**WIFI**

**1st step**- **Cracking WEP Encryption Using Pre-Captured Files**

<https://www.aircrack-ng.org/downloads.html?utm_source=chatgpt.com>

1. wlan.fc.protected ==1
2. aircrack-ng ptw.cap

**2nd step – Cracking WPA/WPA2 Encryption Using a Pre-Captured Handshake**

1. aircrack-ng NinjaJc01-01.cap
2. aircrack-ng -w /usr/share/wordlists/rockyou.txt -b 02:1A:11:FF:D9:BD NinjaJc01-01.cap
3. Wifi:
4. └─$ ls
5. NinjaJc01-01.cap
6. ┌──(kali㉿Kali)-[~/Desktop]
7. └─$ cd ..
8. ┌──(kali㉿Kali)-[~]
9. └─$ ls
10. ┌──(kali㉿Kali)-[~]
11. └─$ cd ..
12. ┌──(kali㉿Kali)-[/home]
13. └─$ ls
14. ┌──(kali㉿Kali)-[/home]
15. └─$ cd ..
17. ┌──(kali㉿Kali)-[/]
18. └─$ ls
19. ┌──(kali㉿Kali)-[/]
20. └─$ cd usr
21. ┌──(kali㉿Kali)-[/usr]
22. └─$ ls
23. ┌──(kali㉿Kali)-[/usr]
24. └─$ cd share
25. ┌──(kali㉿Kali)-[/usr/share]
26. └─$ ls
27. ┌──(kali㉿Kali)-[/usr/share]
28. └─$ cd wordlists
29. ┌──(kali㉿Kali)-[/usr/share/wordlists]
30. └─$ ls
31. ┌──(kali㉿Kali)-[/usr/share/wordlists]
32. └─$ sudo gunzip rockyou.txt.gz
33. [sudo] password for kali:
34. ┌──(kali㉿Kali)-[/usr/share/wordlists]
35. └─$ ls
36. aircrack-ng NinjaJc01-01.cap
37. aircrack-ng -w /usr/share/wordlists/rockyou.txt -b 02:1A:11:FF:D9:BD NinjaJc01-01.cap

**Bluetooth**

Bluetooth Pcap

<https://github.com/mikeryan/crackle/blob/master/tests/01_crack/pairing_and_ltk_exchange.pcap>

1. crackle -i pairing\_and\_ltk\_exchange.pcap -o decrypt.pcap

**IOT**

Step 1: download file from link

<https://github.com/pradeesi/MQTT-Wireshark-Capture/blob/master/mqtt_packets.pcapng>

2. save in kali desktop

3. cd Desktop

4. tshark -r IoT.pcapng -Y "mqtt" -T fields -e mqtt.topic

5. tshark -r IoT.pcapng -Y "mqtt" -T fields -e mqtt.msg

6. echo 48656c6c6f2066726f6d20746865205061686f20626c6f636b696e6720636c69656e74 | xxd -r -p

7. echo 48656c6c6f204d515454 | xxd -r -p