

कार्यालय
आयकर महानिदेशक (अन्वेषण)
रूमनं. 507, पांचवां मंजिल, सिंधिया हाउस
बलॉर्ड एस्टेट, मुंबई - 400001



Office of the
Director General of Income-tax (Investigation)
Room No. 507, 5TH Floor, Scindia House,
Ballard Estate, Mumbai- 400001

dgil.inv.mumbai@incometax.gov.in

Tele Fax (022) 22615700

TENDER DOCUMENT

For Empanelment of Digital Forensics and Data Analysis Service providers for all offices under the administrative control of the Director General of Income Tax (Investigation), Mumbai

INDEX

Section	Particulars	Pages
	Notice Inviting Tender	2-3
I	Scope of Work and other conditions:	4-16
	A. Summary of the job work	4
	B. Technical Qualifications for eligibility	5-6
	C. Special requirements for eligibility	6-9
	D. Ability to document Digital Forensics and Data Analysis for the purposes of the Bhartiya Sakshya Adhiniyam	10
	E. Specific requirements for Manpower and Technical Resources	11-12
	F. Qualifications/skill requirements of Service Provider Personnel	13-14
	G. Eligibility to engage the processing possibilities of a State-of-the-Art Cyber Forensics Lab and training of ITD officials	15
	H. Capacity to deploy Forensic teams at distant geographical locations anywhere in the Country at short notice	16
II	Instructions for the prospective service providers	17-18
III	Indemnity Clauses and Terms of the Contract	19-21
IV	Pricing Model & Terms of Payment	22-23
V	Non-disclosure clauses	24-25
VI	Tendering Process	26-31
	A. Six Stages	26
	B. Two Bids	26
	C. Technical Bid	27
	D. Deadlines for submission of bids	27-28
	E. Modifications to Bids	28
	F. Disqualification	28-29
	G. Opening of Technical Bids	29
	H. Evaluation Method	29-30
	I. Opening and evaluation of Financial Bids	30
	J. Requests for Information	31
VII	Annexure – A (Profile of Organization)	32
	Annexure - B Technical Bid	33
	Annexure – C Financial Bid for Digital Forensics and Data Analysis Work	34-36



Ask

कार्यालय
आयकर महानिदेशक (अन्वेषण)
रूम नं. 507, पांचवां मंजिल, सिंधिया हाउस
बलॉर्ड एस्टेट, मुंबई - 400001



Office of the
Director General of Income-tax (Investigation)
Room No. 507, 5TH Floor, Scindia House,
Ballard Estate, Mumbai- 400001

dg.it.inv.mumbai@incometax.gov.in

Tele Fax (022) 22615700

F.No. Tender Committee/Data Forensic & Analysis/2025-26/

Date: 21.01.2026

**NOTICE INVITING TENDERING FOR EMPANELMENT OF
DIGITAL FORENSICS AND DATA ANALYSIS SERVICE PROVIDERS**

1. The Directorate of Income Tax (Investigation), Mumbai invites tenders in sealed covers from eligible, bona-fide, reliable and resourceful service providers experienced in the field of Digital Forensics and Data Analysis Services for the office of the Director General of Income Tax (Investigation), Mumbai. The empanelment shall be for a period of **three years w.e.f from 02.03.2026 to 28.02.2029** which may be extended for another two years, one year at a time at the administrative convenience of the Director General of Income Tax (Investigation), Mumbai, subject to satisfactory performance of the empaneled service providers.
2. The Offer should be submitted in 2 (two) bid pattern, i.e. (i) **Technical bid** and (ii) **Financial bid**. The Offer submitted for both the bids are to be placed in two separate sealed envelopes (clearly superscribing 'Technical bid' and 'Financial bid') which in turn should be placed in **one single sealed cover**, duly superscribed "**Tenders for empanelment of Digital Forensics and Data Analysis Services for the office of the Director General of Income Tax (Investigation), Mumbai**" and addressed to "The Chairman, Tender Committee and Addl. Director of Income Tax (Investigation), Unit-4, Mumbai" so as to reach the office of the Chairman, Tender Committee, Mumbai, not later than 06:00 P.M. on 10th February, 2026. The correspondence address for submissions of bids is as under:-

**"O/o. Addl.DIT (Investigation), Unit-4 and Chairman, Tender Committee,
Mumbai, 2nd floor,
Scindia House, Ballard Estate, Mumbai-400 001"**

3. The Technical Bid will be opened on 11th February, 2026 at 3.00 P.M., and the Financial Bid on 12th February, 2026 at 3.00 P.M. The Financial Bid of only those Service Providers shall be opened whose technical bid (inclusive of profile of applicant Service Provider) are found eligible in the presence of the Vendors or their representatives who may likely to be present. Detailed information / terms and conditions for the purpose can either be downloaded from www.incometaxindia.gov.in or www.eprocure.gov.in or www.incometaxmumbai.gov.in or Government E-Marketplace (GeM) or Tender Documents can also be collected from the above mentioned office address between 11:30 A.M. to 05:00 P.M. on all working days upto 09th February, 2026.
4. Critical dates of the tender are as under: -

Stage	Time & Date	Place
Last date of availability of tender documents	09 th February, 2026	1. www.eprocure.gov.in 2. www.incometaxindia.gov.in 3. www.incometaxmumbai.gov.in 4. Government E-Marketplace (GeM) 5. Office of Addl. DIT (Inv), Unit-4, Mumbai, 2 nd floor, Scindia House, Ballard Estate, Mumbai-400 001



Ark

Last date for submission of tender documents	06:00 P.M. on 10 th February, 2026	Office of Addl. DIT (Inv), Unit-4, Mumbai, 2nd floor, Scindia House, Ballard Estate, Mumbai-400 001 [The Tender document is to be submitted mandatorily in physical form.]
Opening of tenders:-	03:00 PM on 11 th February, 2026	5 th floor Conference Room, Scindia House, Ballard Estate, Mumbai-400001.
(a) Technical Bid	03:00 PM on 12 th February, 2026	
(b) Financial Bid	03:00 PM on 13 th February, 2026	
(c) Declaration of Bid	03:00 PM on 13 th February, 2026	



Abirama 21.1.26
(S ABIRAMA KARTHIKEYAN)
Addl. DIT (Inv.), Unit-4,
Mumbai
In capacity of Chairman of
Tender Committee

1). The Income Tax Officer (Hqrs) System, Aayakar Bhavan, Mumbai with a request for uploading the Tender Advertisement along with its Annexures on the Department's Official Mumbai Website (www.incometaxmumbai.gov.in) and Income Tax Official Website (www.incometaxindia.gov.in).

2). The ITO(HQ) to PDIT(Investigation)-2, Mumbai with a request to upload the Tender Advertisement along with its all Annexures on Central Public Procurement Portal and Government e-Marketplace (GeM).



Abirama 21.1.26
Addl. DIT (Inv.), Unit-4,
Mumbai
In capacity of Chairman of
Tender Committee

I. Scope of Work and Other Conditions

A. *Summary of the job work*

1. The quotes are being invited for Digital Forensics and Data Analysis Work. These broad categories of services include in their gamut a vast spectrum of jobs that are elaborated upon in this scope outline.

1.1 At the outset, the Service Provider should have the capability to carry out Digital Forensics & Data Analysis and allied services including:

- Password-breaking in all possible OS environments, mobile platforms. This may include springboarding and jailbreaking for iOS devices, and Rooting for Android devices to access data when the target person is non-cooperative.
- Remote access of databases through VPN/SSID based applications or other such architecture in use by present day businesses spread over distant geographical locations for storage and recovery of financial data,
- Recovery of deleted data and
- Analysis of electronic data/electronic evidence assigned to it by the Income tax Department¹ ("ITD") and submit a report in writing for the purposes of the Bharatiya Sakshya Adhiniyam, 2023.
- Review and Analysis of Data shall include, but not be limited to, Bank Statement Analysis, Analysis of emails, social media chats, financial data on applications like Tally, Tally ERP, SAP, Oracle or any other customized RDBMS application using **software** tools, database Analysis through software tools etc., relationship resolution & presentation of analyzed data.
- This in turn may include small pieces of software coding.

¹ In this Document, the terms 'Department', 'Income Tax Department', 'ITD', 'DGIT' 'PDIT' have been used. All these expressions interchangeably mean 'the office of the Director General of income Tax (Investigation), Mumbai' for the purposes of this document.



Ark.

B. Technical Qualifications for eligibility

2.1 The vendor shall possess the capacity to do **Computer backup and imaging work (including laptops, desktops, servers, smartphones and any electronic computing device which can store and process financial and business process data by whatever name called) using forensic software at the time of Search, Seizure and Survey Action** (Examination of digital device for suspected evidence and acquisition of digital evidence involving backup, copying, Imaging and cloning)

2.1.1 The vendor shall possess capability to do a fair **Forensic acquisition** involving collection of data in a forensically sound manner using licensed, open-sourced tools depending upon the operating system. The devices include servers, desktops, mobile phones, **cloud data in mobile phones and third-party cloud services**. The vendor should have capability to access remote/networks and determine hidden systems and servers which are being used for various purposes during the course of search action.

2.1.2 The vendor shall possess capability to do **Data Extraction and Data Remediation** which includes extraction of data from forensic formats such as **E01, EX01, DD, AFF, etc.** into native formats such as **Word, Excel, PDF, SQL, etc.** The vendor should have capability to do Data Remediation including de- duplication of data, removal of system files, culling of files based on files types and partition wise reduction of repeated data and presentation of data in readable formats (Native files).

2.1.3 **The personnel of the vendors shall be qualified to stand as expert witness in courts to describe and defend the methodologies adopted during any of the stages involved in Data Acquisition, Processing, Analyzing, and Presenting.**

2.1.4 The Vendor shall possess capability to do **Basic Data presentations** in which the forensic vendor is expected to perform comprehensive restructuring of data and provide the data which is usable by the Authorized officer for his investigative requirements. This includes providing metadata information, file signature information, and deleted data information and data reconstructed information.

2.1.5 The vendor shall possess capability to locate, identify and analyze encrypted files. Further, the vendor shall also possess capability to break encryption, crack password and access hidden data; the vendor shall then be able to provide such recovered decrypted/password-cracked/unhidden data in a readable format

2.1.6 **Mobile and Tablet backup** (examination of mobile/tablet, examine for suspected evidence & acquisition of digital evidence involving backup, copying imaging cloning)

- The vendor shall possess capability to do **Forensic acquisition** involving collection of data from mobiles, tablets in a forensically sound manner using licensed/open-sourced tools depending upon the operating system.
- The Vendor shall possess capability to do **Data Remediation of mobile data** which includes extraction of text messages, voice notes, call records, documents, and mobile notes.
- The vendor shall possess capability to do **Data retrieval from mobile applications** (wherever possible and applicable), logical examination of mobile phones and determining whether logical backups or physical backups to be taken and perform the specified activity with concurrence from the Authorized Officer.

3.1 **Recovery of Deleted files:** The vendor shall possess capability to do **Data retrieval services**



Ad

from computers which include retrieving data from servers where data has been deleted and/ or databases have been modified, using retrieval techniques from the log files. Where log files are not available, reconstruction of respective data bases using third party tools may be adopted.

3.2 The vendor shall possess capability to **recreate from partial recovered data** in areas of file signatures, deleted files, recreation of partially broken files, carving of partially overwritten files, and reconstruction of broken databases.

4.1 Analysis of data: The vendor shall possess capability to do basic **Investigative analytics** in which, where required, the authorized officer may seek the assistance of the forensics team to perform database interpretations, email keyword searches, normal Web searches, or any other relevant support activities relating to electronic devices and evidences during the conduct of search and vendor shall be capable of same.

4.1.1 The vendor shall possess capability to handle large volume of data in disparate forms; the vendor should also have the tools to index the large volume of data so that the data from disparate sources in various file formats becomes query-abled. The vendor shall possess capability to identify relationships between various data items and provide deep insight into the data being analyzed. Such large data may include Stock Exchange Trade Data/ Commodity Exchange data related to shares, debentures, scrips, futures and options etc.; bank statements; cash flows/ fund trails

4.1.2 The vendor shall possess capability to present the analyzed data in appealing, intuitive and illustrative visualizations. The vendor shall be in a position to employ various visualization tools that may require custom coding as well.



Aak

C. Special requirements for eligibility

5. Over many years of experience with digital data retrieval and analysis ITD officers have become well- acquainted with the possible situations faced by search teams for locating and accessing relevant data and the technology deployed by target persons to conceal data. It is therefore expected of the prospective service providers to match the organizational skill set and to augment it with technical know-how and latest s/w and h/w tools to deal with difficulties faced in getting timely access to financial data, which is at the core of any successful search/survey action by the ITD. Some possible scenarios have been outlined below to give a fair idea to the bidders of the level and scope of forensic support expected of them. It may be clearly understood here that **these anecdotal accounts of the data forensic scenarios are just a few examples of the nature of job requirements to give a perspective to the bidders. The scope of work is certainly broader and much varied not limited to these scenarios.**

Scenario 1: Password Breaking

5.1.1 We usually find encryption in different type of devices and files like mobiles, desktops, laptops, hard drives, document files and tally data. In these cases, password breaking starts with the use of a forensic software like Passware, Access data FTK etc. which have their own dictionaries (thousands of possible passwords which can be alphabets, alphanumeric, numbers, symbols, uppercase and lowercase, spaces etc.) and using several permutations and combinations, they recover the underlying passwords.

5.1.2 Since, password can vary from weak to strong, the software decryption timeline is a challenge and the skills and experience of the forensic team becomes a determining factor in real-time resolution of the encryption and hence, not just the s/w tools deployed but also the active skilled intervention of the forensic manpower is of utmost importance in getting a quick match. There have been situations where we have added our own dictionaries to enhance the decryption process.

5.1.3 The software tools deployed so far automatically detect the file type and complexity level of the password and offer all possible types of attacks including but not limited to dictionary attack, bruteforce attack, xieve attack etc. The task of the forensic manpower is to decide on the tradeoff between no. of types of attacks to be selected and the time taken by the recovery/decryption process.

Scenario 2: Servers Outside India

5.2.1 It is not unusual nowadays to find that database servers of target persons are situated outside India and data has to be retrieved/backed up using our own processes and methods. The forensic team should, firstly, be able to identify if any server is maintained outside India using IP addresses. Then, we take access of the live/running remote server using the credentials which are gathered by asking the target person but in this process, it is for the forensic team to identify the admin who controls the maximum rights of the server.

5.2.2 Once the server data (Accounting, Finance, Stock etc.) is accessed we identify its validity and put checks on the last updation of the data in the server. This is the most significant part of the exercise because evidentiary value of the data has to be ensured and the Forensic team should be able to document the process deployed for accessing the data and categorically ensure that the correct data retrieval and data integrity checks have been put in place while backing up the data.

5.2.3 An important task for the forensic team in such cases is to check if the host of the server is a third- party entity like AWS (Amazon), Microsoft Azure, Salesforce etc. While the host can be the same organization entity/target group but very often such remote servers are hosted by data service providers or cloud service providers. The forensic team should be well-conversant with the procedures/Industry practices for obtaining access to database servers from such third-party hosts.

5.2.4 Once the host is identified, we have to check the configuration of the server as in size of



Ark

database, application size, machine infrastructure, client-side configuration. Since, database is running on the live server, it is usually in raw form and size is voluminous, which makes it necessary to create a backup of the database which is then compressed for its use. After this compressed database is backed up, it is essential for the forensic team to verify and certify the validity of the database i.e. the backup matches with the live data and contains all the updated transactions and summary as required.

5.2.5 The compressed back-up of the database is downloaded by the forensic team along with the application setup files (*where application is executable setup file*) which are connected to the server side. Most importantly, for the evidence purpose, the forensic team has to do the hashing of the application and database downloaded.

5.2.6 After data and front end is downloaded the target persons/organization are asked to arrange an idle machine where this downloaded database and application can be run to create a cloned/dummy/temp server which will replicate the original server. This arrangement has to be achieved during the search action so as to allow for accessing and analysis/investigation by the search team. The forensic manpower has the pivotal role in obtaining and providing data access in readable form to the search team.

Scenario 3: If the remote database uses an application which is web based

5.3 A greater level of complexity is posed by remote servers if the application is web based, and in such situations, we have to create a cloud instance to make a live environment for the database application to run. The database will be separated and isolated and is restored on the cloud space. The server-side application is installed and connected with the database. A major difference in the process deployed here is that the linkage established between the application and database is based on hostname-based configuration and not IP-based configuration. Thereafter, the application is run and tested to check if the database connection is foolproof. Sometimes, all modules and reporting features in the application may not work properly, and the forensic team should have the expertise for troubleshooting or coding required in the backend. Finally, the working of the server and data validity has to be verified from the client-side and query reports and data have to be checked against the live server.

Scenario 4: When Database is present in India but at different location and size of database is large to be downloaded locally.

5.4 A peculiar situation was faced in the case of an organization which was using two different servers for different time periods, specifically for financial years 2010-2020 a database server, say V1 and from financial year 2020 onwards another server, say V2. The V1 server database was hosted by a CSP (Cloud service provider) which was in India at a Mumbai location. V2 was with another third Party CSP (Cloud service provider) in India, say AWS.

- The combined size of the databases of both V1 & V2 servers was 1 TB approx. and could not be downloaded at the premises because of technical and network difficulties. The database was downloaded at the Mumbai data center after proper hashing and validation, and it was then brought to the main premise in Mumbai. V2 server database (back-up) was uploaded in cloud and web-based application was linked to this server and it was made up and running.
- Now, in the case of V2 server, the application setup files were readily available since it was up and running, but due to migration from V1 to V2, the older application was not available for running operations and it was difficult to obtain the setup files. Also, since the V1 server was an older version and not in use, it was found full of bugs and issues like missing modules.
- Therefore, for the V1 database, a local server was created by restoring the database and installing the necessary application. But due to the bugs which were found in the application program, some reporting features were not working properly for which backend queries had to be run and reports were fetched manually using DB Queries.



Ark

Scenario 5: ERP Environment

5.5 Increasingly, all financial data is found stored and managed on ERP solutions and the forensic teams are frequently called upon to create an ERP environment (temp server) for retrieval of imaged data on the customized application taken from the assessee i.e. tables and codes of each database/master files of the ERP application. The backend of such ERP temp server can include but is not limited to Oracle, SAP and other commonly known ERP solutions.

6. Besides the above-described data retrieval scenarios, in general, the service provider shall possess capacity to track **cloud hosting servers** based on database logs retrieved from the physical devices found at the search premises.

6.1 Further, the prospective bidders should have technical experts well-versed with Basic Cloud Services like Compute Service, Storage Service, Network Service, Database Service, Security Service, Support Service ; Advanced Cloud Services consisting of Container Service, Managed Database as a Service, Content Delivery Network, MPLS Connectivity, HSM, DDoS, TLS / SSL Certificate Management, Dual / Multi Factor Authentication, Monitoring Services, Analytics Services ; and Managed Services consisting of Disaster Recovery as a Service and Backup as a Service. The data forensic service providers should have thorough knowledge of cloud deployment models especially Virtual Private Cloud (VPC), and cloud service models including Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

6.2 As a proof of eligibility on this account the prospective bidders shall certify their work experience with any of the major cloud service providers in India i.e. Amazon Web Services India Private Limited, Oracle India Pvt. Ltd, Bharat Sanchar Nigam Limited (BSNL), Cyfuture India Private Limited, ESDS Software solution Pvt. Limited, Google Cloud India Pvt Ltd ,IBM India Private Limited , ITI Limited , Jio Platforms Limited , Microsoft Corporation (India) Private Limited , Netmagic IT Services Private Limited , Nextra Data Limited , Pi Datacenters Pvt. Ltd., RailTel Corporation of India Limited ,Sify Technologies Limited ,Tata Communications Limited, Webwerks India Pvt. Limited , Yotta Infrastructure Solutions Pvt. Ltd. ,Tata Consultancy Services Limited , and Protean eGov Technologies Limited.



Arkh

D. Ability to document Digital Forensics and Data Analysis for the purposes of the Bharatiya Sakshya Adhiniyam, 2023.

7. Data Forensics and Data Analysis Report:- The Service Provider shall carry out forensic analysis of electronic data/electronic evidence assigned to it by the ITD and submit a report in writing.

7.1 Standard Operating Procedures to be followed and recorded in the report:- Service Provider shall carry out restoration & analysis as per Standard Operating Procedure of the Income Tax Department as issued for handling of digital evidence, and as per legal requirements to preserve the legal sanctity and evidentiary value of the data/electronic evidence. Service Provider shall carry out forensic acquisition, restoration & analysis as per prevailing industry technical standards for handling digital data and devices. The standards should meet the legal requirements of Bharatiya Sakshya Adhiniyam and any guidelines that may be issued by the ITD to preserve the legal sanctity and evidentiary value of the data/electronic evidence. A fair extraction of the data should be carried out. Any deviation from the standards shall lead to penal actions which can range from blacklisting of the vendors to prosecution under the relevant laws.

7.2 The report, after analysis, will, inter alia, categorize/group electronic data as under:

7.2.1 Deleted data:

- All types of files including mails/excel files/Doc. Files/ PDF files/Scanned Images/Pictures etc.
- Data files for TALLY or any other accounting software like ERP Packages.
- Data Files with respect to any database software like SQL, Post GRESQL, Microsoft Access etc.
- Data hidden in unallocated sectors/Data hidden in pictures or scanned images.
- Data in mobile phones, tablets, pen drives or any other electronic devices.
- Encrypted Data/Password Protected Data including excel files/Doc Files/PDF Files/RAR Files/ZIP Files etc.
- Log Files including Circular Logs/Flat Logs

7.2.2 Non-deleted data

- All types of files including mails/excel files/Doc. files/ PDF files/scanned Images/Pictures etc.
- Data files for TALLY or any other accounting software like ERP Packages.
- Data Files with respect to any database software like SQL, Post GRESQL and Microsoft Access etc.
- Data hidden in unallocated sectors/Data hidden in pictures or scanned images.
- Data in mobile phones, tablets, pen drives or any other electronic devices.
- Encrypted Data including excel files/Doc Files/PDF Files/RAR Files/ZIP Files etc.
- Log Files including Circular Logs/Flat Logs

7.3 Report shall specify the exact path of the files, salient features/ peculiar characteristics /time signatures, hash values etc.

7.4 The Service Provider shall also aid in carrying out such investigation as required by Investigation Officer including password removal and breaking, text Search, forensic analysis of software system and incorporate the outcome along with its basis in the report.



E. Specific requirements for Manpower and Technical Resources

8. In respect of the above, the service provider shall deploy qualified Manpower & utilize latest software and hardware tools.

8.1 The Service Provider shall use original, authentic and licensed/authorized hardware and software tools for the purpose of legally sound forensic analysis of electronic data/electronic evidence for fair extraction of data. The service provider shall not use pirated software or unlicensed tools. The tools should be state of the art with licenses purchased for automatic upgrades as and when they are rolled out. **The tool(s) should have full capability for the following:**

8.1.1 Analysis of mobile data including images, screenshots, voice messages etc. and extraction of data including WhatsApp/Telegram/Other messaging app messages (or a method to access all such messages) in all devices including Apple, Android and Blackberry devices (to the maximum possible extent of breaking encryptions).

8.1.2 Recovery and restoration of all data from all sectors of the electronic media and devices.

8.1.3 Recovery and restoration of all forms of email on the cloud and mail servers or laptops in OST, PST, DBX, MBOX, MSG, EML, TXT, RTF, HTML, MHTML and other formats.

8.2 Irrespective of the tools utilized for data extraction and analysis, the service provider shall ensure that the forensic analysis data is provided to the investigation officer in a readable and accessible digital format on the device specified by the investigating officer.

8.3 The vendor should have at their disposal the following tools (or similar priced ones) as shown in the in the table below: -

Sr. No	Tools	Same or similar globally accepted tools
1	Hardware Write Blockers	CRU Write blocker/Tableau write blocker
2	Software Write blockers	Safe Block
3	Forensic Hardware based Imager & cloners	Falcon imager/ Logic Cube Tableau Imager TD3/ Tableau Imager, Magnet, Paraben, TX 1
4	Forensic Software Imagers/ Cloners	Encase 7 & above, Forensic Tool kit, Magnet axiom, Paraben forensic replicator etc.
5	Forensic Software Imagers/ Cloners for Apple	Macquisition for Mac, Recon imager for Mac, Paladin for Mac
6	Forensic Data Extraction Platforms	Xways Forensics, OS Forensics, Encase, Forensic Tool Kit, Magnet Axiom etc.
7	Data recovery	X-Ways Forensics/ Encase/Forensic Tool Kit
8	Mobile Phone Acquisition and platforms	Cellebrite UFED touch/ UFED 4PC; Oxygen Investigator/ detective; MobileEdit Express/ Magnet Axiom with Mobile Forensics module, Paraben Device seizure, Encase Mobile
9	Licensed mobile date/backup tools	UFED Physical analyzer/ Oxygen detective
10	Mobile Phone Data Recovery tools for Apple, android and other Mobile OS	Phone Rescue, Dr. Fone, etc.



(Signature)

Sr. No	Tools	Same or similar globally accepted tools
11	Data recovery and Deleted file recovery tools	Ontrack data recovery, Stellar Data Recovery, 7 safe Data Recovery, Disk driller for Mac, etc.
12	Cloud Data acquisition tools	Intella, Mail Xaminer, Nuix analyser, SPF, Magnet Cloud, F response, UFED cloud analyser, Encase Cloud, FTK Cloud
13	Non forensic Backup tools	Macrium Reflect, Acronis True Image, Norton Ghost etc.
14	Email acquisition tools	Paraben Email Analyser, Mail Xaminer, OS forensic Software, Intella email Platform etc.
15	Other Relevant Tools including Database Migration	SQL rebuilder/ Oracle Extractor, DB2 Analyser etc.
16	AI based Data Analysis Tools for data mining, analysis and visualisation	RapidMiner, Tableau, Microsoft Azure Machine Learning, KNIME, Google Cloud AutoML, PyTorch, DataRobot, Talend, H2O.ai, IBM Watson Analytics etc.

8.3.1 Tools given above are only a representative list. Alternative tools with same or similar capability can be considered as replacement with approval of the Department. The Vendor should provide proof of the existence of the above-mentioned tools. The vendor should be able to provide ad hoc tools that may be required from time to time during the period of the existence of the Contract.

8.3.2 It is emphasized here that preference shall be given to Data Analysis service providers who can deploy AI based tools using deep learning algorithms to find patterns in the Dataset which have immediate value to the investigation, or using machine learning to enable more accurate and self-improving keyword search and, since common themes and modus operandi are seen across different searches, such tools should enable utilization of machine learning/deep learning acquired during one search in subsequent searches/projects.



Ask

F. Qualifications/skill requirements of Service Provider Personnel

8.4 The Applicant Service Provider entity or their promoters should have qualified digital forensic specialists with **minimum 3 years of experience** preferably handling the cases relating to Investigation Wing of Income tax Department or other Central/State Enforcement Agencies and should possess all updated forensic instruments such as oxygen forensic, encase etc.

Forensic Services

8.4.1 The Service Provider personnel required for forensic analysis of electronic data/electronic evidence which include off-site restoration and examination of electronic data/electronic evidence must possess at least the minimum knowledge and skills required for this purpose including (but not limited to) the following:

8.4.1.1 Proficiency in using forensic hardware and software tools like Lazesoft, Windows Shell, bash, Nirxlauncher, FTK Imager, Belcasoft, Dumpit, Password Recovery, Oxygen, Cellebrite, hardware based forensic cloners and imagers like Tableau TX1, Tableau TD2u, Magnet Axiom, OpenText Encase, Mobile phone acquisition, backup, data recovery tools for Apple, Android based devices like Cellebrite UFED 4PC etc.

8.4.1.2 Proficiency in using Tableau duplicators, Encase forensics, Password, write-blockers and other latest tools.

8.4.1.3 Proficiency in Relational Database Management Systems like Oracle/Microsoft SQL, etc.

8.4.1.4 The personnel deployed should be proficient in usage of various types of digital systems including mobile phones, memory chips/cards, cloud computing systems, servers, other remote data systems/networks/ Nirxlauncher etc

8.4.1.5 Proficiency in assessing electronic data/files/records/emails/chats/communications/images i-cloud etc. including by way of breaking of passwords and forensic & financial analysis of the same.

8.4.1.6 Proficiency in various versions of Operating Systems like Windows, Linux, MacOS, Android, Ios etc.

8.4.1.7 Proficiency in TALLY/ERP and similar accounting software tools including latest tools such as SAP, etc and analysis of financial statements.

8.4.1.8 The forensic team at its backend should be headed by from financial background like CA to assist in digital forensic analysis. The analysis team may consist of 4 to 5 members. The team members should be a graduate with strong financial and analytical background.

8.4.1.9 Proficiency in representing data in tables/charts/excel based files and jobs of similar nature.

8.4.1.10 Well versed with relevant laws applicable to the area of electronic evidence including relevant provisions of the Information Technology Act, Bharatiya Sakshya Adhiniyam, 2023.

8.4.2 The forensic team provided by each bidder shall preferably have at least 7 (seven) members comprising of:

(a) At least 4 (four) technical persons with necessary qualifications and having knowledge of



Ark

accounting, forensics and computer.

(b) No under trainee personnel shall be deployed to execute the project work.

Data Analysis Services

8.4.3 The Service Provider personnel required for data analysis must be qualified data analysts and possess at least the minimum knowledge and skills required for this purpose including the following:

8.4.3.1 Ability to gather, view, and analyze large volume of data that may be present in various disparate formats.

8.4.3.2 Proficiency in spreadsheet programs like MS Excel.

8.4.3.3 Knowledge of Python, Power BI, SQL, R and MATLAB.

8.4.3.4 Skilled at data visualization and capability to present reports in a format as required. Should be skilled at creating clean, visually compelling charts that will help understand the data.

8.4.3.5 Strong logical skills and statistical knowledge



G. Eligibility to engage the processing possibilities of a State-of-the-Art Cyber Forensics Lab and training of ITD officials

9.1 Cyber Forensics Lab and the requirement to meet state-of the art best practices:
Preference will be given to Service Providers who can deploy servers/solutions on which data of multiple projects/ searches as available with the investigating officers can be kept for an all data or device-cluster keyword search using big data analytics.

Training of ITD officials

9.2 As pointed out at para 5 above, while the ITD human resource has had a long learning curve by way of years of collective experience in data forensics, there are frequent and continuous changes/improvements in the state of the Art, which requires that the learning curve should be steeper. In order to build synchrony with the Investigation teams, the Forensic service providers shall take up free-of-charge training sessions to give hands-on training to ITD officers/officials so as to acquaint them with the latest technological advancements in the areas of data imaging, extraction and analysis, covering various architectural designs of databases, procedural issues, and software tools for all requirements of data retrieval, integrity, back-up, and analysis. Every month a minimum 1 such session shall be taken by qualified/certified trainers engaged by the Service Providers using live examples from situations faced during searches.



[Handwritten signature]

H. Capacity to deploy Forensic teams at distant geographical locations anywhere in the Country at short notice

10. Onsite forensic analysis of electronic evidence/during search operation

10.1 In addition to the forensic analysis of electronic data/electronic evidence which the Service Provider would generally be required to do in the Income-tax Office, it may be required to do these activities at the site out of the office also. For this purpose, whenever required, Service Provider shall be able to depute sufficient number of technically qualified personnel with requisite hardware and software tools at short notice, for onsite forensic analysis of electronic evidence, away from the office in and outside Mumbai (anywhere in the Country). In case of requirement for more technically qualified personnel the Service Provider shall ensure that adequate manpower for the same is provided immediately.

10.2 The Service Provider personnel are required to use their own hardware excluding storage devices (hard disk, pen drive etc.) and software tools for imaging/back up etc. for the above purpose. The Service Provider shall ensure that the hardware and software tools are of high quality. The storage devices (hard disk, pen drive etc.) shall be provided by the ITD.

10.3 The Service Provider shall ensure that adequate man power is made available for forensic analysis/out of office duty in Mumbai. The Service Provider personnel may also be required to travel to any part of India for the above purpose.

10.4 The Service Provider personnel may have to accompany the search & survey teams for the above purpose.

10.5 For out of office premises duty, no additional remuneration or charges shall be payable to the Service Provider/Service Provider personnel.

10.6 Out of office duty may stretch multiple days at a time. Service Provider shall ensure that the personnel are made available for the entire duration for proper conduct of official work of ITD.

10.7 It is also highly necessary that the successful Forensic service providers once empaneled at Mumbai, should be able to engage with their counterparts empaneled by other DGIT Charges so as to get their services with the same procedural rigour and quality as has been mandated by DGIT(Inv.) Mumbai. In other words, in case services of another vendor engaged by another DGIT Charge anywhere in India, are necessitated to be hired for the reason that the search premises lies in the other jurisdiction or any remote station, where the Mumbai Service provider is unable to provide its manpower, then the Mumbai Service provider shall be responsible for ensuring that the quality of service provided by the other/outside vendor is at par with that expected of the Service provider at Mumbai and other guidelines for handling digital evidence are strictly adhered to by that other /outside vender.



II. Other mandatory conditions and general Instructions for the prospective service providers

11.1 The Bidders are advised to study the tender document carefully. Submission of Tender shall be deemed to have been done after careful study and examination of the tender document with full understanding of its implications. Failure to furnish all information responsive to those mentioned in the tender documents or submission of a proposal not substantially responsive to tender conditions may result in rejection of the proposal.

11.2 The quotes are being invited for Digital Forensics and Data Analysis service. The L1 quote for each service will be published and all the qualified bidders shall be provided an opportunity to match the L1 quote in each service. All the qualified bidders who match L1 quote shall be empaneled.

11.3 The office of the DGIT (Investigation), Mumbai makes no commitments, explicit or implicit, that this process will result in a business transaction with anyone. This Tender does not constitute an offer by the department. The bidder's participation in this process may result in selecting the L-1 bidder and further to invite other bidder for empanelment at L-1 rates. The commencement of such empanelment does not, however, signify a commitment by the department to award the bid. The department also reserves the right to accept or reject any bid, and to annul the bidding process at any time, without thereby incurring any liability to the affected Bidder or Bidders. **The offer is only for empanelment and the same would not amount to any work contract or surety with reference to allotment of work.**

11.4 The Bidder should have a reputed client base. The client list should be submitted with the bid.

11.5 The Technical Bid should accompany requisite documents. The Financial Bid shall be submitted separately. The Bidder name, telephone number and complete mailing address shall be indicated.

11.6 If for any reason, it is found that the Technical Bid reveals the Financial Bid related details in any manner whatsoever, the Bid documents will be summarily rejected in the first instance itself.

11.7 All the Bid document submitted shall be serially page numbered and contain the table of contents with the page numbers.

11.8 The annual turnover of bidders in the field of forensic analysis or audit and financial audit services shall be not less than average of Rs. 50 Lakhs in the two preceding financial year i.e., FY 2023-24 and FY 2024-25. In support of this, the Service Providers shall submit self-certified copies of Return of Income filed with the Income Tax Department. The Bidders who are registered under MSME and Startup India companies/ firm/ proprietary will be exempt.

11.9 The Bidders should ensure that the resource persons are made available as and when required by the officers of the office of the Director General of Income Tax (Inv), Mumbai.

11.10 As and when required, the resource person should be ready to travel to any premises within India, and assist them for acquiring of data, retrieval, analysis etc., including requisition at very short notice.

11.11 The Bidder should ensure compliance of strict confidentiality of data and procedures, as the matter dealt with will be of high sensitivity and utmost importance.

11.12 The Income Tax Department reserves the right of accepting the whole or any part of the quotation received and the Bidder shall be bound to perform the same at the rates quoted.

11.13 A consolidated bill will be submitted after completion of the work for payment. The bills have



to be supported by the attendance sheet of the personnels of the service provider accessing the Digital and Intelligence Lab located inside the premises of the office of the DGIT(Inv), Mumbai. The bills will be countersigned by the relevant officers before submitting the same for financial sanction after ascertaining the authenticity of number of hours put-in by the service provider for the project assigned to it. The bills will be cleared within a reasonable time. However, in case of any unexpected delay, the contractor should be in a position to offer credit facility for the period.

11.14 TDS will be made as per law.

11.15 The contract can be terminated at any time after giving **one-month notice** without assigning any reason by the Department and two months' notice by the contractor.

11.16 If the performance of the personnel provided by the Service Provider is not found satisfactory, the Director General of Income-tax (Investigation), Mumbai shall have power to terminate the contract with one month's notice.

11.17 The Income-tax Department, without assigning any reasons, reserves the right to accept or reject any bid, and to annul the bidding process and reject all bids at any time, without thereby incurring any liability to the affected Bidder or Bidders or any obligations to inform the affected Bidder or bidders of the grounds for the action taken by the Income-tax Department.

11.18 The Bidder shall sign his bid with the exact name of the concern which is sought to be empaneled as Service Provider. The Bid document filed by the Bidder shall be typed. No overwriting or cuttings shall be permitted.

11.19 The Service Provider shall not subcontract or permit anyone other than himself to perform any of the work, service or other performance required of the Service Provider under the contract.

11.20 Once the project has concluded/or contract is terminated, the Service Provider shall not keep any data or metadata pertaining to it in any format or in a medium which can be recovered or restored through any means. The certificate and evidence to this effect shall be presented to the department in every project and the violation of the same shall attract severe **penal action** against the Service Provider. The service provider shall enter into a **separate Non-disclosure agreement** with the O/o DGIT (Investigation), Mumbai.

11.21 In the event that new services, not originally covered under the scope of this contract, are required during the contract period, the Income-tax Department reserves the right to obtain competitive rates for such services from empaneled vendors.

11.22 The Income-tax Department reserves the right to empanel new vendors on terms and conditions equivalent to those of existing empaneled vendors.



Read and accepted.
Date Signature and stamp of the Bidder
or Authorized signatory, Place

III. Indemnity Conditions and terms of the Contract

12. No alteration shall be made in any of the terms and conditions of the bid document by scoring out. In the submitted bid, no variation in the conditions shall be admissible. Bids not complying with the terms and conditions listed in this section are liable to be ignored.

12.1 No bid will be considered unless and until all the pages / documents comprising the Bid are properly signed and stamped only by the persons authorized to do so.

12.2 In the event of bid being accepted, the bid will be converted into a contract, which will be governed by the terms and conditions given in the bid document. The instructions to bidders at Section II shall also form part of the contract and shall be duly signed and stamped by the bidder and uploaded with the Technical Bid.

12.3 The terms and conditions of contract given in this section, along with profile of the applicant Service Provider, as prescribed in the Annexure-A, shall be signed and enclosed with the 'Technical Bid', otherwise the tender will be rejected.

12.4 The Income-tax Department does not bind itself to accept the lowest bid.

12.5 Any change in the constitution of the concern of the Service Provider shall be notified forthwith by the Service Provider in writing to the Income-tax Department and such change shall not relieve any former member of the concern from any liability under the contract.

12.6 The Service Provider shall acknowledge that it has made itself fully acquainted with all the conditions and circumstances under which the services required under the contract will have to be provided and the terms, clauses and conditions, specifications and other details of the contract. The Service Provider shall not plead ignorance on any matter as an excuse for deficiency in service or failure to perform or with a view to asking for increase of any rates agreed to the contract or to evading any of its obligations under the contract. In the event of the Service Provider failing to fulfil or committing any breach of any of the terms and conditions of this contract or indulge in following omission or commission then without prejudice to the Income-tax department's rights and remedies to which otherwise, Income-tax department, shall be entitled, the contract shall be terminated forthwith.

12.7 The ITD shall have the right to blacklist such defaulting Service Provider and execute the work or arrange otherwise, at the Service Provider's risk and at the absolute discretion of the Income-tax Department. The cost of such works together with all incidental charges or expenses shall be recoverable from the Service Provider:-

- If the Service Provider or its agents or employees are found guilty of fraud in respect of the contract or any other contract entered into by the Service Provider or any of his partners or representatives thereof with the Income-tax Department; or
- If the Service Provider or any of its partner becomes insolvent or applies for relief as insolvent debtor or commences any insolvency proceedings or makes any composition with its/their creditors or attempts to do so; or if
- At any time during the pendency of the contract, it comes to the notice of the Income-tax Department that the Service Provider has misled it by giving false/incorrect information.
- If the Service provider or any of its partners or any of its employee fails to complete the allocated work or refuses to accept the allocated work or abruptly abandon the work midway.



- If the Service Provider or any of its partner or its employee shares the confidential data with any third party in contravention to the non-disclosure agreement. This blacklisting is in addition to any penalized action financially or otherwise as mentioned in the contract or in the non-disclosure agreement.

12.8 The Service Provider shall comply with all statutory liabilities and obligations of State and Central Government. The Income-tax Department shall not be liable for any contravention/non-compliance on the part of the Service Provider. Any contravention/non-compliance on the part of the Service Provider would be construed as a sufficient ground for termination of the contract at the discretion of the Income-tax Department. Notwithstanding, in the event of the Income-tax Department being imposed with any penalty/fine etc., by any Service Provider/authority due to the non-compliance/contravention on the part of the Service Provider to any statutory laws/rules/regulations etc., the Income-tax Department reserves the right to recover such fine/penalty etc., from the Service Provider by way of recovery from the bills raised by the Service Provider or by any other means.

12.9 The Income-tax Department may discontinue the contract at any point of time, by giving a notice at least 30 days before the intended date of discontinuation, and will not be liable to any additional charges or compensation payable to the Service Provider or any other person.

12.10 The Service Provider may discontinue the contract at any point of time, by giving a notice at least 60 days before the intended date for discontinuation. But, in case of discontinuation without a notice or a notice less than 60 days prior to the intended date of discontinuation. The Income-tax Department will have the right to claim damages, and recover them from the payments due to the Service Provider or by any other means.

12.11 The Service Provider shall be required to enter into an agreement on a non-judicial stamp Paper of not less than Rs. 500/- on receiving the intimation/letter of intent and to start the work with effect from date of the signing of Deed/Agreement.

Security Deposit/ Bank Guarantee

12.12 The ITD reserves the right to impose any such other conditions on the Service Providers who are finally empaneled for the works in order to safeguard the interest of the Department and the Govt. of India. Such **administrative and financial conditions** may include, inter alia, **additional indemnity clauses** and the pre-requisite of a **Security Deposit/ Bank Guarantee** for enforcement of necessary discipline and to effect recovery of damages in the event of non-performance and /or violation on the part of the service provider. Such other conditions shall be enumerated and elaborated upon in the **final contract** to be signed by the service providers eventually empaneled.



Read and accepted.
Date Signature and stamp of the
Bidder or Authorized
signatory, Place

Tenure of the contract:

12.13 Initially, this agreement shall remain in force for a period of **three years** which may be extended for another two years, one year at a time at the administrative convenience of the Director General of Income Tax (Investigation), Mumbai subject to satisfactory performance.

Arbitration:

12.14 In the event of any dispute or differences arising as to the execution of the contract or as to the respective rights or liabilities of the parties hereto or interpretation of any of clause thereof on any condition of agreement (except as to any matters the decision of which is specially provided for or the special conditions), the dispute shall be resolved in accordance with the provisions of the Arbitration & Conciliation Act, 1996 and the Rules there under and any statutory modifications thereof, for the time being in force, shall deemed to apply to the arbitration proceedings. The award of the arbitrator shall be final and binding on parties to the agreement.

Read and accepted.

Date Signature and stamp of the Bidder
or Authorized signatory, Place.



IV. Pricing Model and Terms of payment:

13. It is seen that the entire gamut of services to be hired under the broad categories of Data Forensics and Data Analysis differ in their individual nature and scope wherein some services are manpower intensive requiring intense application of mind at one end of the spectrum whereas on the other there are simple processes like imaging which are almost mechanical in practice. It is therefore decided that all prospective bidders shall submit a **standard manpower requirement** for all kinds of services to be provided separately in man-hours clearly specifying how data size is correlated to the man-hours deployed. A list enumerating the various services to be offered by the vendor for different data complexity scenarios should be included in the technical bid. At the same time financial bids shall also factor in data size for each kind of service giving a **per GB (or upto one GB) rate. However, for illustration purpose the details have called for 100 GB data size with respect to each service.**

13.1 The Service Provider shall keep a proper and comprehensive account of the resources deployed for the forensic analysis of electronic data/electronic evidence which will have to be verified by the Investigating Officer. **The details of the resources deployed should be presented for accounting for the verification of time spent on each resource along with justification for the time spent by each resource on the concerned project. Only after this verification and presentation of proper justification, the invoices will be cleared for payments.**

13.2 The Service Provider shall conduct a daily meeting at the end of each work day with the Investigating Officer to present him with the progress made in the analysis and submit a report of the major findings and the man hours spent and charged to the department. The Service Provider shall also conduct a meeting with the Unit head on a weekly basis and present him with the major findings and the amount charged to the department and the resources deployed in the week. No payment shall be made to the Service Provider if it is found that such meetings have not been conducted and the Investigating Officer as well as the Unit Head have not been kept duly informed about the progress of the project find major findings made.

13.3 The Service Provider shall maintain a worklog at mid action points verified by the Authorized Officer at the premises. Similarly, for post search activity, a worklog is to be maintained and verified by processing Investigating Officer. The work log should capture the work performed, the name of person from the service provider who is performing the work, the start time, the end time, the tools utilized etc., the worklog should match the bill raised by the service provider.

13.4 Once the project has concluded, the Service Provider shall not retain with it any data or metadata pertaining to it in any format or in any medium which can be later recovered or restored through any means. The Service Provider should actively eliminate and destroy any traces of data relating to the project undertaken immediately after the completion of project. Further, a certificate to this effect shall be presented to the ITD in every action along with the bill and any violation of the same shall attract severe penal action against the Service Provider, including cancellation of the empanelment. Also, recovery of damages from the Security Deposit shall be made in the event of non-performance and /or violation on the part of the service provider.

13.5 A consolidated bill will be submitted after completion of the work for payment. The bills have to be supported by the attendance sheet of the personnels of the service provider accessing the Digital and Intelligence Lab located inside the premises of the office of the DGIT(Inv), Mumbai. The bills will be countersigned by the relevant Officers before submitting the same for financial sanction. The



bills will be cleared within a reasonable time. However, in case of any unexpected delay, the contractor should be in a position to offer credit facility for the period.

13.6 Bills pertaining to search actions and post-search actions should be put up separately, clearly stating the nature of actions carried out.

13.7 As already stated at para 10.5 above, for out of office duty, no additional remuneration or charges shall be payable to the Service Provider/Service Provider personnel.



[Handwritten signature]

V. Non-disclosure clauses

14.1 Prohibition on illegal and/or unauthorized usage of Income Tax ITD data: It must be clearly understood that all data imaged/retrieved/extracted/taken/acquired/accessed from the search premises and/or provided by the officer concerned for data retrieval/storage/extraction/clustering/analysis/any service by whatever name called to the Service provider shall be **termed as ITD data and shall belong only and only to the ITD or O/o the PDIT(Inv.) 1 or 2 Mumbai, as the case maybe.** Such data shall in no way or form be kept in the personal custody of the service provider / personnel deployed by service provider, shall not be copied/printed without the explicit approval and direction of the concerned officer, shall not be taken / moved / transmitted / deleted / modified / manipulated / merged / removed by the service provider.

14.2 The Service Provider personnel shall act for and on behalf of the DGIT and shall not make any copy of data held by the ITD in any form and/or manner, in an unauthorized way.

14.3 The Service Provider personnel shall not hold data of the ITD with them independently at any point of time. Such possession will tantamount to illegal and/or unauthorized usage whether actually used or not.

14.4 If Service Provider personnel misuse the data or indulge into illegal and/or unauthorized usage of data or cause a deliberate act of omission or commission, they/Service Provider shall be liable for prosecution under applicable laws in addition to **cancellation of the empanelment** and other consequences, without any notice. Further, they/Service Provider may be **blacklisted from providing any service** to the DGIT in future.

14.5 The clauses regarding illegal and/or unauthorized usage of data are very important and may be noted by Service Provider with due care, as the DGIT office attaches great importance to sensitivity and confidentiality of the data.

14.6 The (Indian) Information Technology Act, 2000 deals with the issues relating to payment of compensation (Civil) and punishment (Criminal) in case of wrongful disclosure and misuse of personal data and violation of contractual terms in respect of personal data and the Service Provider and its personnel shall be accountable for any lapses.

14.7 Further, under section 43A of the (Indian) Information Technology Act, 2000, a body corporate who is possessing, dealing or handling any sensitive personal data or information, and is negligent in implementing and maintaining reasonable security practices resulting in wrongful loss or wrongful gain to any person, then such body corporate may be held liable to pay damages to the person so affected. It is important to note that there is no upper limit specified for the compensation that can be claimed by the affected party in such circumstances. This shall also be applied for the Service Provider and its personnel and shall be accountable for any lapses. Section 43A of the (Indian) Information Technology Act, 2000 is hereby reproduced for more clarification in this regard:-

[43A Compensation for failure to protect data. Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.]

Explanation. – For the purposes of this section:

- (i) "body corporate" means any company and includes a firm, sole proprietorship or other



association of individuals engaged in commercial or professional activities:

- (ii) *"reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;*
- (iii) *Sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.*

14.8 Section 66 of the (Indian) Information Technology Act, 2000 provides that if any person, dishonestly or fraudulently does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to Rs. 5,00,000) or with both. This shall also be applied for the Service Provider and its personnel and shall be accountable for any lapses.

14.9 If any misconducts/malpractices of the Service Provider or and any of its personnel caused any loss/embezzlement of revenue to the government exchequer, the Service Provider shall be accountable for making this loss good and the DGIT (Investigation), Mumbai shall be empowered to recover it or take necessary action as deemed fit and or refer the case to the suitable enforcement agency for taking remedial action, if any, in this regard.

14.10 The Service Provider shall ensure that the evidentiary value of the devices/data imaged/seized/backed up is protected as per Bharatiya Sakshya Adhiniyam, 2023 and any other laws in place with regard to digital evidence and shall provide necessary certificate/documents as mandated by law to that effect. The Service Provider shall also provide the certificate for admissibility of electronic records/data under section 63(4)I of Bharatiya Sakshya Adhiniyam, 2023.

14.11 If the service provider comes to know that its services are being utilized by the DGIT (Inv) in the case of its works of clients or otherwise related to it. The service provider shall immediately inform the DGIT (Investigation) of possible conflict of interest and immediately disposes of all the data related to the case and refrain from providing services in the given case.

14.12 The service provider shall enter into a **separate Non-disclosure agreement** with the O/o PDIT(Investigation), Mumbai.



Adh

Read and accepted.
Signature and stamp of
Bidder or Authorized Signatory

VI. Tendering Process : Delineation of Stages and Relevant Bid Documents

A. Six stages

15.1 Selection of a successful Service Provider will involve a *six (6) stage approach* before issuance of Work Order/letter of appointment.

- (a) Issue of Notification for RFP and Bid Documents
- (b) Receipt of Bids
- (c) Evaluation of Technical Bid and selection of technically qualified bidder
- (d) Evaluation of financial bids and finalization of rates.
- (e) Offer to technically qualified bidders to provide services at L1 rates
- (f) Finalization of vendors to be empaneled.

B. Two bids

15.2 The tender shall be uploaded on the website www.eprocure.gov.in and www.incometaxindia.gov.in and www.incometaxmumbai.gov.in and Government e-Marketplace (GeM) for RFP/ tender notice titled:

“Tender for Providing Digital Forensic and Data Analysis Services for the office of the Director General of Income Tax (Investigation), Mumbai”

15.3 For Digital Forensics and Data Analysis services, the bids are to be submitted in two parts i.e. **Technical Bid and Financial Bid.**

Submission of bids/Sealing and Marking of Bids:

- (a) The Technical Bid along with requisite documents shall be placed in one sealed envelope superscribed “Technical Bid”. The Financial Bid shall be kept in a separate sealed envelope superscribed “Financial Bid”. Both the envelopes shall then be placed in one single sealed envelope superscribed “Tenders for Providing Digital Forensic Services for the office of the DGIT (Investigation), Income Tax Department Mumbai” and addressed to “The Chairman, tender committee, Mumbai”. The Service Provider’s name, telephone number and complete mailing address shall be indicated on the cover of the outer envelope.
- (b) Both the inner envelopes superscribed “Technical Bid” and “Financial Bid” shall have the name and address of the bidder so that if required, they may be returned to the Service Providers without opening them.
- (c) If the outer and inner envelopes are not sealed and marked as required, the Income-tax department shall assume no responsibility for the bid’s misplacement or premature opening.
- (d) If for any reason, it is found that the Technical Bid reveals the Financial Bid related details in any manner whatsoever, or, the Financial Bid is enclosed in the envelope superscribed, “Technical Bid”, the tender document will be summarily rejected in the first instance itself.
- (e) All the Tender documents submitted shall be serially page numbered and contain the table of contents with page numbers.



[Handwritten Signature]

C. Technical Bids

15.4 The Technical Bid submitted by the bidder shall include the following:

15.4.1 Full particulars of Govt. or other organizations, where the Service Provider has provided Digital Forensic and Data Analysis Services (Self-attested copies of the relevant work orders and certificate of work completion are to be enclosed).

15.4.2 Profile of his Organization and other details in the format given as per **Annexure-A**.

15.4.3 The service provider participating in the bid shall submit a self certificate that the bidder has not been blacklisted by any organization in last 3 years from FY 2023-24, FY 2024-25, FY 2025-26 and till date.

15.4.4 The service provider shall submit copy of ITR along with the tax audit report for FY 2023-24 & FY 2024-25. The Service Providers registered under MSME and Startup India companies/ firm/ proprietary may be exempt (proof to be enclosed).

15.4.5 **The service provider shall provide certificates indicating geographical reach of the services and certificates indicating the numbers of digital Forensic experts with qualification and experience in digital Forensic services and number of hardware and software tools.**

15.4.6 The service provider shall submit the work experience certificate with Cloud Service Providers.

15.4.7 The services providers participating in the bid shall submit a No-Objection Certificate affirming that they have no objection to the L-1 rates being offered to all the service providers qualifying the technical bid as mentioned in this document.

15.4.8 The service provider shall submit a certificate stating that necessary compliances are being done related to Bharatiya Sakshay Adhiniyam, Information Technology Act, Income Tax Act, GST Act.

15.4.9 If for any reason, it is found that the Technical Bid reveals the Financial Bid/ pricing-related details in any manner whatsoever, the Bid document will be summarily rejected in the first instance itself.

15.4.10 All the Bid documents/enclosures/attachments submitted shall be serially page numbered and contain the table of contents/Index with page numbers.

D. Deadline for Submission of Bids

16.1 The applicants should submit their applications in a sealed envelope, as described above in the Office of Addl.DIT (Inv), Unit-4, Room No. 209, 2nd floor, Scindia House, Ballard Estate, Mumbai-400 001 on or before date and time as mentioned in the notice inviting applications.

16.2 No acknowledgement, in respect of receipt of any bid, shall be issued.

16.3 Applications for tender must be received by the Income-tax department at the address specified not later than the time and date specified in the Invitation for Bids. After the time and date specified, the link on the website www.eprocure.gov.in and www.incometaxindia.gov.in or www.incometaxmumbai.gov.in or Government E-Marketplace (GeM) shall be disabled.



16.4 The Income-tax department (ITD) may, at its discretion, extend the deadline for submission of applications which will be binding on all the Service Providers.

E. Modifications and Withdrawal of Applications

17.1 No modification or substitution of the submitted application shall be allowed.

17.2 An applicant may withdraw its Tender after submission, provided that written notice of the withdrawal is received by the Income-tax Department before the due date for submission of applications.

17.3 The withdrawal notice shall be prepared in original only and each page of the notice shall be signed and stamped by authorized signatories. The copy of the notice shall be duly marked as "WITHDRAWAL"

F. Disqualification

18.1 The proposal is liable to be disqualified in the following cases or in case bidder fails to meet the tendering requirements as indicated in this tender document.

18.2 Proposal not submitted in accordance with the procedure and formats prescribed in this document or treated as non-conforming proposal.

18.3 During validity of the proposal, or its extended period, if any, the bidder increases his quoted prices

18.4 The bidder qualifies the proposal with his own conditions.

18.5 Proposal is received in incomplete form.

18.6 Proposal is received in after due date and time.

18.7 Bidder has been blacklisted by any Government (Central/State) PSU/department/organization or any Local Authority anywhere in the Country.

18.8 Proposal is not accompanied by all the requisite documents.

18.9 The Bidder shall sign his application with the exact name of the concern which is sought to be empaneled as Service Provider. The Bid document filed by the bidder shall be typed. No overwriting or cuttings shall be permitted.

18.10 Where the bid has been signed by the Authorized Representative on behalf of the concern, the bidder shall submit a certificate of authority and any other document consisting of adequate proof of the ability of the signatory to bind the bidder to the contract. **Income-tax department may outrightly reject any bid, which is/was not supported by adequate proof of the signatory's authority.**

18.11 Information submitted in technical proposal is found to be misrepresented, incorrect or false, accidentally, unwittingly or otherwise, at any time during the processing of the contract (no matter at what stage) or during the tenure of the of the contract including the extension period, if any.



Arb

18.12 Financial bid is enclosed/attached with the Technical bid/any of the annexures to the Technical Bid.

18.13 Bidder tries to influence the proposal evaluation process by unlawful/corrupt/fraudulent means at any point of time during the bid process.

18.14 The Income-tax Department, without assigning any reasons, reserves the right to accept or reject any bid, and to annul the bidding process and reject all bids at any time, without thereby incurring any liability to the affected Bidder or Bidders or any obligations to inform the affected Bidder or bidders of the grounds for the action taken by the Income-tax Department.

18.15 The Income-tax Department reserves the right to reject the bid having deviations from the prescribed terms and conditions.

18.16 Making misleading or false representation in the bid document will lead to disqualification of the Bidder at any stage, even if such mala fide comes to light after the award of the contract.

18.17 Income-tax department, reserves the right to reject any bid (including the lowest one) which in its opinion is not responsive or violating any of the conditions/specifications or which is found to be adopting unethical business practices; without bearing any liability or any loss whatsoever it may cause to the bidder in the process.

G. Opening and Evaluation of Technical Bids

19.1 The Tender Committee appointed by the O/o DGIT(Investigation) Mumbai will open all Technical Bids in the first instance on the appointed date, time and place.

19.2 During evaluation of the bids, the Tender Committee may, at its discretion, ask the Bidder for clarification of its bid. The request for clarification and response shall be in writing.

19.3 No bidder shall contact the Income-tax Department/any officer concerned with the tender process on any matter relating to its bid from the time of the bid opening till the issuance of work order. All bidders are strongly advised to furnish all material information in the bid itself.

19.4 Any effort by a Bidder to influence the Income-tax Department in its decisions on bid evaluation, bid comparison or work order decision will result in rejection of the bid.

19.5 The Financial Bid of only those Service Providers shall be opened whose technical bids (inclusive of profile of applicant Service Provider) are found eligible.

H. EVALUATION METHOD: The criteria of selection as well as rejection.

20 General Conditions

20.1 The bidder should fulfill the eligibility criteria mentioned in Section-1 of this document to qualify



for consideration at the stage of technical evaluation. Only those Bid(s) shall be treated as responsive which fulfill all prescribed criteria/parameters.

20.2 Bids with incomplete response shall be rejected.

20.3 Tendering process shall be finalized only when there are at least three (3) responsive bids.

20.4 Without affecting the sanctity of the above criteria, the Income-tax Department reserves the right to relax any condition of eligibility criteria qualifying the bid(s), based on merit of each case and if the situation so warrants in the interest of the department.

20.5 The Income-tax Department reserves the right to accept or reject any or all bids without assigning any reasons.

I. Opening and evaluation of Financial Bids

21.1 The results of the bid will be communicated in writing to the qualifying bidder. The unsuccessful bidders will be notified separately.

21.2 The Price Bid shall comprise the price component for all the services indicated in the bid document. The price quoted by the bidders shall exclude all applicable taxes such as GST, CESS, wherever applicable.

21.3 Income-tax Department shall deduct tax at source as per the rules and issue necessary certificates to the Service Provider.

21.4 The prices once accepted by the Income-tax Department shall remain valid till the contract remains in force.

21.5 Rates quoted shall include statutory obligations as may be applicable.

21.6 Amounts/Prices shall be quoted in Indian Rupees only and both in figures and words. If there is a discrepancy between words and figures, the amount written in words shall be taken as the bid price.

21.7 The Income-tax Department does not bind itself to accept the lowest bid. In a normal situation, the contract shall be awarded to the lowest responsive bidder. However, mere lowest rates are not the sole criteria of selection. Income-tax department, is not bound to accept the lowest rates.

22. Department reserves the right to negotiate the price with the finally short-listed bidder before awarding the contract. It may be noted that Income Tax Department will not entertain any price negotiations with any other bidder.



Adh

J. Requests for Information

Bidders are required to direct all communications related to this document through the designated Contact person for Director General of Income-tax (Inv), Mumbai. All queries relating to the Bid, technical or otherwise, must be in writing only to the designated contact person. The Department will not answer any communication initiated by Respondents later than five business days prior to the due date of opening of the bids. If the Department, in its absolute discretion, deems that the originator of the question will gain an advantage by a response to a question, then department reserves the right to communicate such response to all Respondents.

Designated Contact Person : **The Chairman, Tender Committee and Addl.DIT(Inv.), Unit-4, 2nd Floor, Room No. 209, Scindia House, Ballard Estate, Mumbai-400 001.**
Email: Mumbai.addldit.inv4@incometax.gov.in

Read and accepted.
Signature and stamp of
Bidder or Authorized Signatory



VII. Annexures to the Tender Document

Annexure 'A'

PROFILE OF ORGANIZATION

(To be submitted along with Technical Bid)

Sr. No.	Description		
1.	Name and address of the Entity	:	
2.	Name & Address of the Owner(s)	:	
3.	PAN & GST Registration No. of the Entity (Proof to be enclosed)	:	
4.	Year of Commencement of Entity (Minimum 3 years of experience of the entity or the promoter of the Entity in Digital Forensic Services is pre-requisite) (Proof to be enclosed)	:	
5.	Copies of IT Returns along with Tax Audit Report having minimum average turnover of Rs. 50 lakhs in last two Fys. 2023-24 and 2024-25. Registered under MSME and Startup India companies/ firm/ proprietary may be exempt. (proof to be enclosed)	:	
6.	Year of formation/Year of Incorporation (Proof to be enclosed)	:	
7.	Number of Digital Forensic Specialists Available with qualification (to be enclosed with evidence for having educational qualification and experience in Digital Forensic Services) (minimum 7 person in your organisation)	:	
8.	Details of the services provided (enclose documentary proof of the same) with satisfactory completion certificates of the concerned organisations/Government Departments or agencies	:	
9.	Client list to be enclosed (Give details of clients, nature of work entrusted, tools used, brief discription of forensic techniques employed by you alongwith your specific contribution in enhancing the outcome of the proceedings)	:	
10.	Enforcement agencies who had taken Services from you in last 3 years (Proof to be enclosed)	:	
11.	Any specific Core competency/ Forensic Knowledge (Give details)	:	
12.	Any specific Proprietary Software developed by your entity (Give details)	:	
13.	Availability and specialized experience in the use of AI based Data Analytical Tools	:	
12.	Any other remarks*	:	

Note: Please attach extra sheet in support of your information, if space in the column is insufficient.

It is also requested to ascertain the quantum of work before submitting the tender.

Signature & Seal of bidder

Page 32 | 36



[Handwritten Signature]

Annexure —‘B’

TECHNICAL BID DOCUMENT
(On the letter head of the concern submitting the bid)

To,
The Director General of Income Tax (Investigation),
Scindia House, Ballard Estate,
Mumbai- 400 001

Ref: Tender Notice dated_____.

Sir,

I/We hereby undertake to provide the Digital Forensic and Data Analysis services for the office of the Director General of Income Tax (Inv.), Mumbai as specified in the Bid/tender document and agree to hold this offer for entire contract period.

I/We have understood the Instructions to Bidders and Terms and Conditions of Contract as enclosed with the invitation to the tender and have thoroughly examined the specifications of services to be rendered and are fully aware of the nature of the services to be rendered and my/our offer is to provide the services strictly in accordance with the requirements.

Certified that I/We have enough experience in providing Digital Forensics services and related works.

Sr. No.	Description	:	Check
1.	Name and address of the registered Agency	:	Yes/No
2.	Name & Address of the Owner(s)	:	Yes/No
3.	PAN & GST Registration No. (Proof to be enclosed)	:	Yes/No
4.	Year of Commencement of Agency (Minimum 3 years of experience in Digital Forensic Services)	:	Yes/No
5.	Copies of IT Returns along with Tax Audit Report having minimum average turnover of Rs.50 lakhs in last two Fys. 2023-24 and 2024-25. Registered under MSME and Startup India companies/ firm/ proprietary may be exempt. (proof to be enclosed)	:	Yes/No
6.	Year of formation/Year of Incorporation (Proof to be enclosed)	:	Yes/No
7.	Number of Digital Forensic Specialists Available with qualification (to be enclosed with evidence for having experience in Digital Forensic Services)	:	Yes/No
8.	Proof of the existence of the tools as mentioned in para 8.3 of the bid .	:	Yes/No
9.	Client list (Certificate from clients to be enclosed)	:	Yes/No
10.	Geographical reach of services (Certificate to be enclosed of services provided in F.Y. 2023-24,2024-25,2025-26)	:	Yes/No
11.	Enforcement agencies who had taken Services of the applicant in last 3 years	:	Yes/No
12.	Certificate that vendor has not been blacklisted by any organization in last 3 years from FY 2023-24, FY 2024-25, FY 2025-26 and till date.	:	Yes/No
13.	Certificate stating that necessary compliances are being done : related to Bharatiya Sakshay Adhinyam, Information Technology Act, Income Tax Act, GST Act.	:	Yes/No
14.	Copy of No Objection Certificate affirming that Service Provider: has no objection to LI rates being offered to other Service Providers qualifying the Technical Bid.	:	Yes/No
15.	Any other remarks* (w.r.t. specialized skill, experience, patented technology etc. which makes the bidder desirable for Data forensics and/ or Data Analysis work. Specialized Software tools/ AI based data analytics experience and experience with CSPs for data access may be mentioned here. Relevant certificates are to be enclosed)	:	Yes/No

If response to any of the items mentioned at Sr.No 1-14 above is not furnished or if any response to any item at Sr. No. 1-14 is negative, the bid may be rejected.

Signature of the Authorized Signatory

DECLARATION

I / We hereby certify that the information furnished above is full and correct to the best of my/our knowledge and belief. I/We understand that in case any deviation is found or any document submitted is non-genuine in the above statement at any stage, the agency will be blacklisted and may not be permitted to bid in future.

(Signature of Authorized Signatory with date)



(Handwritten signature)

Annexure —‘C’

FINANCIAL BID DOCUMENT FOR DATA FORENSICS AND DATA ANALYSIS WORK

Having examined the bidding documents and having submitted the technical bid for the same, we, the undersigned, hereby submit the Financial Bid for providing Digital Forensic and Data Analysis services for the office of The Director General of Income Tax (Inv.), Mumbai is as below:-

1. Name and address of the registered Agency :
with telephone number of the applicant contractor
2. Permanent Account Number (PAN) :
3. Names and Addresses of the Proprietor/Partners/Directors and their PAN
4. Rate Chart (Exclusive of GST) :

PART A

(Rate for Forensic Services at the premises of Search/Survey)

Sr. No	Category of Forensic Digital Device and Forensic Services	Criteria*	Rate (in ₹)^		Rate (in ₹)^
	Imaging/cloning, digital seizer, hash generation and reporting – master and working copy	Standard Maximum Man-Hours for 100GB data size* (3)	Maximum Rate per Man Hour ^ (4)	Total cost for 100GB data size (5) Col. (3)* Col. (4)	Total Cost for 100GB data size quoted by the Service Provider (6)
(a)	Pendrives	36 min.	₹ 850/-	₹ 510/-	
(b)	Mobiles and tablets	36 min.	₹ 850/-	₹ 510/-	
(c)	Hard disks	36 min.	₹ 850/-	₹ 510/-	
(d)	CD/DVD	36 min.	₹ 850/-	₹ 510/-	
(e)	Desktop and laptops	36 min.	₹ 850/-	₹ 510/-	
(f)	Other digital devices	36 min.	₹ 850/-	₹ 510/-	
(g)	Local Server	36 min.	₹ 850/-	₹ 510/-	
(h)	Cloud Server	1 hrs.	₹ 850/-	₹ 850/-	

* Note: If the size of the data exceeds the prescribed limit, a proportionate rate shall be applied to the excess.

^ Rates exclusive of applicable taxes

Note 2: The rates quoted by the Service Providers should be in figures and in words also.



PART B
(Rate for Carving, Extraction and Indexing)

Sr. No (1)	Category of Forensic Digital Device and Forensic Services (2)	Standard Maximum Man-Hours for 100GB data size* (3)	Maximum Rate per Man Hour ^ (4)	Total cost for 100GB data size (5) Col. (3)* Col. (4)	Total Cost for 100GB data size quoted by the Service Provider (6)
	Carving, Extraction, Indexing				
(a)	Extraction, Carving & Indexing of Pen Drive etc.	24 mins.	₹ 850/-	₹ 340/-	
(b)	Extraction, Carving & Indexing of HDD, Laptop, Desktop, Tablet, Mobile and CD/DVD	1 hrs.	₹ 850/-	₹ 850/-	
(c)	Extraction, Carving and Indexing of Server Data	1 hrs.	₹ 850/-	₹ 850/-	
(d)	Indexing, Keyword List inclusion (using User Friendly Forensic Tools with proven results)	2 hrs.	₹ 850/-	₹ 1,700/-	
(e)	Indexing of server data	1.4hrs	₹ 850/-	₹ 1,190/-	

* In case the data size is more than 100GB, then proportionate rate shall be applied.
^ Rates exclusive of applicable taxes
Note : The rates quoted by the Service Providers should be in figures and in words also.

PART C
(Rate for Data Analysis)

Sr. No (1)	Category of Forensic Digital Device and Forensic Services (2)	Standard Maximum Man-Hours for 100GB data size* (3)	Maximum Rate per Man Hour ^ (4)	Total cost for 100GB data size (5) Col. (3)* Col. (4)	Total Cost for 100GB data size quoted by the Service Provider (6)
	Data Analysis				
(a)	Keyword search without emails	48 mins.	₹ 850/-	₹ 680/-	
(b)	Data Visualization/tabulation for device-wise results/findings	1.5 hrs.	₹ 850/-	₹ 1,275/-	
(c)	Mounting of ERP data on Temp Server	2 hrs.	₹ 850/-	₹ 1,700/-	
(d)	Discovery of patterns in the data set using AI based tools	1 hr.	₹ 850/-	₹ 850/-	
(e)	Deleted data recovery (file carving, volume shadow recovery, file signature analysis etc.) and decoding (mobile devices)	2 hrs.	₹ 850/-	₹ 1,700/-	
(f)	Password recovery from file	2 hrs.	₹ 850/-	₹ 1,700/-	



Add

(g)	Mobile Image Mounting and Analysis	2 hrs.	₹ 850/-	₹ 1,700/-	
(h)	Analysis of the CDR and IPDR Data	1 hr.	₹ 850/-	₹ 850/-	
(i)	Analysis of the audio data to find speaker identification and transcription	3 hrs.	₹ 850/-	₹ 2,550/-	
(j)	Review & analysis of data (including HDD, laptops, tablets, mobile, phones, emails. (Local or cloud server etc.) Using keyword search	4 hrs.	₹ 850/-	₹ 3,400/-	
(k)	Keyword search and Indexation of backed-up email data	2 hrs.	₹ 850/-	₹ 1,700/-	
(l)	Mounting Data from Back-up Cloud Server	1.2 hrs.	₹ 850/-	₹ 1,020/-	
(m)	Review & analysis of data (including HDD, laptops, tablets, mobile, phones, emails. (Local or cloud server etc.)	1 hr.	₹ 850/-	₹ 850/-	
(n)	Discovery of patterns in the data set like Financial Server, Tally, Busy Data	2 hrs.	₹ 850/-	₹ 1,700/-	
(o)	Basic Visualisation/Tables of device wise data set for further analysis	1 hr.	₹ 850/-	₹ 850/-	
(p)	Network Asset Discovery and Identification of Firewall, Local/Cloud Servers, Storage, clients	1 hr.	₹ 850/-	₹ 850/-	
(q)	File Categorisations, classification and extraction (exporting of relevant data) and reporting (mobile devices)	2 hrs.	₹ 850/-	₹ 1,700/-	
(r)	Customised cloud/server ERP Applications (Isolated and Replicated Server Creation)	4 hrs.	₹ 850/-	₹ 3,400/-	

* In case the data size is more than 100GB, then proportionate rate shall be applied.

^ Rates exclusive of applicable taxes

Note : The rates quoted by the Service Providers should be in figures and in words also.

(Quotations are invited for Digital Forensics and Data Analysis services. The maximum permissible rate for each service is specified in this Tender document. Bidders wishing to quote rates lower than the prescribed maximum rates may submit their bids accordingly. The L1 bidder will be determined by the Tender Committee as per the applicable evaluation criteria.)



Ad