

TOR-Unveil: Forensic Analysis Report

Chain of Custody

Report Generated:	2025-12-22 12:41:34 UTC
Analysis ID:	0f5a0a82-1310-41b6-9260-b03daf419472
PCAP Filename:	tor_only.pcap
Analysis Duration:	14.89s
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 20 potential guard nodes with an average confidence of 4885.0%. The system analyzed network traffic patterns to probabilistically correlate TOR entry and exit nodes.

Analysis Overview

Metric	Value
Total Guard Candidates	20
Average Confidence Score	4885.0%
Improvement Factor	1.00x
Circuit Paths Identified	10
Correlation Trend	stable

Top Guard Node Candidates

Rank	Nickname	IP Address	Country	Confidence	Flags
1	TorRelay15	10.24.179.98	NL	48.9%	Guard, Exit, Fast
2	TorRelay1	10.249.11.99	GB	48.2%	Guard, Fast, Running

3	TorRelay2	10.167.27.216	FI	47.6%	Guard, Exit, Fast
4	TorRelay6	10.242.193.1	GB	47.3%	Guard, Exit, Fast
5	TorRelay13	10.242.201.129	GB	47.0%	Guard, Exit, Fast
6	TorRelay8	10.205.28.65	CA	47.0%	Guard, Exit, Fast
7	TorRelay11	10.210.126.35	DE	46.7%	Guard, Exit, Fast
8	TorRelay19	10.35.18.83	NL	46.5%	Guard, Fast, Running
9	TorRelay65	10.131.6.109	GB	46.3%	Guard, Fast, Running
10	TorRelay79	10.113.38.212	FI	45.3%	Guard, Exit, Fast

AI Risk Assessment

■ ■ **AI DECISION SUPPORT NOTICE:** The following AI-generated risk scores provide **investigative prioritization only**. These scores indicate statistical patterns worthy of further analysis — they do NOT identify individual users or prove any connection to specific activities. Always cross-reference with additional intelligence sources before drawing conclusions.

Risk Level	Count	Recommendation
HIGH	0	Immediate Review Recommended
MEDIUM	0	Further Investigation Warranted
LOW	20	Standard Processing

AI Summary: AI analysis identified 0 high-priority, 0 medium-priority, and 20 low-priority candidates for further investigation.

Rank	Fingerprint	Risk Score	Risk Band	Top Factors
1	A29CC4A1BB77...	37.8%	LOW	N/A
2	7A65740AE410...	36.8%	LOW	N/A
3	82374F15F451...	36.6%	LOW	N/A
4	1AA76BF4A0A4...	35.9%	LOW	N/A
5	5711F5FAA3E2...	35.8%	LOW	N/A
6	A0B0DB35D10B...	35.3%	LOW	N/A
7	3828CEA96BB2...	35.3%	LOW	N/A
8	33D4FE91BCC4...	34.8%	LOW	N/A
9	180FC07B7E12...	33.8%	LOW	N/A
10	FDAF054E65D0...	33.0%	LOW	N/A

Identified Circuit Paths

Path 1 (Confidence: 48.9%)

Role	Nickname	IP	Country
------	----------	----	---------

Guard	TorRelay15	10.24.179.98	NL
Middle	TorRelay0	10.99.100.223	NL
Exit	TorRelay0	10.99.100.223	NL

Path 2 (Confidence: 48.9%)

Role	Nickname	IP	Country
Guard	TorRelay15	10.24.179.98	NL
Middle	TorRelay1	10.249.11.99	GB
Exit	TorRelay0	10.99.100.223	NL

Path 3 (Confidence: 48.9%)

Role	Nickname	IP	Country
Guard	TorRelay15	10.24.179.98	NL
Middle	TorRelay3	10.152.108.102	SE
Exit	TorRelay0	10.99.100.223	NL

Path 4 (Confidence: 48.9%)

Role	Nickname	IP	Country
Guard	TorRelay15	10.24.179.98	NL
Middle	TorRelay9	10.223.20.203	US
Exit	TorRelay0	10.99.100.223	NL

Path 5 (Confidence: 48.9%)

Role	Nickname	IP	Country
Guard	TorRelay15	10.24.179.98	NL
Middle	TorRelay12	10.122.12.123	SE
Exit	TorRelay0	10.99.100.223	NL

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.