TOR FORENSIC ANALYSIS REPORT

RESTRICTED - Law Enforcement Use Only
Generated: 2025-12-17 15:23:42

Case ID: TEST-123

Investigator: Test

Report Date: 2025-12-17 15:23:42

1. EXECUTIVE SUMMARY

Analysis of captured network traffic identified a persistent encrypted connection matching Tor guard node behavior. The correlation engine has determined the following:

Primary Finding	Tor Guard Node Identified
Guard Node IP	5.6.7.8
Country	■ Unknown
City	Unknown
ISP/Hosting	Unknown
Confidence Level	High
Confidence Score	93.0%
Correlated Sessions	5

2. FORENSIC ASSESSMENT

The client maintained a persistent encrypted connection to this relay that matches Tor guard behavior. The connection pattern, timing characteristics, and traffic volume are consistent with Tor's guard node selection protocol.

Key Indicators:

• Persistent TLS connection to single relay

• Traffic patterns consistent with Tor cell sizes (512 bytes)

• Connection duration matches guard rotation period

• Correlated across 5 flow windows

• Timing patterns match expected Tor latency profiles

3. EVIDENCE CHAIN

Source File:	test.pcap
Analysis Engine:	TOR Flow Correlation Engine v1.0.0
Total Flows Analyzed:	0

4. CONFIDENCE ASSESSMENT

The confidence score of **93.0%** indicates a **High** probability of correct identification.

Level	Score Range	Interpretation
High	75-100%	Strong correlation - suitable for investigative lead
Medium	50-74%	Moderate correlation - requires corroboration
Low	0-49%	Weak correlation - insufficient for identification

5. OPERATIONAL LIMITATIONS

■■ **IMPORTANT:** This report provides investigative intelligence, not cryptographic proof.

• Results should be corroborated with independent evidence

• Traffic patterns may be mimicked or obfuscated by adversaries

• Guard nodes may host multiple users simultaneously

• Timing-based analysis has inherent accuracy limitations