

Forum:[Hack Forums](#)

Thread: [Can't capture WPA2 4-way handshake on one AP help?](#)

odedor444 - October 2, 2025, 6:29 am

I'm testing two WPA2 APs with Kali and a TP-Link Archer T3U Plus (monitor mode). On AP #1 I capture the 4-way handshake reliably using:

```
airodump-ng -c <chan> --bssid <BSSID> -w capture wlan0  
sudo aireplay-ng --deauth 0 -a <BSSID> wlan0
```

On AP #2 I only see one client (~-70 dBm) (I have more than 1 devices connected to this network, but they're far from my network adapter). I spam deauths for minutes (aireplay shows ACKs) but no handshake appears. While attacking, the client's Lost count jumps huge (?7000).

Quick questions:

Could low signal cause no handshake?

Would a stronger adapter (Alfa) likely help?

How can I tell if PMF/WPA3 is blocking deauths?

Any quick checks I should paste (iw dev, airmon-ng, aireplay output)?

Thanks.

DramaKing - October 2, 2025, 7:06 am

(Oct 2, 2025 06:29 AM)odedor444 Wrote: [\[CITE\]](#) I'm testing two WPA2 APs with Kali and a TP-Link Archer T3U Plus (monitor mode). On AP #1 I capture the 4-way handshake reliably using:

```
airodump-ng -c <chan> --bssid <BSSID> -w capture wlan0  
sudo aireplay-ng --deauth 0 -a <BSSID> wlan0
```

On AP #2 I only see one client (~-70 dBm) (I have more than 1 devices connected to this network, but they're far from my network adapter). I spam deauths for minutes (aireplay shows ACKs) but no handshake appears. While attacking, the client's Lost count jumps huge (?7000).

Quick questions:

Could low signal cause no handshake?

Would a stronger adapter (Alfa) likely help?

How can I tell if PMF/WPA3 is blocking deauths?

Any quick checks I should paste (iw dev, airmon-ng, aireplay output)?

Thanks.

Losing packets like that is most likely a problem.

You shouldn't be using airodump-ng.
Airodump-ng will at least tell you the security type.
Without an external antenna, you will have zero gain. An EDUP AXE3000 or similar should be better.
Anyone who has been hacking WPA2 for any length of time will tell you that spamming deauth packets continuously is a bad idea.

odedor444 - October 2, 2025, 7:21 am

(Oct 2, 2025 07:06 AM)DramaKing Wrote: [\[CITE\]](#)

Losing packets like that is most likely a problem.

You shouldn't be using airodump-ng.

Airodump-ng will at least tell you the security type.

Without an external antenna, you will have zero gain. An EDUP AXE3000 or similar should be better.

Anyone who has been hacking WPA2 for any length of time will tell you that spamming deauth packets continuously is a bad idea.

Thanks for your help,

1. What do you think is causing the problem ?
2. What should I be using instead of airodump-ng ?
4. I have TP-Link Archer T3U Plus AC1300 which is an external antenna, but maybe its not as strong as Alfa ?
5. What are the alternatives ?

DramaKing - October 2, 2025, 8:23 am

(Oct 2, 2025 07:21 AM)odedor444 Wrote: [\[CITE\]](#) Thanks for your help,

1. What do you think is causing the problem ?
2. What should I be using instead of airodump-ng ?
4. I have TP-Link Archer T3U Plus AC1300 which is an external antenna, but maybe its not as strong as Alfa ?
5. What are the alternatives ?

Signal isn't that bad, but you're missing a lot of packets. Funny that I can't actually find an example of a 'Lost' column.

hcxdump tool is about the best and most advanced WiFi auditing tool. It won't give you the errors that you get with a .cap file and aireplay-ng. hcxtools is the de facto suite for converting capture files, anyway. Run 'hcxdump tool -i wlan0 -o test.pcapng -t 5 --enable_status=11 | tee test.log'

I apparently looked at the wrong T3U. It has a high-gain antenna. All I can do is theorize about OFDM, bandwidth, and other things that could be a problem for an 802.11ac adapter.

You might also try airgeddon. It checks for WPA3 for you.