TOR Traffic Correlation & Probable Origin Analysis

DUAL-SIDE PCAP CORRELATION REPORT

Report Number:	70002
Case ID:	CASE-DEMO
Date & Time (UTC):	2025-12-23 05:41:56 UTC
Investigating Unit:	Tamil Nadu Police 2025
Analysis Mode:	Dual-Side (Entry + Exit Correlation)

1. ANALYSIS METRICS SUMMARY

Metric	Value
Exit Nodes Observed	3
Candidate Guards Analyzed	5
Guard-Exit Pairs Matched	6
Final High-Confidence Guards	3
Correlation Mode	guard+exit_indirect

2. TOP PROBABLE CONNECTIONS ESTABLISHED (>90% Confidence)

#	Guard IP	Exit IP	Guard Conf.	Exit Score	Origin IP
1	51.159.211.57	185.220.101.11	95%	48%	192.168.1.4
2	51.159.211.57	192.42.116.184	95%	48%	192.168.1.4
3	51.159.211.57	192.42.116.192	95%	48%	192.168.1.4
4	178.254.44.163	185.220.101.11	95%	47%	192.168.1.4
5	178.254.44.163	192.42.116.184	95%	47%	192.168.1.4

3. PRIMARY FINDING: BEST MATCH

Guard Node IP:	51.159.211.57
Country:	[FR] France
ISP:	SCALEWAY
Confidence Level:	High (≥80%)
Inferred Client Network Identifier:	192.168.1.4

4. EXIT NODES DETECTED IN CORRELATION

#	IP Address	Country	ISP	Score
1	185.220.101.11	[DE] Germany	Stiftung Erneuerbare Frei	48%
2	192.42.116.184	[NL] The Netherlands	Church of Cyberology	48%
3	192.42.116.192	[NL] The Netherlands	Church of Cyberology	48%

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 the highest confidence correlation from dual-side PCAP analysis. Entry-exit matching uses flow timing, burst patterns, and Tor consensus verification. Results should be corroborated with independent evidence.