

**EXPRESSION OF INTEREST FOR RESELLING OF
SOFTWARE & HARDWARE PRODUCTS**

C-DAC Cyber Forensics Tools



Issued by

CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

(The Premier R&D organization of the

Ministry of Electronics and Information Technology (MeitY), Govt. of India)

Thiruvananthapuram, Kerala, 695033

Phone:0471 2727508 Fax:0471 2723456 Email: tpc@cdac.in

Website:www.cdac.in

Dated:15th October 2026

Table of Contents

1. Introduction	3
2. Brief about C-DAC	3
3. Brief description about the Products	4
4. Invitation for Expression of Interest	17
5. Who can apply	18
6. How to Apply	18
7. Selection of Reseller Partner	18
8. Re selling license, Validity & Renewal	20
9. Deliverables	20
10. Training for Reseller Partners	21
11. Technical support	21
12. Cost for Registration of Reseller	21
13. Interpretation of the Clauses in the EoI Document	22
Annexure-I	24
Details of the Reseller Partner	24

1. Introduction

The Centre for Development of Advanced Computing (C-DAC) is seeking "Expression of Interest" (EOI) from Indian companies who are interested in reselling the "Cyber Forensics hardware and software tools" designed and developed by CDAC with the support of Ministry of Electronics & IT (MeitY). This Reseller partnership is available on non-exclusive basis, allowing companies to acquire licenses to market, sell and support the product.

CDAC is inviting interested companies to respond with their company details, collaboration details, sales projections, and financial details. The rates for the reseller registration fee to become a Reseller Partner, software product fee, and license subscription fee have been approved by the Competent Authority of C-DAC after evaluating the development cost of the products.

Expressions of Interest (EOI) are being solicited on behalf of M/s Technology Promotion Centre (TPC), C-DAC, Thiruvananthapuram, from reputable firms/companies registered in India. These firms/companies should possess relevant experience and insights in marketing, implementation, or similar products through reselling. C-DAC has designed and developed 16 Cyber Forensics tools. These solutions are now available for reselling, enabling the industry to effectively market and implement them for various client projects.

This document provides comprehensive information regarding the products, different license details of products, terms and conditions for companies to submit their Expression of Interest and establish a Reseller Partnership with CDAC, in accordance with the terms outlined herein. Any further technical details / inputs required for the marketing & sale of products can be had directly from CDAC.

2. Brief about C-DAC

Centre for Development of Advanced Computing (C-DAC) is the premier R&D organization of the Ministry of Electronics and Information Technology (MeitY), Govt. of India for carrying out R&D in IT, Electronics and associated areas. It is a national Centre of Excellence, pioneering application-oriented research, design and development in Electronics and Information Technology.

The Centre has contributed significantly to the growth of the industry in general and the electronics sector in particular through the indigenous development of commercially viable systems and products, foreign technology absorption, adaptation and upgrades, consultancy and training and turnkey implementation of contract projects. The Centre has several firsts to its credits and is the recipient of prestigious national level awards for excellence in application-oriented R & D.

The different technology verticals of C-DAC include High Performance Computing (HPC), Quantum Computing, Artificial Intelligence (AI), Strategic Technologies, Digital India RISC-V (DIR-V), Software Technologies, e-Governance, Healthcare & Educational Technologies, Cyber Security & Forensics, Automotive and

Communication Technology, Power Electronics & Renewable Energy, Intelligent Transportation Systems (ITS) and others.

3. Brief description about the Products

The Resource Centre for Cyber Forensics (RCCF), established in 2002 by the Department of Electronics & Information Technology, Government of India, serves as a national hub for Cyber forensics research and development. It focuses on creating forensic solutions to support law enforcement agencies in the scientific analysis and investigation of Cyber-crimes. Currently operating within the Cyber Forensics Section (CFS) of CDAC Trivandrum, RCCF has specialized teams dedicated to various areas of forensic research, such as Disk, Live, Mobile, and Network forensics, along with CDR analysis.

RCCF research teams have developed several tools, starting with the flagship disk image analysis tool, CyberCheck. Over time, other notable products like TrueImager, MobileCheck, SIMXtractor, Win-LiFT, and Advik CDR Analyzer were created and deployed. In the second phase of research, tools such as PhotoExaminer, WebInvestigator, Advik IPDR Analyzer and Advik Lite were also developed. Together, these tools are combined into a portable field kit, TrueTraveller, designed for comprehensive Cyber forensic investigations. Recently 4 new tools have been developed namely Dhi-Trace: A forensics Data Analytics Tool, FinTrace: Financial Transaction Tracer for Banks, FinFraudEx - Financial Fraud Examination Tool and I-FIRST (IoT Forensics Incident Response System). The following section describes each tool in detail.

A. CyberCheck

CyberCheck is a forensic data recovery and analysis tool which enables law enforcement officers to quickly and efficiently analyze images of hard disks, USB drives and other storage media. One of the salient features of CyberCheck is that it can be used by multiple users concurrently and it supports multitasking. The file carving facility of CyberCheck supports carving of more than 400 types of files. The indexing process of CyberCheck can be stopped and resumed later.

Features

- Supports analysis of TrueBack, Raw, EnCase and Virtual disk (VDI, VHD & VMDK) image files.
- Supports the analysis of FAT12/16/32, exFAT, NTFS, Linux EXT2/3/4, UFS, Btrfs, HFS and YAFFS2 file systems.
- AI based Fintech file detection and export
- Supports preview of disks and volumes.
- Recovers deleted files and folders. Detects unallocated areas and disk slack areas.
- Decryption of VeraCrypt and TrueCrypt encrypted disks.
- USN Journal Analysis, Jump List file analysis and Link file analysis
- WhatsApp web analysis

- Registry analysis and Shell Bag analysis support.
- Sophisticated data carving facility to carve documents, images, audio and video.
- Index based search facility supporting Unicode, multiple keywords, fuzzy-search, regular expression, hash-based search and result filtering based on file meta information.
- Browser forensics feature to extract forensically relevant information from Google Chrome, Internet Explorer, Microsoft Edge, Firefox, Safari and Opera.
- Signature mismatch detection, overwritten file detection and password protected file detection.
- Advanced timeline analysis with multiple events option.
- Known good file filtering with NSRL dataset.
- Document language detection.
- Recycle bin analysis and thumbnail database analysis
- Evidence hash verification using MD5, SHA1, SHA256 and SHA512 algorithms.
- Can convert proprietary evidence file formats to RAW image.
- Categorized export of files and folders.
- File hash computation using MD5, SHA1, SHA256 and SHA512 algorithms.
- File bookmarking & bulk file export and Report generation.

B. MobileCheck Suite

MobileCheck Suite is a digital forensics solution for Basic phones, Feature Phones, Smart phones, GPS Devices and Drones. The solution supports preview, acquisition, analysis and reporting of evidence from mobile devices.

Features

- Supports Forensic Preview, Acquisition & Analysis of Android, iPhone, Feature phone, Basic Phone, and GPS devices
- Phone Artefact Analysis – Analysis of Contacts, SMS, Call Logs, and other phone-related artefacts.
- Social media & Messaging App Analysis – Supports analysis of data from applications such as WhatsApp, Telegram, Signal, and other supported social applications.
- File System Analysis – Analysis of deleted and undeleted files and data.
- Cloud Data Analysis – Analysis of supported cloud services such as Gmail, Google Drive, Twitter, and other available cloud artefacts.
- Visual Analytics – Provides Timeline Analysis and Link Analysis for identifying relationships and activity patterns.

- Geolocation Analysis – Latitude and Longitude Analysis for examining location-related information and movement patterns.
- Drone Analysis – Analysis of drone flight paths and flight logs to identify movement and operational information.

C. Win-LiFT

Win-LiFT is a Windows Live Forensics Tool consisting of ImagerBuilder, Imager and Analyzer. Live Forensics involves acquisition of volatile data from the Suspect's machine and analysis of the acquired data. Win-LiFT enables volatile and non-volatile data acquisition using Win-LiFT Imager and analysis of the same using Win-LiFT Analyzer. Win-LiFT ImagerBuilder runs on the Investigator's machine and builds the Win-LiFT Imager tool into a USB device.

Features

Win-LiFT ImagerBuilder

- Option to enter Crime details
- Investigator can choose from available artifacts depending on case requirement
- Builds the Imager tool to USB

Win-LiFT Imager

- Captures following volatile/non-volatile artifacts from Windows Systems
- Physical Memory content
- Collects Information regarding
- System/Process/Network/File System Details/Others
- Registry Files, Browser Files, Event Log Files
- Browser Cache, Recent File Cache, ShimCache, Amcache
- Windows 10 artifact files - SRUM, Photos, Picture Password etc.
- Snapshot of Desktop Screen
- Hashing of all acquired files, Log and Report Generation
- Minimal tampering ensured by file system level reconstruction of files

Win-LiFT Analyzer

- Advanced Memory Analysis from Windows 7 / 10
- Running Process details
- Process Reconstruction
- BitLocker Key Reconstruction
- Internet Usage based Information
- MFT Records
- Structural Analysis of Reconstructed Executables
- Forensic Data Carving
- Event Log Analysis

- Browser/Cache Forensics of Chrome/Firefox/Maxthon/Safari/Edge/IE/Yandex/Brave, UC Browser/Opera
- Detailed Report Generation
- Independent Loading /Analysis of Memory dump
- Hash Verification of acquired files
- List/Tree/Summary/Gallery View
- Text-Hex (Raw files)/Parent-Child (Running processes) View

D. TrueImager

TrueImager is a high speed, lightweight, portable disk imaging hardware solution with battery backup support. The unit is capable of performing Hashing, Imaging and Cloning operations of source storage media and performs Wiping and Formatting of destination disk. It has all advanced features of disk forensics.

Features

Hardware Features

- Portable and handheld device with a 7-inch capacitive touch LCD.
- Built-in battery backup support.
- External Power Adapter: 100–230V (Input), 19V 3.42A (Output).
- Dimensions (W × D × H): 29.7 × 18 × 7.3 cm.
- Net Weight: 1.8 kg.

Other Features

- Provides Hash, Hash & Image, and Clone operations for source media.
- Provides Wipe and Format operations for destination disks.
- Provides Verify and Restore from Image files
- Support storage media with interfaces IDE, SATA, micro-SATA, mini-SATA, USB, PCIe, M.2, U.2 and memory cards as source media Supports USB and SATA disks as destination media.
- Supports USB & SATA disks as destination media
- Provides built-in write protection for suspect disks.
- Supports SHA-1, SHA-2, and MD5 hashing algorithms.
- Supports two modes of data capture: Linux DD and CDAC TrueBack format.
- Formats destination media with file systems exFAT, EXT4, NTFS and HFS+
- Provides S.M.A.R.T. data for HDDs and SSDs.
- Supports Secondary Hashing.
- Supports Partition Imaging of source media.
- Supports Secondary Imaging with configurable split file size.
- Provides visual display of Source and Destination disks.

- Provides Blank Disk Check facility for source and destination disks.
- Supports automatic probing of source and destination disks.
- Provides HPA/DCO detection and disabling for imaging operations.
- Generates report files for Hash and Image operations.
- Provides Report File Export functionality.
- Provides Write Verification for Hash & Acquire operations.
- Supports imaging multiple source disks to a single destination disk.
- Supports up to four concurrent tasks.
- Provides an Automatic Shutdown facility.
- Provides Disk Browsing functionality.
- Provides File and Content Sorting & Filtering facilities.
- Displays an Overall Process Log.

E. NeSA- Network Session Analyzer

NeSA (Network Session Analyzer) is a network forensics tool to capture and analyze network traffic. Data sent through the network can be captured, reconstructed and exported using this tool.

Features

- Loads pcap formatted dump files and rebuilds TCP sessions.
- Supports Data Level Analysis and Packet Level analysis
- Reconstructs files from HTTP, FTP, SMTP and POP3 packets.
- Searching and Filtering
- Built in Hex, Thumbnail, File and Mail view.
- Powerful filter for filtering TCP sessions and packets.
- Regular expression-based search capability.
- Supports port customization and time zone-based analysis.
- Loads multiple pcap files.
- Merging and sorting of packets.
- Can capture from multiple interfaces
- Report generation.

F. SIMXtractor

SIMXtractor is a forensic solution for imaging and analyzing SIM cards. The tool contains a SIM Card Reader, SIM Imager (Imaging of SIM cards) and SIM Analyzer (Analysis of SIM cards). The tool supports both GSM and CDMA SIM cards.

Features

1. SIM Card Reader

SIM Card Reader is a hardware-based reader with USB support. The hardware utility has

- Supports USB 2.0
- Support for 5V, 3.3V and 1.8 V SIM cards

- Supports ISO-7816 Standard cards
- PC/SC compatible Card Reader
- Works with all versions of Windows (32 bit and 64 bit)

2. SIM Imager

SIM Imager is a software utility to image the contents of the SIM card. The features of the SIM Imager are

- Generates an image file of the SIM card contents
- Supports MD5, SHA-1 and SHA-2 hashing methods
- Generates hash values for all files individually and total hash of all files
- Generates a report after seizing process with investigation details
- Write blocking of SIM Cards done

3. SIM Analyzer

SIM Analyzer is a software utility to analyze a SIM card image. The main features of SIM Analyzer are

- Analyzes Call logs, Contacts, Messages, and Network related information
- Searching facility
- Multiple images can be loaded and Analysed
- Highlights Recovers deleted SMS, Incoming and Outgoing SMS
- Facility to generate custom PDF reports

G. Advik CDR Analyzer

Advik is a Call Data Record Analysis tool which can import and analyze CDR logs of any service provider in India and generates a comprehensive report of frequency statistics including service provider details and subscriber details (SDR) of CDR numbers.

Features

- Seize and Acquire CDR Logs
- Support to import SDR
- Customizable Preset facility for single click data import
- Call Flow Visualizer
- Smart grid Data Filters
- Customizable Filters
- Advanced Search with scripting support
- Filter History
- New Number Analysis
- Timeline Analysis
- Frequency Analysis
- Link Analyzer
- Geo-Analyzer

- Suspect List
- IMEI Analysis
- Customizable Reports
- Group Analysis
- Preliminary CDR Analysis
- Geo-Fencing
- Support for Azimuth in Cell-id Logs
- Service Call Analysis
- Integration with Advanced Forensics Data Analytics Tool

H. Advik IPDR Analyzer

Advik IPDR Analyzer Imports and analyzes IPDR logs from different service providers, generating comprehensive reports that include correlation with CDR, SDR, and Cell-ID data.

Features

- Import and manage IPDR
- Case Based Analysis
- Automatic Importing of IPDRs
- Preset Management
- IPDR Analysis
- Filters
 - Probable WhatsApp sessions
 - Direct Communication
 - App Based Filters
 - Country Based Filters
 - 15+ Other Filters
- Customized Search
 - Create and Save Queries for searching later.

I. Advik Lite

Advik Lite is a light weight Call Data Record Analyzer tool which can import and analyze CDR/IPDR logs and generates comprehensive reports.

Features

- Import CDR/Tower CDR/IMEI CDR/ IPDR
- Filter History/Nested Filters
- Advanced Search with Scripting support
- Import, Search and Manage SDR
- Import and Manage Cell-ID
- Customizable Report
- Link Analysis
- TimeLine Analysis
- Frequency Analysis

- Suspect List
- Call Flow Visualizer
- Geo Analysis

J. PhotoExaminer

PhotoExaminer is a Microsoft Windows-based cyber forensic application for classifying, enhancing, analyzing and generating the reports of image and video evidences. It provides nested search and filter options to reduce the overall dataset of digital images to only the relevant images.

Features

- Supports MOV, MP4, AVI, JPEG, PNG, BMP and TIFF
- Data Carving - Images and Videos.
- Extract metadata of images and videos.
- Skin color image detection.
- Image classification with filters.
- Increase Resolution of thumbnails and small images.
- Enhance dark images.
- Basic image enhancements
- Error Level Analysis
- Hidden Pixel Identification
- Thumbnail Mismatch Identification
- Filter for identifying face images.
- Video Source Camera Identification.
- Video Frame Extraction
- HEIF Forensics
- Similarity Check
- Object Identification
- Face Watchlist
- Video snapshot and scene extraction.
- Searchable and sortable Gallery
- Integration with Advanced Forensics Data Analytics Tool
- Customizable Report.

K. WebInvestigator

WebInvestigator is an Internet Forensics Tool that allows cybercrime investigators to analyze forensically relevant artefacts related to Internet usage of the Suspect's Windows Computers. The tool works in two modes, Live and offline. In the offline mode, the tool analyses data/files collected from the suspect's machine using any cyber forensics tool. In the Live mode, the tool acquires the Internet usage related data/files from the system where the tool is being executed and analyses those files to retrieve Internet-related evidence.

Features

- Browser Forensics of Chrome, Opera, Firefox, Safari, IE and Edge Web Browsers to retrieve the forensically sound information such as details of Visited Sites, Download Files, Bookmarks Information, Searched Keywords etc.
- Physical Memory Analysis to retrieve URLs visited, Searched Queries, Visited Facebook pages and photos etc.
- Analysis of Social Media Apps Locally Installed:
 - I. Facebook Messenger App Analysis to retrieve the Profile Details, Chats, Calls, Contacts, and Groups of the User
 - II. Twitter App Analysis to retrieve details of Visited Accounts
 - III. Facebook App Analysis to identify the User details such as Profile Picture, Friends and People Searched using the App
 - IV. Xbox App Analysis to identify the Profile Details, Contact Details and Last Message Details
- Analysis of Cloud Apps Locally Installed to retrieve details of Uploaded/Downloaded files from Google Drive, OneDrive & Dropbox, Flip drive
- Skype App Analysis to retrieve the details such as Account Details, Chat Information, Call Details, Messages and Contact List
- Your Phone App Analysis to retrieve Contacts, Installed Apps List, SMS Information, Gallery File Details
- Mailbox App Analysis to retrieve sent, received, and deleted emails, recovers attachments in their original form, and analyses email headers.
- Other Analysis Features:
 - Keyword/Grep Searching Summary/Text-Hex View
 - Multiple Case Loading Saving and Reloading of Cases
 - Facility to Enter Crime Details Save and Print Report
 - Bookmarking Facility Append to Report Facility
 - Detailed Report Generation Customization of report

L. Dhi-Trace

Dhi-Trace is a Forensics Data Analytics tool that ingests evidence from CDAC developed Cyber Forensics tools as well as from loose files to correlate and uncover meaningful insights. It applies AI driven analytics to identify entities, patterns, relationships between evidences from different silos of evidences and generates comprehensive reports while maintaining traceability and evidentiary integrity.

Features

- Entity Recognition: Automatically identifies key entities such as names, locations, dates, numbers and more within documents, enabling rapid extraction of relevant information.

- Entity Watchlist: Add persons or entities of interest to watchlist and instantly identify any matches in newly added evidence, streamlining investigation efforts.
- Person Profiling: Generates detailed profiles of individuals by correlating data across multiple evidence sources, offering a consolidated view of activities and associations of that person.
- Document Clustering: Automatically group similar documents based on content and generate concise summaries to assist investigators in quickly understanding large volumes of text
- Object Detection & Classification: Detects and classifies visual elements such as weapons, vehicles, and more by enhancing the value of photographic evidence.
- Face Detection & Search: Enables face detection in images, supports matching and tagging, and facilitates quick retrieval of visual data related to persons of interest
- Dhi-GPT: An intelligent assistant that answers queries related to the provided evidence while citing and referencing the source evidences for complete traceability
- NSFW Detection: Detects not-safe-for-view content in images enabling safer monitoring and automatically flags sensitive media for review
- Face Watchlist: Stores persons of interest and searches across all cases to find matching or similar faces.
- Case Management: Organizes evidence and analysis by case, helping investigators manage multiple investigations efficiently and separately.
- OCR on Documents & Images: Extracts text from scanned, printed, or handwritten documents and images, making unsearchable files instantly readable and that can be indexed for further search and analysis.
- Geographical Analysis: Visualizes and analyzes location-based data including GPX tracks and coordinates, with geo-fencing capabilities for mapping movements and zones.
- Data Ingestion: Ingests evidence from C-DAC's Cyber Forensics tools and loose files such as emails, spreadsheets, images, logs, and presentations for comprehensive analysis.
- Case-Based Analysis: Organizes evidence and analysis by case, helping investigators manage multiple investigations efficiently and separately.
- Web based system: Access the tool securely through a web interface with login controls, offering both flexibility and strong security.
- Comprehensive Reports: Generates customizable, case-specific reports that consolidate findings, preserving evidentiary integrity for legal or investigative use.

- **Multi-User Support:** Facilitates secure access for multiple users with role-based permissions, enabling collaborative investigation within a controlled environment

M. FinTrace - Financial Transaction Tracer for Banks

FinTrace is a customer financial data extraction and analysis solution developed for banks and financial organizations to extract the details of their customer transactions and uncover the suspicious activities. This forensic tool utilizes machine learning techniques to improve accuracy in detecting complex fraud patterns. It has the bulk input capability so that it can process a set of customers simultaneously and uncover the transaction details and extract the relationship between transactions to help the security teams to quickly identify suspicious accounts and fraud patterns.

Features

- **Fraudulent Transaction Monitoring**
 - Suspicious Transaction Detection
 - Machine learning-based prediction and inference process.
- **Financial Profile Analyzer**
 - FinTrace Dashboard
 - Customer / Account summary
 - Regular / Recurring Credits/ Debits
 - Highest Value Transactions
- **Relationship Extraction**
 - Direct and indirect transaction flow visualization
 - Customer-to-customer association mapping
 - Risk-based node coloring
- **Trend and Behavior Analysis**
 - Transaction Trend Analysis
 - Monthly Trend
 - EOD Balance Trend
 - Customer Spending & Earning Behavior Analysis
- **Report Generation**
 - PDF and Excel Report Generation
 - Suspicious Transaction Reports
 - Suspicious Customer List Reports

N. FinFraudEx - Financial Fraud Examination Tool

FinFraudEx is a financial fraud detection tool which can analyze the financial documents and payroll files to detect financial irregularities. Financial documents can be extracted from the disk using the disk forensics tool CyberCheck that has built-in capabilities to detect fintech documents. The tool performs analytical review of bank statements, account statements, payroll datasets, and transaction logs to

identify suspicious financial patterns. The solution integrates machine learning models and rule-based engine to strengthen the detection and increase precision. Further the suspect's account and transaction records can be examined and traced using the FinTrace tool.

Features

- Account Statement Analysis
 - Counterparty analysis
 - Tag Detection
 - Account Imbalance Detection
- Payroll Data Analysis
 - Duplicate Key Detection
 - Ghost Employee Detection
 - Payroll Anomaly Detection
- Intelligent Data Processing
 - Support processing of logs in various formats including Excel, CSV, and PDF.
 - Machine Learning Models.
 - Rule based Engine which supports 35 + rules
- Transaction Log Analysis
 - Suspicious Transaction Detection
 - Customer Risk Rating
 - Suspicious Customer List generation
- Visualizations
 - Transaction Trend Analysis
 - Customer Behavior Analysis
 - Risk Scoring Dashboards
 - Link Analysis

O. I-FIRST (IoT Forensics Incident Response System)

I-FIRST (IoT Forensics Incident Response System) is a complete field kit that includes all hardware & software tools to identify root cause and impact of a cyber-attack or a malicious incident in an IoT Ecosystem. The first version supports Substation Automation System and Advanced Metering Infrastructure systems in power sector. The kit includes all software and hardware tools required for data extraction and analysis from various components from a IoT ecosystem. The kit also includes the software IFIS (IoT Forensics Inquisitor Software) which is a dedicated software for correlating all evidences and to identify the root cause and impact of the incident.

Features

- Offline Data Acquisition from edge devices of SAS and AMI systems, including SM, BCU, and PR.

- Live Data Acquisition from computing devices in SAS and AMI systems, including HMI, Historian, Data Concentrator, HES, and other Workstations.
- Hashing of Acquired Data to ensure data integrity and authenticity.
- Log Analysis of affected workstations and systems.
- Firmware Analysis of hex dumps acquired from edge devices.
- Root Cause Analysis to understand the Cyber Kill Chain or identify the cause of system malfunction.
- Includes a High-Specification Laptop pre-installed with required software tools.
- Includes a Bootable USB for disk imaging operations.
- Includes UART/JTAG/SPI/I²C to USB Bridge for interfacing with and acquiring data from embedded devices.
- Includes Dupont Wires for hardware interfacing and connectivity.
- Includes Antistatic Covers for protection of electronic components and devices.
- Includes a 3 TB HDD for data storage and evidence acquisition.
- Report Generation in PDF format.
- Optimized for Easy Mobility and field-level forensic operations.
- Dimensions: 45 cm (L) × 28 cm (B) × 12 cm (D).

P. TrueTraveller

TrueTraveller is a portable forensic kit and is a complete solution for performing digital forensics Seizure, Acquisition and Analysis. The kit includes a laptop installed with digital forensics software tools and an integrated disk imaging hardware solution with battery backup. The kit can be easily carried out for on-location forensic investigation.

Features

- Compact, portable tool kit to perform cyber forensics activities in the field
- Incorporates an integrated hardware tool, TrueImager v5.0 (TI5.0) for hashing and imaging hard disk, USB, memory cards and SSDs.
- Includes a laptop suitable for installing forensic software tools and carry out analysis at site.
- Includes SATA/IDE and USB write blockers
- The following list of cyber forensics software tools are installed in the laptop
 - Seizure & Acquisition Tool: CDAC's TrueBack
 - Mobile Forensics & Analysis Tool: CDAC's MobileCheck Suite
 - Acquired Image/Data Analysis Tool: CDAC's CyberCheck Suite
 - Live Forensics Tool: CDAC's Win-Lift

- Cell Phone Number Tracing & Analysis Tool: CDAC's Advik
- SIM Card Acquisition & Analysis Software: CDAC's
- Internet Forensics Tool: CDAC's WebInvestigator
- Image Forensics Tool: CDAC's PhotoExaminer
- Provides Interfacing Cables required for connecting forensic components and storage media to the unit.
- Includes memory card reader, IDE to USB, m-SATA to SATA, μ -SATA to SATA, M.2 to PCIe and U.2 to PCIe adapters
- The kit includes a Printer, Scanner, Camera, screw driver set, torch, Faraday bag for mobile phones and antistatic bags.

4. Invitation for Expression of Interest

- 4.1 C-DAC invites “Expression of Interest” (EOI) in the format given in Annexure-I. Companies can become Reseller partner of C-DAC based on the information furnished in Annexure – I, subject to the assessment by C-DAC.
- 4.2 Expression of Interest (EOI) sought from interested industry vendors for marketing and sales of the Cyber Forensics hardware & software tools developed by C-DAC through the Reseller Partners.
- 4.3 The cost for the Cyber Forensics hardware & software tools has been finalized by the Competent Authority of C-DAC.
- 4.4 This invitation of EOI will be kept open till 16/10/2027. No companies can apply for this EOI after the EOI closure date. However, C-DAC reserves the right to extend the date at the same/ revised terms and conditions after the due date.
- 4.5 Interested companies may submit the expression of interest as per the guidelines stated in this EOI (see section 7.0 and section 8.0)
- 4.6 The companies must have a clear understanding of the terms and conditions stated in the EOI. They should then submit the EOI, duly signed. C-DAC shall assess the information provided by the companies and will intimate the company if they qualify to become reseller partner within 14 days of sending the application. The company shall then pay the reseller registration fee to C-DAC in order to become a reseller partner of C-DAC.
- 4.7 Participating in this Expression of Interest (EOI) does not ensure any affiliation with C-DAC, unless the company is empaneled as a Reseller partner of CDAC.
- 4.8 The product is offered on non-exclusive basis.
- 4.9 The submission of the EOI shall include all such documents that are specified here in to prove the authenticity of their offer and any claim made therein. All cost and expenses associated with submission of EOI shall be borne by the company while submitting the EOI and C-DAC shall have no liability, in any manner in this regard, or if it decides to terminate the process of short listing for any reason whatsoever.
- 4.10 C-DAC reserves the right of rejecting any offer without assigning reasons.

- 4.11 There is neither a business guarantee nor any commitment for funding support from C-DAC to the selected Reseller Partner.

5. Who can apply

Any Indian entity duly incorporated or registered under the applicable laws of India, including a Company incorporated under the Companies Act, 2013, a Limited Liability Partnership registered under the Limited Liability Partnership Act, 2008, or a partnership firm registered under the Indian Partnership Act, 1932, including Micro, Small and Medium Enterprises (MSMEs) and entities recognized as Startups by the Department for Promotion of Industry and Internal Trade (DPIIT), Societies and Trusts, intending to acquire reseller licenses from C-DAC for the marketing, sale, and implementation of C-DAC developed Cyber Forensics hardware and software tools shall be eligible to apply as a reseller, subject to fulfilment of the eligibility requirements specified in this EOI.

6. How to Apply

Interested companies may send expression of interest by filling the template as per Annexure – 1 along with supporting documents to

Section Head,

Technology Promotion Centre,

Centre for Development of Advanced Computing (CDAC)

Vellayambalam, Thiruvananthapuram, Kerala, India, 695033

Phone: 0471 2727508

Fax: 0471 2723456

Email: tpc@cdac.in

Website: www.cdac.in

7. Selection of Reseller Partner

- 7.1 The Reseller Partner is selected based on the response to expression of interest submitted by interested companies and evaluated as per clause 4.6 above.
- 7.2 If selected, the company shall pay reseller registration fee in part or lumpsum (as per payment milestone mentioned in clause 12.4) to become Reseller partner of C-DAC.
- 7.3 C-DAC shall issue are seller partner certificate on receiving their seller registration fee as stipulated in the payment terms.
- 7.4 The Reseller Partnership License is granted on a non-exclusive basis for a fixed term of 3 years. No automatic renewal shall apply.
- 7.5 The Reseller partnership license can be extended beyond 3 years for a period of another 2 years at the terms and conditions relevant at that time.
- 7.6 Reseller partner/s having a valid Reseller partnership license with C-DAC, only will be permitted to quote for C-DAC products for various business opportunities, subject to the applicable scope of authorization, product category, and compliance with GeM, tender, and other Government procurement requirements.
- 7.7 There seller registration fee is non-refundable.

- 7.8 The Reseller Partnership is liable to get terminated if the Reseller is found to be blacklisted or debarred by any Central/State Government department, PSU, Public Sector Bank, or autonomous body. A self-declaration to this effect shall be submitted.
- 7.9 Right of the IPR generated by C-DAC on the applications used with the products shall remain with C-DAC.
- 7.10 The Reseller Partner shall employ his best endeavor to commercialize the said product on a commercial scale within India and abroad at prices to be fixed by him subject to prior written approval from C-DAC and strict compliance with applicable export control regulations as per the applicable laws in India.
- 7.11 The Reseller Partner is required to provide progress reports on their reselling activities to C-DAC every six months. The reports submitted under this EOI shall, at a minimum, include the product name, quantity, cost per license, total value, customer name, sector (e.g., State Police, PSU, Academic Institution), and broad status of the opportunity. Customer-specific and opportunity-specific information shall be treated as confidential information of the Reseller Partner and shall be used by C-DAC solely for monitoring, compliance, and internal record-keeping purposes. C-DAC shall not use such information to directly solicit, bypass, or interfere with the same opportunity or customer, except where the Customer expressly requires the OEM's direct involvement or where disclosure is required under applicable law or Government procurement rules.
- 7.12 The Reseller Partner must obtain written permission from C-DAC before introducing any necessary modifications or improvements during the reselling process covered by this agreement. All Intellectual Property Rights, including patents, copyrights, and trade secrets in any modifications, enhancements, derivative works, or bug fixes—whether developed by C-DAC or suggested/contributed by the Reseller Partner—shall vest exclusively and perpetually with C-DAC. These modifications and improvements will then become an integral part of the software.
- 7.13 The Reseller Partner shall notify to C-DAC the change, if any, in its Registered Office within 15 days of such changes and shall also notify the changes in agreement within the aforesaid stipulated period.
- 7.14 The Reseller Partner shall not on its own name or in the name of any third party, file any patent/copyright Application for the grant of patent/copyright of the said products hereby licensed and shall also not oppose at any time any patent application made by C-DAC.
- 7.15 C-DAC reserves the right to sell its products directly to select Government ministries, departments and strategic institutions in exceptional or mandated cases at C-DAC's own discretionary terms and institutional rates. In such instances, C-DAC shall not use any customer-specific or opportunity-specific information obtained from the Reseller Partner as the basis for such direct engagement.

8. Re selling license, Validity & Renewal

- 8.1 The company/firm must pay a reseller registration fee as mentioned in Table.1 and submit copy of Company Profile, Technical Collaborations, Locations of offices, Strength of company – Marketing & Technical (for Presales & Post sales support), to qualify and become a Reseller partner.
- 8.2 As a Reseller partner, the company/firm shall have the authority to market and implement the products mentioned in the EOI for a period of three (3) years, starting from the date of release of reseller partner certificate by C-DAC.
- 8.3 On successful Payment of Reseller Registration fee grants the partner validity for a period of 3 years from the date of release of reseller partner certificate by C-DAC.
- 8.4 After three years a new reseller partnership is to be taken by the company/firm based on the EOI conditions prevailing at that time.
- 8.5 The partner should have a valid Reseller Partnership for providing any technical support on the reselling deliverables made by C-DAC.
- 8.6 Any customization requirements of the Reseller Partner shall be entertained by C- DAC only if a valid reseller partnership exists. Such customizations shall be undertaken by C-DAC at a cost basis on mutually agreed terms and conditions in contract mode.
- 8.7 Expiry or termination of the Reseller Partner appointment shall not affect the Reseller Partner's obligations in respect of any sale, deployment, warranty, support, training, or other commitments undertaken by it prior to such expiry or termination in respect of any customer. The Reseller Partner shall remain responsible for fulfilling all such obligations for the relevant customer and transaction, unless C-DAC expressly assumes such responsibility in writing or the applicable customer contract provides otherwise.

9. Deliverables

- 9.1 On payment of Reseller Registration Fee and become the reseller partnership with C-DAC, the following list of deliverables shall be provided by C-DAC to the Reseller Partner for product marketing support of Cyber Forensics Tools.
 - Reseller Partnership certificate
 - Brochure softcopy
 - Product Specification Document
 - Technical compliance sheet.
 - Technical Manual- (Hardware and Software Specification to run the applications)
 - User Manual
 - Product Training
- 9.2 The evaluation version of Software tools with a validity period of 12 months will also be provided to resellers. Online hardware tool demonstrations shall be provided by the C-DAC team, with registered resellers given full access for direct hardware testing and evaluation at C-DAC premises. This service is accessible to companies that possess a valid Reseller partnership with C-DAC.

10. Training for Reseller Partners

- 10.1 Upon 100% payment of reseller registration fee (and 40% in case of startups), training for product marketing, software installation, configuration and administration shall be provided up to two working days.
- 10.2 The training shall be conducted at C-DAC Thiruvananthapuram premises.
- 10.3 The travel boarding and lodging expenses of the trainee(s) during the period of training shall be borne by the Reseller Partner.
- 10.4 For training requested outside C-DAC Thiruvananthapuram premises; air travel, boarding and lodging charges of C-DAC officials shall be borne by the Reselling Partner. C-DAC shall also charge manpower per day as per C-DAC rules prevailing at the time of training for any outstation training requested by the Reseller partner. Nomination of the C-DAC trainers and period of stay for out station training will be decided by C-DAC on mutual consultation, depending on the type of training requested.
- 10.5 Additional training may also be given by C-DAC either at the premises of C-DAC Thiruvananthapuram or at the location identified by the Reseller Partner on payment basis at mutually agreed terms and conditions.

11. Technical support

- 11.1 During the license period, C-DAC shall offer remote assistance to the Reselling Partner for the implementation process. This installation support will be provided to the Reseller Partner up to a maximum of two sites.
- 11.2 If any onsite support is requested by the Reseller Partner, C-DAC shall support on mutually agreed terms and conditions.
- 11.3 For onsite support outside C-DAC premises travel, boarding and lodging charges of C-DAC officials shall be borne by the Reseller Partner. C-DAC shall also charge manpower per day as per C-DAC rules prevailing at the time of support request for out station support. Size of the C-DAC team and period of stay for outstation support shall be decided by C-DAC on mutual consultation, depending on the type of support requested

12. Cost for Registration of Reseller

- 12.1 The products shall be commercialized through Reseller Partners by paying a reseller registration fee for obtaining the Reseller Partnership certificate and then subscribing the deployment license from C-DAC during the period of validity of the partnership.
- 12.2 The cost of Cyber Forensics tools, along with the price distribution, can be obtained from C-DAC upon submitting a response to the EOI.
- 12.3 The Reseller Partnership with C-DAC requires reseller partners to pay a reseller registration fee plus applicable taxes, for the marketing and implementation of Cyber Forensics tools. Only reseller partners who have a valid partnership with C-DAC are eligible to subscribe the products.

12.4 The one-time fee of Rs 2 lakh plus taxes for Authorized Reseller- Companies other than Start-ups and Rs. 1 Lakh for startups recognized by DPIIT; needs to be paid to become an authorized Reseller Partner of C-DAC (T) in single instalment. However early bird registrations will have the benefits mentioned in the table [1].

Table1: Details of Early Bird registration fee

Category	Reseller Registration Fee (in Rs.) for Early bird		Payment Terms
	First 6 months	7 th month onwards	
Authorized Reseller- other than Start-ups	50,000 plus applicable taxes	1,50,000 plus applicable taxes	The onetime registration fee of 2 lakh can be paid in two instalments: i) Rs.50,000/- plus taxes to become reseller partner (ii) Rs.1,50,000/- plus taxes to obtain the forensic software license for deployment <i>Failing to complete the payment within 12 months of payment of the first instalment, the license is liable get terminated automatically and whatever the amount paid to C-DAC will be forfeited. No refund shall be permitted in this regard</i>
Startups recognized by DPIIT	25,000 plus applicable taxes	75,000 plus applicable taxes	The onetime registration fee of 1 lakh can be paid in two instalments: ii) Rs.25,000/- plus taxes to become reseller partner (ii) Rs.75,000/- plus taxes to obtain the forensic software license for deployment. <i>Failing to complete the payment within 12 months of payment of the first instalment, the license is liable get terminated automatically and whatever the amount paid to C-DAC will be forfeited. No refund shall be permitted in this regard</i>

12.5 The selected companies/firms interested in purchasing and marketing C-DAC products shall be provided with the detailed cost and license pack of the products.

13.Interpretation of the Clauses in the EoI Document

In case of any ambiguity/dispute in the interpretation of any of the clauses in the EoI document, the interpretation of the clauses by Executive Director, C-DAC Thiruvananthapuram shall be final and binding on all parties

For any queries please contact:

Section Head (Technology Promotion Centre)
Vellayambalam, C-DAC, Thiruvananthapuram
Contact: 0471 2727508, 0471 2723333 (extn: 220/450), 9847069184
email: tpc@cdac.in

Annexure-I

Details of the Reseller Partner

A	COMPANY PROFILE
1.	Name and address of the Organization & Website details:
2.	Name of the Contact Person: Address: Mobile: Landline: Fax: E-Mail:
3.	Year of Incorporation:
4.	Type of Organization a. Public Sector/Limited/Private Limited/Partnership/ Society/Any other b. Names of Directors of the Board/Proprietors c. Name and address of NRI(s), if any d. Documentary proof as listed below • Certificate of Incorporation, • Memorandum of Association (MoA), • Articles of Association (AoA), • LLP Agreement, • Partnership Deed, • Bye Laws etc. whichever is applicable to the bidder.
5.	Category of the firm: Large/Medium/Small scale unit /others
6.	Address of the Registered Office: (Include Certificate of Registration)
7.	The turnover is to be supported by financial statements of accounts/ Annual reports duly certified by a Chartered accountant/Balancesheetsoflast3years/ Income tax returns for the last 3 years period.
8.	Number of Offices with addresses (Excluding Registered Office): India, Abroad:
9.	Certificate of registration
10.	Permanent Account Number
11.	GST Reg. No.
12.	ISO or any equivalent Certification
B.	OTHER REQUIREMENTS
13.	The total manpower strength at various levels to be furnished
14.	The in-house technological expertise available to be furnished, if available

15.	List of products/technologies worked with as regular activity in last here years. Give the list of products/technologies with general specifications and the customers.
16.	List of PSUs/Govt.customers that the organization dealt with for last 3 years
17.	The details of sales and marketing to be furnished
C.	Expression of Interest: Spell out the extent of interest and envisaged market potential

**No part of the above 18 fields shall be dropped in furnishing the details and if details are dropped the application will be considered incomplete and subject for rejection of reseller application.*

I affirm that the information provided above is accurate to the best of my understanding. I confirm that we have fully understood the terms and conditions, as well as the costs specified in the Expression of Interest (EOI) for the products. As a Reseller Partner of CDAC, we are committed to actively promoting and implementing these products.

Signature with Name& Seal:

Place:

Date: