Network Capture Troubleshooting Report

`dns-failures-lab.pcap`

Report ID	`PCAI-2026-1106-XA2R`
Version	1 (Sample)
Generated	2026-11-06 11:18:54 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: DNS server 192.168.10.1 returned SERVFAIL 12 times . . . 6
4.2 F02: 12 of 120 queries to DNS server 192.168.10.1 went unanswered . . . 6

5 Remediation roadmap **6**
5.1 Within 24 hours . . . 6
5.2 Strategic . . . 7

6 Coverage: checked and clean **7**

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

8 Capture quality and mode metrics **8**

9 Next capture guidance **8**

A Appendices **8**
A.1 Event log . . . 8
A.2 Methodology and scoring . . . 9
A.3 Vocabulary . . . 9

SAMPLE

Executive summary

dns-failures-lab.pcap
5 Nov 2026 · 09:30:00–09:31:36 UTC · 96.5 s

Medium | High confidence

DNS server 192.168.10.1 returned SERVFAIL 12 times

14.29% of answers from 192.168.10.1 were SERVFAIL. 1 more finding: section 3.

Affected: 192.168.10.1

NETWORK IMPACT

53 /100 **Degraded**

0 40 75 90

FINDINGS · 2

Critical 0 | High 0 | Medium 2 | Low 0 | Info 0

COVERAGE · 11 AREAS

1 with a finding | 3 pass | 7 not assessed

Not assessed: no TCP connections in...

204	96	3	1	0	26
frames	flows	hosts	protocol	destinations	checks run

The fault lies with name resolution

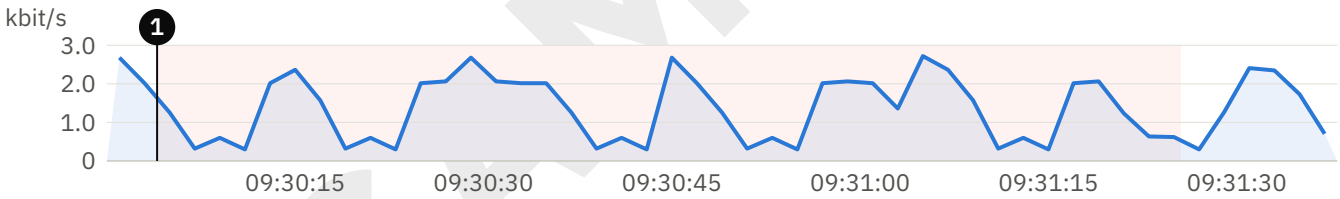
Figure 1 · section 4.1

Where the fault lies



Traffic peaked at 2.7 kbit/s during F01

Figure 2 · UTC



1 09:30:04 DNS | A DNS server fails lookups (SERVFAIL) | A DNS server leaves queries unanswered

Recommended actions

Within 24 hours	Resolver 192.168.10.1 cannot complete these lookups	Network Operations
Within 24 hours	Check that resolver 192.168.10.1 is up and reachable on...	Network Operations
Strategic	Capture again and re-run the analysis	Network Operations

Capture point: host-side (high). Figures use all 204 frames. Limitations: section 2.3.

SAMPLE

2 Scope, evidence and limitations

The analysis covers dns-failures-lab.pcap (20.2 kB, 204 frames) from 2026-11-05 09:30:00.000 UTC to 2026-11-05 09:31:36.498 UTC (96.5 s).

2.1 Evidence integrity

File	`dns-failures-lab.pcap`
Size	20.2 kB
SHA-256	`a6d97cbd32b06ee213a1bef84661fbb2e39e4e70813ea6ae4db908c54d58c3bf`
Format	pcap
Link types	ethernet
Snapshot length	262,144
Frames	204
Capture point	Host-side, high confidence
First packet	2026-11-05 09:30:00.000 UTC
Last packet	2026-11-05 09:31:36.498 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 was taken on one host: traffic between other hosts, and frames the network sends elsewhere, are not in it; checks that need them read “not visible from this capture point”.
- 7 coverage areas were assessed partly or not at all; section 6 names the missing inputs.
- Host activity outside this capture (processes, logons, other network segments) is not visible.

3 Findings summary

ID	Title	Severity	Confidence	Roles	First seen	Status
F01	DNS server 192.168.10.1 returned SERVFAIL 12 times	Medium	High	Affected `192.168.10.1`	2026-11-05 09:30:04 UTC	Open
F02	12 of 120 queries to DNS server 192.168.10.1 went unanswered	Medium	High	Affected `192.168.10.1`	2026-11-05 09:30:04 UTC	Open

SAMPLE

4 Detailed findings

4.1 F01: DNS server 192.168.10.1 returned SERVFAIL 12 times

Medium Network problem · Open · Confidence: High · Reference PCAI-2026-1106-XA2R-F01

14.29% of answers from `192.168.10.1` were SERVFAIL.

Affected	`192.168.10.1` · `02:10:00:00:00:01`
First seen	2026-11-05 09:30:04.000 UTC (T+4.000 s)
Last seen	2026-11-05 09:31:25.500 UTC (T+85.500 s)

Evidence

- SERVFAIL means the resolver could not complete the lookup: its forwarders or the authoritative servers are unreachable, or DNSSEC validation failed.
- SERVFAIL: 12 of 84 responses
- Names: crm.example.org (SERVFAIL x6, 2 clients), partner.example.net (SERVFAIL x6, 2 clients)

Remediation: A01 (Within 24 hours, Network Operations); A05 (Strategic, Network Operations)

4.2 F02: 12 of 120 queries to DNS server 192.168.10.1 went unanswered

Medium Network problem · Open · Confidence: High · Reference PCAI-2026-1106-XA2R-F02

10% of lookups sent to `192.168.10.1` got no answer (12 were retried by the client); each one costs the application a timeout of a second or more.

Key facts for F02: as under F01.

Evidence

- Unanswered DNS queries stall every application that needs a name: the client waits for its timeout, then retries or moves to the next resolver.
- Queries: 120, responses: 84, unanswered: 12
- Client retries: 24
- Names that timed out: intranet.example.org (TIMEOUT x6, 2 clients), vpn.example.com (TIMEOUT x6, 2 clients)

Remediation: A02 (Within 24 hours, Network Operations); A03 (Within 24 hours, Network Operations); A04 (Within 24 hours, Network Operations); A05 (Strategic, Network Operations)

5 Remediation roadmap

5.1 Within 24 hours

ID	Step	Owner	Effort	Verification	Findings
A01	Resolver `192.168.10.1` cannot complete these lookups: check its forwarders' reachability and the DNSSEC validation errors in its logs; a name that resolves only with checking disabled fails DNSSEC validation. Linux, macOS `dig @192.168.10.1 {NAME}` Linux, macOS `dig @192.168.10.1 {NAME} +cd` Replace {NAME} with a failing name from the evidence.	Network Operations	Small	The failing names resolve with NOERROR.	F01
A02	Check that resolver `192.168.10.1` is up and reachable on UDP and TCP 53 from `192.168.10.23`. Linux, macOS `dig @192.168.10.1 example.com` Windows `nslookup example.com 192.168.10.1`	Network Operations	Small	`192.168.10.1` answers in under 100 ms and no queries go unanswered in a new capture.	F02
A03	If it forwards upstream, check its forwarders and its outbound UDP/53.	Network Operations	Small		F02

SAMPLE

ID	Step	Owner	Effort	Verification	Findings
A04	Give clients a second resolver (DHCP option 6).	Network Operations	Small		F02

5.2 Strategic

ID	Step	Owner	Effort	Verification	Findings
A05	Capture again after applying the steps and re-run the analysis.	Network Operations	Small	The new capture shows none of these problems.	F01, F02

6 Coverage: checked and clean

What this capture let the engine check:

- **Checks:** 26 of 100 checks ran, in 4 of 11 areas; the table below gives the reason for each one that could not run.
- **Decoded:** 1 protocol (DNS).
- **Hosts:** 3 hosts, 0 destinations outside the network (section 7).
- **Protocols:** 1 protocol; in cleartext: DNS (UDP/53).
- **Passwords:** no login exchange in the capture, and no credential was sent readable.
- **TLS:** no TLS handshake in the capture.

Area	Checks evaluated	Checks matched	Not run	Status	Reason
TCP connections	0	0	9	Not assessed	No TCP connections in the capture
Packet loss	0	0	8	Not assessed	Only 0 TCP data packets: too little to judge loss
Latency	0	0	4	Not assessed	No complete TCP handshakes to measure round-trip time
Receive windows	5	0	0	✓ Pass	
DNS	14	2	0	Medium F01, F02	
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	0	0	6	Not assessed	No TLS handshakes in the capture
Applications and services	0	0	27	Not assessed	No application service endpoints identified
Capture quality	5	0	0	✓ Pass	

7 Assets and communications

The capture holds 96 flows (by addresses, ports and protocol) between 2 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, Affected	7.6 kB	9.3 kB	39
192.168.10.23	02:10:00:00:00:23	not observed		4.6 kB	3.8 kB	
192.168.10.31	02:10:00:00:00:31	not observed		4.6 kB	3.8 kB	

SAMPLE

7.2 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)	4.6 kB	3.8 kB
192.168.10.31	192.168.10.1	53	DNS (UDP/53)	4.6 kB	3.8 kB

8 Capture quality and mode metrics

Capture point	Host-side, high confidence: 100% of the unicast IP frames involve 192.168.10.1.
Position on the TCP paths	Undetermined
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 0
Network health impact	53 of 100
Network issues found	2
DNS queries	120
DNS queries without an answer	12
DNS answer time, 95th percentile	1,396 ms

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.

SAMPLE

A Appendices

A.1 Event log

Time (UTC)	ID	Observation
2026-11-05 09:30:04.000 UTC T+4.000 s	F01	First seen: DNS server 192.168.10.1 returned SERVFAIL 12 times
2026-11-05 09:30:04.000 UTC T+4.000 s	F02	First seen: 12 of 120 queries to DNS server 192.168.10.1 went unanswered
2026-11-05 09:31:25.500 UTC T+85.500 s	F01	Last seen: DNS server 192.168.10.1 returned SERVFAIL 12 times
2026-11-05 09:31:25.500 UTC T+85.500 s	F02	Last seen: 12 of 120 queries to DNS server 192.168.10.1 went unanswered

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.
- 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