CYBER X

CYBER X

2024

INTRODUCTION TO CYBERX

Cyber-crimes present a multifaceted challenge that extends across various domains, posing significant threats to individuals, businesses, and nations alike. One of the primary challenges is the dynamic and evolving nature of cyber threats, as malicious actors continually adapt their tactics to exploit vulnerabilities in technology.

Additionally, the anonymity afforded to perpetrators in the virtual realm makes it challenging for law enforcement to identify and apprehend cyber criminals. The financial impact of cyber-crimes is substantial, with organizations facing not only direct financial losses but also costs associated with mitigating breaches, implementing security measures, and recovering from reputational damage. Furthermore, the potential for cyber-attacks to compromise critical infrastructure, intellectual property, and personal information underscores the urgent need for interagency cooperation and robust cybersecurity measures to address this persistent and evolving threat.

EXHIBITION

Various government agencies have been making tools for cyber-crime investigation and cyber security. There is no single platform that makes one aware about these products. With this background, Academy has started “Cyber X – Cyber Products Exhibition” wherein, Academy will ask the government agencies to host their Cyber products in this exhibition hall. Every year about 1000 IPS officers visit Academy for various training programs. One visit to this exhibition hall will apprise them about these products. Our team members will also give demo of these products if officers desires so.

To start with CDAC Thiruvananthapuram and CDAC Hyderabad have shared their cyber-crime investigation tools in this exhibition hall. NCR&IC in BPR&D has also collaborated with various institutions like IITs, NITs, IIITs to come up with AI based tools. A start-up company incubated by IIT Kanpur has shared the access to their cloud-based cryptocurrency analysis tool. Academy is also hosting a prototype blockchain tool developed to store the evidence developed through research cell of the Academy.

In future, Academy proposes to approach NFSU, RRU, IITs, NITs, IIITs, DRDO and similar organizations to promote “Make in India” cyber products among law enforcement agencies. Academy will also promote these products through digital platforms like e-library and Knowledge Management System. Metaverse for the exhibition will be available soon.

LIST OF TOOLS

1 Cyber Security Tools

1. E-Samarthak -Multistage Attack Prediction using Machine Learning [CDAC Hyderabad] -(50,000)
2. AppSamvid – Application whitelisting software[CDAC Hyderabad] -(70,000)
3. M-Kavach -Mobile Device Security Solution [CDAC Hyderabad] -(Free)
4. Parikshan – Insightful App Security Analysis [CDAC Hyderabad] -(14 lakh/year)
5. USB Pratirodh [CDAC Hyderabad] -(Free)
6. App security toolkit [NCR&IC, IIT Patna]

2 Digital Forensics Tools

7. CyberCheck – Disk Forensic Tool [CDAC Thiruvananthapuram] -(3.75 lakh)
8. MobileCheck – Mobile forensics tool [CDAC Thiruvananthapuram] -(3 lakh)
9. NeSA – Network Packet Session Analyzer [CDAC Thiruvananthapuram] -(70,000)
10. PhotoExaminer – Forensic Multimedia Analysis Tool [CDAC Thiruvananthapuram] -(1 lakh)
11. SIMXtractor – SIM Card Imaging and Analysis Tool [CDAC Thiruvananthapuram] -(5,000)
12. TrueImager – Forensic Disc Imaging Tool [CDAC Thiruvananthapuram] -(3 lakh)
13. TrueTraveller – Portable Cyber Forensic Field Kit [CDAC Thiruvananthapuram] -(15lakh)
14. Win-Lift – Windows Live Forensics Tool [CDAC Thiruvananthapuram] -(1.35 lakh)

3 Blockchain Based Tools

15. Blockchain Enabled Evidence Securing and Tracking- Prototype. [SVPNPA]
16. Blockstash Intelligence for cryptocurrency transaction visualization. [Startup of IITK]
17. BaaS- Blockchain as a Service [CDAC Hyderabad] -(Free)

LIST OF TOOLS

4 Investigation Tools

18. Advik – IPDR Analyzer [CDAC Thiruvananthapuram] -(1.8 lakh)
19. Advik – CDR Analyzer [CDAC Thiruvananthapuram] -(1.2 lakh)
20. WebInvestigator – Internet Forensics Tool for Windows [CDAC Thiruvananthapuram] -(1.15 lakh)

5 AI & ML Based Tools

21. FakeCheck – [CDAC Hyderabad]
22. NSFW (not safe for work) Content Blocker - Obscene detection browser extension [NCR&IC, IIIT Allahabad]
23. Testa - Obscene detection mobile application [NCR&IC, IIT Patna]
24. Obscene detection [NCR&IC, IIT Patna]
25. StopPorn - Browser extension tool [NCR&IC, IIITDM Kancheepuram]
26. Fake and Obscene Image Detection Tool [NCR&IC, NIT Meghalaya]
27. File-Gateway [NCR&IC, IIITDM Kancheepuram]
28. Deep Fake Detection Tool [NCR&IC, NIT Calicut]
29. Fake Face and Video Detection System [NCR&IC, IIT Patna]
30. Doctoring Detection Tool [NCR&IC, IIT Jodhpur]
31. Proton [NCR&IC, NIT Calicut]
32. Speech to Text [SVPNPA]

6 Other Tools

33. Handbook on IoT Device Security Evaluation [CDAC, Hyderabad]
34. Criminal Case Management System

For additional information Contact us –

1. SVPNPA, Hyderabad – cyberx@svpnpa.gov.in, 040 24234486 / 040 24235743
2. CDAC, Thiruvananthapuram – cyber-tvm@cdac.in, 0471 2781500 / 0471 2781555
3. CDAC, Hyderabad – esuraksha@cdac.in, 9100682644 / 04029564391

List of tools available in CyberX

S.No.	Tool Name	Description
1	Blockchain enabled evidence securing & tracking	To improve integrity and trust on evidence gathered during investigation by ensuring transparency on chain of custody and storing the evidence in an immutable (tamper-proof) way and providing convenient 24x7 query access of case evidence to all stakeholders.
2	Blockstash intelligence for cryptocurrency transaction visualization	Blockstash is a cutting-edge SaaS Crypto Forensics Platform that empower crypto investigations. It offers advanced features for comprehensive scrutiny, providing insights into blockchain activities and aiding in fraud detection and compliance. Simplify complex investigations, trace digital footprints, and seamlessly generate detailed reports.
3	Advik IP Data Record Analyzer	Import and analyze IPDR logs from different service providers, generating comprehensive reports that include correlation with CDR, SDR, and Cell-ID data.
4	Advik Call Data Record Analyzer	This tool can import and analyze CDR/IPDR logs and generates a comprehensive report of frequency statistics including device provider details and subscriber details(SDR) of CDR numbers.
5	CyberCheck	It is a web based forensic data recovery and analysis tool to enable Law Enforcement Officers to quickly and efficiently analyze digital evidence files of storage media.
6	MobileCheck	Digital forensics solution for Basic phones, Smartphones and GPS Devices. This tool supports acquisition, analysis & reporting of evidence from mobile devices.
7	NeSA (Network Session Analyser)	It is the networks forensics tool to capture and analyze network traffic. Data sent through the network can be captured, recreated and exported using this tool. Major features include Data Reconstruction, analysis mode, searching and filtering.

8	PhotoExaminer	It is Windows based cyber forensic application for classifying, enhancing, analyzing and generating the report of image and video evidence.
9	SIMXtractor	It is a forensic solution for imaging and analyzing SIM cards. It contains a SIM Card Reader, SIM Imager and Analyser. It works with both GSM and CDMA SIM cards.
10	TrueImager	It is a high speed, lightweight, portable disk imaging hardware tool with battery backup support. It is capable of performing Hashing, Imaging and Cloning operations of source storage media and can also perform wiping and formatting of destination disk.
11	TrueTraveller	It is a portable forensic kit and is a complete solution for performing digital forensics Seizure, Acquisition and Analysis which can be carried out for on-location forensic investigation.
12	Web Investigator	It is an Internet Forensics tool that allows cyber crime investigators to acquire and analyze forensically relevant artifacts related to Internet usage of the suspect's Windows computers
13	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.
14	AppSamvid	App Samvid is application whitelisting software for Microsoft Windows based operating systems. Whitelisting allows only the pre-approved files to execute on the operating system. This is in contrast to traditional signature based antivirus software approach of blacklisting the virus files. Whitelisting has the advantage over blacklisting as it does not require frequent virus definition updates. App Samvid can protect operating systems against computer malware (such as Viruses and Trojans).
15	Blockchain-as-a-Service (BaaS)	National Blockchain Framework is an initiative of Ministry of Electronics and Information Technology (MeitY) to make India ready for large scale adoption of Blockchain and enable trust for applications in the domain of e-Governance.

16	E-Samarthak	It is a Multistage attack prediction using machine learning and MITRE ATT&CK Framework tool. It also predicts the cyber attacks (Ransomware, APT, Botnets, Fileless malware) to strategize the early mitigation.
17	Handbook on IoT Device Security Evaluation	It is the first-of-its-kind compilation in the world, comprising detailed security evaluation procedures, tools and techniques, that are essential elements in performing the security analysis of IoT devices.
18	M-Kavach 2	It 2 is a comprehensive mobile device security solution addressing emerging threats related to Android based mobile devices. The major emphasis is on advising the users against security misconfigurations, detection of hidden/ banned apps and scanning the device for potential malicious apps installed on the user's mobile device.
19	Parikshan	Parikshan is an Automation tool mainly focused on performing static and dynamic analysis of mobile applications. The tool has the capabilities to identify the security vulnerabilities and perform penetration testing for a few of them. As an outcome, a detailed security audit report is generated containing the information about the identified vulnerabilities which aids to carry out further analysis.
20	USB Pratirodh	This software solution controls the usage of removable storage media like pen drives, external hard drives, cell phones and other supported USB mass storage devices. Only authenticated users can access the removable storage media.
21	Criminal Case Management System (CCMS)	This tool helps senior officers to assist the progress of investigation by enhance the State Police’s capabilities in managing, analyzing, and cross-referencing criminal databases.
22	NSFW Content Blocker	It is a browser extension to block obscene image and video content on Google sites and other pornographic websites.
23	Deep Fake Detection Tool	It is a desktop tool with a user-friendly graphic interface. It can detect whether multimedia content is deep fake audio, video, or image content with a certain confidence Score.

24	Testa	Automated obscene content detection tool for mobile phones. It is an Android mobile app that can run on a mobile device to scan and identify obscene content.
25	App security toolkit	This android app can identify those apps that are stealing the privacy of a user by giving each app a score and highlight them with different color range (red-high, green-low)
26	Obscene detection	This web-based tool detects obscene content from the input video. It also extracts faces from the video if present. From the input video, key frames are analyzed and an obscene score is given to those frames in the result.
27	Fake Face and Video Detection System	This is a web-based tool to detect fake multimedia content (images and videos). This tool can also fetch deep-fake videos from Twitter.
28	StopPorn (Browser extension)	This tool blocks obscene photo and video content while browsing internet through FireFox
29	Doctoring Detection Tool	It is a Desktop application to detect deep fake image, video and audio with a certain confidence score.
30	Fake and Obscene Image Detection Tool	This tool analyzes and detects obscene content and forged images from websites as well as locally saved images. It can identify the manipulation in an image and highlight those areas which are manipulated.
31	File-Gateway	This desktop tool works in the back-end once we run it. If we put any obscene and forged porn videos in the folder where the tool is stored, it will delete all those videos only if this tool is running. It will delete if found any obscene video otherwise it will ignore the video.
32	Proton	It is a desktop application to scan social media profiles (Instagram, Facebook, twitter/X) and it identifies the privacy gaps on a social media profile of an individual. Only works on Mozilla Firefox browser. Generate the end report with Comment analysis for cyberbullying, No. of followers, privacy scan report if found any.

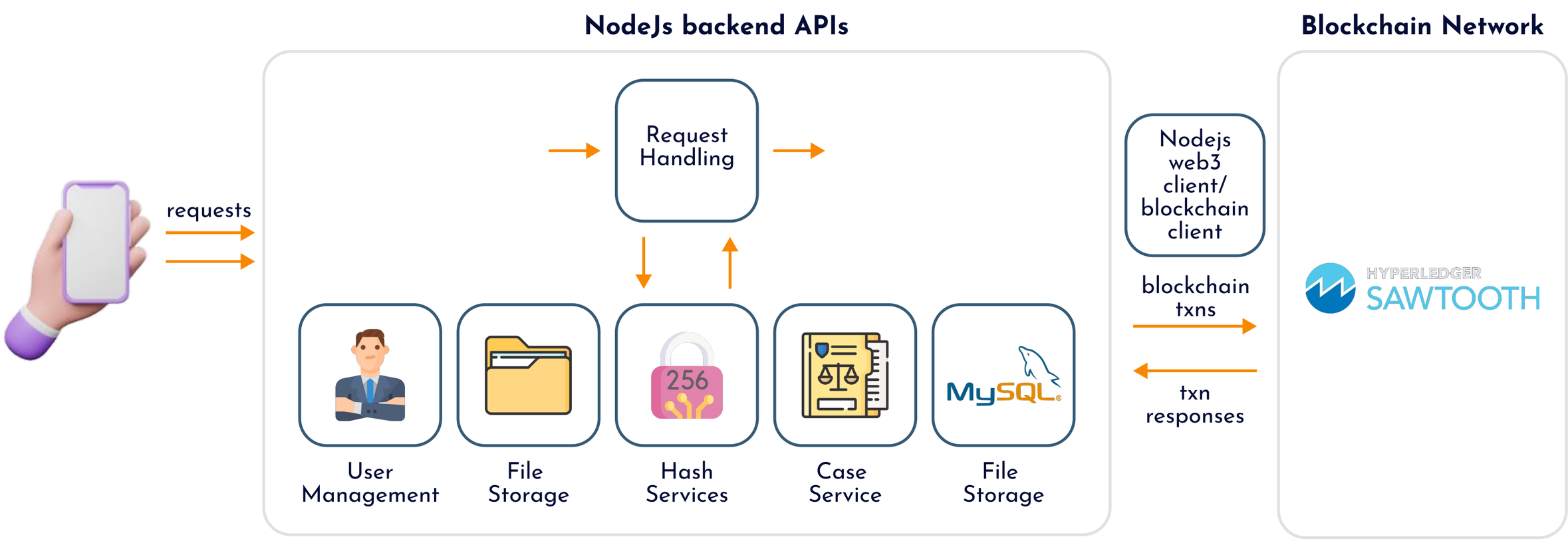
USE OF BLOCKCHAIN TECHNOLOGY FOR EVIDENCE HANDLING

Blockchain enabled Evidence Securing & Tracking

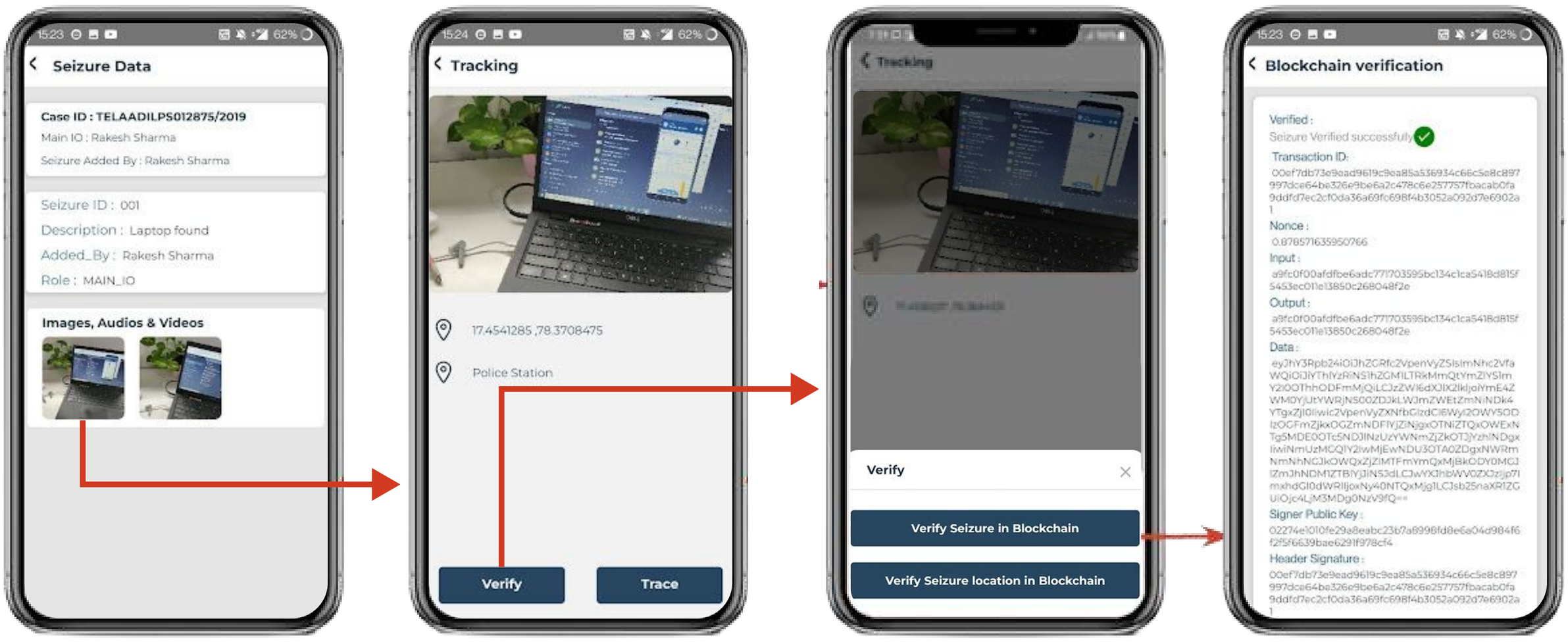
To improve integrity and trust on evidence gathered during investigation by ensuring transparency on chain of custody and storing the evidence in an immutable (tamper-proof) way and providing convenient 24x7 query access of case evidence to all stakeholders.

Technical Overview

The system facilitates the digital input of evidence details, including Seized items, Crime details, and Arrest details. Uploaded files are stored on a designated server, with IDs generated in the background, encompassing metadata and SHA-256 file hashes. This data is sent as a payload to the blockchain. In the verification process, the hash is computed from the file content at the URL, cross-referenced with the blockchain-stored hash. Successful verification requires matching hashes, and any file modifications at the server lead to verification failure against the blockchain hash.



Blockchain Verification & Seizure Location Updation



Conceptualised and designed by: Mr A Y V Krishna, IPS, ADGP, Assam, 09445056302
Developed by: [x]cube LABS, **Email:** balanagendar.singh@xcubelabs.com, saiprasad.dasyam@xcubelabs.com

24X7
CRYPTO SURVEILLANCE

1000+
CRYPTOCURRENCIES AND TOKEN

1BN+
TAGGED ADDRESSES

1000+
CRYPTO EXCHANGES ADDED

10+
CROSS-CHAIN MONITORING

10+
CASES INVESTIGATED

TRUSTED AND VERIFIED TOOL

We developed our crypto forensics tool with the feedback of multiple Law enforcement agencies and crypto exchanges.

We investigated more than 100 cases, successfully trace the culprits, and find there KYC information from crypto exchanges.

CONTACT US

REQUEST DEMO | COLLABORATE

Email contact@blockstash.com
Phone +91 8808682517(India)

LEADING THE WAY TO TRANSPARENT CRYPTOCURRENCY SOLUTIONS.

blockstash.in

CRYPTO CRIME INVESTIGATION AND ANALYSIS

Blockstash is a cutting-edge SaaS Crypto Forensics Platform that empower crypto investigations. Our tool offers advanced features for comprehensive scrutiny, providing insights into blockchain activities and aiding in fraud detection and compliance. Simplify complex investigations, trace digital footprints, and seamlessly generate detailed reports.

UNCOVER LEADS BEFORE THEY VANISH

- Network Visualization
- Case Management
- Active Address Tagging
- Blockchain Honeypots
- Report Generation
- NFT Forensics
- Open-Source Intelligence (OSINT)
- Darkweb Monitoring
- Crypto Compliance
- ML based Behavior Analysis

NATIONWIDE FORENSIC NETWORK

Our goal is to establish a comprehensive nationwide forensic network, enabling us to expedite investigations by harnessing collective investigation data from across the country.

Incubated at **IIT Kanpur,** Blockstash stands on a strong foundation, backed by a team of seasoned experts in the realm of cryptocurrency and blockchain technology.

MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY GOVERNMENT OF INDIA

Advik

IPDR Analyzer

Import and analyze IPDR logs from different service providers, generating comprehensive reports that include correlation with CDR, SDR, and Cell-ID data.

Automatic Importing of IPDRs

Effortlessly import IPDRs with the automated feature, streamlining your data processing and analysis for increased productivity and ease of use.

Domain Mapping

Determines the domain details of an IP address, allowing the user to identify the website or online service associated with that particular IP.

Search & Filters

20-plus filters help to efficiently narrow down your results & find the most relevant information. Search with multiple conditions to align your analysis with the specific criteria.

Probable WhatsApp Records

Identifies the records related to WhatsApp Communication and presents them to the user for further analysis.

Link Analyzer

Presents relationships between IP addresses and mobile numbers in both tabular form and graph representation to illustrate the connections and patterns

Comprehensive Reports

The consolidated report includes the findings and analysis conducted throughout the analysis process. Save your findings in multiple formats.

Correlation with CDR, SDR & Cell ID

Identify relationship between mobile numbers from IPDR with CDR and determine location as well as address information from SDR & Cell-ID Logs.

Geo Distance

Identify geographical distance between different IPDR data points.

Common Number Analysis

Identify the common IPs, Mobile numbers or IMEI numbers from multiple IPDR data files.

CYBER FORENSICS SECTION
Centre for Development of Advanced Computing
(R&D Organization of Ministry of Electronics and Information Technology Govt. of India)
Technopark Campus, Kariyavattom P.O, Thiruvananthapuram - 695 581
Ph.No: +91 471 278 1500, 2781555
Email: cyber-tvm@cdac.in, Web: www.cyberforensics.in

Advik

Call Data Record Analysis Tool

Advik Call Data Record Analyser which can import and analyse CDR/IPDR logs of any service provider in India and generates a comperhensive report of frequency statistics including dervice provider details and subscriber details(SDR) of CDR numbers

1 Importing Logs

- CDR / Tower CDR / IPDR / SDR / Cell ID.
- Automatic importing.
- Preset Management.
- Large Collection of inbuilt presets.

2 Analysis

- Link Analysis.
- Suspect List.
- Geographical Analysis.
- Call Flow Visualizer.
- New Number Analysis.
- Group Analysis.
- Preliminary CDR Analysis.

3 Search and Filter

- Customizable Search.
- SDR Search.
- IMEI/Phone Number Search.
- 20+ Inbuilt Filters.
- Customizable Filters.
- Filter History.

4 Reports

- Customizable Reports.
- Option to export to different formats.

5 Advik User Access Control

- Manage users.
- Manage user privileges.

6 Other Features

- Case-Based Analysis.
- Customizable UI.
- Online Tutorial.

CYBER FORENSICS SECTION
Centre for Development of Advanced Computing
(R&D Organization of Ministry of Electronics and Information Technology Govt. of India)
Technopark Campus, Kariyavattom P.O, Thiruvananthapuram - 695 581
Ph.No: +91 471 278 1500, 2781555
Email: cyber-tvm@cdac.in, Web: www.cyberforensics.in

CyberCheck

Disk Forensics Tool

CyberCheck is a web based forensic data recovery and analysis tool to enable Law Enforcement Officers to quickly and efficiently analyse digital evidence files of storage media.

Processes TrueBack, EnCase, Raw images and Virtual Disk images: VDI, VHD & VMDK.

Recovers deleted files, folders and partitions. File hash and file signature based analysis options.

Supports the analysis of file systems such as FAT, exFAT, NTFS, Linux EXT, UFS, HFS & YAFFS2.

Data carving from disk, slack areas, unallocated areas and files.

Data Recovery

- Deleted file and folder recovery
- Data carving of 400+ file formats
- Partition recovery
- Preview of disk & volumes
- File metadata extraction

Analysis Features

- Disk indexing and fuzzy searching
- Timeline analysis
- Known good file filtering using NSRL dataset
- Overwritten and signature mismatch file detection
- Password protected file detection

Artifacts Extraction

- Registry analysis
- Thumbnail extraction from thumbcache database
- Recycle Bin data extraction
- Link file analysis
- Windows 10 artifacts extraction
- ShellBag analysis
- Browser forensics

Other Features

- Feature-rich bulk file export
- Bookmarking and report generation
- Evidence hash verification
- File hash computation
- Evidence conversion to RAW image
- Web browser based user interface supporting concurrent users
- Multiple case analysis support

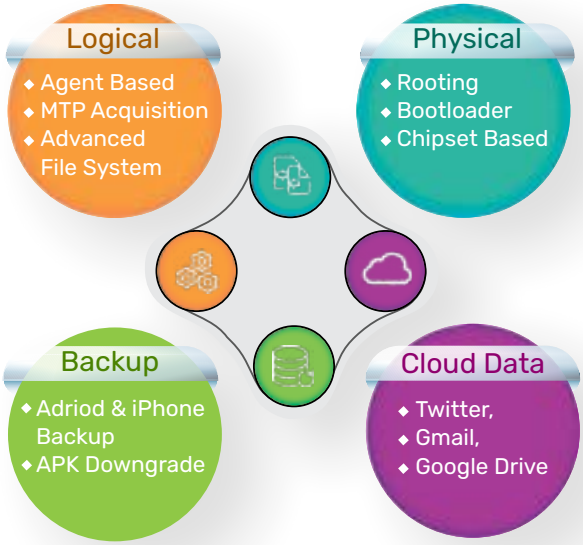
CYBER FORENSICS SECTION
Centre for Development of Advanced Computing
(R&D Organization of Ministry of Electronics and Information Technology Govt. of India)
Technopark Campus, Kariyavattom P.O, Thiruvananthapuram - 695 581
Ph.No: +91 471 278 1500, 2781555
Email: cyber-tvm@cdac.in, Web: www.cyberforensics.in

MobileCheck

A Forensic Solution for Mobile Phones & Smart Phones

Digital forensics solution for Basic phones, Smart phones and GPS Devices. The solution supports acquisition, analysis & reporting of evidence from mobile devices. The major tools in the MobileCheck solution are Imgaer, Analyser & SmartPASSeR.

MobileCheck Imager



Supports

- iPhones
- Android Phones
- Basic Phones
- Feature Phones
- GPS Devices
- Memory Cards

MobileCheck Analyser

- **Analysis Supports :-** MobileCheck Files, Binary Files, Phone backup, Cloud Data, SIMXtractor Files, UFED Physical Files
- **Social Apps :-** WhatsApp, Telegram, Signal, Instagram, LinkedIn etc
- **Phone Artefacts :-** Contacts, Call Logs, Messages, Notes etc
- **File System and Deleted Data :-** EXT2, FAT32, YAFFS, F2FS etc
- **Malware Scanner :-** Trojan, Virus, Spyware etc
- **Cloud Analysis :-** Gmail, Google Drive, Twitter etc
- **Visual Analytics :-** TimeLine and Link Analysis
- **Custom Report :-** Supports report generation

CYBER FORENSICS SECTION
Centre for Development of Advanced Computing
(R&D Organization of Ministry of Electronics and Information Technology Govt. of India)
Technopark Campus, Kariyavattom P.O, Thiruvananthapuram - 695 581
Ph.No: +91 471 278 1500, 2781555
Email: cyber-tvm@cdac.in, Web: www.cyberforensics.in

NeSA

Network Packet Session Analyser

NeSA (Network Session Analyser) is the networks forensics tool to capture and analyse network traffic. Data sent through the network can be captured, recreated and exported using this tool.

Major Features

Data Reconstruction

With the help of flexible and powerful filtering system, data from HTTP, SMTP, POP3 and FTP session can be recreated and visualized in an analysis friendly manner. The tool has built-in data viewers including a Mailview, to help the analyst to concentrate on analysis.

Analysis Modes

NeSA supports both data level and packet level analysis of network data. In data level, the analyst can concentrate on the data and can avoid the nuts and bolts of network protocols. But if he/she wishes to dig deeper, the packet analysis mode is ready to extend its helping hands.

Searching & Filtering

Searching and filtering helps to reach analyst's goals faster. Flexible filter expressions are provided for packet level analysis and for data level analysis. The data level filtering supports filtering based on date, time, IP, MAC and port. The regular expression based searching gives the analyst the full power that he expects from a tool.

Other Features

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

CYBER FORENSICS SECTION
Centre for Development of Advanced Computing
(R&D Organization of Ministry of Electronics and Information Technology Govt. of India)
Technopark Campus, Kariyavattom P.O, Thiruvananthapuram - 695 581
Ph.No: +91 471 278 1500, 2781555
Email: cyber-tvm@cdac.in, Web: www.cyberforensics.in

PhotoExaminer

Forensic Multimedia Analysis Tool

PhotoExaminer is a Windows based cyber forensic application for classifying, enhancing, analysing and generating the report of image and video evidences.

Supported Images

- Multimedia folders or disk images
- Data Carving

Evidence Filtering

- Make and Model Filtering
- Source Camera filtering
- Skintone Filtering
- Metadata based filtering

Image Search

- Image Similarity Search
- Face Search

Analysis

- Source Camera Identification
- Error Level Analysis
- Thumbnail Mismatch Identification
- Hidden Pixel Analysis

Views

- Gallery View
- Tabular Metadata Viewer
- Image Viewer
- Video Player

Image Enhancements

- Basic Image Enhancements
- Dark Image Enhancement
- Super Resolution

Reports

- Customizable Report
- Metadata Report

CYBER FORENSICS SECTION
Centre for Development of Advanced Computing
(R&D Organization of Ministry of Electronics and Information Technology Govt. of India)
Technopark Campus, Kariyavattom P.O, Thiruvananthapuram - 695 581
Ph.No: +91 471 278 1500, 2781555
Email: cyber-tvm@cdac.in, Web: www.cyberforensics.in

SIMXtractor

SIM Card Imaging & Analysis Tool

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

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)

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

SIM Analyser

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

CYBER FORENSICS SECTION
Centre for Development of Advanced Computing
(R&D Organization of Ministry of Electronics and Information Technology Govt. of India)
Technopark Campus, Kariyavattom P.O, Thiruvananthapuram - 695 581
Ph.No: +91 471 278 1500, 2781555
Email: cyber-tvm@cdac.in, Web: www.cyberforensics.in

MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY GOVERNMENT OF INDIA

TrueImager

Forensic Disc Imaging Tool

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.

Hardware Specifications

Battery Backup

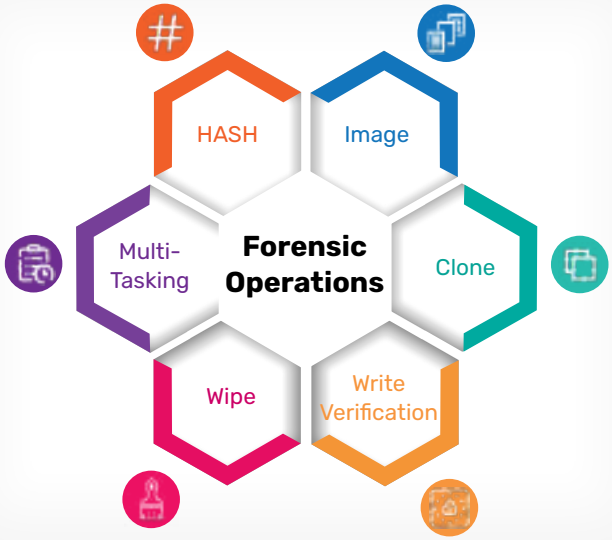
Supported Source Disk

IDE, mSATA, PCIe, SATA, SATA, USB

Built-in Write Protection

Destination Interfaces

SATA, USB



Data Verification & Reporting

- Report Generation
- S.M.A.R.T Verification
- Disk Browsing
- Report File Exporting
- Auto Shut Down
- Overall Process Log

CYBER FORENSICS SECTION
Centre for Development of Advanced Computing
(R&D Organization of Ministry of Electronics and Information Technology Govt. of India)
Technopark Campus, Kariyavattom P.O, Thiruvananthapuram - 695 581
Ph.No: +91 471 278 1500, 2781555
Email: cyber-tvm@cdac.in, Web: www.cyberforensics.in

TrueTraveller

Portable Cyber Forensic Field Kit

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 investigations.

Major Features

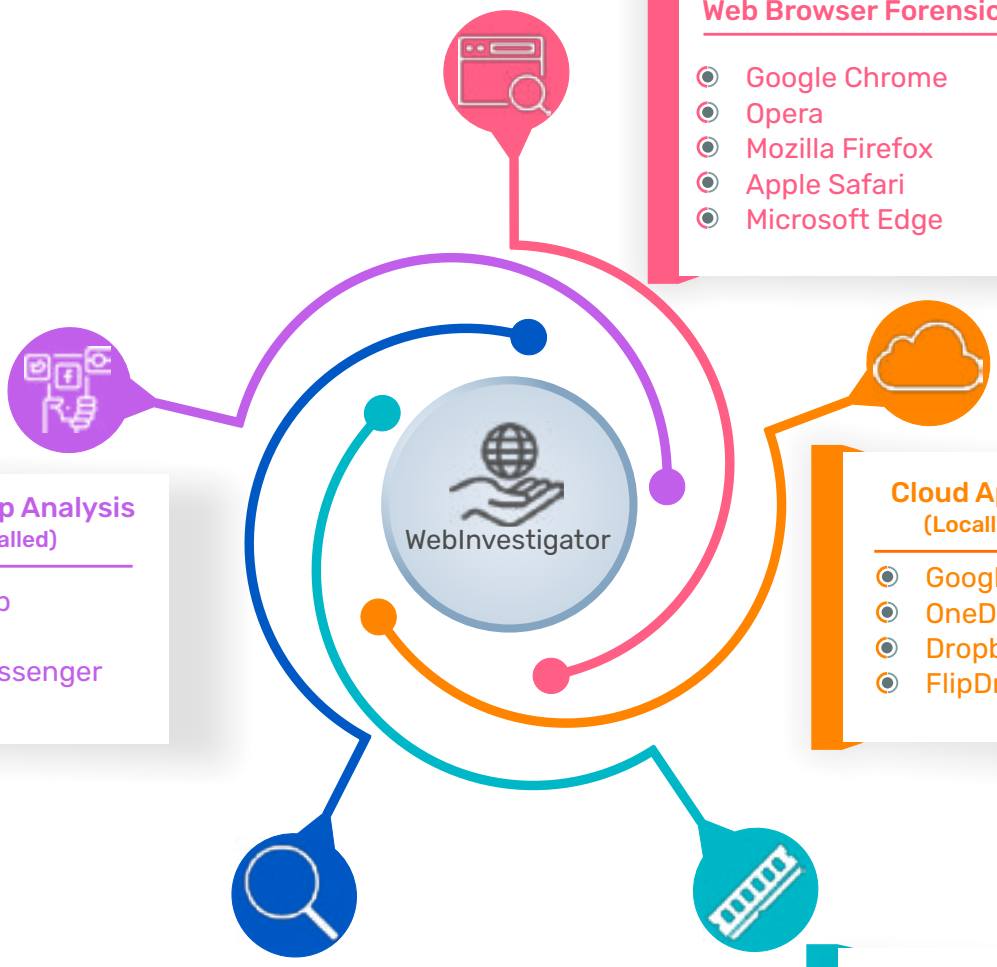
- Easily portable kit with Trolley support
- Disk imaging hardware tool capable of performing multi-tasking
- SATA & USB ports for interfacing destination media
- Includes adapters for IDE, memory cards, m-SATA & µ-SATA disks
- Includes Write Blockers for SATA, IDE, USB disks
- Includes CyberCheck Suite for Disk Image Analysis, MobileCheck for Mobile Forensics
- Includes Win-LiFT for Live forensics, Advik for CDR Analysis and NeSA for Network forensics
- Includes hardware dongle for SIM card seizure and acquisition
- Includes portable printer,scanner, camera, screw driver set & torch.

CYBER FORENSICS SECTION
Centre for Development of Advanced Computing
(R&D Organization of Ministry of Electronics and Information Technology Govt. of India)
Technopark Campus, Kariyavattom P.O, Thiruvananthapuram - 695 581
Ph.No: +91 471 278 1500, 2781555
Email: cyber-tvm@cdac.in, Web: www.cyberforensics.in

WebInvestigator

Internet Forensics Tool for Windows

WebInvestigator is an Internet Forensics Tool that allows cyber crime investigators to acquire and 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.



Web Browser Forensics

- Google Chrome
- Opera
- Mozilla Firefox
- Apple Safari
- Microsoft Edge

Social Media App Analysis (Locally Installed)

- Facebook App
- Twitter
- Facebook Messenger
- Xbox

Cloud App Analysis (Locally Installed)

- Google Drive
- OneDrive
- Dropbox
- FlipDrive

Analysis Features

- Keyword/Grep Searching
- Detailed Report Generation
- Customisation of Report

Physical Memory Analysis

- Visited Sites
- Searched Keywords
- Email ID's

CYBER FORENSICS SECTION
Centre for Development of Advanced Computing
(R&D Organization of Ministry of Electronics and Information Technology Govt. of India)
Technopark Campus, Kariyavattom P.O, Thiruvananthapuram - 695 581
Ph.No: +91 471 278 1500, 2781555
Email: cyber-tvm@cdac.in, Web: www.cyberforensics.in

Win-LiFT

Windows Live Forensics Tool

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 data acquisition using Win-LiFTImager and analysis of the same using Win-LiFTAnalyzer.

Win-LiFTImagerBuilder

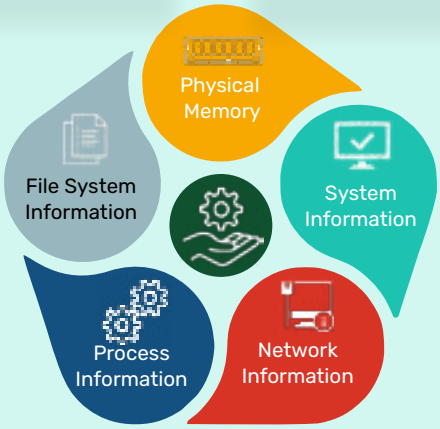
Tool for building Win-LiFTImager

- Runs in the Investigator's machine
- Case based Artifact Selection
- Builds Win-LiFTImager tool into a USB

Win-LiFTImager

Volatile Data Acquisition Tool

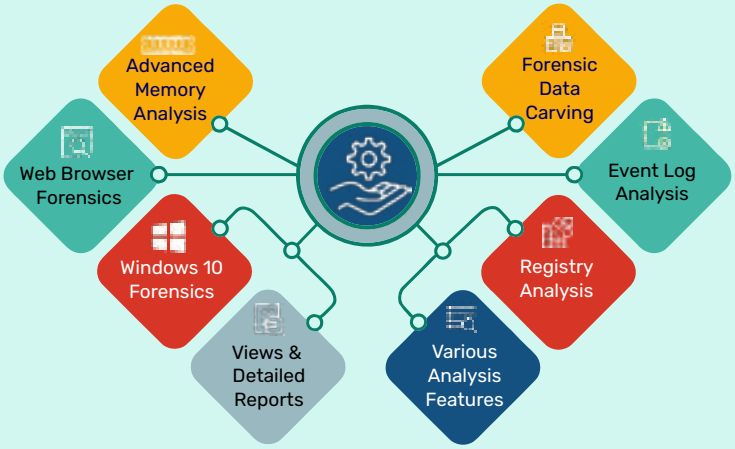
- Runs in the Suspect's machine from the USB
- Acquires volatile / major non-volatile artifacts
- Ensures minimal tampering
- File System Level Dumping



Win-LiFTAnalyzer

Volatile Data Analysis Tool

- Runs in the Investigator's machine
- Analyses the data collected by Win-LiFTImager



CYBER FORENSICS SECTION
Centre for Development of Advanced Computing
(R&D Organization of Ministry of Electronics and Information Technology Govt. of India)
Technopark Campus, Kariyavattom P.O, Thiruvananthapuram - 695 581
Ph.No: +91 471 278 1500, 2781555
Email: cyber-tvm@cdac.in, Web: www.cyberforensics.in

AppSamvid

Application Whitelisting Software

About AppSamvid:

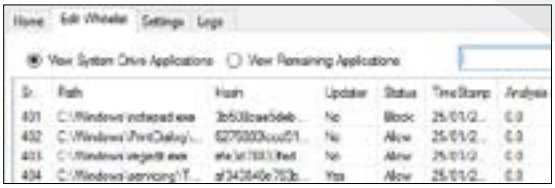
AppSamvid is application whitelisting software for Microsoft Windows based operating systems. Whitelisting allows only the pre-approved files to execute on operating system. This is in contrast to traditional signature based antivirus software approach of blacklisting the virus files. Whitelisting has the advantage over blacklisting as it does not require frequent virus definition updates. AppSamvid can protect operating system against computer malware (such as Viruses and Trojans).

Features:

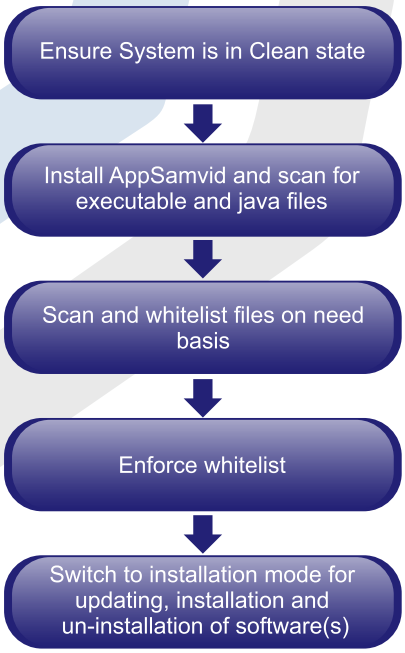
- Whitelists executable and java files (.exe, class, .war, .jar)
- Has Installation Mode:
  - To allow updating of software
  - To allow installation and/or un-installation of software
- Folder Scan and File scan option to add executable files to database
- Password based access to user interface
- Supports operating system updating via Microsoft Updates
- Bundled with heuristic malware engine to gain confidence on which files to whitelist
- Allows files to be made as Trusted Updater
- Can identify potential updater files to help the user find which files can be made as trusted updater(s)

Supported Operating Systems

- Windows 7 (32 and 64-bit)
- Windows 10 version 1607 (32 and 64-bit)



Usage Flow



Download link : https://www.cdac.in/appsamvid
e-mail: esuraksha@cdac.in

Ministry of Electronics & Information Technology
Government of India

प्रगत संगणन विकास केन्द्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय की वैज्ञानिक संस्था, भारत सरकार
A Scientific Society of the Ministry of Electronics and Information Technology, Government of India

Plot No: 6&7, Hardware Park Sy. No.1/1, Srisailam Highway Raviryal (V & GP), Via Ragaanna guda, Maheshwaram (M), Ranga Reddy District, Hyderabad – 501510.

Blockchain-as-a-Service

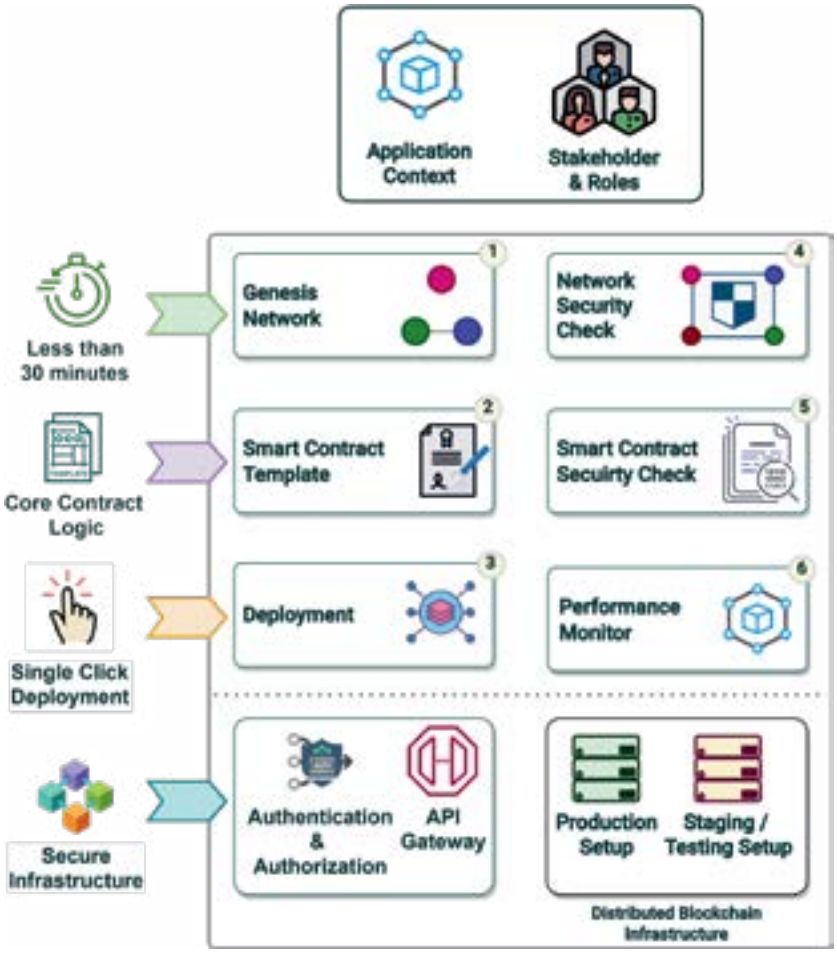
Enabling Trust in Digital Systems

National Blockchain Framework

National Blockchain Framework is an initiative of Ministry of Electronics and Information Technology (MeitY) to make India ready for large scale adoption of Blockchain and enable trust for applications in the domain of e-Governance. BaaS is component developed under National Blockchain Framework

BaaS Features

- Rapid end-to-end Blockchain Application Development
- Security Audited Blockchain Containers
- Smart Contract Templates
- Integrated Container Management Dashboard
- Easy deployment with Bring Your Own Infrastructure (BYOI) support
- Supports Hyperledger Fabric and Sawtooth



For any blockchain based application development, contact: *cdacchain@cdac.in*

E- Samarthak

E- Samarthak

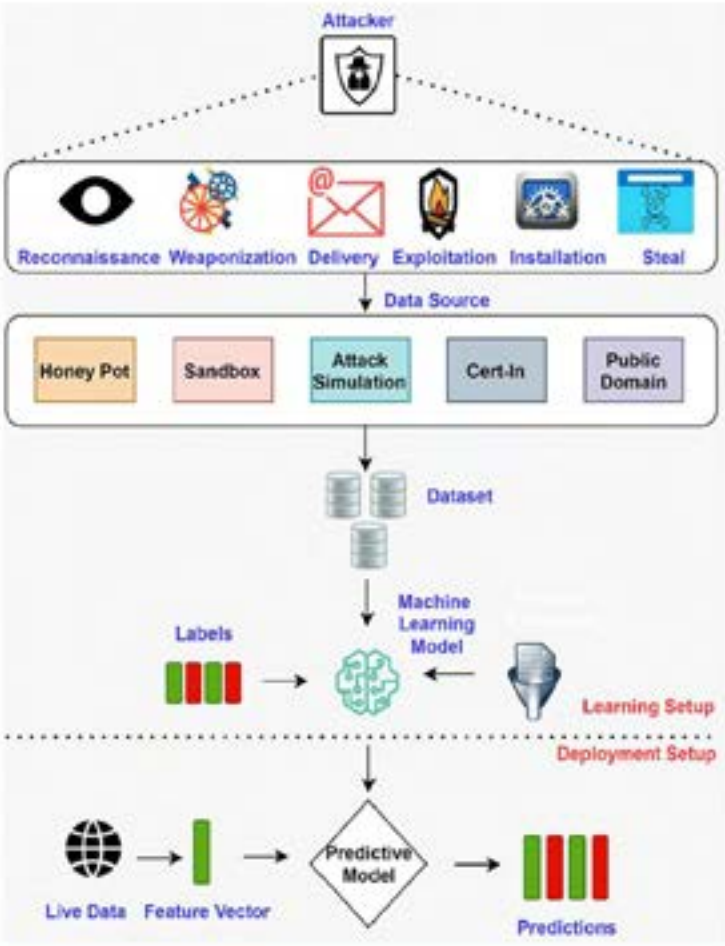
Multistage Attack Prediction using Machine Learning

Multistage Attack

- Modern Cybersecurity threats such as Ransomware, APT, Botnets, File less malwares are considered as Multi-Stage attacks.
- Most of the multi-stage attacks evade discovery as most endpoint protection products focus on one of the stages of an attack and are reactive in nature.
- Multistage attack hides the entire activity chain preventing security experts from perceiving the entire context of the attack.

Approach/Methodology

The solution leverages Machine learning models & MITRE ATT&CK Framework for detecting and predicting Multi-Stage attacks. ML models are trained on best features and datasets inline with MITRE adversary techniques and provide comprehensive insight for end-to-end attack



Salient Features

- Indicators of compromise (IoC) derived for different Adversary Techniques.
- Visualize attack by mapping it to the MITRE ATT&CK Framework.
- Analyze Binaries, Process and Network Traffic.
- Near real-time detection of Drive by Download.
- Leverage Machine Learning for detecting multi-stage attacks.
- Predicts the cyber-attacks to strategize the early mitigation.

E-mail: esuraksha@cdac.in

Ministry of Electronics & Information Technology, Government of India

प्रगत संगणन विकास केन्द्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
A Scientific Society of the Ministry of Electronics and Information Technology, Government of India

Plot No. 6 & 7, Hardware Park, Sy No. 1/1, Srisailam Highway, Pahadi Shareef Via (Keshavagiri Post)
Hyderabad - 501510

आज़ादी का अमृत महोत्सव

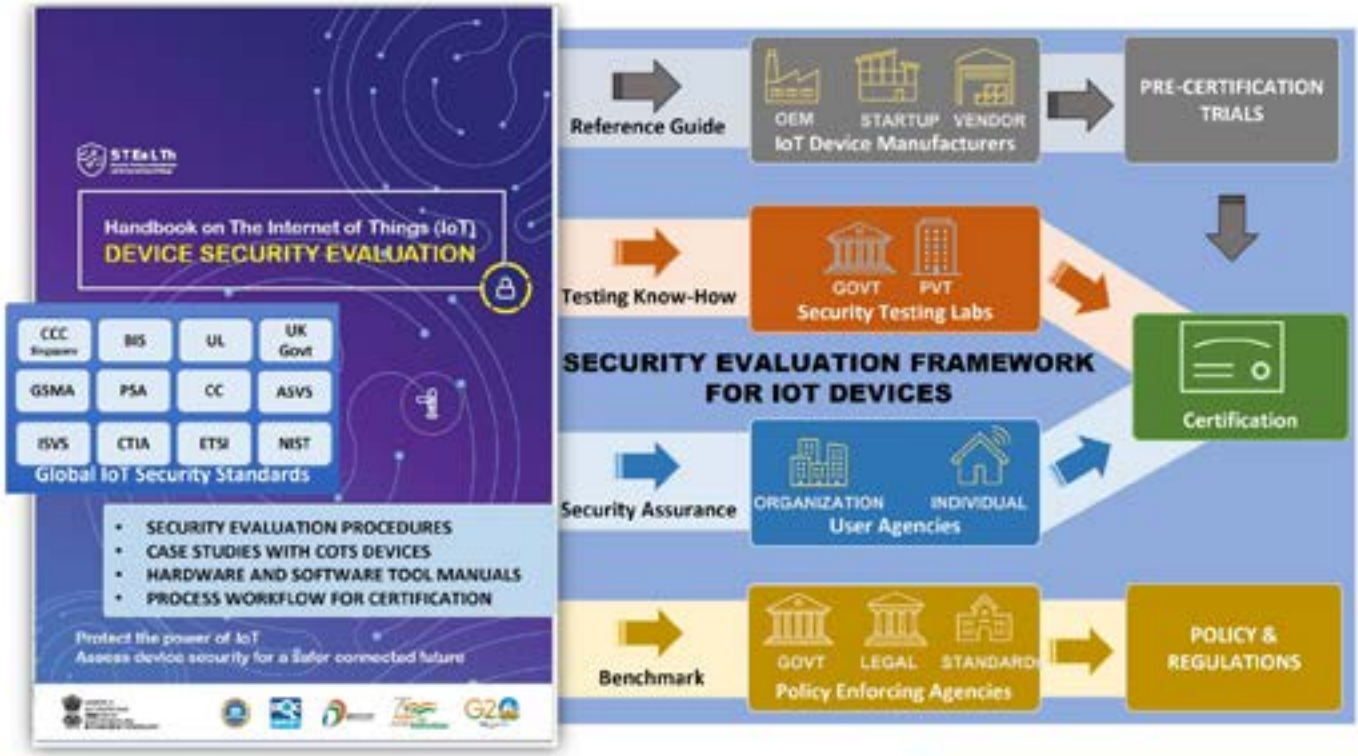
Digital India

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय
भारत सरकार
Ministry of Electronics and Information Technology
Government of India

STEaLTh
Security Testing and Evaluation Lab for the Internet of Things

HANDBOOK on IoT Device Security Evaluation

The Internet of Things (IoT) is becoming a pervasive technology and we are witnessing its use in application domains like Consumer Electronics (CE), Industrial Control Systems (ICS), Automotive Industry, Healthcare, etc. However, while its benefits are undisputed, an aspect that is often ignored during its development is incorporating adequate device security mechanisms. This poses a threat to application domains and critical infrastructures where these devices are deployed. Since there is a dearth in the availability of detailed security testing procedures, there is no common framework to evaluate the security of such devices, comprehensively. This handbook is the first-of-its-kind compilation in the world, comprising detailed security evaluation procedures, tools and techniques, that are essential elements in performing the security analysis of IoT devices. It is based on global IoT security standards, thereby providing comprehensive and world-wide applicability.



USP's

- First of its kind in the World
- Global IoT Security Standandards Compliant
- Comprehensive coverage of IoT Device Security
- Detailed Procedures with Case Studies
- Essential Tool Manuals with How-Tos

Prospective End Users

- Security Testing Labs
- Security Certification Bodies
- IoT Product Developers and Manufacturers
- Regulators and Policy Makers
- Citizens, Industries and User Agencies

For more details contact: esuraksha@cdac.in

STANDARDISATION TESTING AND QUALITY CERTIFICATION DIRECTORATE
NEW DELHI

CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
HYDERABAD

इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

Digital India Power To Empower

Azadi Ka Amrit Mahotsav

प्रगत संगणन विकास केंद्र
सी डैक CDAC
॥ज्ञानादेव तु कैवल्यम्॥
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

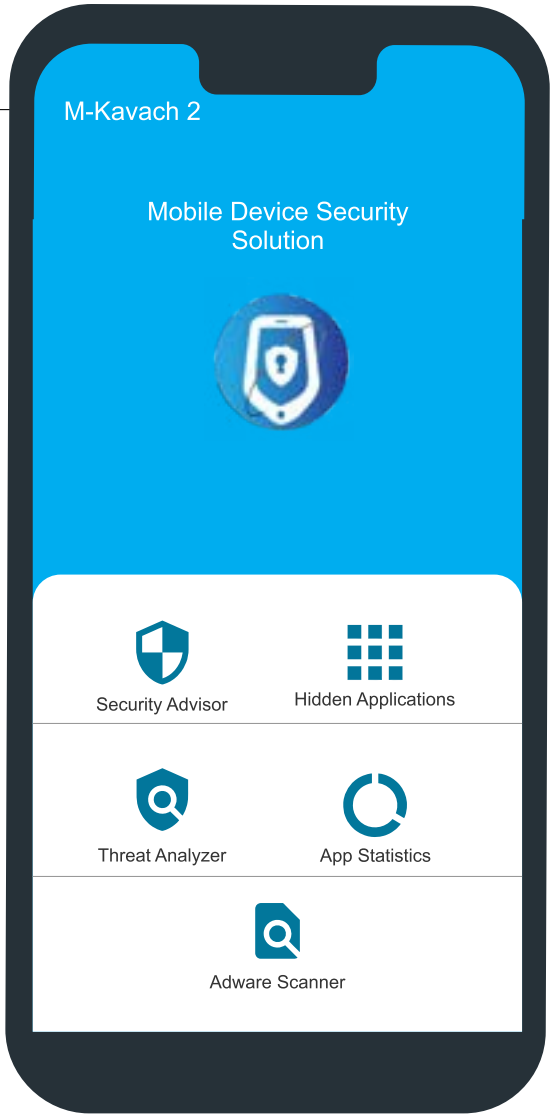
M-KAVACH 2

M-Kavach 2 is a comprehensive mobile device security solution addressing emerging threats related to Android based mobile devices. The major emphasis is on advising the users against security misconfigurations, detection of hidden/ banned apps and scanning the device for potential malicious apps installed on the user's mobile device.

Scan & Install

Salient Features

- **Threat Analyzer:**
  Detects potential malicious apps on the user's device.
- **Security Advisor:**
  Provides a holistic security status of the device.
- **Detection of Hidden/BannedApps:**
  Identifies the existence of any hidden/banned apps on the user's device.
- **App Latest Update Statistics:**
  Notify the users regarding the apps not updated for longer durations.
- **Adware Scanner:**
  Notify the users about the adware present on the device.



Contact Details : mkavach@cdac.in +91 90142 02885

PARIKSHAN

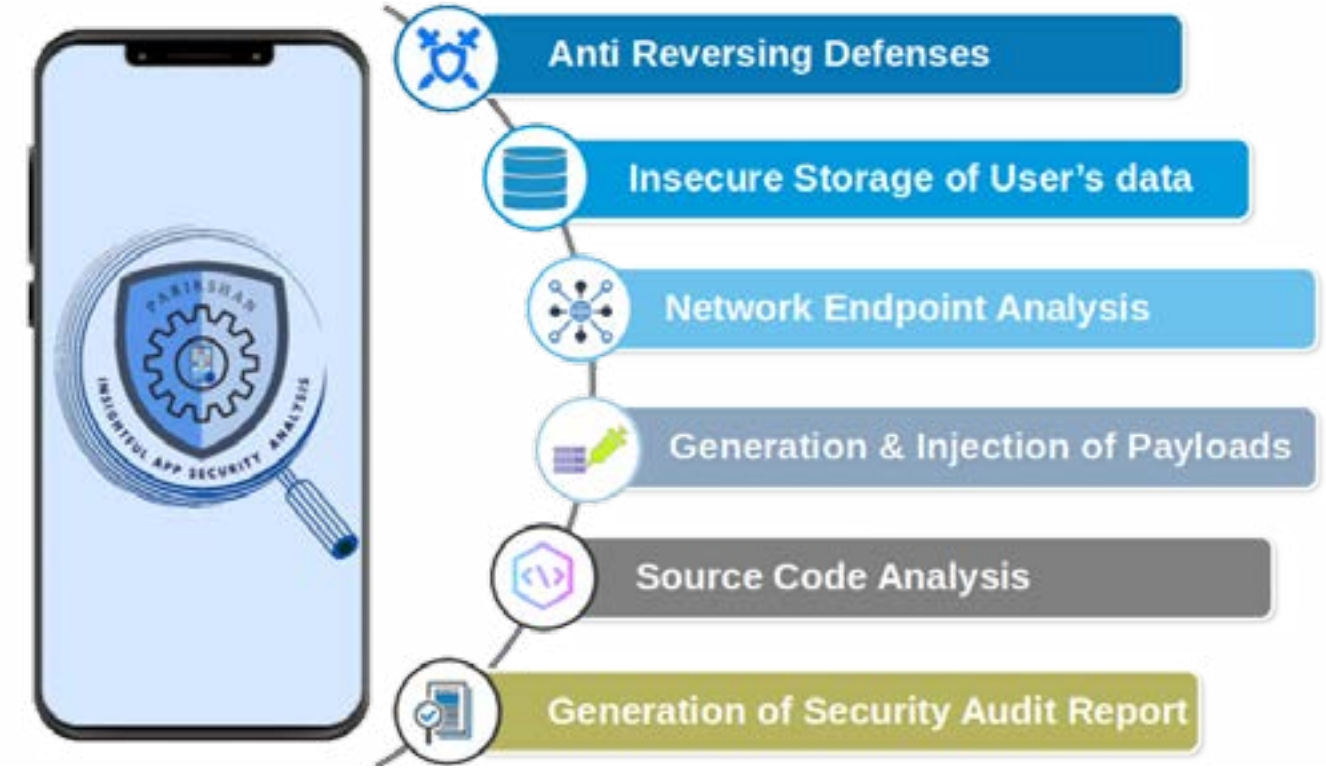
Insightful App Security Analysis

Mobile applications witnessed rampant proliferation from multiple App Stores and these applications handles user's sensitive information and critical device resources. Hence, the security assessment & penetration testing of the mobile applications has become paramount in-order to prevent mis-utilization of data & resources. Apparently, an automation tool performing fast pace security analysis becomes inevitable.

Parikshan is an Automation tool mainly focused on performing static and dynamic analysis of mobile applications. The tool has the capabilities to identify the security vulnerabilities and perform penetration testing for few of them. As an outcome, a detailed security audit report is generated containing the information about the identified vulnerabilities which aids to carry out further analysis.

Salient Features

- Automated Security Analysis, Vulnerability Assessment & Penetration Testing of Mobile Applications.
- Adheres to OWASP Top 10 Mobile Vulnerabilities and executes a total of 24 Static & 12 Dynamic test cases.
- Analysis of device logs and storage to identify leakage of user sensitive data.
- Generation and Injection of payloads during Dynamic Analysis.
- Real time capture of Geo-location information of the network endpoints communicated by the application
- Generation of detailed Audit Report of identified Vulnerabilities



Contact Details : mkavach@cdac.in +91 90142 02885

प्रगत संगणन विकास केंद्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

USB PRATIRODH

Standalone Version

USB Pratirodh is a software solution which controls unauthorized usage of portable USB mass storage devices

ABOUT USB PRATIRODH

USB Pratirodh controls the usage of removable storage media like pen drives, external hard drives, cell phones and other supported USB mass storage devices. Only authenticated users can access the removable storage media.

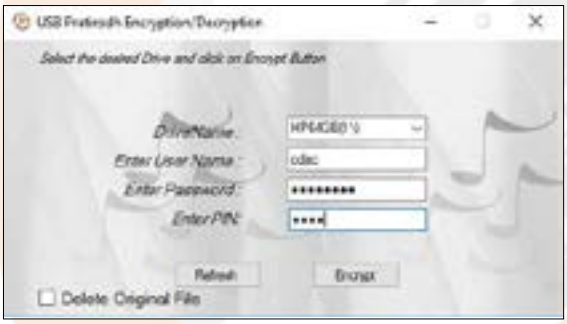
FEATURES

Device Control

All USB devices are uniquely identified. User can add or remove the devices to the database. User can bind one or more USB devices to be accessed using enabled username. Any unauthorized new USB device cannot be accessed, unless it is registered.

User Authentication

Whenever a USB device gets plugged in, the user is asked to authenticate with username and password. Only authenticated user can access the device. If the user fails to authenticate, user gets access denied message.



Secure Storage

Data on the USB storage devices can be encrypted.

Malware Detection

USB Pratirodh scans the plugged USB device for malware. Detected malware can be deleted by the user to keep his PC free from malware.

BENEFITS

- USB device control with password protection
- Data Encryption on USB devices
- Auto run protection and Malware Detection
- Configurable read / write privilege protection

SYSTEM REQUIREMENTS:

Works with Microsoft Windows 7 and Windows 10

Download link : https://www.cdac.in/usbpratirodh

e-mail: esuraksha@cdac.in

Ministry of Electronics & Information Technology
Government of India

प्रगत संगणन विकास केन्द्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय की वैज्ञानिक संस्था, भारत सरकार
A Scientific Society of the Ministry of Electronics and Information Technology, Government of India

Plot No: 6&7, Hardware Park Sy. No.1/1, Srisailam Highway Raviryal (V & GP), Via Ragaanna guda, Maheshwaram (M), Ranga Reddy District, Hyderabad – 501510.

प्रगत संगणन विकास केंद्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

Hyderabad

Pricing details of various Mobile Security Products

Vishleshak Pricing Details

Activity	Description	No.of Mobile Applications Supported	Amount in INR
On Prem Deployment & Licence Activation	Setup and Activation of Licence. ● Provisioning of Mobile Device ● Demonstration ● One Day Hands on Training with sample test cases	-	₹ 1,50,000 /-
On Prem Deployment	Mobile application analysis support	50	₹ 5,00,000 /-
Total Cost			**₹ 6,50,000 /-** *

* Excluding Taxes

Parikshan Pricing Details

Name of Tool	Description	Quantity	Product Pricing	Duration	Deployment
Parikshan	Setup, Deployment, Minor Bug Fixing & Feature Upgradation	100 unique apps* + 1 Device for Dynamic Analysis	14 Lakhs* (Exclusive of applicable taxes)	1 Year	On-Premise

* For one year or number of apps, whichever is earlier, access to the automation tool is terminated subsequently.

M-Prabandh MDM's Pricing Details

Cost Category	Annual Price in INR
Maximum Retail Price (MRP)** **for upto 50 devices**	₹ 70,000.00
Maximum Retail Price (MRP) for **50 devices and above**	₹ 1200.00 (per additional device)

Note:

- The solution would be offered as an on prem deployment model
- Server-side resources and mobile devices need to be provided by the client
- C-DAC managed deployments would be worked out on a case-to-case basis
- On prem deployment would be done remotely and would be supported over eMail/phone call/remote desktop
- Annual licensing covers AMC (Annual Maintenance Contract) for up to 1 year, which includes upgrades and bug fixes.

M-Kavach SDK's Pricing Details

Activity	Quantity (No. of active users)	Annual Price (in INR)	Price Range
Base Price	01 License + upto 100K	₹ 1,00,00.00	₹ 1,00,00.00
(No. of active users)	100K - 500K	₹ 1,00,00.00 + ₹ 0.50 per active user	₹ 1,00,00.00 to ₹ 3,50,00.00
	500K - 1M	₹ 3,50,00.00 + ₹ 0.25 per active user	₹ 3,50,00.00 to ₹ 6,00,00.00
	1M - 10M	₹ 6,00,00.00 + ₹ 0.10 per active user	₹ 6,00,00.00 to ₹ 16,00,00.00
	10M - 100M	₹ 10,00,00.00 + ₹ 0.02 per active user	₹ 10,00,00.00 to ₹ 30,00,00.00
	Above 100M	₹ 30,00,00.00 + ₹ 0.01 per active user	₹ 30,00,00.00 and above
Total (in INR)		Base integration price + Royalty charges based on no. of active users	

*__Note__:

- Annual licensing covers AMC (Annual Maintenance Contract) for up to 1 year, which includes upgrades and bug fixes.
- Base price should be paid upfront.
- Royalty should be paid on a half-yearly basis for the additional active users

CDAC's Product Costs (in Rs. Lakhs)								
Sl no	Product Name	Base Cost to Authorized Reseller	Cost for Govt Agencies	Cost for Private Agencies	Cost for Other Vendors	Cost for Academia	GeM Price/ MLP	Cost for Additional User License
1	CyberCheck	2.50	3.75	4.00	3.50	1.20	5.00	1.00
2	MobileCheck	2.00	3.00	3.20	2.80	0.95	4.00	NA
3	Advik Lite	0.25	0.38	0.40	0.35	0.10	0.50	NA
4	Advik CDR Analyser	0.80	1.20	1.30	1.10	0.40	1.60	NA
5	Advik Web	1.20	1.80	1.90	1.70	0.55	2.40	0.30
6	PhotoExaminer	0.65	1.00	1.05	0.90	0.30	1.30	NA
7	WinLiFT	0.90	1.35	1.45	1.25	0.40	1.80	NA
8	WebInvestigator	0.75	1.15	1.20	1.05	0.35	1.50	NA