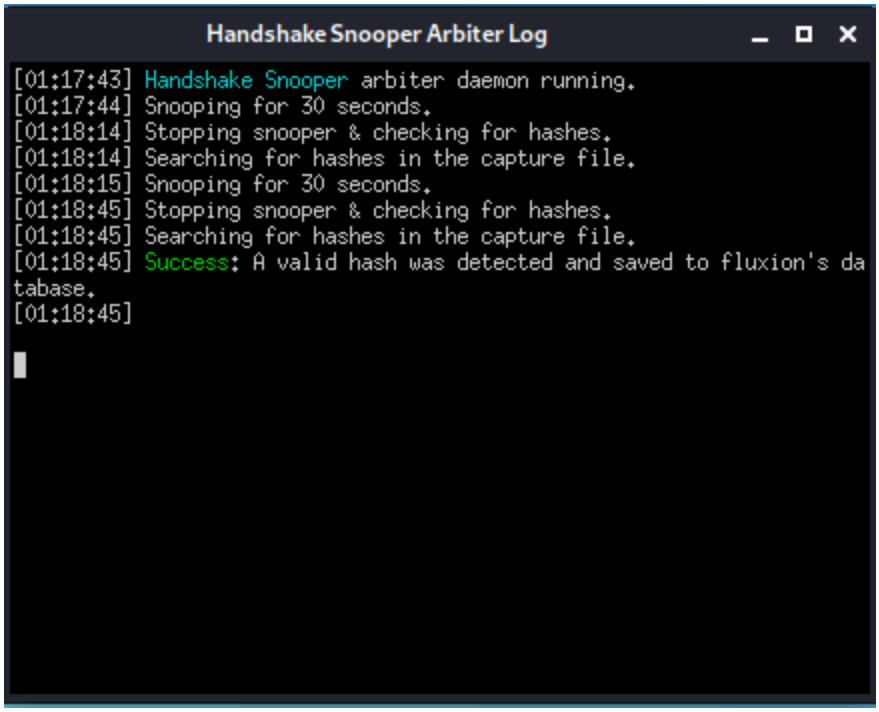
9/16 공부내용_공재호

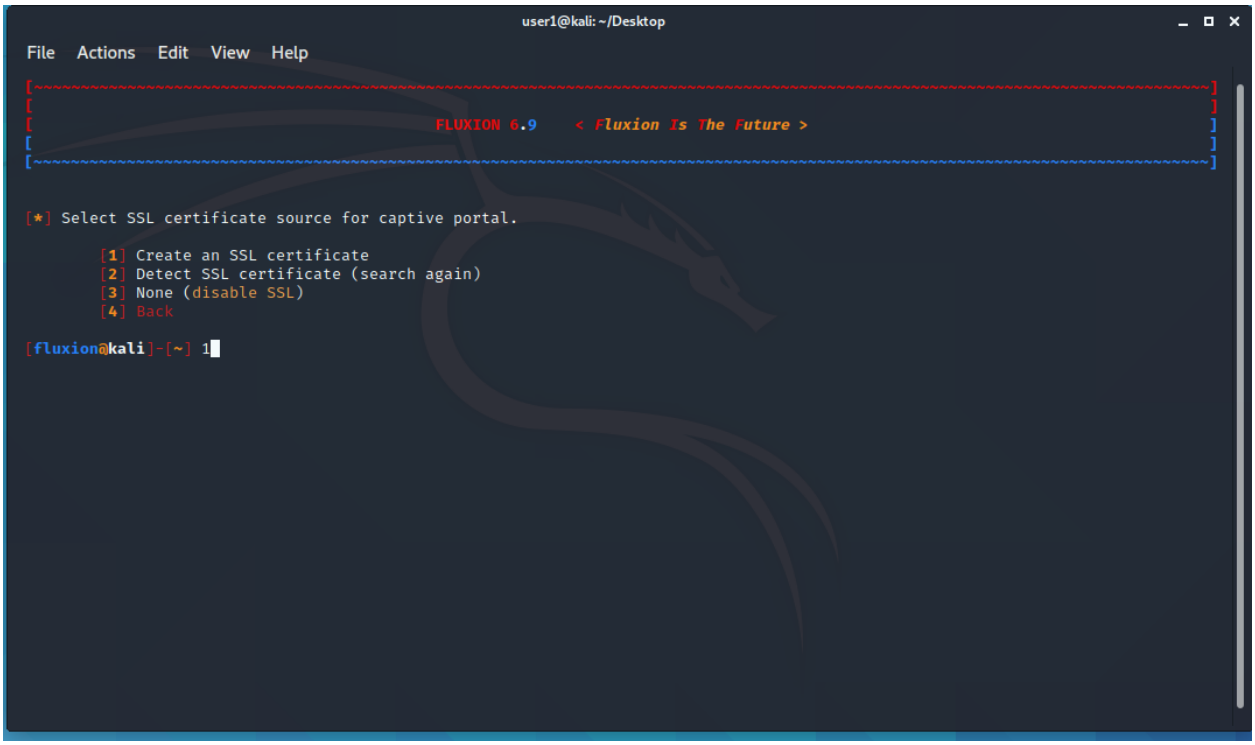
Asignee	
Joined	@Sep 16, 2020 3:57 PM
Location	공재호
Title	

- virtualBox 에서 패킷 잡다보면 잡힐때도 있고 안잡힐때도 있어서 너무 시간 오래걸림. 한번 시도할때마다 재시도할때 많음.. 그래서 그냥 가상머신 말고 자체 칼리로 시도함

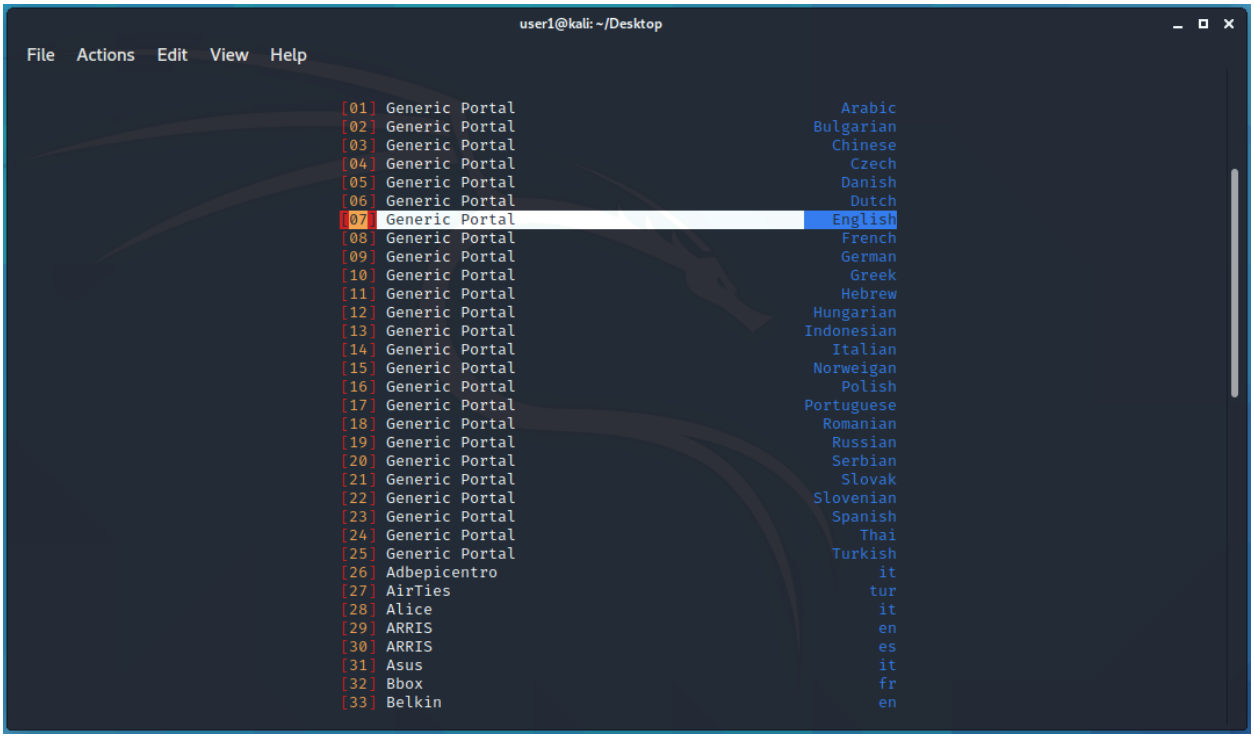
선택한 wifi 해쉬값 얻기 성공



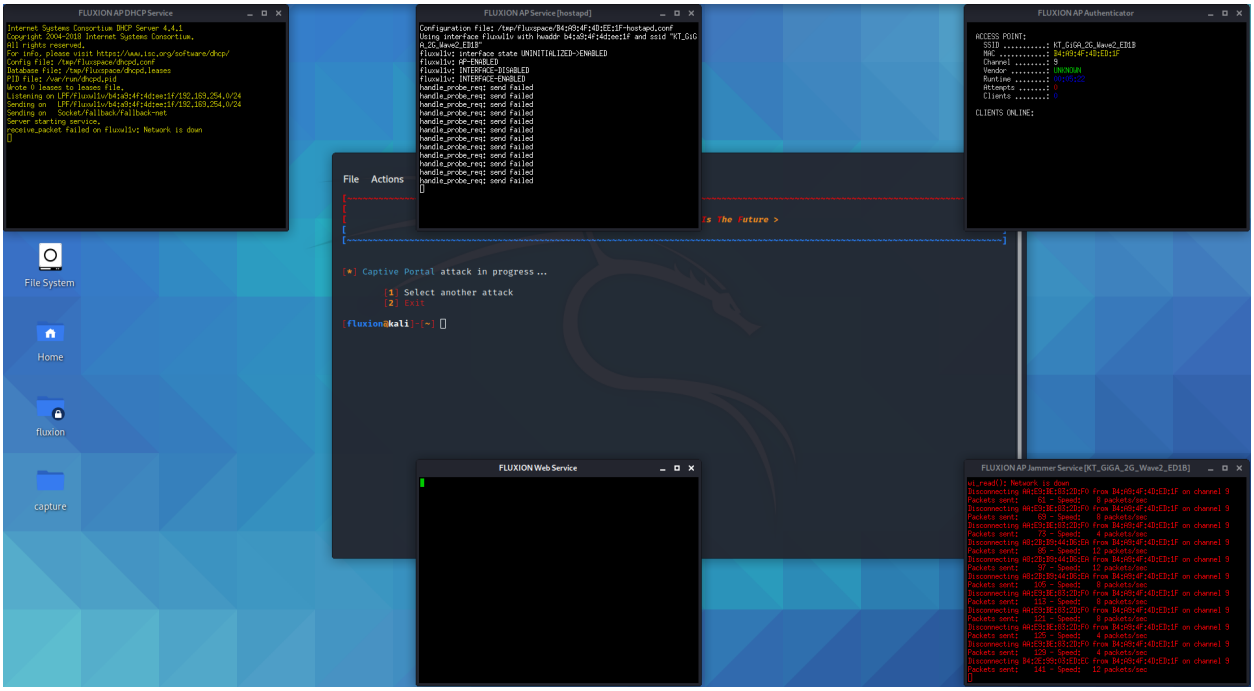
SSL 인증파일 생성


user1@kali: ~/Desktop
File Actions Edit View Help
FLUXION 6.9 < Fluxion Is The Future >
[*] Select SSL certificate source for captive portal.
[1] Create an SSL certificate
[2] Detect SSL certificate (search again)
[3] None (disable SSL)
[4] Back
[fluxion@kali]-[~] 1

영어로

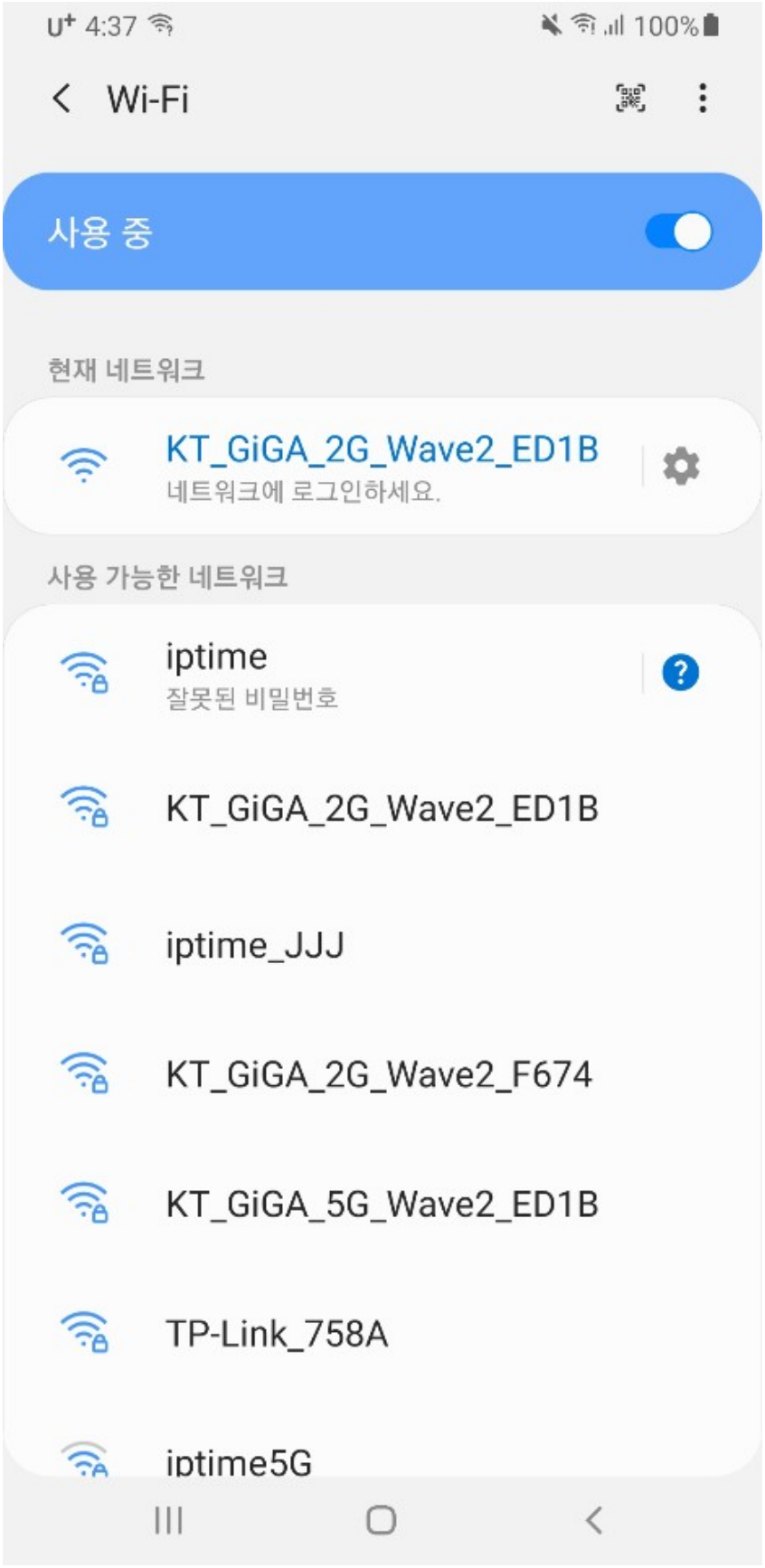

user1@kali: ~/Desktop
File Actions Edit View Help
[01] Generic Portal Arabic
[02] Generic Portal Bulgarian
[03] Generic Portal Chinese
[04] Generic Portal Czech
[05] Generic Portal Danish
[06] Generic Portal Dutch
[07] Generic Portal English
[08] Generic Portal French
[09] Generic Portal German
[10] Generic Portal Greek
[11] Generic Portal Hebrew
[12] Generic Portal Hungarian
[13] Generic Portal Indonesian
[14] Generic Portal Italian
[15] Generic Portal Norweigan
[16] Generic Portal Polish
[17] Generic Portal Portuguese
[18] Generic Portal Romanian
[19] Generic Portal Russian
[20] Generic Portal Serbian
[21] Generic Portal Slovak
[22] Generic Portal Slovenian
[23] Generic Portal Spanish
[24] Generic Portal Thai
[25] Generic Portal Turkish
[26] Adbepicentro it
[27] AirTies tur
[28] Alice it
[29] ARRIS en
[30] ARRIS es
[31] Asus it
[32] Bbox fr
[33] Belkin en

ㅋㅋDEAUTH만 되고 또 계속안됨 ㅎㅎ

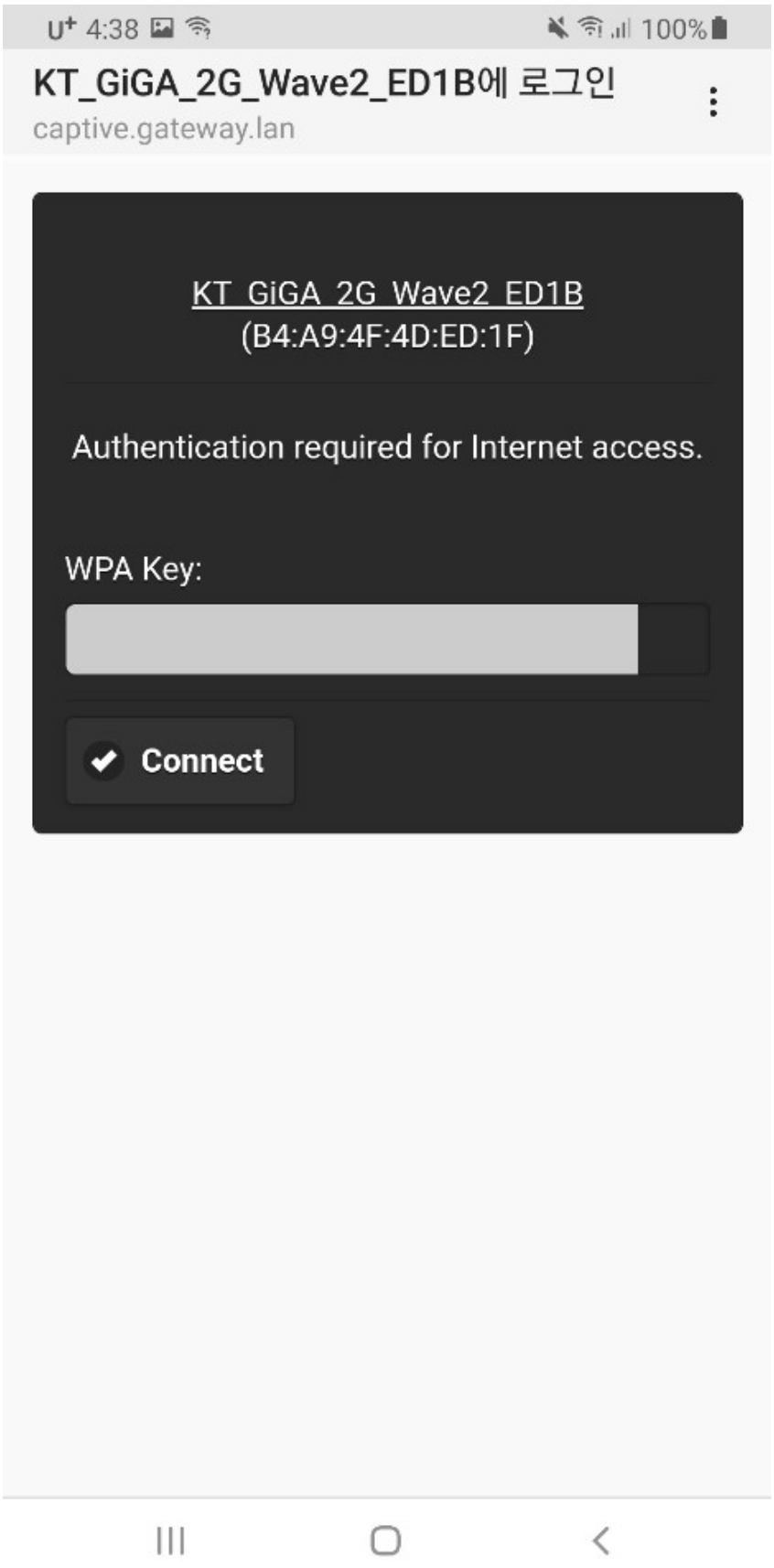


드디어 설정다른값을 주고 하니 성공...

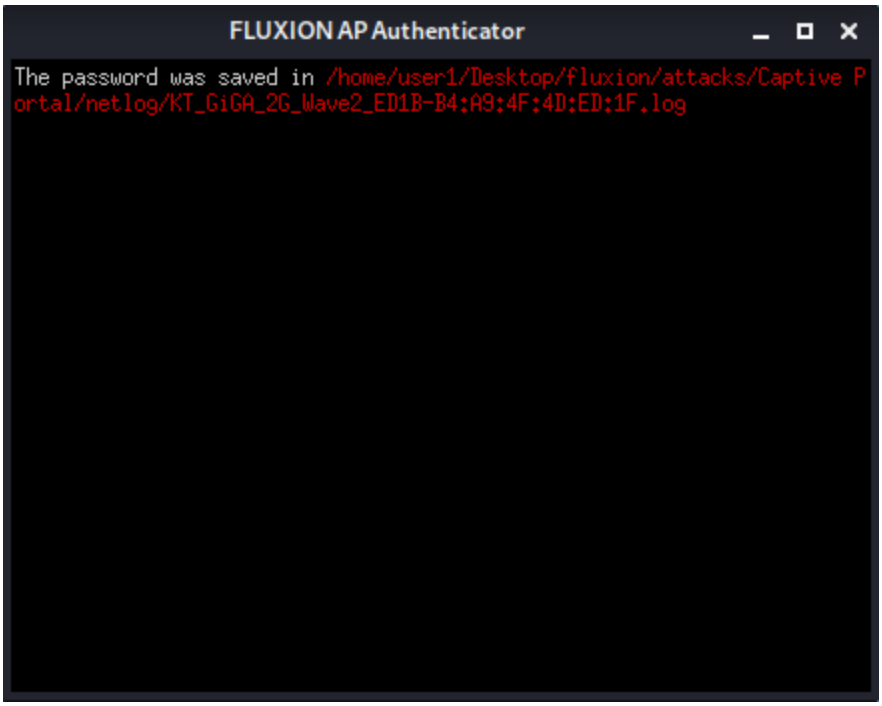
해당 와이파이 DEAUTH로 연결 안되고 똑같은 AP로 연결됨


U+ 4:37
100%
Wi-Fi
사용 중
현재 네트워크
KT_GiGA_2G_Wave2_ED1B
네트워크에 로그인하세요.
사용 가능한 네트워크
iptime
잘못된 비밀번호
KT_GiGA_2G_Wave2_ED1B
iptime_JJJ
KT_GiGA_2G_Wave2_F674
KT_GiGA_5G_Wave2_ED1B
TP-Link_758A
iptime5G

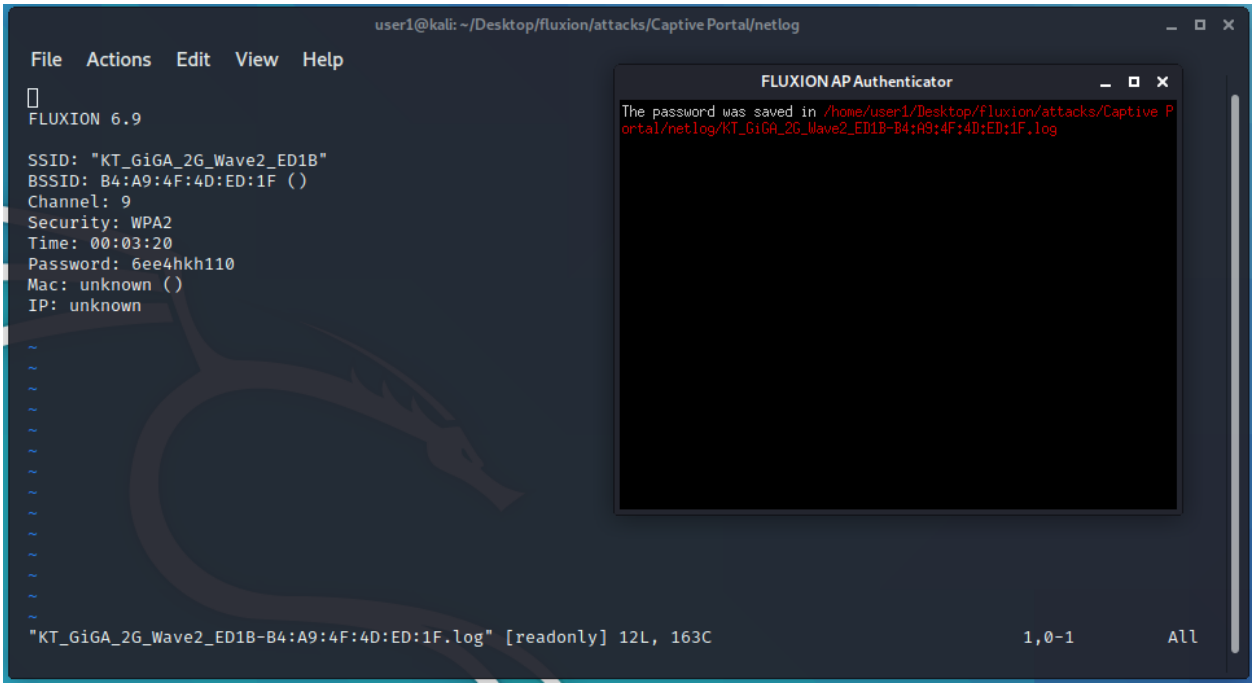
- 사용자가 여기에 비밀번호를 입력하면....


U+ 4:38
100%
KT_GiGA_2G_Wave2_ED1B에 로그인
captive.gateway.lan
KT_GiGA_2G_Wave2_ED1B
(B4:A9:4F:4D:ED:1F)
Authentication required for Internet access.
WPA Key:
Connect

성공!!


FLUXION AP Authenticator
The password was saved in /home/user1/Desktop/fluxion/attacks/Captive P
ortal/netlog/KT_GiGA_2G_Wave2_ED1B-B4:A9:4F:4D:ED:1F.log

비밀번호 얻기 성공


user1@kali: ~/Desktop/fluxion/attacks/Captive Portal/netlog
File Actions Edit View Help
FLUXION 6.9
SSID: "KT_GiGA_2G_Wave2_ED1B"
BSSID: B4:A9:4F:4D:ED:1F ()
Channel: 9
Security: WPA2
Time: 00:03:20
Password: 6ee4hkh110
Mac: unknown ()
IP: unknown
"KT_GiGA_2G_Wave2_ED1B-B4:A9:4F:4D:ED:1F.log" [readonly] 12L, 163C
1,0-1
All
FLUXION AP Authenticator
The password was saved in /home/user1/Desktop/fluxion/attacks/Captive P
ortal/netlog/KT_GiGA_2G_Wave2_ED1B-B4:A9:4F:4D:ED:1F.log

Fluxion 원리

1. 선택한 해당 wifi(wpa, wpa2)의 정보를 얻어 해쉬값으로 저장.
2. 해당 wifi에 deauth attack
3. 얻은 정보를 바탕으로. [해당 wifi]로 보이는 AP생성
4. 사용자는 새로생긴 AP에 연결. 기존 AP 연결이 안되기 때문에. → 이때 사용자는 비밀번호 입력!!
5. Fluxion은 받은 비밀번호를 이용하여 기존 AP에 연결가능한지 확인.
6. 새로 얻은 비밀번호로 접속 가능하면 log파일로 자동 저장됨.

→ 비밀번호 탈취 성공 !!!