TOR Traffic Correlation & Probable Origin Analysis

ENTRY-SIDE PCAP ANALYSIS REPORT

Report Number:	70005
Case ID:	CASE-1766469660
Date & Time (UTC):	2025-12-23 06:04:02 UTC
Investigating Unit:	Tamil Nadu Police 2025
Analysis Mode:	Entry-Side (Guard Correlation)

1. PRIMARY FINDING: INFERRED GUARD NODE

Guard Node IP:	178.254.44.163
Country:	[DE] Germany
ISP / ASN:	EVANZO-MK
Confidence Level:	High (≥90%)
Correlated Sessions:	5

2. PREDICTED EXIT NODES (From Tor Consensus)

#	IP Address	Country	ISP	Bandwidth	Probability
1	37.114.50.27	[DE] Germany	Florian Kolb	0.2 MB/s	88%
2	45.66.35.21	[NL] The Netherlands	Sabotage LLC	0.2 MB/s	75%
3	185.231.33.38	[SC] Seychelles	Datashield	0.2 MB/s	62%
4	45.66.35.35	[NL] The Netherlands	Sabotage LLC	0.2 MB/s	49%
5	109.71.252.182	[DE] Germany	Florian Kolb	0.2 MB/s	36%

3. ANALYSIS METRICS

Metric	Value
Total Sessions Analyzed	5
Sessions Correlated	5
Correlation Mode	entry_only

4. 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

5. FORENSIC NOTICE

This report provides investigative intelligence based on traffic correlation analysis. Results should be corroborated with independent evidence. Guard nodes may serve multiple users simultaneously. This analysis does NOT constitute cryptographic proof of user identity.