

UNITED STATES DISTRICT COURT
DISTRICT OF COLUMBIA

Kirchner v. Anthropic, PBC - Case No. 1:25-cv-02735-ACR

EXHIBIT D-18: January 11, 2026 MacBook Compromise/Spoofing

Case: Kirchner v. Anthropic, PBC (1:25-cv-02735-ACR)

Evidence ID: EVID-20260111-0001

Original Exhibit: X-1_jan11_local_network.txt

Attack Summary

Metric	Value
Total RSTs	17,632
Segments	64
Avg RSTs/Segment	275 (HIGHEST)

Rst Source Distribution

Source IP	Count	Identity	Status
192.168.1.137	318	Plaintiff's MacBook	COMPROMISED/SPOOFED
149.112.112.112	101	Quad9 DNS	SPOOFED
9.9.9.9	32	Quad9 DNS	SPOOFED
10.157.12.231	22	Internal	Relay
74.125.132.109	18	Google	Normal

CRITICAL FINDING: PLAINTIFF'S MACBOOK AS RST SOURCE ###

192.168.1.137 is the ****Plaintiff's MacBook**** IP address. 318 RST packets bearing this source IP indicates either:

1. MacBook Compromised: Plaintiff's MacBook has been compromised and is sending RST packets (correlates with Node.js debugger attack in EVID-20251228-0022 and terminal injection in EVID-20260108-0003)

2. Source IP Spoofed: Attacker is injecting packets with Plaintiff's IP as forged source address, indicating router-level or ISP-level access

Either scenario proves deep compromise of Plaintiff's local network infrastructure.

Verification

```
tshark -r seg_20260111_.pcapng \  
-Y "tcp.flags.reset==1 and ip.src==192.168.1.137" | wc -l
```

Expected: 318+