Wifi Protocol 3 (개선 필요)

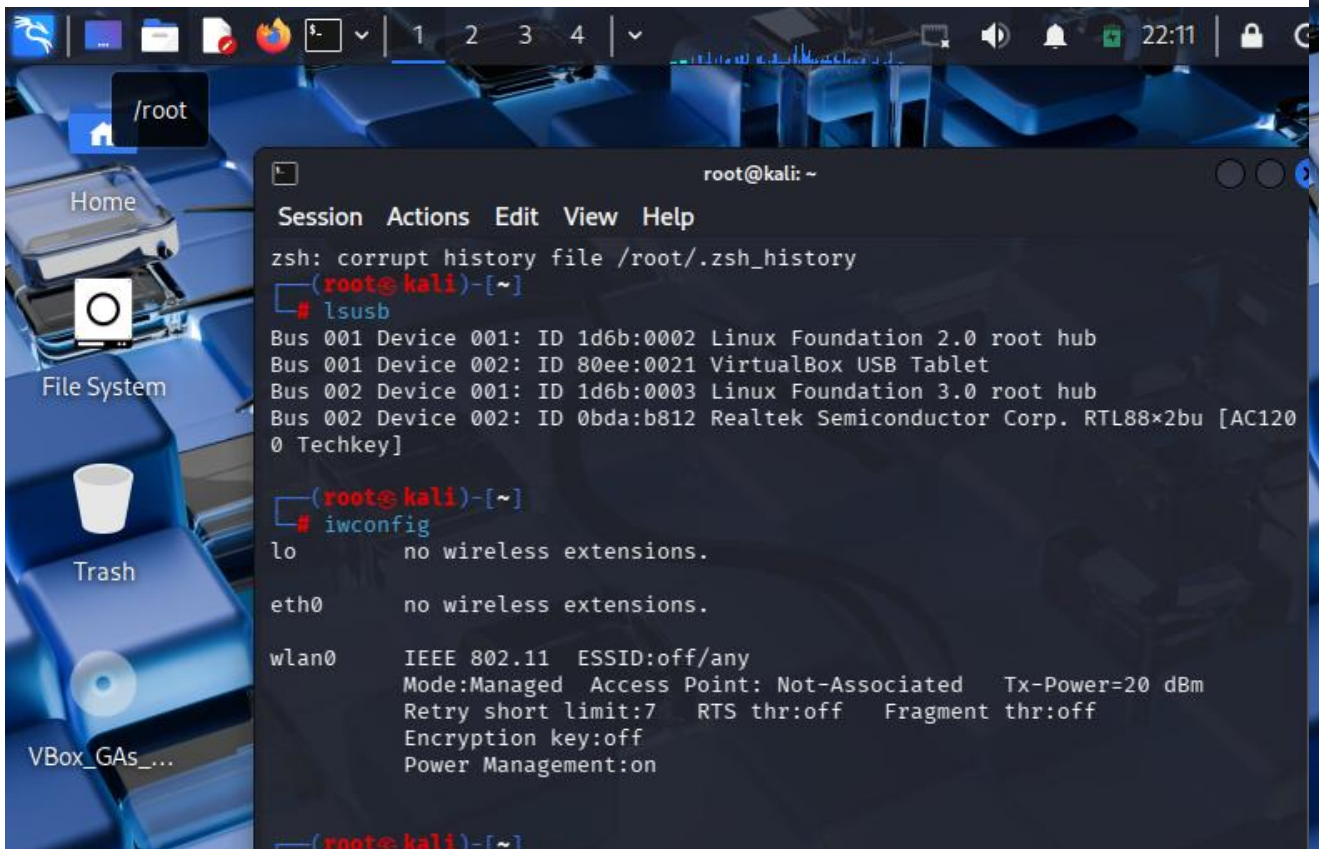
20210638 최무송

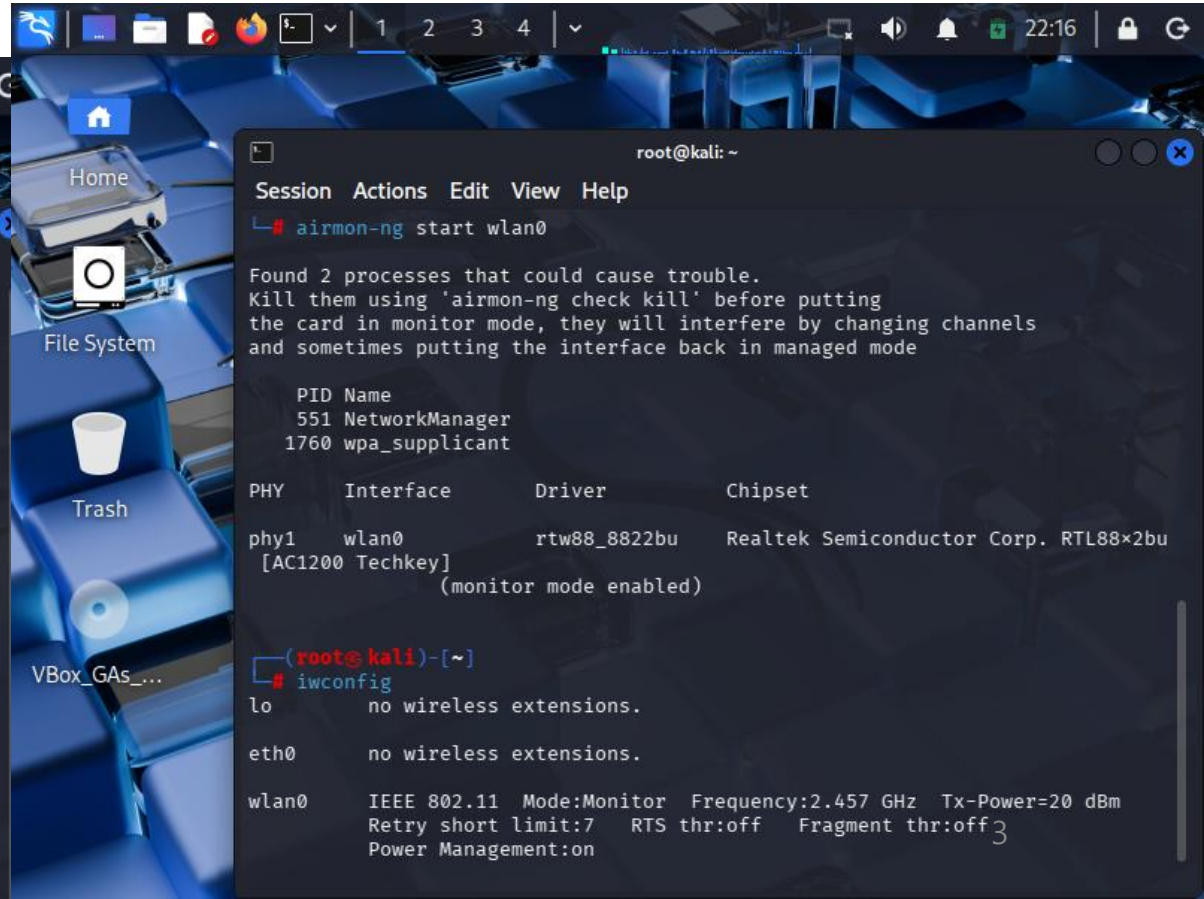
TODO

- Fragattacks
- KRACK (Key Reinstallaion AttaCK)
- PMKID offline dictionary attack

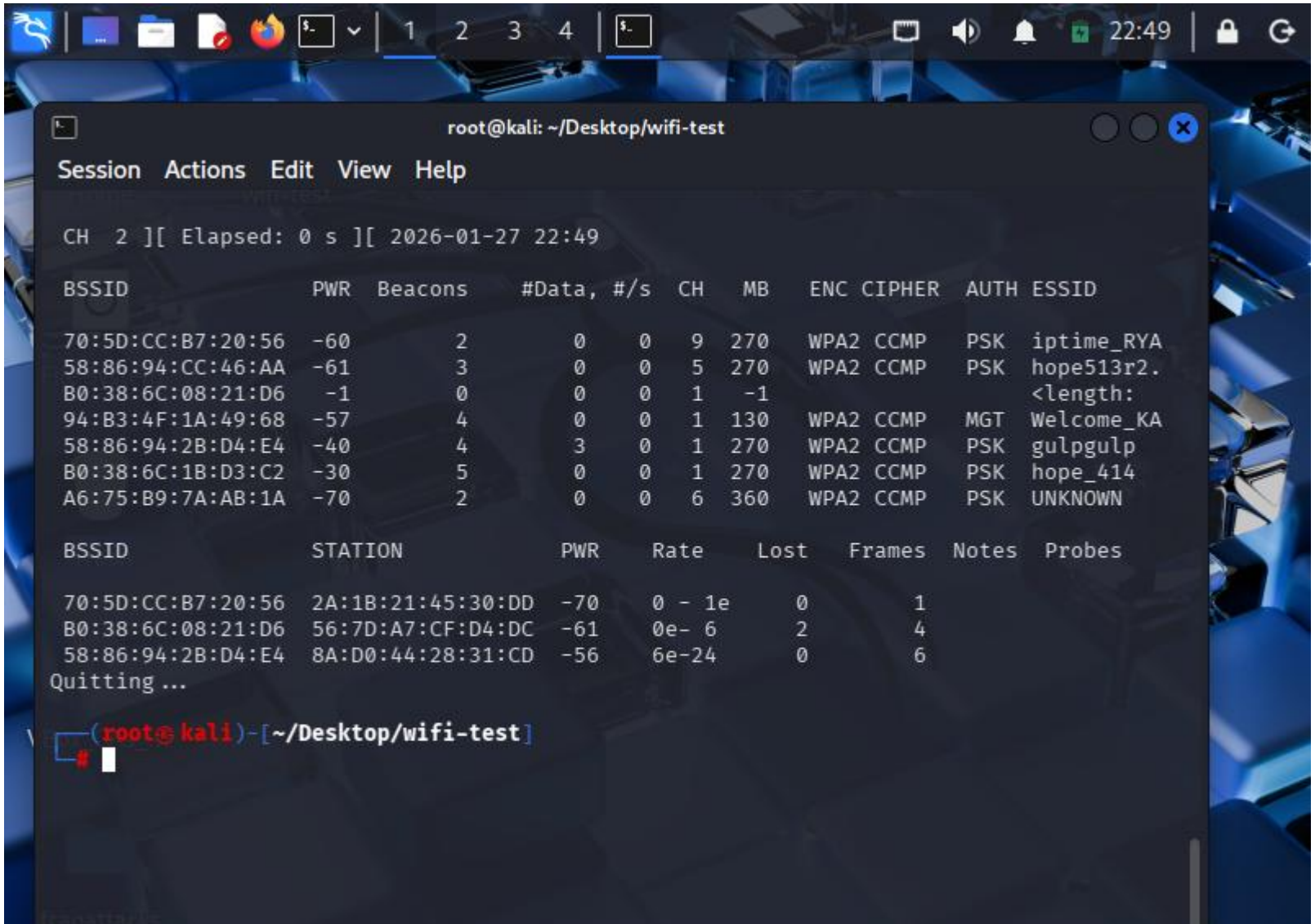
Environment

- OS: Kali linux
- Wireless LAN: ipTIME A3000UA





Scaning…

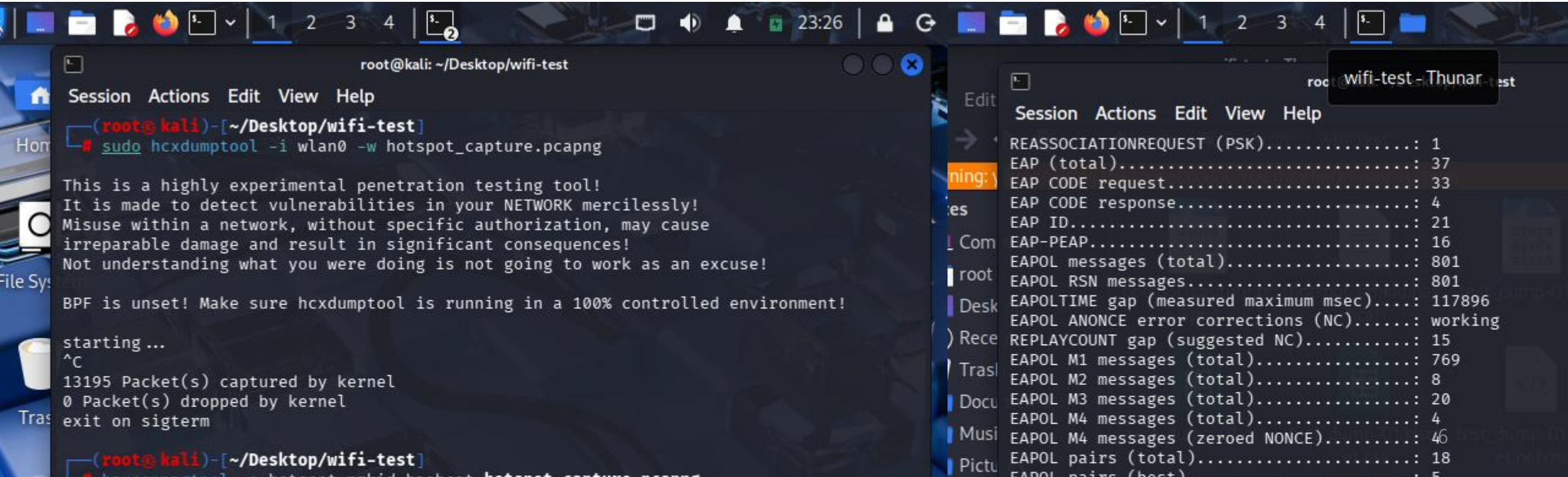

1 2 3 4
22:49
root@kali: ~/Desktop/wifi-test
Session Actions Edit View Help
CH 2][Elapsed: 0 s][2026-01-27 22:49
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
70:5D:CC:B7:20:56 -60 2 0 0 9 270 WPA2 CCMP PSK iptime_RYA
58:86:94:CC:46:AA -61 3 0 0 5 270 WPA2 CCMP PSK hope513r2.
B0:38:6C:08:21:D6 -1 0 0 0 1 -1 <length:
94:B3:4F:1A:49:68 -57 4 0 0 1 130 WPA2 CCMP MGT Welcome_KA
58:86:94:2B:D4:E4 -40 4 3 0 1 270 WPA2 CCMP PSK gulpgulp
B0:38:6C:1B:D3:C2 -30 5 0 0 1 270 WPA2 CCMP PSK hope_414
A6:75:B9:7A:AB:1A -70 2 0 0 6 360 WPA2 CCMP PSK UNKNOWN
BSSID STATION PWR Rate Lost Frames Notes Probes
70:5D:CC:B7:20:56 2A:1B:21:45:30:DD -70 0 - 1e 0 1
B0:38:6C:08:21:D6 56:7D:A7:CF:D4:DC -61 0e- 6 2 4
58:86:94:2B:D4:E4 8A:D0:44:28:31:CD -56 6e-24 0 6
Quitting ...
(root@kali)-[~/Desktop/wifi-test]
#

Utilization (example)

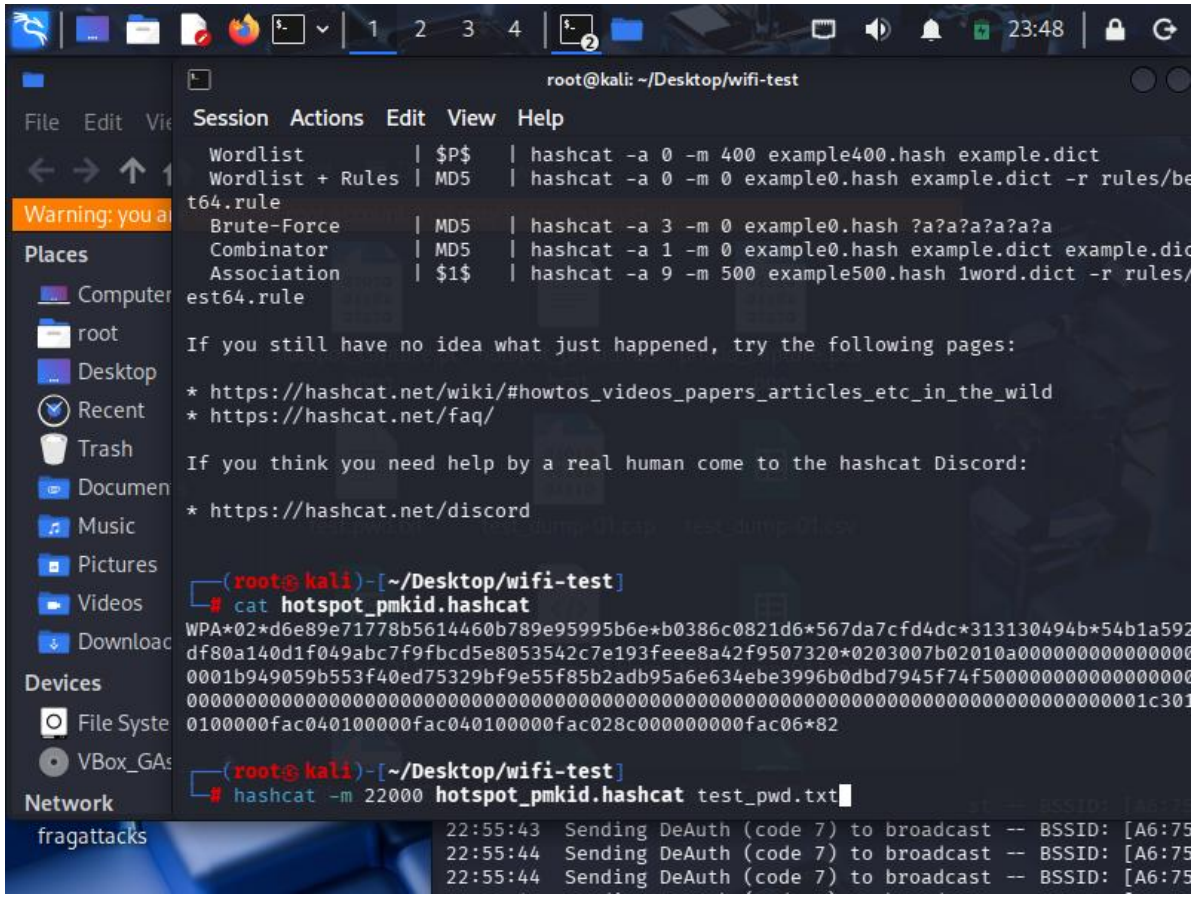
- Connecting WLAN card with Kali linux
- Run with monitor mode
- Scan wifi packets with airodump-ng command
- Capture 4-way Handshake with aireplay-ng command
  - (Deauth: aireplay-ng –deauth [num] –a [MAC addr] wlan0)
- Dictionary attack with Aircrack-ng command

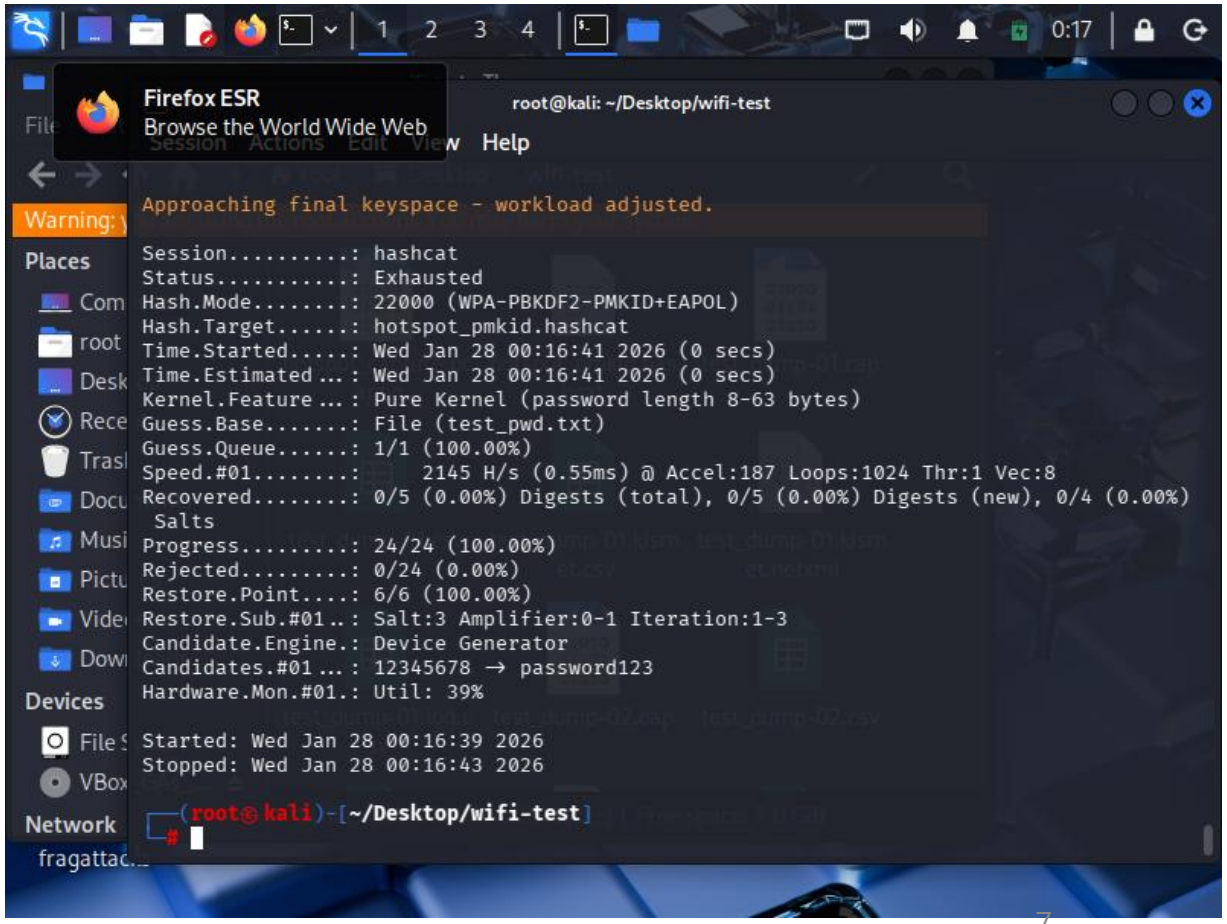
PMKID offline dictionary attack

- Client-less attack
  - Attacker receives EAPOL Message 1 from AP
  - Dictionary attack can be possible for PMKID in M1



Dictionary attack





KRACK

- MitM attack
  - Key installation by resending Message 3
  - Utilize same key (parameters get reset when reinstalled)

- Packets can be replayed, decrypted, and/or forged which causes
  - Bypassing HTTPS
  - Intercept important information

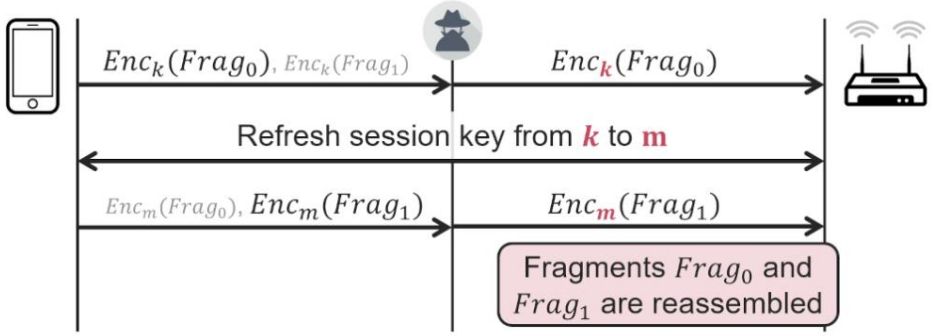
- https://youtu.be/Oh4WURZoR98

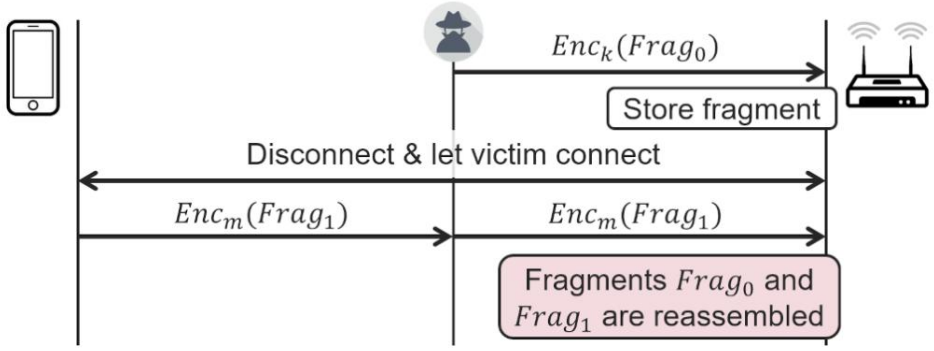
Vulnerability check (KRACK)

- vanhoefm/krackattacks-scripts
  - It creates virtual AP on device. It can test its connected client by resending M3s in different situations

Fragattacks

- Injecting unencrypted wi-fi frame
  - Aggregation attack → fixed by "is aggregated" flag
  - Mixed key attack can use reassemble fragments that were decrypted by different keys → more likely a theoretical attack
  - Fragment cache attack can send malicious fragment that can be combined within the other fragments → fixed by removing fragments when disconnection or (re)connection
  - [FragAttacks: Breaking Wi-Fi through Fragmentation and Aggregation]





Vulnerability check (Fragattacks)

- vanhoefm/fragattacks
  - Check by sending various fragmented pings to devices in different conditions.

Reference

- New attack on WPA/WPA2 using PMKID
- ccs2017.pdf (KRACK Attacks: Breaking WPA2)
  - vanhoefm/krackattacks-scripts
- usenix2021.pdf (FragAttacks: Security flaws in all Wi-Fi devices)
  - vanhoefm/fragattacks