Network Capture Troubleshooting Report

`tls-handshake-failure-lab.pcap`

Report ID	`PCAI-2026-1106-HX2Q`
Version	1 (Sample)
Generated	2026-11-06 11:19:00 UTC
Engine	PcapAI Analysis Engine 0.2.0 · ruleset 2026.10.1
Classification	TLP:CLEAR

SAMPLE

Document control

Version history

Version	Date	Change
1	2026-11-06	Initial report

Distribution

TLP:CLEAR Disclosure is not limited, subject to copyright.

Data handling

Captures and reports are stored in Amazon S3 in the us-west-2 region. Uploads without an account and their reports are deleted 24 hours after upload; account reports are kept for 30 days, or for as long as a Pro subscription lasts.

Support: info@pcapai.com

SAMPLE

Contents

1 Executive summary **4**

2 Scope, evidence and limitations **5**
2.1 Evidence integrity . . . 5
2.2 Versions . . . 5
2.3 Limitations . . . 5

3 Findings summary **5**

4 Detailed findings **6**
4.1 F01: TLS handshakes with 203.0.113.44 (portal.example.net):443 (portal.example.net) fail with alerts (handshake_failure (no common cipher suite / parameters) from server x8) . . . 6

5 Remediation roadmap **6**
5.1 Immediately . . . 6
5.2 Strategic . . . 6

6 Coverage: checked and clean **6**
6.1 TLS versions and certificates . . . 7

7 Assets and communications **7**
7.1 Asset inventory . . . 7
7.2 External destinations . . . 7
7.3 Other conversations . . . 8

8 Capture quality and mode metrics **8**
8.1 Services . . . 8

9 Next capture guidance **9**

A Appendices **9**
A.1 Protocol breakdown . . . 9
A.2 Methodology and scoring . . . 9
A.3 Vocabulary . . . 9

SAMPLE

Executive summary

`tls-handshake-failure-lab.pcap`
5 Nov 2026 · 09:30:00–09:30:30 UTC · 30.4 s

High | High confidence

Secure (TLS) connections fail during the handshake

8 of 8 TLS handshakes ended with a fatal alert.

Affected: 203.0.113.44

NETWORK IMPACT

75 /100 **Impaired**

0 40 75 90

FINDINGS · 1

Critical 0 | High 1 | Medium 0 | Low 0 | Info 0

COVERAGE · 11 AREAS

1 with a finding | 7 pass | 3 not assessed

Not assessed: only 4 DNS queries in...

262	18	3	2	2	66
frames	flows	hosts	protocols	destinations	checks run

The fault lies with the server 203.0.113.44:443

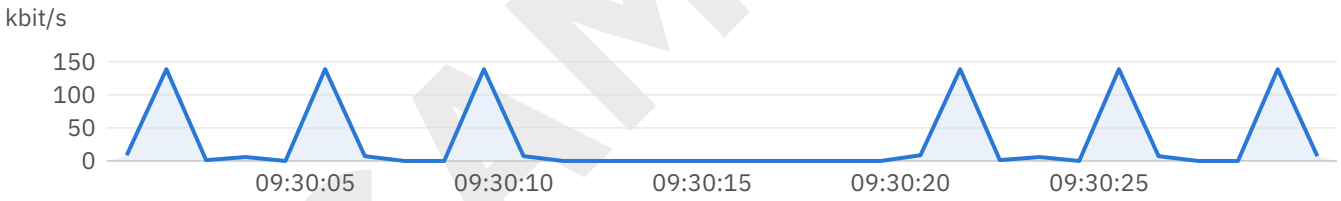
Figure 1 · section 4.1

Where the fault lies



Traffic ranged from 0.0 to 139 kbit/s

Figure 2 · UTC



Recommended actions

Immediately	Act on the alert reason	Application Owner
Strategic	Capture again and re-run the analysis	Network Operations

Capture point: segment (high). Figures use all 262 frames. Limitations: section 2.3.

SAMPLE

2 Scope, evidence and limitations

The analysis covers tls-handshake-failure-lab.pcap (116.0 kB, 262 frames) from 2026-11-05 09:30:00.000 UTC to 2026-11-05 09:30:30.365 UTC (30.4 s).

2.1 Evidence integrity

File	`tls-handshake-failure-lab.pcap`
Size	116.0 kB
SHA-256	`252f6bcde0368d77b7b9cd599e4d38d354a1f2ddecdaeb88b372dc0b864d0335`
Format	pcap
Link types	ethernet
Snapshot length	262,144
Frames	262
Capture point	Segment, high confidence
First packet	2026-11-05 09:30:00.000 UTC
Last packet	2026-11-05 09:30:30.365 UTC

2.2 Versions

Engine	PcapAI Analysis Engine 0.2.0 · ruleset 2026.10.1
Content	2026.10.1 (`sha256:f246f84c4791dd30`)
ATT&CK	19.2
Intelligence lists	service categories 2026-10-09.1; GeoLite2 Country 2026-02-17; GeoLite2 ASN 2024-07-29

2.3 Limitations

- The capture saw one network segment: traffic on other segments and beyond the gateway is not in it.
- 3 coverage areas were assessed partly or not at all; section 6 names the missing inputs.
- Encrypted traffic (TLS 1.3 application data, SMB3 encryption, LDAP sealing) hides content; only metadata was analyzed.
- Host activity outside this capture (processes, logons, other network segments) is not visible.

SAMPLE

3 Findings summary

ID	Title	Severity	Confidence	Roles	First seen	Status
F01	TLS handshakes with 203.0.113.44 (portal.example.net):443 (portal.example.net) fail with alerts (handshake_failure (no common cipher suite / parameters) from server x8)	High	High	Affected `203.0.113.44`		Open

4 Detailed findings

4.1 F01: TLS handshakes with 203.0.113.44 (portal.example.net):443 (portal.example.net) fail with alerts (handshake_failure (no common cipher suite / parameters) from server x8)

High Network problem · Open · Confidence: High · Reference PCAI-2026-1106-HX2Q-F01

8 of 8 TLS handshakes ended with a fatal alert.

Affected	`203.0.113.44` · `portal.example.net` · port 443

Evidence

- A fatal TLS alert during the handshake names the disagreement: TLS version, cipher suites, certificate trust or the requested host name (SNI).
- handshake_failure (no common cipher suite / parameters) from server x8

Remediation: A01 (Immediately, Application Owner); A02 (Strategic, Network Operations)

5 Remediation roadmap

5.1 Immediately

ID	Step	Owner	Effort	Verification	Findings
A01	Act on the alert reason (handshake_failure (no common cipher suite / parameters) from server x8): version mismatch means enable TLS 1.2 or 1.3 on both sides; unknown_ca or certificate_unknown means install the correct intermediate and root certificates; handshake_failure means align cipher suites; unrecognized_name means fix SNI / virtual-host configuration. Verify · Linux, macOS `openssl s_client -connect 203.0.113.44:443 -servername {HOST}` Replace {HOST} with the host name the clients connect to.	Application Owner	Small	The TLS handshake with `203.0.113.44:443` completes.	F01

5.2 Strategic

ID	Step	Owner	Effort	Verification	Findings
A02	Capture again after applying the steps and re-run the analysis.	Network Operations	Small	The new capture shows none of these problems.	F01

6 Coverage: checked and clean

What this capture let the engine check:

- **Checks:** 66 of 100 checks ran, in 8 of 11 areas; the table below gives the reason for each one that could not run.
- **Decoded:** 2 protocols (DNS and TLS).
- **Hosts:** 3 hosts, 2 destinations outside the network (section 7).
- **Protocols:** 2 protocols; in cleartext: DNS (UDP/53).
- **Passwords:** no login exchange in the capture, and no credential was sent readable.
- **TLS:** 6 TLS handshakes with 1 service; none older than TLS 1.2 (section 6.1).

SAMPLE

Area	Checks evaluated	Checks matched	Not run	Status	Reason
TCP connections	9	0	0	✓ Pass	
Packet loss	8	0	0	✓ Pass	
Latency	4	0	0	✓ Pass	
Receive windows	5	0	0	✓ Pass	
DNS	0	0	14	Not assessed	Only 4 DNS queries in the capture: too few to judge
DHCP	0	0	7	Not assessed	No DHCP exchanges in the capture
LAN (ARP, broadcast, switching)	0	0	13	Not assessed	No broadcast or ARP traffic in the capture
Routing and MTU	2	0	0	✓ Pass	
TLS	6	1	0	High F01	
Applications and services	27	0	0	✓ Pass	
Capture quality	5	0	0	✓ Pass	

6.1 TLS versions and certificates

6 TLS handshakes with 1 service: TLS 1.3 (6). None negotiated a version older than TLS 1.2. No certificate was visible; TLS 1.3 handshakes and resumed sessions show none.

Server	Name (SNI)	Versions	Clients	Certificate	Findings
198.51.100.40:443	www.example.org	TLS 1.3 (6)	2	Not visible	—

7 Assets and communications

The capture holds 18 flows (by addresses, ports and protocol) between 6 address pairs.

7.1 Asset inventory

3 internal hosts, from IP traffic, ARP, Ethernet senders and the entities of the findings.

IP	MAC	Hostname	Roles	Bytes sent	Bytes received	Risk
192.168.10.1	02:10:00:00:00:01	not observed	DNS server	370 B	306 B	
192.168.10.23	02:10:00:00:00:23	not observed		6.5 kB	49.3 kB	
192.168.10.31	02:10:00:00:00:31	not observed		6.5 kB	49.3 kB	

7.2 External destinations

2 external destinations exchanged traffic with internal hosts, most bytes first. Bytes are summed over their conversations; out counts the bytes the internal hosts sent.

Names come from HTTP Host, TLS SNI and DNS answers, the network owner from the GeoLite databases and the reputation from the service-category lists; section 2.2 dates each source.

Destination	Network owner	Protocol	Internal hosts	Reputation	Bytes out (conversations)	Bytes in (conversations)
198.51.100.40 www.example.org		TLS (TCP/443)	192.168.10.23 192.168.10.31	Not listed	9.0 kB	96.1 kB
203.0.113.44 portal.example.net		TLS (TCP/443)	192.168.10.23 192.168.10.31	Not listed	3.7 kB	2.2 kB

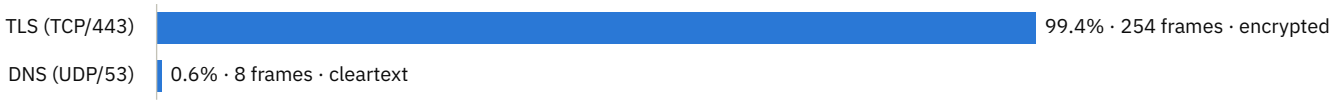
SAMPLE

7.3 Other conversations

The 2 conversations the destinations table does not list, by bytes. Address A sent the first packet.

Address A	Address B	Ports at B	Protocol	Bytes A → B	Bytes B → A
192.168.10.23	192.168.10.1	53	DNS (UDP/53)	153 B	185 B
192.168.10.31	192.168.10.1	53	DNS (UDP/53)	153 B	185 B

Figure 3. Cleartext protocols carried 0.6% of the captured bytes



Share of captured bytes per protocol, with frames; 2 protocols in total. Source: all 262 frames, tls-handshake-failure-lab.pcap. Table: section A.1.

8 Capture quality and mode metrics

Capture point	Segment, high confidence: 3 hosts on the local network exchange unicast traffic; 100% of it goes to or from the gateway MAC.
Position on the TCP paths	Near the client
Frames cut by the snapshot length	0
Packets dropped by the capture tool	not reported
Segments acknowledged but not captured	0
Duplicate frames (captured twice)	0
One-sided TCP sessions	0 of 14
Network health impact	75 of 100
Network issues found	1
TCP connection attempts	14
TCP connections established	14
TCP connection attempts that failed	0
TCP retransmissions	0
Estimated packet loss	0.0%
Handshake round trip, median	24 ms
Handshake round trip, 95th percentile	24 ms
Server response time, 95th percentile	74 ms
DNS queries	4
DNS queries without an answer	0
DNS answer time, 95th percentile	14 ms

8.1 Services

Service	Server	Clients	Requests	Unanswered	Errors	95th percentile
TLS	203.0.113.44 (portal.example.net):443	2	8	0	8	not measured
TLS	198.51.100.40 (www.example.org):443	2	6	0	0	28 ms

SAMPLE

9 Next capture guidance

Why a new capture would help

- The capture is shorter than 5 minutes.
- Some areas could not be assessed because their protocols were absent.

How to capture

- Capture on a SPAN port or TAP of the gateway uplink or the server segment.
- Capture for at least 15 minutes, ideally during business hours.
- Use the full snapshot length.
- Do not use capture filters that drop ARP, DNS or DHCP.

A Appendices

A.1 Protocol breakdown

Protocol	Protection	Bytes	Share	Frames
TLS (TCP/443)	encrypted	111.1 kB	99.4%	254
DNS (UDP/53)	cleartext	676 B	0.6%	8

A.2 Methodology and scoring

Detection rules inspect captured protocol data. Findings with the same rule and key entities are merged; the report lists them in order of severity, confidence and first appearance.

Confidence follows fixed rules. High: the primary signal, every required check passes, at least one strong check passes and no alternative remains open. Medium: the primary signal, no required check fails, and either no strong check passes or an alternative remains open. Low: a partial primary signal, or a required check could not be evaluated.

Each finding scores its severity weight (Critical 90, High 75, Medium 45, Low 20) times a confidence factor (High 100%, Medium 85%, Low 60%); exposures are capped at 75 and indicators at 40. Overall risk is the highest finding score plus at most 15 points for attack breadth across tactics, affected hosts and linked findings. Bands: Low 0-24, Guarded 25-49, Elevated 50-74, Severe 75-100.

A host's risk is the highest score of the findings that name it, weighted by its role (suspected source 100%, affected or impersonated 80%, client or server of an exposure 70%), plus 3 points for each further finding, at most 10, capped at 100.

Every observation lists the Wireshark frames it rests on and a display filter that selects them in the original capture.

Framework references list the controls to review for each finding. They do not state compliance or non-compliance; applicability depends on the organization's scope.

MITRE ATT&CK® is a registered trademark of The MITRE Corporation. Technique, tactic and mitigation names come from ATT&CK 19.2, © The MITRE Corporation, used under its terms of use.

A.3 Vocabulary

- Threat: activity that indicates an attack in progress or completed.
- Exposure: a weakness that could be used against the network; no attack on it was observed.
- Indicator: a signal worth reviewing; on its own it is not evidence of an attack.
- Severity: Critical, High, Medium, Low or Info, set by the finding profile and its conditions.
- Confidence: High, Medium or Low, set by the automatic checks listed on each finding.
- Risk bands: Low 0–24, Guarded 25–49, Elevated 50–74, Severe 75–100.
- Frame: one captured packet, numbered as in Wireshark.
- Conversation: all traffic between two IP addresses, in both directions, as in the Wireshark IPv4 and IPv6 conversation statistics.

SAMPLE

- TCP session: one TCP connection.
- Exchange: one request with its response.
- Observation: one evidence row of a finding, with its frames and display filter.
- Check: one detection rule evaluated on the capture. Area: the checks of one attack family.
- Host: an internal device of the asset inventory. Destination: an external address that exchanged traffic with internal hosts.
- Bytes: out is sent by the internal host and in is received by it. Request and response bytes count the application message; conversation bytes count whole frames.

SAMPLE