Network Traffic Analysis Report

Source Host: 192.168.56.132

Timeframe of Capture: 2025-10-17 12:41:58 to 12:42:19 (~21 seconds)

1. Most Active Protocols

Transport Layer:
- TCP is the predominant transport protocol, responsible for all packet transmissions.
- Connection lifecycle is evident from [SYN], [ACK], and [FIN, ACK] packets.

Application Layer:
- TLS (TLSv1.2 and TLSv1.3) dominates, securing HTTP traffic (HTTPS).
- HTTP is used minimally for portal detection and file downloads.

Summary:
TCP underpins all communications while TLS shows strong encrypted traffic preference.

2. Suspicious or Unusual Traffic

1. TCP Duplicate ACKs:
- Frames 60-63, 80-81.
- Indicates packet loss or out-of-order delivery; low security risk.

2. Unencrypted HTTP File Download:
- Frame 123: PDF download from ndl.ethernet.edu.et via HTTP.
- Risk: Possible interception; should use HTTPS.

3. Rapid Connection Attempts:
- Multiple SYN packets to same destination within milliseconds.
- Likely retry logic or load balancing; low risk.

4. Expected Firefox Behavior:
- Portal detection requests to detectportal.firefox.com and CDN connections are normal.

3. Key Insights About Network Communication

User Activity:
- Active browsing via Firefox.

File Download Event:

- PDF download from ndl.ethernet.edu.et; multiple TCP sessions over HTTP and HTTPS.

Network Environment:
- VMware virtualized environment.

Communication Pattern:
- Single user actions trigger multiple concurrent connections; TLS usage dominates.

4. Protocol and Traffic Summary

Protocol | Count | Percentage | Notes

TCP | ~250 | 62% | Connection management
TLSv1.2/TLSv1.3 | ~80 | 20% | Encrypted HTTPS
HTTP | ~15 | 4% | Unencrypted requests
Ethernet | ~400 | 100% | Frame layer packets

Observations:
- HTTPS dominates; HTTP minimal.
- High TCP overhead; multiple concurrent connections.

5. Anomalies and Concerns

Item | Severity | Notes/Recommendation

Unencrypted HTTP PDF download | Medium | Prefer HTTPS
Rapid SYN packets / Retry Storm | Low | Monitor network reliability
TCP Duplicate ACKs | Low | Monitor packet loss; normal behavior

Other observations: Firefox portal detection, settings checks, and multiple HTTPS connections are standard behavior.

6. Recommendations

Short-term:
- Migrate educational PDF downloads to HTTPS.
- Monitor retry behavior and network reliability.

Medium-term:
- Implement DNS-over-HTTPS for privacy.
- Monitor sustained connection failures.

Long-term:
- Audit internal web services for HTTPS compliance.
- Implement HTTP Strict Transport Security (HSTS) where possible.

Executive Summary:
The capture shows normal web browsing by a Firefox user in a VMware environment. TLS-secured traffic dominates. Minor HTTP use for portal detection and file download was observed. No malicious activity detected. Overall, the network demonstrates good security posture.

Report Generated: October 17, 2025

Capture Duration: ~20 seconds

Total Packets Analyzed: 432 frames