CENTRE FOR CYBERCRIME INVESTIGATION TRAINING & RESEARCH

CCITR NEWSLETTER

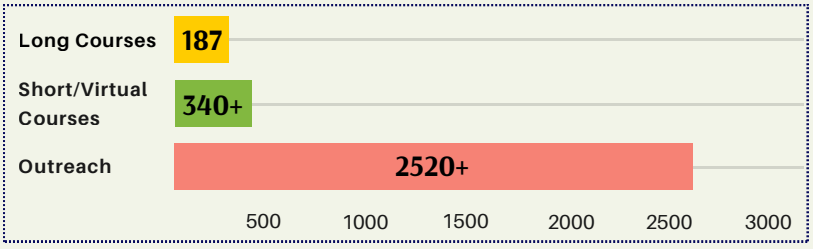
January 2026 | Volume 04 | Issue 01

"The recent MeitY advisory to all Intermediaries highlights the vital role of intermediaries in cybercrime investigations through due diligence, timely content removal, and digital evidence preservation. These measures strengthen platform accountability, enable swift law enforcement action, help trace offenders, and protect victims. I urge all officers to stay informed and work closely with intermediaries to ensure effective compliance and investigations."

DR M. A. SALEEM, IPS
DGP, CID, SPECIAL UNITS & ECONOMIC OFFENCES
BENGALURU, KARNATAKA

TRAINING HIGHLIGHTS

December 2025



110	Karnataka Police Academy (KPA), Mysuru
24	CID Karnataka
91	Police Personnel
2520+	Outreach Programs
305+	Virtual Training Series on Digital Investigation

3050+ PARTICIPATED

LATEST UPDATES IN CYBERCRIME

Bengaluru Police Bust Illegal SIM Box Racket

Bengaluru Central Crime Branch (CCB) have busted an illegal SIM box setup in Electronic City that convert international calls into local calls. The setup was used to facilitate vishing and digital arrest scams. A complaint was lodged by the service provider that multiple SIMs were being used in one area. Acting on the complaint, the police team raided a data centre operating out of a rented room and seized 28 SIM boxes, 1,193 SIM cards, a laptop, three routers, a portable CCTV camera, and several documents.

Reference: India Today (2025) Bengaluru Cybercrime Police bust illegal call conversion racket, accused on run. Available at: https://www.indiatoday.in/cities/bengaluru/story/bengaluru-cybercrime-sim-box-racket-kerala-accused-dubai-ecity-raid-2830758-2025-12-04 (Accessed: 07 Jan 2026)

CBI Dismantles International Cybercrime Network

The Central Bureau of Investigation (CBI) has taken down a transnational cybercrime network that targeted US nationals. The accused impersonated as officials from US agencies such as the Drug Enforcement Administration (DEA), Federal Bureau of Investigation (FBI) etc. Victims were threatened with fake cases of money laundering or smuggling drugs and were then forced to transfer funds to cryptocurrency wallets and foreign bank accounts. The fraud resulted in losses of around USD 8.5 million. CBI conducted searches in Delhi, Noida and Kolkata. The operation led to the arrest of six key accused and seizure of ₹1.88 crore in cash, 34 electronic devices and related documents.

Reference: CBI (2025) CBI Dismantles a Major Transnational Cyber Crime Network. Available at: https://cbi.gov.in/press-detail/NzQ1MA== (Accessed Accessed: 07 Jan 2026)

MeitY Advisory on Due Diligence Obligations for Intermediaries

The Ministry of Electronics and Information Technology (MeitY) has issued an advisory dated 29 December 2025, to all intermediaries, directing them to strictly enforce due diligence under the IT Act and IT Rules 2021 to curb obscene, vulgar, pornographic, paedophilic and other unlawful content. MeitY has reiterated that compliance with Section 79 of the IT Act and the IT Rules, 2021, is mandatory for intermediaries to retain safe harbour protection. Platforms are required to remove unlawful content promptly upon receiving court orders or authorised government notices. They are also required to remove prima facie sexually explicit content within 24 hours of receiving a complaint from the affected individual. The advisory warns that non-compliance may lead to loss of statutory immunity and penal action under applicable laws.

Reference: MeitY (2025) Advisory to All Intermediaries including Social Media Intermediaries. Available at: https://www.meity.gov.in/static/uploads/2025/12/a95c3656a958089e655f755ad354ac27.pdf (Accessed: 07 Jan 2026)

GhostPairing Scam Used to Hijack WhatsApp

GhostPairing is a new WhatsApp scam that hijacks accounts by abusing the linked devices feature. In this modus operandi, victims receive a message claiming that a photo or video of them has been shared online, often framed as a social media post. The message contains a link prompting the victim to view the image. When the victim clicks the link, they are redirected to a login page. Scammers trigger a WhatsApp Link Device request in the background, and OTP is sent to victim. The victim is tricked into entering the linking code shown on their screen, unknowingly pairing the attacker's device with their WhatsApp account. Once linked, the attacker gains access to victim's WhatsApp account.

Reference: Mint (2025) What is GhostPairing? The WhatsApp scam that hijacks accounts. Available at: https://www.livemint.com/technology/tech-news/what-is-ghostpairing-the-whatsapp-scam-that-hijacks-accounts-without-otps-or-sim-swaps-11766202437121.html (Accessed: 07 Jan 2026)

New Uber Portal for Police Data Requests

Uber has launched a dedicated Portal (lert.uber.com) for cyber police and law enforcement to request ride, driver and user data under Section 94 BNSS 2023 (Section 91 CrPC). Starting from 1 January 2026, Uber will accept all law enforcement data requests only through this portal; email requests will no longer be processed. Officers must sign up using official NIC/GOV email IDs, submit case details online, and can track request status in real time through the dashboard.

Reference: UBER (2026) Public safety response portal. Available at: https://lert.uber.com/s/?language=en_US (Accessed: 07 Jan 2026)

Maharashtra Launches AI-Based Platform for Cybercrime Investigation

The Government of Maharashtra has launched MahaCrimeOS AI in collaboration with Microsoft. The system has been integrated with existing police workflows to assist officers in handling large volumes of cybercrime complaints. MahaCrimeOS AI supports automated analysis and clustering of complaints, enabling identification of common indicators such as phone numbers, bank accounts, URLs and digital payment identifiers across multiple cases.

Reference: Microsoft (2025) Microsoft unveils MahaCrimeOS AI to combat cybercrime at scale. Available at: https://news.microsoft.com/source/asia/2025/12/12/maharashtra-leads-indias-ai-powered-cybercrime-fight-microsoft-unveils-mahacrimeos-ai-to-combat-cybercrime-at-scale/ (Accessed: 07 Jan 2026)

OSINT Tool

WhatsApp.CheckLeaked.cc

WhatsApp.CheckLeaked.cc is an online OSINT (Open-Source Intelligence) platform designed to assist investigators in determining whether a given WhatsApp-linked mobile number appears in publicly exposed data leaks or indexed breach datasets. By inputting a mobile number, the platform searches publicly accessible breach records and indicates whether the number has been associated with known data exposures. The tool can be also used for identification of VoIP-based numbers. This tool supports preliminary investigative assessment by helping investigators understand the public breach footprint of a number strictly within the scope of open-source records.

Reference: CheckLeaked.cc (2026) OSINT Platform for Breach Verification. Available at: WhatsApp.CheckLeaked.cc (Accessed: 18 July 2025)

DIGITAL FORENSICS INSIGHTS

Analysis of Tor Browser on iOS

IncognitoDarkNet is a Tor client application for iOS used to access the dark web and data related to Tor activity is stored in `observations.db` and `default.realm` database. On parsing these databases investigators can reconstruct Tor Browser usage and activity timelines on the device. The `observations.db` contains website visits including some of the onion links. The `default.realm` database contains full URL strings with paths and parameters along with timestamps.

Reference:Gerisson (2023) When Commercial Forensic Tools Fail: Manual Extraction of Tor Browser Evidence from iOS Devices. Available at: https://medium.com/@gerisson/when-commercial-forensic-tools-fail-manual-extraction-of-tor-browser-evidence-from-ios-devices-40b02e2523e3 (Accessed: 8 January 2026)

Tracking User Activity via the iOS Bumble Application

Bumble is a location-based dating and social networking application that enables users to connect through profile matching. It can be a valuable source of evidence in investigations involving online harassment, stalking, impersonation, fraud, or relationship-related disputes. On iOS devices, Bumble stores forensic artifacts within its application sandbox, primarily `/private/var/mobile/Containers/Data/Application/<Bumble_UUID>/`. These artifacts include chat messages, message creation and modification timestamps, sent and received indicators, read status, and internal user identifiers. Account-related information such as display name, user ID, last known location coordinates with timestamps, and application version details may also be present. By analysing these artifacts, investigators can reconstruct communication timelines, establish interactions between users, and correlate conversations with specific times and locations.

Reference: Forensafe (2025) iOS Bumble. Available at: https://forensafe.com/blogs/ios-bumble.html (Accessed: 8 January 2026)

Digital Forensic Tools Latest Upgrades

Passware Kit 2026 v1
Release date: 16 Dec, 2025

Berla iVe Software v4.14
Release date: 17 Dec, 2025

IPED 4.3.0
Release date: 02 Jan, 2026

OSForensics V11.1 build 1015
Release date: 15 Jan, 2026

FORENSICS TITBIT

Windows BAM & DAM Artifacts

The Background Activity Moderator (BAM) and Desktop Activity Moderator (DAM) are Windows features for tracking application execution activity. Each executed application generates registry entries that record the program path and execution timestamps, allowing the operating system to manage background and desktop application behaviour efficiently. These records contain execution metadata tied to specific user accounts and retained for up to seven days.

Location of the artifacts on Windows (10 v1709 - 11):
BAM:

- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\ {SID}`

DAM:

- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\dam\State\UserSettings\ {SID}`

What IO can obtain from BAM & DAM artifacts?

- Evidence of application execution (even if the executable file is deleted).
- Full path of executable (from where the application was run).
- Last execution timestamps.
- User-specific execution data mapped to Security Identifiers (SIDs).

Reference: CyberEngage (2025). BAM and DAM in Windows Forensics: Tracking Executed Applications. https://www.cyberengage.org/post/bam-and-dam-in-windows-forensics-tracking-executed-applications (Accessed: 07 Jan 2026).

Detecting Applications via the Windows IconCache

The Windows IconCache database stores cached icon data to speed up icon rendering for files and applications. In digital forensics, this artifact can indicate the presence of executables or applications on a system, even if the original files have been deleted. IconCache artifacts are typically found in `%localappdata%/IconCache.db` and `iconcache_*.db` files under `%localappdata%/Microsoft/Windows/Explorer/`. These databases store icon path references associated with files that existed on the system. By examining these artifacts, an analyst can understand what applications or tools were present on the system. Although the IconCache does not confirm that a program was actually run, it can help support activity timelines when combined with other system artifacts.

Reference: ThinkDFIR (2025) Examining the IconCache database. Available at: https://thinkdfir.com/2025/12/28/examining-the-iconcache-database/ (Accessed: 8 January 2026)

Knowledge Corner - Upcoming Webinars

DFU Decoded: Unlocking Hidden Truths with Media Intelligence by Cellebrite
(January 28, 2026 | 10:30 AM IST)

Breaking Down the Browsers by Magnet Forensics
(January 28, 2026 | 04:30 PM IST)

Six Pillars of Digital Forensics By Magnet Forensics
(February 04, 2026 | 06:30 PM IST)

Smartwatch Forensics by MOBILedit
(February 5, 2026 | 02:30 PM IST)

FOSS TOOLS CORNER

NTFSTool

ntfstool is an open-source forensic utility used to parse and analyse NTFS (New Technology File System) artifacts from live system. It enables investigators to inspect low level filesystem structures such as boot records, file records and metadata that are not always visible through standard operating system tools. The tool also supports the examination of BitLocker-encrypted volumes, allowing investigators to identify encryption status and extract relevant metadata.

Usage

Syntax: `ntfstool <command> [OPTIONS]`

Here:

- `ntfstool.exe`: executable file of the tool
- `command`: specifies the operation to perform
- `OPTIONS`: used for target file and output selection

Common commands include:

- `info`: Display information about all detected disks and volumes
- `help`: Display available commands and usage information
- `mft.dump`: Dump the $MFT file in supported formats such as CSV, JSON, or raw
- `bitlocker.info`: Display BitLocker information for a volume including encryption metadata

Example:

To extract the raw Master File Table (MFT) from volume 2 on disk 2 and save to specified output file

- `ntfstool.exe mft.dump disk=2 volume=2 output=d:\mft.raw`

Reference: thewhiteninja (2026) NTFSTool, GitHub. Available at: https://github.com/thewhiteninja/ntfstool (Accessed: 07 January 2026).

Training & Visits to CCITR

Level 2 Training for Judicial officers



Corps of Military Police (CMP) Visit



Level 1 Training for Officers from District Police



Investigation in Virtual Environment Training for Bengaluru City Police



ಶ್ರೀಮತಿ ವಿದ್ಯಾ.. ಕೆ
ಜಿಲ್ಲಾ ಮತ್ತು ಸತ್ರ ನ್ಯಾಯಾಧೀಶರು

ನುಡಿ-ನಮನ

"ಎರಡು ದಿನಗಳ ವಿಸ್ತೃತ ಸೈಬರ್ ಅರಿವಿನ ಕಾರ್ಯಾಗಾರ;
ನಮಗೆಲ್ಲ ನೀಡಿತು ಸೈಬರ್ ಸಂಬಂಧಿತ ಜ್ಞಾನ ಬಂಡಾರ:

Digital evidence, Block Chain, Darkweb, crypto currency;
ಮುಂತಾದ ವಸ್ತುವಿಷಯಗಳನ್ನು ಪರಿಣಿತರಿಂದ ಉಣಬಡಿಸಿ:

ಸೈಬರ್ ಅಂಗಳದಲ್ಲಿ ಬರುವ ನಾನಾ ರೂಪದ ಅಪರಾಧಗಳು;
ಇಂದಿನ ಹೈಟೆಕ್ಕುಗದಲಿ ಕಂಗಾಲಗುವಂತಹ ಸವಾಲುಗಳು:

ತಂತ್ರಜ್ಞಾನ ಕ್ರಾಂತಿಮಂತ್ರದ ಮಾಯೆ ಮನ್ವಂತರಗೊಂಡಂತೆಲ್ಲ;
ಯಾರು ಯಾರಿಗೆ ವಂಚಿಸುವರೋ ನಾ ಕಾಣೆ ಆ ದೇವನೇ ಬಲ್ಲ:

ಮಹಿಳ, ಮಕ್ಕಳು, ಮುಗ್ಧ ಅಮಾಯಕರ ಜೊತೆಗೆ ಸುಶಿಕ್ಷಿತರು;
ಸೈಬರ್ ಹಾವಳಿಗೆ ಅರಿತು ಅರಿಯದೆಯೇ ಬಲಿಯಾಗುತಹರು:

ಮುಂದೊದಗಬಹುದಾದ ಅನಾಹುತಗಳ ಬಗ್ಗೆ ಜಾಗ್ರತೆ, ಎಚ್ಚರಿಕೆ;
ಅರಿಯಬೇಕಾದ ಅವಶ್ಯಕತೆಯಿದೆ ನ್ಯಾಯಾಧೀಶರುಗಳ ವೃಂದಕೆ:

ಈ ಕಾರ್ಯಕಮ್ಮಟದಿಂದ ನಮಗೆಲ್ಲ ಸೈಬರ್ ಜ್ಞಾನವ ಭಿತ್ತಿ;
ಪ್ರಶಾಂತ ವಾತವರಣದೊಂದಿಗೆ ಕೊಂಡೊಯ್ಯುತೆ ನೆನಪಿನ ಬುತ್ತಿ:

ನ್ಯಾಯದಾನದ ರೂವಾರಿಗಳಾದ ನಮಗೆ ಈ ಕಾರ್ಯಾಗಾರ ಅವಿಸ್ಮರಣೀಯ;
ಇನ್ನೂ ಹೆಚ್ಚೆಚ್ಚು ಸೈಬರ್ ಜ್ಞಾನ ಪ್ರಚುರಪಡಿಸಲೆಂಬುದೇ ನಮ್ಮ ಆಶಯ"

Centre for Cybercrime Investigation Training & Research,
2nd Floor, Annexe-2 Building, CID HQRS, # 1, Carlton House,
Palace Road, Bengaluru, Karnataka - 560001
080-22094436 | spccpscid@ksp.gov.in | ccitr.org