	Table	- Software controlled positioning and soldering processes. - Motor-controlled movement of the transportation table - Precision linear guidance
CTDS.5	Vacuum	- Operation and position must be controlled by software - Availability of connection for optional vacuum pipette
CTDS.6	Soldering	- Operation and position must be controlled by software - Precision linear guide for z-adjustment - Vibration-free lowering and lifting off of the soldering head - Theta adjustment of the heating head - "Vacuum Lift" for automatically desoldering components - Mechanical protection to prevent movement during soldering

Desoldering Station requirements		
Requirement #	**Category**	**Description**
		- Heating element with sufficient power output - Temperature sensor in the soldering head
CTDS.7	Insertion head	- Operation and position must be controlled by software - Precision linear guide for z-adjustment - x-, y- and theta precision guides for component alignment - Motor-controlled lowering of the insertion head with limit switches at both ends - Anti-rotation guidance of the vacuum pick-up - Automatic deactivation of the vacuum pick-up by a sensor system on the insertion head
CTDS.8	Bottom heater	Temperature-controlled heater
CTDS.9	Top heater	Top heater with digital regulation for temperature monitoring
CTDS.10	Temperature sensors	Yes, including sufficient number of type K thermocouples for temperature-profile configuration
CTDS.11	Positioning sensors	Yes
CTDS.12	Software	- Program, store and read Process steps - Availability of predefined temperature profiles - Availability of special functions to facilitate process adaptation
CTDS.13	Other features	- Connection option for compressed air or nitrogen - Support for long circuit boards
CTDS.14	Power Supply	200-240VAC ; 50Hz
CTDS.15	Warranty	3-years warranty must be included

LOT 3: DIGITAL FORENSIC SOFTWARE TOOLS (DATA RECOVERY SOFTWARE TOOLS, SMARTPHONE FORENSIC INVESTIGATION SOFTWARE TOOLS, COMPUTER FORENSIC INVESTIGATION SOFTWARE TOOLS, COMPUTER FORENSIC INVESTIGATION SOFTWARE - PASSWORD RECOVERY KIT) AND TRAINING (TRAINING ON COMPUTER FORENSIC INVESTIGATION SOFTWARE, TRAINING ON SMARTPHONE FORENSIC INVESTIGATION SOFTWARE)

Data recovery Software Tool

The requested Data recovery Software Tool shall comply with the following requirements:

Data recovery Software Tool requirements		
Requirement #	**Category**	**Description**
DRST.1	Make & Model	<< to be specified by bidder>>
DRST.2	Main purpose	A professional data recovery tool intended for digital forensic labs
DRST.3	Multi-Platform	Windows, Mac OS, Linux versions
DRST.4	Forensic Mode	A forensic report can be created and presented
DRST.5	RAID	Reverse RAIDs support: Yes. Flexible RAID reconstruction module with custom-defined RAID configurations
DRST.6	Virtual Object (RAID, custom regions) Mounting	Yes
DRST.7	Viewer / Editor	File, Hex / Tex
DRST.8	Disk Imaging	Advanced multi-pass disk imaging algorithm with variable parameters. Runtime imaging. Split images.
DRST.9	Sector Map	Creating/working sector maps, support for 3d party sector maps
DRST.10	Drive Copy Wizard	Yes
DRST.11	Image format	Creation and Reading: RDI, Byte-by-byte, and VMDK
DRST.12	Symbolic Links Management	Yes
DRST.13	Data Recovery over network	The software should work over a corporate Network and Internet. Advanced algorithms to traverse NAT and firewalls.
DRST.14	Data Recovery Hardware support	Yes; DDI, USB Stabilizer. Handling of severe hard drive read instabilities.

Data recovery Software Tool requirements		
Requirement #	**Category**	**Description**
DRST.15	Data Recovery Hardware	One USB Stabilizer Tech device must be included
DRST.16	Automatic updates	Automatic updates shall be provided for the duration of the Support and Maintenance Services
DRST.17	Support and Maintenance	1 year

Smartphone Forensic Investigation Software

The requested smartphone forensic investigation software shall comply with the following requirements:

Smartphone Forensic Investigation Software requirements		
Requirement #	**Category**	**Description**
SFIS.1	Make & Model	<< to be specified by bidder>>
SFIS.2	Provider credentials	The provided software must be developed by a leader in the field of digital forensics tools.
SFIS.3	Genuine license	The selected bidder shall provide a genuine license for the duration of the specified Software and Maintenance period in the form of a genuine activation key or a genuine USB dongle or vendor license certificate.
SFIS.4	Software category	The suggested product should be a highly functional software tool specially developed and used for digital forensic investigations of mobile devices and cloud data sources.
SFIS.5	Key Features	The suggested Software Tool shall support the following features: - Acquire data from a very high-number of devices - Support different operating systems and different chipsets (Android, BB, iOS, WP, Chinese Chipset, etc.) - Ability to acquire and display the device's technical information - Import backups and images (iTunes, Android, JTAG, Chip-Off) - Ability to analyze data from high number of unique apps - Ability to decrypt apps databases (list of apps to be provided) - Ability to recover a wide range of deleted data

Smartphone Forensic Investigation Software requirements		
Requirement #	**Category**	**Description**
		- Ability to conduct data analysis (Social graph, timeline, key evidence) - Ability to search data by criteria including keywords - Ability to recover passwords to encrypted backups and images - Ability to bypass screen lock (list of devices and OSs to be specified) - Ability to extract data from cloud sources (iCloud, Google, Microsoft, Onedrive, dropbox etc.) and from a wide range of social media (list of supported social media to be specified) - Ability to import and analyze call data records (also known as CDR files) and visually analyze connections between callers - Ability to extract media files - Ability to extract locations history - Ability to acquire geo coordinates from different sources such as mobile devices, cloud storage, media cards and imported images. - Ability to visualize route and common location of several users - Ability to visualize location within maps and determine frequently visited places, routes, and common locations of device owners (including across multiple device images). - Ability to analyze contacts from multiple sources such as the Phonebook, Messages, Event Log, Skype, chat and messaging applications in Aggregated Contacts. - Ability to export data to widely used file formats, such as PDF, RTF, XLS, SML, etc.
SFIS.6	Mobile Data Evidence	The collection and analysis of the following mobile data evidence shall be covered: - Service provider - Unique Identity Number - Location Area Identity (LIM) - Call logs - Contacts - International Mobile Subscriber Identity (IMSI) - Text message data - SMS - Multimedia messages - Images and Pictures - Videos - Sounds and Audios - WAP and WEB Browsers cache history

Smartphone Forensic Investigation Software requirements		
Requirement #	**Category**	**Description**
		○ History ○ Cache files ○ Cookies ○ Bookmarks ○ Saved pages and files ○ Search history ○ Saved login and passwords ○ Geolocation - Emails - Calendar - Previous SIM data - Telephone number - Integrated Circuit Card Identifier (ICCID) - International Mobile Equipment Identity (IMEI) - Applications data
SFIS.7	Encrypted electronic evidence discovery & decryption solution	- Encryption identification and analysis - Decrypts or recovers passwords for APFS, Apple DMG, - BitLocker, Dell, FileVault2, LUKS, McAfee, PGP, Symantec, TrueCrypt, and VeraCrypt disk images. - Password recovery for more than 300 file types (MS Office, PDF, Zip and RAR, QuickBooks, FileMaker, Lotus, Notes, Bitcoin wallets, password managers, and other applications. - ACUEFI compatible tool that acquires memory images of - Windows, Linux, and Mac computers. - Works with Windows computers that have Secure Boot enabled. - Hardware acceleration support - Cross-platform Kit Agents for acceleration - Live memory analysis - Email notifications
SFIS.8	Automatic updates	Automatic updates shall be provided for the duration of the Support and Maintenance Services
SFIS.9	Support and Maintenance	3 years

Training on Smartphone Forensic Investigation Software

The following table summarizes the requirements regarding the training program on the delivered Smartphone Forensic Investigation Software:

Smartphone Forensics – Training requirements		
Requirement #	**Category**	**Description**
TSFIS.1	Training Module Goal	The end-users shall be trained on the utilization of the Smartphone Forensic Investigation Software tool
TSFIS.2	Details of the training module / curriculum	- General introduction on the tool environment and its features. - Familiarization with the common work procedures and investigations techniques and procedures - Developing workflows and extraction methodologies to customize search paths, create custom search profiles, to mine user credentials and tokens, and save results for analysis. - Trainees must learn initial extraction methodology of an iDevice and Android device and follow up by importing multiple extraction formats of Android, Apple and other device and data types. - Deliver methodology to locate, recover, and process data types in extracted datasets. - Deep dives into the tool investigation capabilities such as analytics, database parsing, lost data recovery, alternate data sets and advanced tools. - Methodologies for the elaboration of professional, impartial, accurate, and consistent investigation reports. - Administration tasks
TSFIS.3	Training courseware and training materials	Comprehensive training courseware and associated training materials shall be delivered prior to commencement of training.
TSFIS.4	Module Duration	3 days; Up to 12 participants
TSFIS.5	Place of Execution	Client Facility in Beirut
TSFIS.6	Qualification / Expertise required to the trainees	- Technicians with basic knowledge of PCs and the windows operational system - Technicians with basic knowledge of Digital Forensics investigations and with working familiarity with mobile device extraction and analysis

Computer Forensic Investigation Software

The requested Computer Forensic Investigation software shall comply with the following requirements.

Two sources are required. Consequently, two tables must be completed for the two sources respectively.

Computer Forensic Investigation Software requirements		
Requirement #	**Category**	**Description**
CFIS.1	Make & Model	<< to be specified by bidder>>
CFIS.2	Provider credentials	The provided software tool must be developed by a leader in the field of digital forensics software
CFIS.3	Genuine license	The selected bidder shall provide a genuine license for the duration of the specified Software and Maintenance period in the form of a genuine activation key or a genuine USB dongle or vendor license certificate.
CFIS.4	Software category	The proposed product must be a highly functional software tool specially developed and used for digital forensic investigations of computers.
CFIS.5	Process Automation	The proposed solution shall support workflow automation through automated investigation workflows allowing investigators to easily recover and analyse digital evidence.
CFIS.6	Artifact collection and analysis	- The solution shall support comprehensive artifact collection and analysis capabilities. - The solution shall allow the investigator to collect both local device and cloud-based activity (e.g. Facebook, Twitter, Instagram, Google, iCloud, WhatsApp and LinkedIn), as well as internet browser history, videos, documents and location data to ensure all relevant evidence is highlighted. - The solution shall enable the investigator to provide conclusive results with a detailed analysis of findings.
CFIS.7	Device support	- Mac devices (including APFS, HFS+ and FileVault 2 decryption support) - Windows-based devices - Linux-based devices
CFIS.7	Decryption support	- Broadest OS/decryption support - Broadest support of encryption types - Provides decryption support to acquire encrypted evidence without data corruption, damage (e.g. Microsoft Windows 10 Bitlocker XTS-AES, Dell Data Protection, Symantec, PGP, APFS, HFS+, FileVault 2)
CFIS.8	Image analysis	- Support of Optical Character recognition - Extraction of text evidence from PDFs, images and scanned documents
CFIS.9	AI	The solution must allow automatic identification of images of particular interest, including nudity, drugs, weapons and explicit sexual content using artificial intelligence and machine learning.

Computer Forensic Investigation Software requirements		
Requirement #	**Category**	**Description**
CFIS.10	Reporting	- The solution should leverage open standard evidence file format to ingest other evidence file formats to enable a more comprehensive conclusion. - The bidder shall provide evidence about the quality of the reporting module of the solution and the reliability of evidence acquisition.
CFIS.11	Mobile data	Support of data evidence acquisitions from the latest smartphones and tablets, including high number of mobile device profiles (including latest device profiles)
CFIS.12	Extensibility	Offers extensibility through scripting and automated code commands that streamline and automate tasks and extend the capabilities of the tool
CFIS.13	Automatic updates	Automatic updates shall be provided for the duration of the Support and Maintenance Services
CFIS.14	Support and Maintenance	- Three years from license activation for the first source - One year from license activation for the second source

Training on Computer Forensic Investigation Software

The following table summarizes the requirements regarding the training program on the delivered Computer Forensics. The training shall be proposed for the two proposed sources.

Computer Forensics – Training Requirements		
Requirement #	**Category**	**Description**
TCFIS.1	Training Module Goal	The end-users shall be trained on the utilization of the Computer Forensic Investigation Software tool
TCFIS.2	Details of the training module / curriculum	- General introduction on the tool environment and its features. - Familiarization with the common work procedures and investigations techniques and procedures - Developing workflows and extraction methodologies to customize search paths, create custom search profiles, to mine user credentials and tokens, and save results for analysis. - Deliver methodology to locate, recover, and process data types in extracted datasets.

Computer Forensics – Training Requirements		
Requirement #	**Category**	**Description**
		- Deep dives in to the tool investigation capabilities such as analytics, database parsing, lost data recovery, alternate data sets and advanced tools. - Learn the process and methodologies for maintaining forensically sound evidence, producing professional and accurate reports, supplying supporting documentation, and preparedness to deliver findings in a more understandable way to the end user whether it is a manager, client, or a jury - Administration tasks
TCFIS.3	Training courseware and training materials	Comprehensive training courseware and associated training materials shall be delivered prior to commencement of training.
TCFIS.4	Module Duration	3 days; Up to 12 participants
TCFIS.5	Place of Execution	Client Facility in Beirut
TCFIS.6	Qualification / Expertise required to the trainees	- Technicians with basic knowledge of PCs and the windows operational system - Technicians with basic knowledge of Digital Forensics investigations

Computer Forensic Investigation Software - Password Recovery Kit

The requested Computer Password Recovery Kit software shall comply with the following requirements:

Computer Password Recovery Kit requirements		
Requirement #	**Category**	**Description**
CFIS-PK.1	Make & Model	<< to be specified by bidder>>
CFIS-PK.2	Main functionality	The tool must identify password-protected items on a computer and decrypts them
CFIS-PK.3	File types	The software must recognize 280+ file types and works in batch mode recovering their passwords.
CFIS-PK.4	Detect encrypted items	The software must find encrypted or password-protected documents, archives and other files
CFIS-PK.5	Extract encryption keys and passwords from memory images	- Quickly scan memory images and hibernation files. - Extract encryption keys for FileVault 2, TrueCrypt, VeraCrypt and BitLocker for decryption of encrypted disks and containers.

Computer Password Recovery Kit requirements		
Requirement #	**Category**	**Description**
		- Build possible passwords dictionaries or extract account passwords for Windows and Mac.
CFIS-PK.6	Hardware acceleration and distributed password recovery	- Increase password recovery speed by using a GPU (Graphics Processing Unit) card. - Distribute password recovery tasks over a network of Windows or Linux computers for linear scalability.
CFIS-PK.7	File Types	All supported file types must be specified
CFIS-PK.8	Automatic updates	Automatic updates shall be provided for the duration of the Support and Maintenance Services
CFIS-PK.9	Support and Maintenance	1 year

***** The trademarks shown in the Annexes act as reference, the bidder may submit another equivalent trademark with the same or higher performance.**

ANNEX 2 – TRAINING REQUIREMENTS

The following table summarizes the general requirements for the different training programs.

Training programs general requirements		
Requirement #	**Category**	**Description**
GTRE.1	General requirements	- The bidder must provide trainings to end-users and administrators on the new systems in order to build in house core competencies - The bidder must provide a task-oriented training, giving the participants the knowledge & information and providing them with the procedures required to perform each of their set tasks.
GTRE.2	Training programs	The bidders must provide the proposed training program covering: - Training Module goals - Details of the training module / curriculum - Module Duration - Place of Execution - Qualification / Expertise required to the trainees
GTRE.3	Training courseware and training materials	Comprehensive training courseware and associated training materials shall be developed, submitted for review and approval, and delivered prior to the commencement of training.

ANNEX 3 – MAINTENANCE AND SUPPORT

The following table provides the requirements for maintenance and support:

Support and Maintenance requirements		
Requirement #	**Category**	**Description**
SMSR.1	Warranty	The hardware shall be covered by a comprehensive warranty for the duration specified for each item.
SMSR.2	Initial Support and Maintenance services	The bidder shall provide first-line operations support, preventive maintenance, warranty maintenance and on-call remedial maintenance of the system for the period specified for each item.
SMSR.3	Renewal of Support and Maintenance services	- System maintenance shall be provided throughout the life of the system, so long as contractual maintenance coverage is renewed by end-users. - The bidder shall not refuse to renew the maintenance contract or unilaterally modify the terms of the maintenance contract. - The value of the support and maintenance contract renewal shall not exceed 10% of the price of the solution.
SMSR.4	Preventive Maintenance	Preventive maintenance shall be scheduled and performed on a regular basis.
SMSR.5	Remedial Maintenance	- Bidder shall correct all system problems, whether caused by hardware or software or both in combination, when the problem reduces the functional or performance capabilities of the system - Remedial maintenance coverage shall be provided during official opening hours. - Diagnostics and remediation shall be initiated within the guidelines described below: - **Critical incident:** Two hours to answer and forty-eight hours to repair. - **Major incident:**Four hours to answer and three business days to repair. - **Minor incident:**One business day to answer and five business days to repair.
SMSR.6	Software Maintenance	- Bidder shall provide software maintenance support to maintain continuity of the system and to rapidly respond to and correct problems with system functional capabilities and databases. - Software maintenance shall include the replacement of software that becomes obsolete or for which the manufacturer discontinues support during the maintenance period. - Bidder shall provide software updates, modifications and patches and associated documentation updates to maintain

Support and Maintenance requirements		
Requirement #	**Category**	**Description**
		optimum operational capabilities for the duration of the support and maintenance period.
SMSR.7	Hardware Maintenance	- For the avoidance of doubt, Warranty shall include the cost of original spare parts. - For the avoidance of doubt, Maintenance and Support services shall include the cost of Labour and transportation. - Awarded bidder shall dispatch a field service technician on-site where required. All service interventions must be performed under the supervision of end-user. - Defective media units (Disks, Flash(s), HDD...) shall be retained by the end-user and shall be replaced by new ones. - Hardware maintenance shall include the replacement of hardware that becomes obsolete or for which the manufacturer discontinues support during the initial maintenance period. - Awarded Bidder shall provide firmware updates and patches to maintain optimum operational capabilities for the duration of the support and maintenance period.

ANNEX 4 – PROJECT MANAGEMENT REQUIREMENTS

Project Management Implementation

The following table provides the requirements for Project Management Implementation:

Project Management Implementation requirements		
Requirement #	**Category**	**Description**
PMP-G.1	Project Management	- The selected bidder shall be responsible for all aspects of project management, including planning, staffing, performance monitoring and oversight, sub-contractor management, project coordination, quality assurance and reporting of all Project management related tasks. - The awarded bidder must ensure the management of both project's deadlines and deliverables.
PMP-G.2	Project Plan	The bidder must provide an initial draft Project Plan, including ALL foreseen tasks and resources required, which will be updated and approved at the beginning of the execution phase.
PMP-G.3	Reporting frequency	-The contractor must organise meetings (both remote, in the first place, and face-to-face when it is already in the process of installation in the country), on the status of the project; these meetings should take place at least fortnightly and will be complemented by concise reports (2-3 pages) weekly, that will cover on the main milestones, challenges, etc., in the implementation of the project.
PMP-G.4	Personnel Assignments and Access	-All contractors, subcontractors and other persons assigned by the bidder to the Lebanese LEA project shall be informed of (and assume) their responsibilities with respect to the confidentiality of facilities, capabilities, work processes and data. -In the event of a breach of contract, the replacement of any person assigned to the project may be unilaterally requested, and the bidder must then replace the person by someone else with the appropriate qualifications for the assigned position in a timely manner.

Project Milestones & Time Schedules

The following table summarizes the Project Milestones and Time Schedules requirements:

Requirement #	Category	Deliverable	Timelines
PMP-T.1	Project Milestones & Time Schedules	**Event:** Supply of All the Items **Deliverables:** Delivery, Acceptance of Delivery, Installation report, User Acceptance Report signed by the relevant authority in the Institution and configuration details of items installed.	Within 120 Days from the Date of issue of Notification of Award.
PMP-T.2		**Event:** Installation and Commissioning of items **Deliverables:** Installation and commissioning report signed by the relevant authority.	Within 14 Days from the Date of Delivery of items.
PMP-T.3		**Event:** Schedule training events **Deliverables:** Schedule training events, fix the dates, and agree on the final agenda and training material content.	Within 60 Days from the Date of issue of Notification of Award.
PMP-T.4		**Event:** Training acceptance **Deliverables:** Training Acceptance Report signed by the relevant authority.	Within 7 Days from the Date of Delivery of training.

ANNEX 5 – ACCEPTANCE PLANS

Acceptance requirements

The following table provides the requirements for Acceptance:

Acceptance requirements		
Requirement #	**Category**	**Description**
ACCR.1	Systems installation	- The selected bidder shall be responsible for all aspects of system implementation, as required to accomplish the successful delivery of the solution and associated implementation services in accordance with the specified system requirements and established delivery timeline objectives.
ACCR.2	User Acceptance Report	- The selected bidder must successfully complete the Installation and Commission as well as the associated User Acceptance report in line with the approved templates.
ACCR.3	Acceptance test plan	- The selected bidder must provide acceptance testing plan covering the functional requirements. The acceptance test plan must be attached to the User Acceptance Report. - The bidder must provide the detailed acceptance plan templates no later than two weeks after the contract signature.
ACCR.4	Proof of Concept	- The shortlisted bidder may be requested to prepare for a proof-of-concept (POC) to illustrate the compliance, the quality and the performance of the proposed solution. - In such a case, the shortlisted bidder shall setup a functional POC environment to illustrate the solution and prove its compliance with the requirements.

Hardware acceptance Plan

The following table provides the responsibility matrix regarding the Acceptance plan for Hardware deliverables.

	Shipment	Custom clearance	Local Permits	Local delivery	"Count" acceptance by LEA	Installation	Testing and commissioning	LEA Functional acceptance	Preparation of demo	Demonstration for ACT	ACT Acceptance	Payment
Awarded bidder	A	A	A	A	A	A	A	A	A	A	I	
ACT / FIIAAP	I	I	I	I	R	I	I	I	I	R	A	A
The following abbreviations apply: - **R: R**esponsible; **A: A**ccountable; **I: I**nformation - **LEA: L**aw **E**nforcement **A**gency												

Software Acceptance Plan

The following table provides the responsibility matrix regarding the Acceptance plan for Software deliverables.

	Delivery of licenses & kits	Installation	Testing and commissioning	LEA Functional acceptance	Preparation of demo	Demonstration for ACT	ACT Acceptance	Payment
Awarded bidder	A	A	A	A	A	A	I	
ACT / FIIAAP	I	I	I	I	I	R	A	A
The following abbreviations apply: - **R: R**esponsible; **A: A**ccountable; **I: I**nformation - **LEA: L**aw **E**nforcement **A**gency								

Training Acceptance Plan

The following table provides the responsibility matrix regarding the Acceptance plan for Training.

	Delivery of training material	Training Delivery as per curriculum	LEA training acceptance	ACT Acceptance	Payment
Awarded bidder	A	A	A	I	
ACT / FIIAAP	I	I	I	A	A
The following abbreviations apply: - **R: R**esponsible; **A: A**ccountable; **I: I**nformation - **LEA: L**aw **E**nforcement **A**gency					

ANNEX 6 – BILL OF QUANTITY

The technical offer must include a Bill of Quantity in line with the following templates.

The system performances remain the ultimate responsibility of the awarded contractor. The bidder may suggest any required changes to the Bill of Quantity with the required clear justifications during the clarification period. The country of origin of the solution components and system must be provided.

The commercial offer must quote every single item provided in the Bill of Quantity table. The item numbers must remain unchanged.

Bill of Quantity – Lot 1 (Digital Forensic IT Hardware)

The following table contains the bill of quantity for Lot 1 which is defined above. The requirements for each item are further detailed in Annex 1 of the present document.

Item Ref. #	Item name	Requirements (refer to Annex 1)	Description	Model / Item(s) reference no	Country of origin	Quantity
1.1	Network Attached Storage – Configuration A					1
1.2	Network Attached Storage – Configuration B					1
1.3	Network Attached Storage – Configuration C					1
1.4	Switch for "NAS – Configuration C"					1
1.5	Tape Storage					1
1.6	Forensic Workstations – Configuration A					1
1.7	Forensic Workstations – Configuration B					1

Item Ref. #	Item name	Requirements (refer to Annex 1)	Description	Model / Item(s) reference no	Country of origin	Quantity
1.8	Forensic Workstations – Configuration C					1
1.9	Forensic Workstations – Configuration D					11
1.10	Forensic Laptop – Configuration A					1
1.11	Forensic Laptop – Configuration B					1

Bill of Quantity – Lot 2 (Digital Forensic Hardware Tools)

The following table contains the bill of quantity for Lot 2 which is defined above. The requirements for each item are further detailed in Annex 1 of the present document.

Item Ref. #	Item name	Requirements (refer to Annex 1)	Description	Model / items reference nº	Country of origin	Quantity
2.1	Data Recovery Tool – PCI express for workstation					1
2.2	Data Recovery Tool – Portable data recovery system for SATA HDD/SDD					1
2.3	Data Recovery Tool – Mobile data recovery systems					1

Item Ref. #	Item name	Requirements (refer to Annex 1)	Description	Model / items reference nº	Country of origin	Quantity
2.4	Data Recovery Tool – Portable Write blockers for data recovery					1
2.5	Data Recovery Tool – Portable PCIe HDD Duplicator					1
2.6	Chip tools - Cold Chip-off station					1
2.7	Chip tools - Desoldering station					1

Bill of Quantity – Lot 3 (Digital Forensic Software Tools)

The following table contains the bill of quantity for Lot 3 which is defined above. The requirements for each item are further detailed in Annex 1 of the present document**.**

Item Ref. #	Item name	Requirements (refer to Annex 1)	Description	Model / items reference no	Country of origin	Quantity
3.1	Data Recovery Software tool					1
3.2	Smartphone Forensic Software					4
3.3	Training on Smartphone Forensic Software					1
3.4	Computer Forensic Software	(1st source with 3 years SMS)				2
3.5	Training on Computer Forensic Software					1
3.6	Computer Forensic Software – alternative solution	(2d source with 1 year SMS)				1
3.7	Computer Password Recovery Kit					1

ANNEX 7 – COMPLIANCE MATRIX TEMPLATE

This annex provides the template for the compliance matrix that must be completed by the bidder.

Compliance Matrix				
Requirement #	**Category**	**Description**	**Compliance**	**Notes**
Requirement numbers as referenced in this document	Category as expressed in this document.	Description as expressed in this document.	Refer to note 1*.	

***Note 1:**

This field must be completed with one of the following values:

- **Fully Compliant**
- **Partially Compliant**
- **Not Compliant**

Fully compliant means that the solution fully complies with the expressed requirement without any kind of reservation or deviation. In case the solution contains additional features the bidder may provide additional information in the Notes.

Partially Compliance: in case of partial compliance the bidder must describe the deviations in the Notes.

Not compliant: the bidder may provide additional information in the Notes.

Firmado por OSET SERRA MARIA ANGELES - DNI ***7952** el día 15/02/2024 con un certificado emitido por AC Sector Público