



COEDF

अनुसंधानम् | विश्लेषणम् | परिणामः

Real Time Forensic Insights

TMFS

Field-ready intelligence to expose device anomalies and risks.

Tactical Mobile Field Forensic Solution

NFSU Center of Excellence in Digital Forensics (CoEDF) developed TMFS, a portable platform for analyzing data at rest and data in transit, including file systems, logs, and live network traffic. TMFS detects anomalous communications, hidden processes, unauthorized connections, and backend server interactions in real time, enabling rapid on-site investigation and actionable intelligence along with field triaging capabilities.

Exposing Hidden Threats in Real Time



Real Time Data Packets Monitoring

The system captures network traffic in real time. It tracks ongoing communications and data transfers.

Suspicious or unusual activity can be flagged immediately.



Anomaly & Threat Detection

TMFS identifies hidden apps, background processes, and unauthorized connections. It detects unusual patterns that may indicate compromise.

Investigators get actionable insights on potential threats.



Backend Communication Analysis

The tool monitors interactions with servers, cloud services, and remote hosts. It helps uncover hidden or unauthorized device communications. Investigators can determine if the device is being



Field Triaging & Data Acquisition

TMFS enables field triaging to quickly assess a device on-site. It performs thorough data acquisition of files, contacts, messages, logs, and app data. Investigators can rapidly determine which information is relevant for further analysis.



National Forensic Sciences University

Knowledge | Wisdom | Fulfilment

An Institution of National Importance
(Ministry of Home Affairs, Government of India)

CONTACT

+91 9099952950

coedf@nfsu.ac.in

www.nfsu.ac.in

f /nfsu_official

t @nfsu_official

i @nfsu_official

National Forensic Sciences University
Sector 9, Gandhinagar 382007, Gujarat, India