TorTrace-AI

Forensic Analysis Report
Tor Network Attribution System

CLASSIFICATION: FOR AUTHORIZED USE ONLY

Report Generated:	2025-11-14 01:01:48
Analysis System:	TorTrace-AI v1.0
Institution:	VIT Chennai
Hackathon:	TN Police Hackathon 2025

Executive Summary

This report contains Tor network attribution analysis results generated by TorTrace-AI, a multi-layer AI-powered forensic system designed for authorized law enforcement investigations.

Analysis Overview:
• Total PCAP Files Analyzed: **6**
• Unique Guard Nodes Identified: **3**
• Total Attribution Predictions: **18**
• Analysis Methodology: Multi-Method Ensemble (GNN + Timing Correlation + Traffic Fingerprinting)
• Success Rate: **100%**

Attribution Confidence:
The system employs a weighted confidence scoring mechanism combining graph neural network analysis (50%), timing correlation (25%), traffic fingerprinting (15%), and flow strength analysis (10%).

Identified Guard Nodes

The following table presents the top Tor guard nodes identified through multi-method analysis, ranked by detection frequency and confidence score.

Rank	Relay Nickname	IP Address	Avg Confidence	Detections
1	SENDNOOSEplz	204.137.14.106	89.7%	6
2	titamon3	178.218.144.18	84.8%	6
3	hubbabubbaABC	83.108.59.221	84.2%	6

Analysis Methodology

1. PCAP Traffic Analysis
Deep packet inspection correlates captured traffic with known Tor relay database (6,538 relays). Extracts timing patterns, packet sizes, and flow characteristics.

2. Timing Correlation Engine
Statistical analysis of inter-packet arrival times and cross-correlation between entry and exit flows to identify probable guard relay candidates.

3. Website Fingerprinting (CNN-LSTM)
Deep learning model classifies encrypted traffic patterns using convolutional and recurrent neural networks to identify visited destinations from packet sequences.

4. Graph Neural Network Predictor
Models Tor network topology as directed graph. Employs PageRank, betweenness centrality, and degree centrality to predict guard nodes based on network structure and observed traffic patterns.

5. Ensemble Confidence Scoring
Combines results from all methods using weighted voting:

- GNN Analysis: 50%
- Timing Correlation: 25%
- Traffic Fingerprinting: 15%
- Flow Strength: 10%

Legal Notice & Disclaimer

Authorization:
This analysis report is generated for authorized law enforcement use only. All analysis methods comply with applicable regulations and are intended solely for lawful investigation purposes.

Accuracy Disclaimer:
Attribution confidence scores represent probabilistic estimates based on available network data and traffic patterns. Results should be corroborated with additional investigative evidence. The system does not decrypt or inspect Tor traffic content.

Privacy & Ethics:
TorTrace-AI respects user privacy and the anonymity goals of the Tor network. This system is designed as a defensive tool for identifying malicious actors while preserving legitimate privacy use cases.

Technical Support:
For questions regarding this report or analysis methodology, contact:

- Developer: Yash, VIT Chennai
- Email: yashwanthbalaji.2408@gmail.com
- Project: TN Police Hackathon 2025, Problem Statement #4

System Version: TorTrace-AI v1.0
Report Generated: 2025-11-14 01:01:48

--- End of Report ---