TOR-Unveil: Forensic Analysis Report

Chain of Custody

Report Generated:	2025-12-21 23:16:53 UTC
Analysis ID:	4b391228-19c4-4ffd-8301-c563be8d642d
PCAP Filename:	tor_only.pcap
Analysis Duration:	4.35s
Case ID:	AUTO
Investigator:	System
Agency:	TN Police Cybercrime Division

Executive Summary

This report presents the results of an automated TOR traffic analysis using the Flow Time-Density Correlation (FTDC) method. The analysis identified 0 potential guard nodes with an average confidence of 0.0%. The system analyzed network traffic patterns to probabilistically correlate TOR entry and exit nodes.

Analysis Overview

Metric	Value
Total Guard Candidates	0
Average Confidence Score	0.0%
Improvement Factor	1.00x
Circuit Paths Identified	0
Correlation Trend	stable

Top Guard Node Candidates

Rank	Nickname	IP Address	Country	Confidence	Flags

Identified Circuit Paths

Methodology

Flow Time-Density Correlation (FTDC) Analysis

The analysis employs a multi-factor correlation approach:

1. **Temporal Correlation:** Compares timing patterns between exit node traffic and potential guard node activity using sliding window analysis (50ms default).

2. **Bandwidth Correlation:** Analyzes bandwidth capacity and utilization patterns to identify relays capable of handling observed traffic volumes.

3. **Circuit Pattern Matching:** Uses weighted scoring across three dimensions: - Bandwidth Score (50%): Relay capacity vs. required throughput - Quality Score (30%): Uptime, flags, and reliability metrics - Network Proximity (20%): Geographic and AS-level proximity analysis

4. **Iterative Improvement:** Bayesian-like updating mechanism that refines confidence scores as more correlation data becomes available.

Confidence Interpretation:
- High (>70%): Strong correlation evidence, prioritize for investigation
- Medium (40-70%): Moderate correlation, requires additional validation
- Low (<40%): Weak correlation, consider as background noise

Legal and Technical Disclaimers

IMPORTANT: This report contains probabilistic correlation analysis results. The system does NOT: - Decrypt TOR traffic or compromise user anonymity through cryptographic attacks - Perform active network attacks or exploit vulnerabilities - Guarantee 100% accuracy in guard node identification

Results should be used as investigative leads requiring additional corroboration through traditional forensic methods. All analysis respects the integrity of the TOR network and is intended solely for lawful cybercrime investigation purposes.

Chain of Custody: This report was generated automatically by the TOR-Unveil system. Any manual modifications to this document invalidate its forensic integrity.