SZÉCHENYI EGYETEM
UNIVERSITY OF GYÖR

CYBERSECLAB

Etikus hackelés alapjai

IEEE 802.11, WiFi

Dr. Hidvégi Timót

egyetemi docens, IT biztonsági szakértő

Tartalomjegyzék

Tiltott adatszerzés és az információs rendszer elleni bűncselekmények

- Büntető Törvénykönyv / 2012. évi C. törvény
  - információs rendszer: az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezés, vagy az egymással kapcsolatban lévő ilyen berendezések összessége
- 375. §: Információs rendszer felhasználásával elkövetett csalás
- 386. §: Védelmet biztosító műszaki intézkedés kijátszása
- 422. §: Tiltott adatszerzés
- 423. §: Információs rendszer vagy adat megsértése
- 424. §: Információs rendszer védelmét biztosító technikai intézkedés kijátszása

https://www.police.hu/sites/default/files/2012._evi_c._torveny.pdf

Előnyök / hátrányok

- Előnyök
  - Mobilitás
  - Könnyű telepíthetőség
  - Skálázhatóság (könnyű új felhasználót hozzáadni)
  - Csökkentett költségek
- Hátrányok
  - Biztonság
  - Megbízhatóság (pl.: interferencia gondok, akadályok, stb)

Eszközök


RTL-SDR.COM
DVB-T+DAB+FM+SDR
RTL2832U R820T2 TCXO


HackRF One
GREAT SCOTT GADGETS
RESET
3V3
DFU
1V8
RF
USB
RX
TX
ANTENNA
CLKOUT
CLKIN

????

SZÉCHENYI EGYETEM
UNIVERSITY OF GYŐR
GÉPÉSZMÉRNÖKI, INFORMATIKAI ÉS VILLAMOSMÉRNÖKI KAR

CYBERSECLAB

Eszközök

WiFi Pineapple Tetra Basic

- https://hak5.org/
- https://downloads.hak5.org/pineapple/tetra
- https://www.cyberpunk.rs/wifi-pineapple-nano-tetra

Antennák

- Omnidirectional (egyirányú)
- Directional
- Yagi
- Planar
- Sector
- Grid

WiFi nevek, rövidítések, linkek

- AP (Access Point)
- STA (állomás)
- SSID (Service Set Identifier): AP neve. Folyamatosan sugározza a hálózat.
- BSSID: AP MAC címe
- Sávszélesség
  - Az az adatmennyiség, amely egy adott rendszerről egy másik rendszerre átvitelre kerül egy időegység alatt. Gyakran mérik olyan egységekben, mint MB/sec, GB/sec.
- Demo WPA2
  - https://wiki.wireshark.org/uploads/__moin_import__/attachments/SampleCaptures/wpa-Induction.pcap
- Wireshark filter
  - https://semfionetworks.com/wp-content/uploads/2021/04/wireshark_802.11_filters_-_reference_sheet.pdf
  - https://www.wifi-professionals.com/2019/03/wireshark-display-filters

Linkek

- Wireless Penetration Testing Cheat Sheet
  - https://gist.github.com/dogrocker/86881d2403fee138487054da82d5dc2e
- Wireless Penetration Testing Checklist
  - https://gbhackers.com/wireless-penetration-testing-checklist-a-detailed-cheat-sheet/

- Eszközök
  - https://www.wifi-antennas.com/topic/43-list-of-usb-wireless-adapters-monitor-mode/
  - https://null-byte.wonderhowto.com/how-to/buy-best-wireless-network-adapter-for-wi-fi-hacking-2019-0178550/

IEEE 802.XX

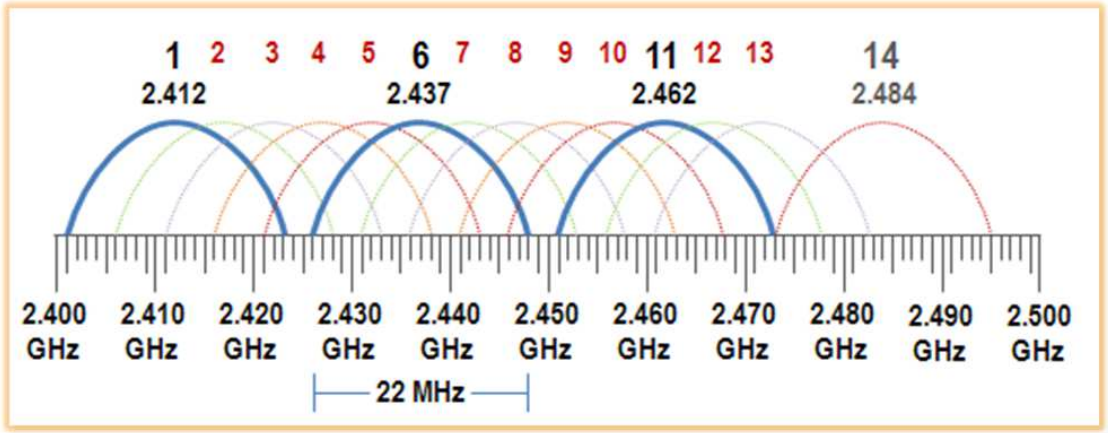
IEEE 802.1	Networking and Network Management	IEEE 802.10	Interoperable LAN Security
IEEE 802.2	LLC	IEEE 802.11	Wireless LAN (WLAN), MESH
IEEE 802.3	Ethernet	IEEE 802.12	100BaseVG
IEEE 802.4	Token Bus	IEEE 802.13	Unused
IEEE 802.5	Defines the MAC Layer for a Token Ring	IEEE 802.14	Cable Modems
IEEE 802.6	MANs	IEEE 802.15	Wireless PAN
IEEE 802.7	Broadband LAN Using Coaxial Cable	IEEE 802.15.1	Bluetooth Certification
IEEE 802.8	Fiber Optic TAG	IEEE 802.15.2	
IEEE 802.9	Integrated Services LAN	IEEE 802.15.3	High-Rate Wireless PAN

IEEE 802.11

Protocol	Release Date	Frequencies	Rates	Modulation	Channel Width	Notes
Legacy	1997	2.4-2.5GHz	1 or 2Mbit	FHSS/DSSS	1MHz/20MHz	No implementations were made for IR
802.11b	1999	2.4-2.5GHz	1, 2, 5.5, 11Mbit	DSSS	22MHz	Proprietary extension: up to 33Mbit
802.11a	1999	5.15-5.25/5.25-5.35/5.725-5.875GHz	6, 9, 12, 18, 24, 36, 48, 54Mbit	OFDM	20MHz	Proprietary extension: up to 108MBit
802.11g	2003	2.4-2.5GHz	Same as 802.11a and 802.11b	DSSS /OFDM	20MHz/22MHz	Proprietary extensions: up to 180Mbit/125MBit
802.11n	2009	2.4 and/or 5GHz	Up to 600Mbit	DSSS/OFDM	20/20 or 40MHz	

IEEE 802.11b csatornakiosztás

- Európa: 1 - 13
- USA: 1 - 11
- Japán: 1 - 14



Channel	Central Frequency
1	2.412 GHz
2	2.417 GHz
3	2.422 GHz
4	2.427 GHz
5	2.432 GHz
6	2.437 GHz
7	2.442 GHz
8	2.447 GHz
9	2.452 GHz
10	2.457 GHz
11	2.462 GHz
12	2.467 GHz
13	2.472 GHz
14	2.477 GHz

5 GHz-es tartomány

Channel	Frequency (MHz)
36	5180
40	5200
44	5220
48	5240
52	5260
56	5280

Channel	Frequency (MHz)
60	5300
64	5320
100	5500
104	5520
108	5540
112	5560
116	5580
132	5660
136	5680
140	5700
149	5745
153	5765
157	5785
161	5805
165	5825

IEEE 802.11 demo

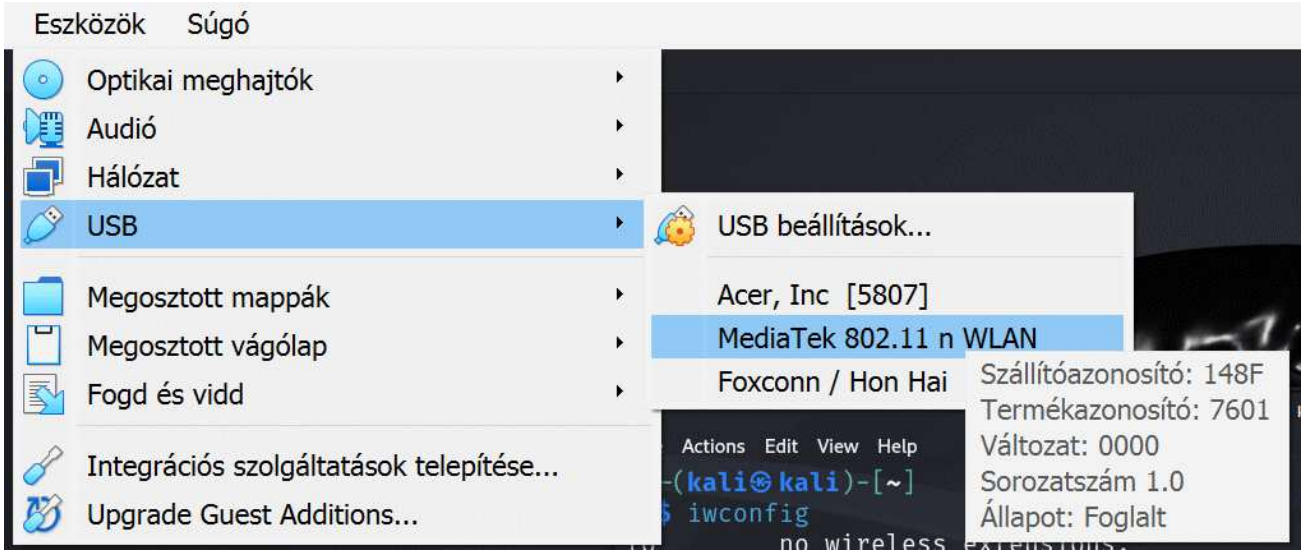
- Wireless Router
- Kali Linux VM
  - RTL8812AU driver telepítése (ha szükséges)
    - https://webelektronika.com/article/20210416-wifi-driver-install

WiFi működési módok

- Infrastruktúra
  - Legalább egy AP és egy állomás van.
- Ad-Hoc (Independent Basic Service Set, IBSS)
  - Egyik résztvevő állomás átvállal feladatot az AP-től (pl: hitelesítés). Ez az állomás nem továbbít csomagokat.
- Wireless Distribution System
  - AP-k egymással kommunikálnak
- Monitor mode
  - Nem az a „klasszikus” vezetéknélküli mód

WiFi kártya felcsatolása VM-re

- USB filter alkalmazása
  - https://webelektronika.com/article/20220104-virtualbox-filter-usb
- USB filter nélkül



Monitormód, demo

- Hálózati kártya adatai
  - ifconfig, iwconfig alkalmazása
  - (a képen a wlan0 még nincs monitormódban)

Frame-ek csoportjai

Management frames

Type Field	Subtype Field	Description
0	0	Association Request
0	1	Association Response
0	2	Re-association Request
0	3	Re-association Response
0	4	Probe Request
0	5	Probe Response
0	6	Measurement Pilot
0	7	Reserved
0	8	Beacon
0	9	ATIM
0	10	Disassociation
0	11	Authentication
0	12	Deauthentication
0	13	Action
0	14	Action No ACK
0	15	Reserved

Control frames

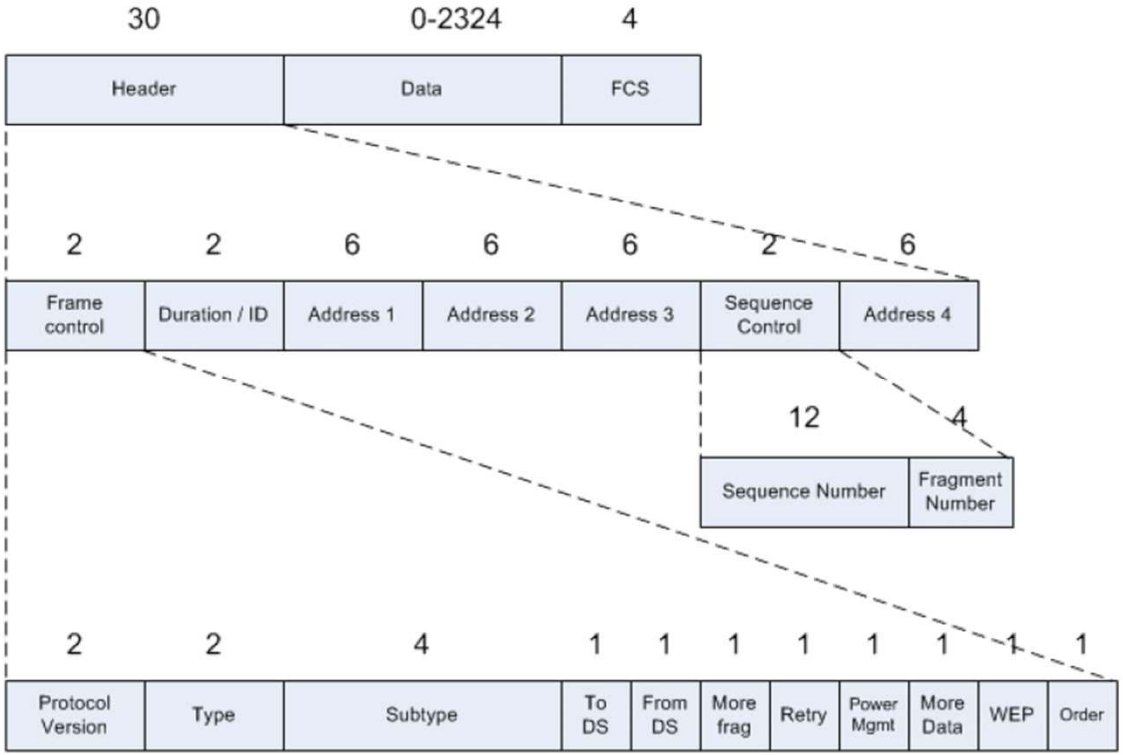
Type Field	Subtype Field	Description
1	0-6	Reserved
1	7	Control Wrapper
1	8	Block ACK Request
1	9	Block ACK
1	10	PS-Poll
1	11	RTS
1	12	CTS
1	13	ACK
1	14	CF End
1	15	CF End + CF-ACK

Data frames

Type Field	Subtype Field	Description
2	0	Data
2	1	Data + CF ACK
2	2	Data + CF Poll
2	3	Data + CF ACK + CF Poll
2	4	Null Function (No Data)
2	5	CF ACK (No Data)
2	6	CF Poll (No Data)
2	7	CF ACK + CF Poll (No Data)
2	8	QoS Data
2	9	QoS Data + CF ACK
2	10	QoS Data + CF Poll
2	11	QoS Data + CF ACK + CF Poll
2	12	QoS Null (No Data)
2	13	Reserved
2	14	QoS CF Poll (No Data)
2	15	QoS CF ACK + CF Poll (No Data)

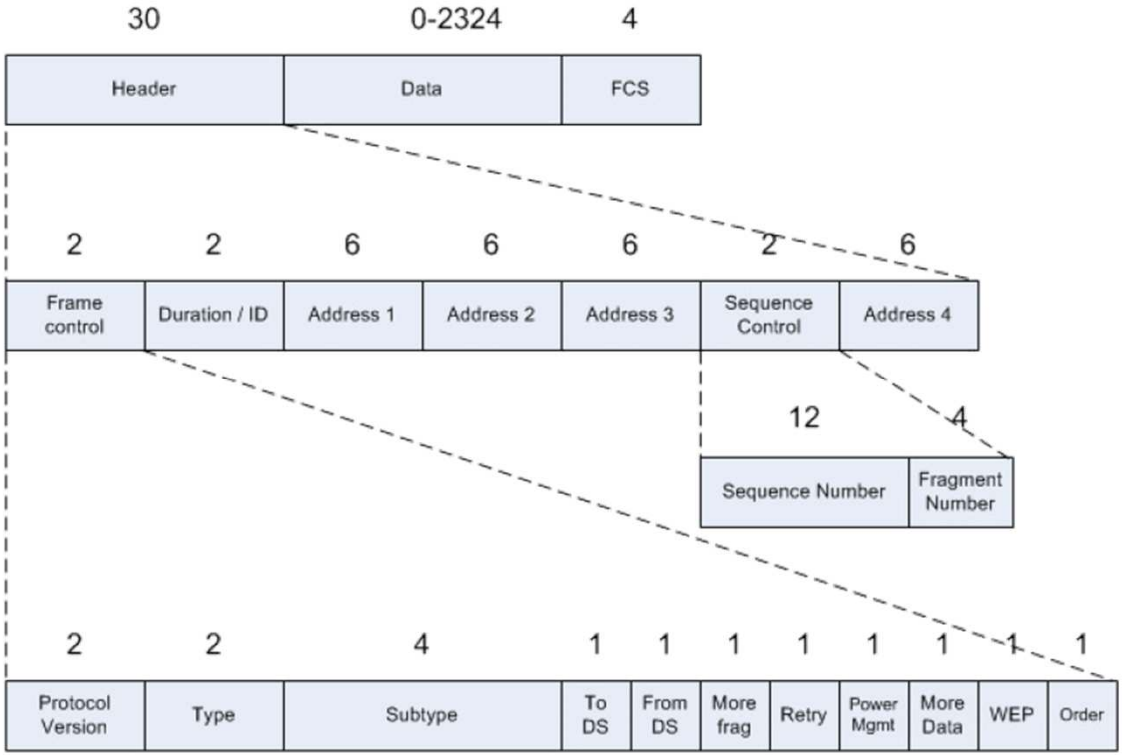
IEEE 802.11 MAC Frame, Data mező, FCS

- Mérete: max 2324 byte (MAC Service Data Unit: 2304 byte)
  - WEP: 8 byte -> 2304+8=2312 byte
  - WPA (TKIP): 20 byte -> 2304+20=2324 byte
  - WPA2 (CCMP): 16 byte -> 2304+16=2320 byte
- Frame Check Sequence (FCS):vezetéknélküli frame ciklikus redundanciaellenőrzése. Összes korábbi mezőben CRC-t hajtanak végre -> FCS létrejön. A célállomás is kiszámítja az FCS-t.



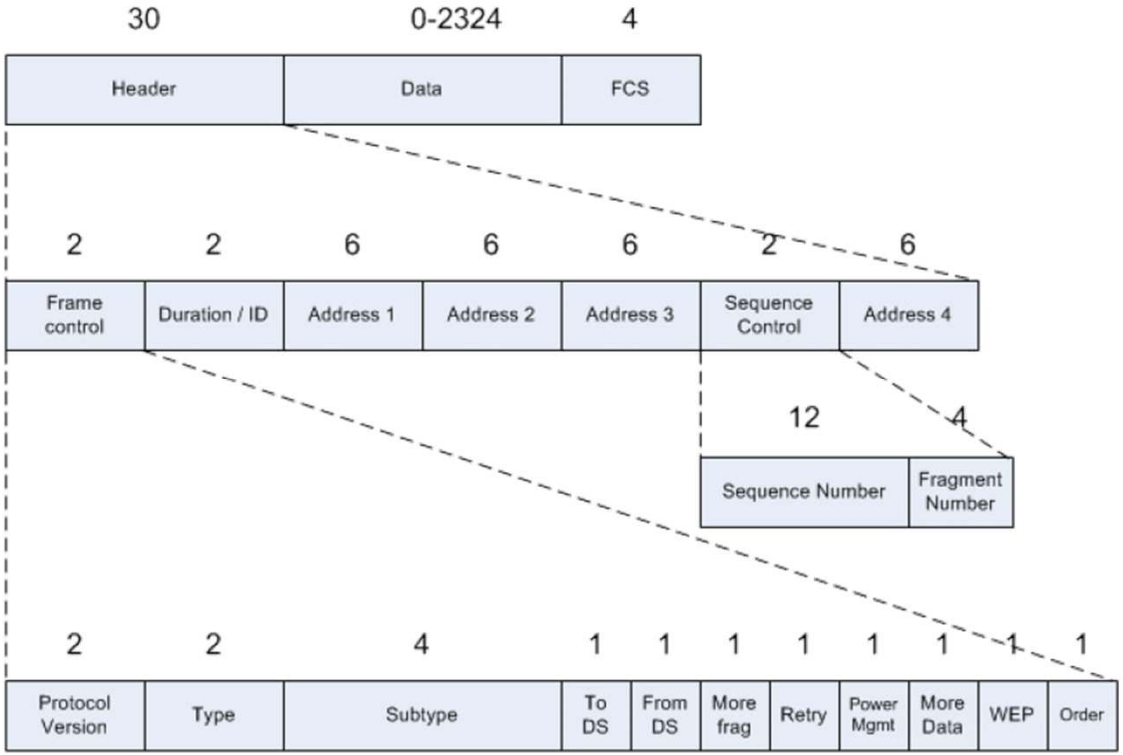
IEEE 802.11 MAC Frame, Sequence Control

- Sequence Number (12 bit): Jelzi a frame-ek számát (0-4095 között lehet). 4095 után ez újra 0 lesz
- Fragment Number (4 bit): Jelzi a frame-ek töredékeinek a számát



IEEE 802.11 MAC Frame, Frame Control

- Protocol version: használt protokoll verziója (0)
- (Sub)Type: keret funkcióját adja meg
  - contor (1), value (2), management (3)
- To/From DS: a keret be-/kilép a rendszerből
- More frag:
- Retry: jelzi a kerettovábbítást
- Power Mgmt: a küldő STA milyen módban van (aktív (0) vagy energiatakarékos (1))
- WEP: jelzi, hogy használnak-e titkosítást
- Order:



Címek

- DA: Destination Address; SA: Source Address
- RA: Recipient Address; TA: Transmitter Address

ToDS	FromDS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	
0	1	DA	BSSID	SA	
1	0	BSSID	SA	DA	
1	1	RA	TA	DA	SA

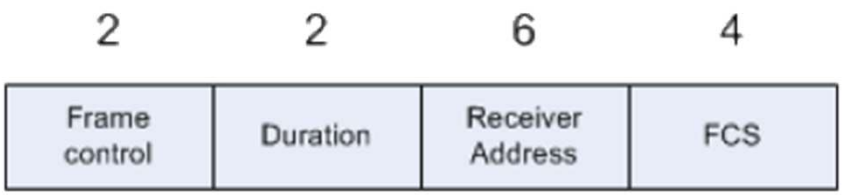
- 0 0: IBSS mód
- 0 1: AP szól az STA-hoz
- 1 0: STA beszél az AP-hoz
- 1 1: AP kommunikál egy másik AP-val

Control Frames

Type Field	Subtype Field	Description
1	0-6	Reserved
1	7	Control Wrapper
1	8	Block ACK Request
1	9	Block ACK
1	10	PS-Poll
1	11	RTS
1	12	CTS
1	13	ACK
1	14	CF End
1	15	CF End + CF-ACK

ACK frame

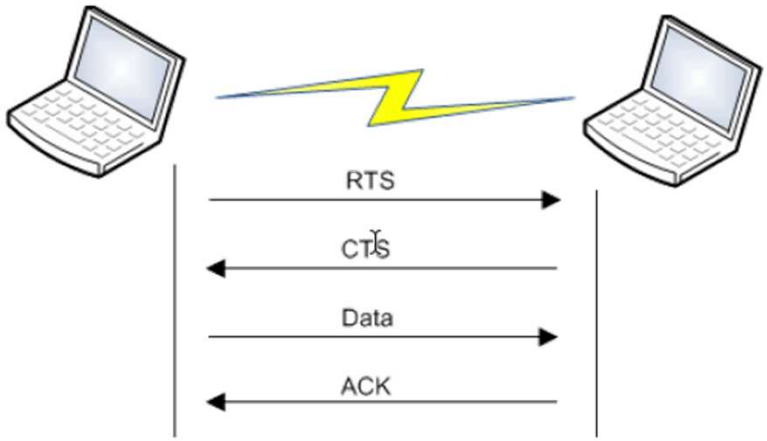
- Ezt a keretet a küldő állomás kapja, hogy a fogadó jól kapta-e meg a csomagot. Type: 1, SubType: 13




```
> Frame 1: 10 bytes on wire (80 bits), 10 bytes captured (80 bits)
v IEEE 802.11 Acknowledgement, Flags: ........
    Type/Subtype: Acknowledgement (0x001d)
  v Frame Control Field: 0xd400
        .... ..00 = Version: 0
        .... 01.. = Type: Control frame (1)
        1101 .... = Subtype: 13
      > Flags: 0x00
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: AboCom_11:c0:f6 (00:12:0e:11:c0:f6)
```

RTS / CTS

- RTS/CTS (Request to Send/Clear to Send) segít az ütközések elkerülésében (CSMA/CA, csatorna hozzáférési mód) -> plusz csomagok kellenek a kommunikációhoz
- 1. „A” küld RTS-t a „B”-be
- 2. Ha nincs ütközés (és a kérést elfogadják), akkor „B” küld egy CTS-t. (lehetőség a folytatásra)
- 3. „A” küld adatot
- 4. Sikeres adatküldés után „B” küld „ACK”-et



- RTS

2	2	6	6	4
Frame control	Duration	Receiver Address	Transmitter Address	FCS

- CTS

2	2	6	4
Frame control	Duration	Receiver Address	FCS

RTS / CTS

wlan.fc.type_subtype == 28

wlan.fc.type_subtype == 28

No.	Time	Source	Destination	Protocol	Length	Info
86	5.648961		CiscoLinksys…	802.11	38	Clear-to-send, Flags=.....C
91	5.654947		CiscoLinksys…	802.11	38	Clear-to-send, Flags=.....C
98	5.842998		Apple_82:36:…	802.11	38	Clear-to-send, Flags=.....C
1…	5.845998		CiscoLinksys…	802.11	38	Clear-to-send, Flags=.....C

```
> Frame 86: 38 bytes on wire (304 bits), 38 bytes captured (304 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 Clear-to-send, Flags: ........C
    Type/Subtype: Clear-to-send (0x001c)
  > Frame Control Field: 0xc400
    .000 0000 0110 1000 = Duration: 104 microseconds
    Receiver address: CiscoLinksys_82:b2:55 (00:0c:41:82:b2:55)
    Frame check sequence: 0x58cb0955 [unverified]
    [FCS Status: Unverified]
    [WLAN Flags: ........C]
```

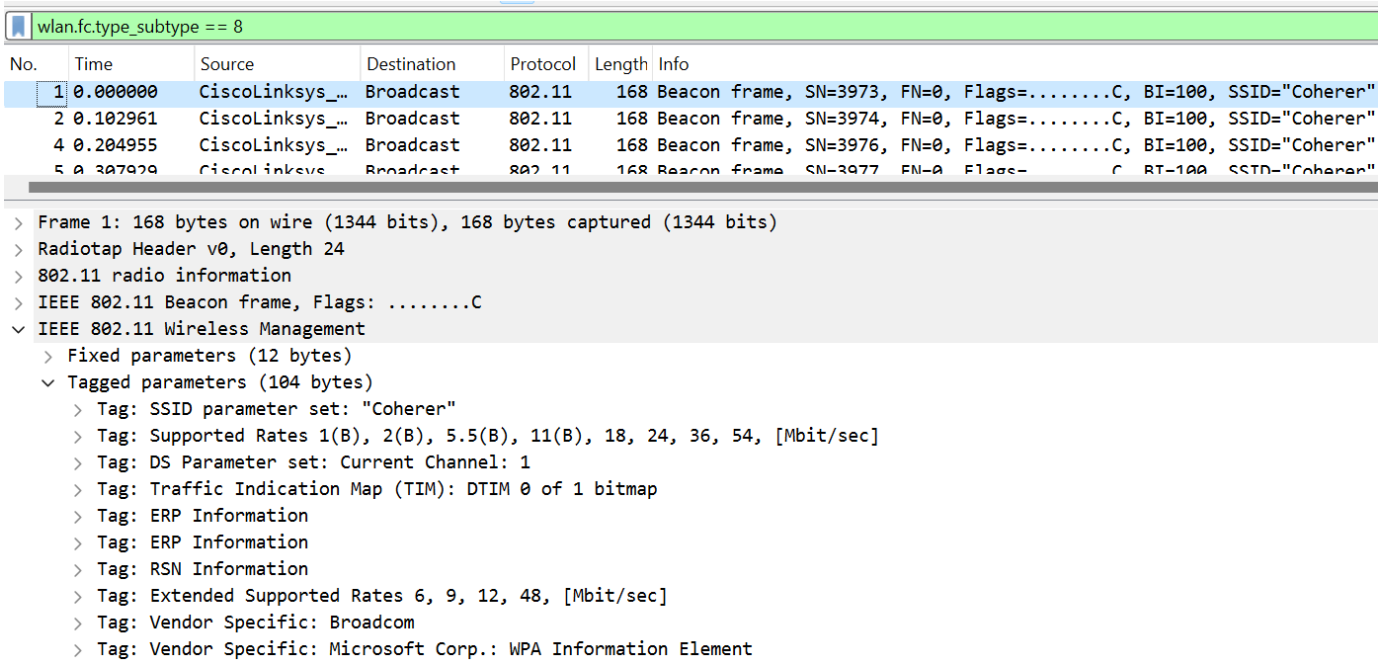
Management csomagok

Type Field	Subtype Field	Description
0	0	Association Request
0	1	Association Response
0	2	Re-association Request
0	3	Re-association Response
0	4	Probe Request
0	5	Probe Response
0	6	Measurement Pilot
0	7	Reserved
0	8	Beacon
0	9	ATIM
0	10	Disassociation
0	11	Authentication
0	12	Deauthentication
0	13	Action
0	14	Action No ACK
0	15	Reserved

Beacon csomagok

- Másodpercenként kb 10-szeres sebességgel küldik ki. AP küldi, szinkronizáció a feladata.
- Különböző információkat adnak a hálózatról

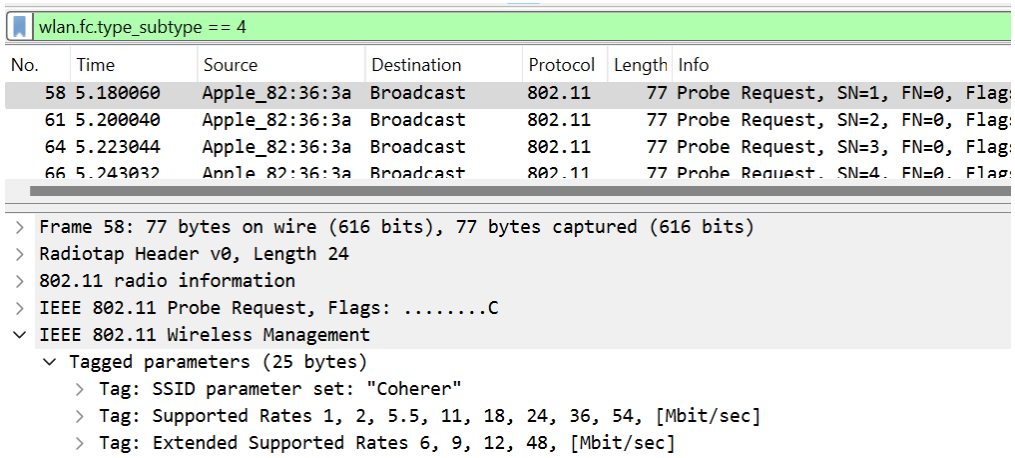
wlan.fc.type_subtype == 8



Probe Request / Response

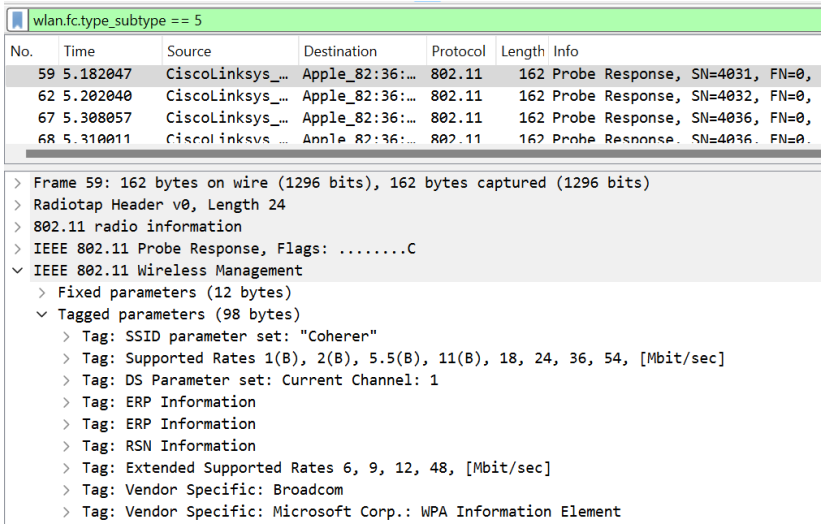
- AP-ok keresésére alkalmazzák
  - Probe request: Ezeket küldik az STA-k, hogy milyen AP-ok vannak a hatótávon belül.

wlan.fc.type_subtype == 4



  - Probe Response: Csomópont (AP, állomás) küldi ezt a választ.

wlan.fc.type_subtype == 5



Null frame

- MAC fejlécekből és FCS-nől áll ez a keret. STA-k jelzik, hogy energiatakarékos üzemmódra váltanak.

  wlan.fc.type_subtype == 36

Hitelesítés

- Kötelező
- Néhány típus
  - Nyílt rendszerhitelesítés (OSA)
    - *Az alapértelmezett hitelesítési protokoll a IEEE 802.11 szabvány szerinti protokoll. Ennek a hitelesítésnek a folyamata három lépésben zajlik*
      - 1. A vezeték nélküli hálózati hozzáférést igénylő számítógép elküld egy hitelesítési kérelmet a hozzáférési pontnak.
      - 2. A hozzáférési pont válaszul egy véletlenszerű hitelesítési kódot generál, amely csak az adott munkamenetre érvényes.
      - 3. A hozzáférést kérő számítógép elfogadja a kódot, és csatlakozik a hálózathoz.

Hitelesítés (megosztott kulcs)

- A folyamat öt lépésből áll
  - *1. A vezeték nélküli hálózati hozzáférést igénylő számítógép elküld egy hitelesítési kérelmet az AP-nek*
  - *2. Az AP erre egy szöveget generál, és visszaküldi azt a kérelmezőnek.*
  - *3. A számítógép ezt a szöveget a kulccsal titkosítja, és elküldi az üzenetet a hozzáférési pontnak.*
  - *4. Az AP megkapja az üzenetet, és összehasonlítja azt az eredeti szöveggel. Ha a két szöveg pontosan megegyezik, akkor a hozzáférési pont elküldi a végleges hitelesítési kódot a számítógépnek.*
  - *5. A számítógép elfogadja a hitelesítési kódot a hozzáférési ponttól és csatlakozik a hálózathoz*

Hitelesítés (központi kiszolgáló)

- Hitelesítés központi kiszolgálóval
  - Az előző technikák mellett egya vezeték nélküli hálózathoz való hozzáférést kérő számítógépet egy központi központ segítségével is lehet hitelesíteni.
    - *Active Directory, LDAP (Light Weight Directory)Access Protocol)*
    - *RADIUS szerver*
      - például: https://www.freeradius.org
    - *How to secure your Wifi network with Freeradius*
      - https://medium.com/hackernoon/how-to-secure-your-wifi-network-with-freeradius-94e0812a83bf

Tesztkörnyezet

- mdk3
  - Telepítés
    - *sudo apt update*
    - *sudo apt upgrade*
    - *sudo apt install mdk3*
  - Használat
    - *sudo mdk3 --help*
    - *sudo mdk3 wlan0 b -a -g -f ssidLista*

- mdk4
  - Telepítés
    - *sudo apt update*
    - *sudo apt upgrade*
    - *sudo apt install mdk4*
  - Használat
    - *mdk4 wlan0 b -a -g -f ssidLista*

Támadások

- WLAN infrastruktúra ellen
  - Megszerzett azonosítók alkalmazása
  - DoS támadások
    - *Hitelesítési támadások*
    - *CTS-RTS támadások*
    - *Jelinterferencia vagy spektrumzavarás támadások*
  - Evil Twin, MAC címmásolással
  - Rogue AP
- Kliens ellen

- Probe támadások
  - Demo: 2025. januárban bemutató

Evil Twin

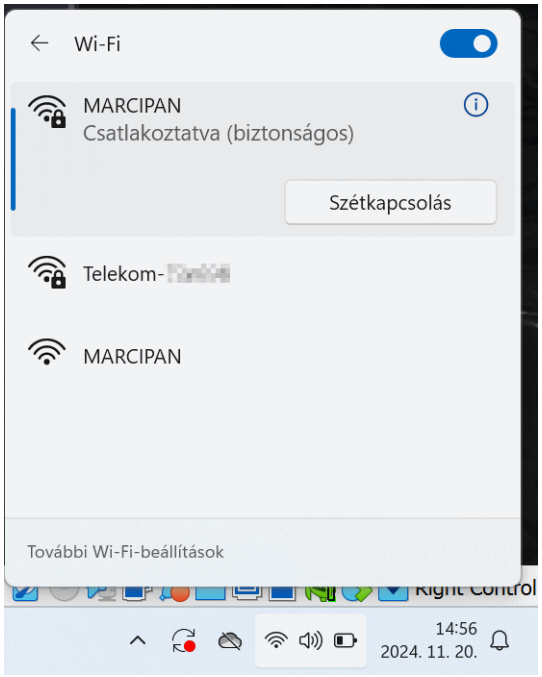
- A WiFi-re csatlakoztatott eszközök nem tudják megkülönböztetni az azonos SSID nevet sugárzó két AP-ot.
  - Lehetőség nyílik a rosszindulatú hozzáférési pontok (AP) használatára
  - Forgalom lehallgatása, Man-in-the-Middle (MitM)
  - Rosszindulatú kódok, backdoors-ok bejuttatása a céleszközökbe
- Demo: 2025. januárban bemutató

Evil Twin támadás

- airbase-ng alkalmazása

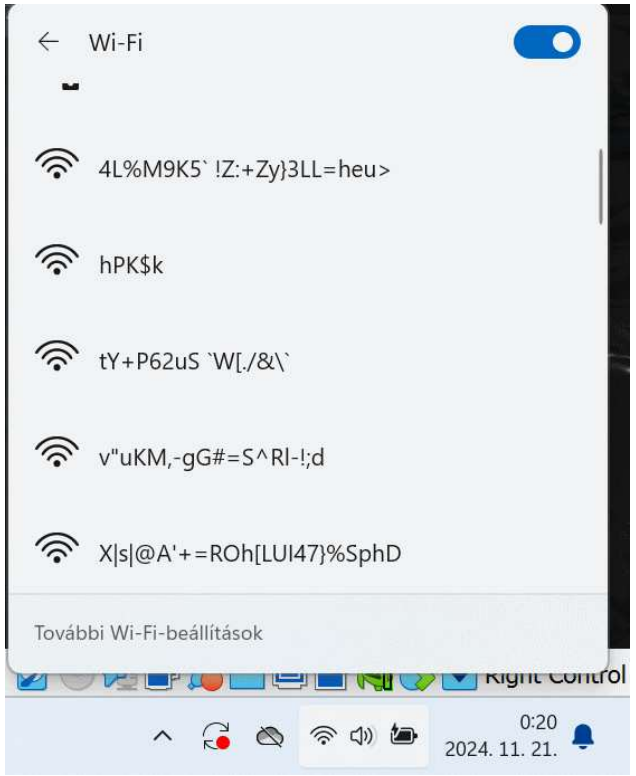
```
┌──(kali㉿kali)-[~]
└─$ sudo airbase-ng --essid CzberSecLab_Fake -c 11 wlan0
08:33:22  Created tap interface at0
08:33:22  Trying to set MTU on at0 to 1500
08:33:22  Trying to set MTU on wlan0 to 1800
08:33:22  Access Point with BSSID C2:AB:64:85:E3:D1 started.
```

```
┌──(kali㉿kali)-[~]
└─$ sudo airbase-ng -a E8:DE:[redacted] --essid MARCIPAN -c 11 wlan0
08:45:47  Created tap interface at0
08:45:47  Trying to set MTU on at0 to 1500
08:45:47  Access Point with BSSID E8:DE:[redacted] started.
```



Beacon flood

- Beacon csomagok létrehozása a cél
  - beacon flood
- Hálózati kártya monitormódban
- Adott SSID-val rendelkező beacon flood
  - sudo mdk3 wlan0 b -a -g -f ssidLista
- Véletlen SSID beacon flood
  - sudo mdk3 wlan0 b



Deauthentication az adott csatornán az összes kliensnél

- mdk3 használata
  - sudo mdk3 wlan0 d -c 11

WEP

- Van állomás a hálózaton
- Nincs állomás a hálózaton

WiFi adatok a Windows OS-en

- netsh alkalmazása

```
C:\Users\timot>netsh wlan show profiles

Profiles on interface Wi-Fi:

Group policy profiles (read only)
---------------------------------
    <None>

User profiles
-------------
    All User Profile     : Ad[redacted]
    All User Profile     : Al[redacted]
    All User Profile     : MA[redacted]
    All User Profile     : hl[redacted]
    All User Profile     : Te[redacted]
    All User Profile     : eduroam


C:\Users\timot>
```

Industrial and Research Lab for Cybersecurity

- Web
  - https://cyberseclab.eu
- Facebook
  - https://www.facebook.com/IndustrialandResearchLab
- Github
  - https://github.com/cyberseclabor
- Linkedin
  - https://www.linkedin.com/company/industrial-and-research-lab-for-cybersecurity

SZÉCHENYI EGYETEM
UNIVERSITY OF GYŐR
GÉPÉSZMÉRNÖKI, INFORMATIKAI ÉS VILLAMOSMÉRNÖKI KAR

CYBERSECLAB

Industrial and Research Lab for Cybersecurity