TOR Traffic Correlation & Probable Origin Analysis

EXIT-SIDE PCAP ANALYSIS REPORT

Report Number:	70004
Case ID:	CASE-1766469443
Date & Time (UTC):	2025-12-23 05:59:06 UTC
Investigating Unit:	Tamil Nadu Police 2025
Analysis Mode:	Exit-Side (Exit Node Detection)

1. VERIFIED TOR EXIT NODES DETECTED

#	IP Address	Country	ISP	Packets	In Consensus
1	185.220.101.11	[DE] Germany	Stiftung Erneuerbare	210	Yes
2	192.42.116.184	[NL] The Netherlands	Church of Cyberology	40	Yes

2. PROBABLE GUARD NODES (Inferred from Exit Traffic)

#	IP Address	Nickname	Country	Bandwidth	Probability
1	171.25.193.78	DFRI27	[SE] Sweden	0.0 MB/s	88%
2	80.79.117.42	takei	[EE] Estonia	0.0 MB/s	75%
3	94.142.241.153	as214958tor8	[NL] The Netherlands	0.0 MB/s	62%

3. FLOW FINGERPRINT ANALYSIS

Metric	Value
Burst Entropy	2.892
Micro-gap Average	539.49 ms
Size Variance Slope	469.95
Circuit Lifetime	411.45 s

4. TRAFFIC PROFILE

Metric	Value
Total Packets	875

Total Bytes	139.3 KB
Total Flows	63
CDN Filtered	0

5. CORRELATION METHOD

Technique	Description
Time-window alignment	Millisecond-level temporal correlation
Packet burst similarity	Burst pattern matching across flows
Flow size distribution	Statistical comparison of packet sizes
Guard stability	Bandwidth weighting from Tor consensus
Tor consensus verification	Cross-reference with live relay data

6. FORENSIC NOTICE

This report provides investigative intelligence based on exit-side traffic analysis. Guard node predictions are probabilistic based on Tor consensus bandwidth weighting.