22003/87/2023-I4C
Government of India
Ministry of Home Affairs
Indian Cyber Crime Coordination Centre (I4C)
CIS Division

2nd January 2024

To,
The DGPs/ CPs
States/ UTs

DIG P on Leave
SSP(T2c)
SP(CC)

Sub: Utilization of Services Offered by 'National Cyber Forensic Laboratory' by State/ UT LEAs- reg

The Ministry of Home Affairs (MHA) has set up the Indian Cyber Crime Coordination Centre (I4C) to create an effective framework and ecosystem for prevention, detection, investigation and prosecution of cybercrime in a comprehensive and coordinated manner. National Cybercrime Forensic Laboratory (NCFL) is one of the facilities created by I4C for the LEAs of States/ UTs.

2. The NCFL has been setup with the objective of assisting investigating Officers of State/ UT Police in digital forensic analysis during the early stages of investigation. It is equipped with advanced cyber forensic tools and provides an opportunity to the investigating officers to benefit from expeditious examination of digital artifacts related to a crime. Since its inauguration in the year 2019, the NCFL, has successfully examined over 9000 digital devices and artifacts for different States/UT's and enforcement agencies.

3. For seamless access of the NCFL services, an online portal (https://ncfl-i4c.mha.gov.in/) has been developed through which the investigating officers can seek an appointment with NCFL for forensic analysis. The portal also provides the facility of remote access to various digital forensic services, such as memory forensics, mobile forensics, image enhancement, malware analysis, crypto analytics, etc. Any new service or information relevant for LEAs are being updated regularly on the web portal.

4. Brief details of the various forensic facilities and tools available with NCFL has been attached along with (Annexure 1). The SOP for online appointment and utilizing online forensic services can be accessed on NCFL website (https://ncfl-i4c.mha.gov.in/).

4. In this regard, it is requested to direct all officers concerned to utilize the services of NCFL. For any further clarification or additional information, the officials concerned may contact Shri Kandle Goutham Kumar, DC (NCFL) at email gouthamkumar.kandle@gov.in with a copy to dir-i4c2@gov.in.

With regards,

Yours sincerely,

Nishant Ks
(Nishant Kumar)
Director NCFL,
I4C, MHA

Attached: *Annexure 1*

Comp. I / II & SP Sandosh
Please sensitize all officers on the NCFL for better utilization, Please

Annexurel 1

SERVICES AVAILABLE AT NCFL, NEW DELHI

This notice is intended for all police officers across India who are interested in utilizing the Forensic Analysis Services offered by National Cyber Forensic Laboratory (NCFL) of Indian Cyber Crime Coordination Center (i4c) for digital investigation pertaining to Cyber Crime.

The facilities can be availed in two modes: Remote Service or Onsite Service.

1. **Remote Servlices**

Under this service NCFL will provide online access of its forensic tools to IOs at their place.

Service Offered	Description	Tool
A. Memory Forensics	**a) This facility can be used to analyze memory storage devices such as:** 1. Hard Disks installed in Desktops, Laptops 2. USBs ,Memory cards 3. External drives **b) The following data/information can be extracted from these devices:** 1. Deleted data from entire system, from drive or from folders. 2. Runtime system activity, including open network connections and recently executed commands or processes. 3. Extraction of different type of files on the basis of search criterion like Excel, Word PDF, etc. 4. 'System Information' such as login/logout details, USB connections, last accessed files/applications, etc. 5. Internet browsing history. 6. Wi-Fi & Network connections detail. 7. Applications installed & usage details. 8. Virtual Machine details.	FTK Enterprise
B. Mobile Forensics	**a) This facility is used for acquisition and analysis of broad range of mobile devices such as:** 1. Android Smartphones 2. IOS Devices 3. Basic Feature Phones 4. SIM cards	Oxygen Enterprise

	b) The following data/information can be extracted from mobile devices: 1. Extraction of Logical Data like available/deleted Call logs, SMSs, Contacts etc. 2. Extractions of Deleted Data (only for supported models) 3. Extraction of Apps data and details like WhatsApp, Skype, Messenger (only for supported models) 4. Internet browsing history 5. Timeline details 6. Recovery of available/deleted images and videos. 7. Email details 8. Network/Wi-Fi Connections details	

2. **Onsite Services**

Under this service IO or their representative is required to visit NCFL physically to submit and collect the digital evidence.

Services Offered:

a) **Memory Forensics:** Functionality as mentioned in 1.A with option of multiple tools.
b) **Mobile Forensics:** Functionality as mentioned in 1.B with option of multiple tools.
c) **Malware Forensics:** Analysis of malicious links,devices and applications (Android & Windows)
d) **Crypto Currency Forensics:** Tracing the origins and ownership of cryptocurrency assets and tracking flow of funds by analysing transaction data.
e) **Cloud Forensics:** Using the credentials or tokens from the device to extract data such as docs, pictures, videos etc. stored on drives – Google drive, OneDrive, Dropbox, etc.
f) **Image & Video Enhancement:** Recovery of video and metadata from DVR surveillance systems and enhancement of blurred images and videos.
g) **Advanced Mobile Forensic:** Attempt to unlock and extract data from locked android and iOS devices.(Only limited models supported)

The detailed SOP to avail these services is available at *https://ncfl-i4c.mha.gov.in/*