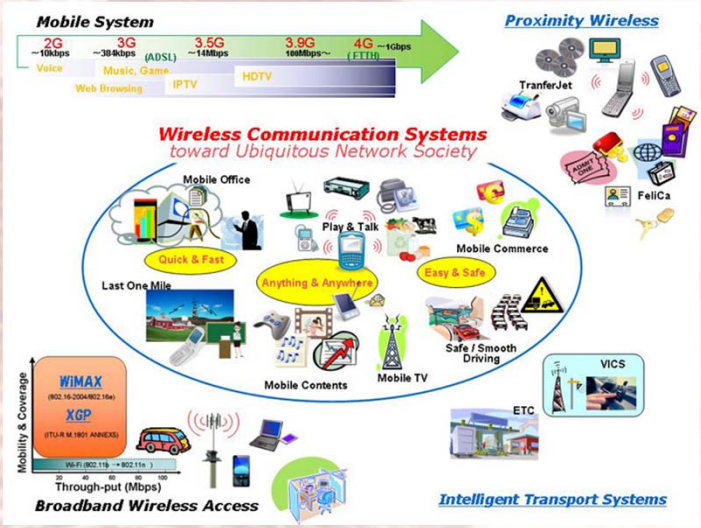

Bežična forenzika
Kristian Skračić
Žad Deljkić
Predrag Pale

Zašto forenzika bežičnih mreža?

- Wi-Fi je postala **rasprostranjena** tehnologija
- Za razliku od žičanih mrežnih veza
  - koje se koriste u privatnim prostorima, kontroliranim, sigurnim
- Bežične se koriste za **svepristuan** pristup
  - u uredima drugih ljudi,
  - kafićima, restoranima, javnim prostorima,
  - sveučilištima, knjižnicama,
  - domovima, podzemnim željeznicama,
    busevima itd...
- I koristi se u **raznim uređajima**:
  - ne samo u računalima, tabletima, pametnim telefonima već i u
  - bežičnim telefonima, Bluetooth slušalicama,
  - TV daljinskim upravljačima, sustavima za zabavu
  - autima, igračkama, osvijetljenju, pametnim
    domovima, bežičnim zvoncima na vratima...



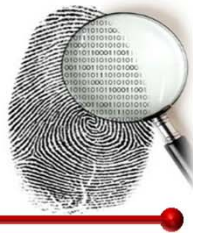
Zašto forenzika?

- Bežične mreže mogu biti (postati):
  - spore, nedostupne, nepouzdane …
  - ili korisnici mogu sumnjati da ih netko prisluškuje
- to može biti zbog:
  - **tehničkih** razloga
    - neispravne opreme
    - nekompatibilnih uređaja
    - interferencije iz okoline
  - **ljudske** greške
    - pogrešne konfikuracije
    - lošeg održavanja
    - korisničkog neznanja
  - **napada**
    - pokušaja krađe/korumpiranja/implantiranja informacija
    - pokušaja zloupotrebe resursa
    - usmjerenih na onemogućivanje legitimnih korisnika
    - ugrožavanja žrtvine slike
    - korištenja žrtvinog sustava za napad na konačni cilj

Forenzička analiza
pokušava
- diskriminirati
- otkriti uzrok i mehanizam
- pomoći u popravku

IEEE 802.11 osnove

IEEE 802.11 - bežični standard

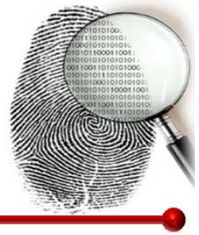


- specificira protokole za WLAN promet
  - u frekvencijskim rasponima 2.4, 3.7, i 5 GHz

- Promet je često enkriptiran (WPA, WEP...)
  - Bez dekripcije je **nemoguće analizirati** promet

- Raspon napada **specifičnih** bežičnim mrežama:
  - DoS slanjem **deautentikacijskih** okvira
  - **brute force** enkripcijskog ključa
  - **ARP spoofing** – man in the middle
  - Jednostrano **zaobilaženje izolacije klijenata**
  - **Lažne** pristupne točke

Zašto toliko layer 2 protokola?

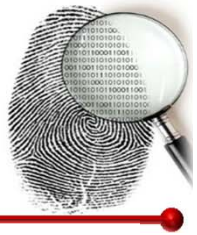


- Zašto nismo samo koristili **postojeće** Ethernet standarde preko RF baš kao što smo koristili za bakar, optička vlakna?

- Jer, radio frekvencija i bakar nemaju iste **fizičke karakteristike**
  - signali poslani preko njih se ne ponašaju na isti način!
- Kako bi izolirali Layer 3 protokole (primarno IP) od tih razlika u fizičkim karakteristikama
  - posredni protokol je potreban kako bi pružio uniformno sučelje mrežnom sloju
    - neovisno o fizičkom mediju

IEEE 802.11™

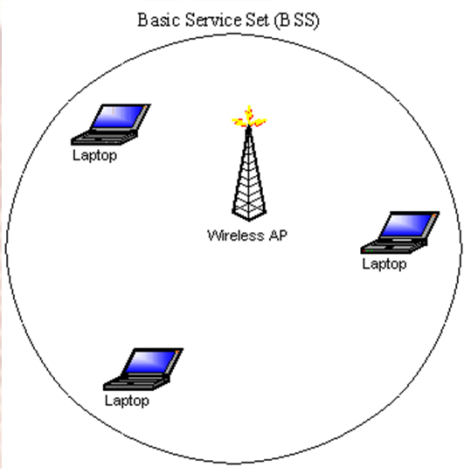
802.11 osnove - terminologija

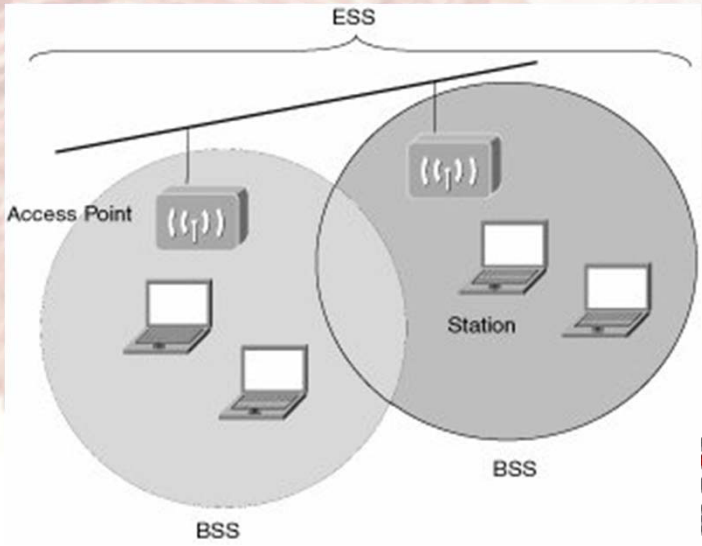


- **Stanica** – laptop, pametni telefon...

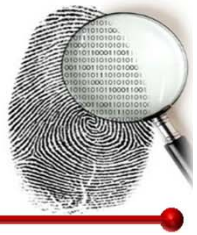
- **AP** – access point (pristupna točka)
  - Stanice se spajaju na nju
  - Radi na specifičnom kanalu (koji odgovara frekvenciji, ~2.4/5GHz)

- **BSS** – basic service set
  - AP + sve stanice spojene na njega
  - BSSID – MAC adresa od AP-a
- **ESS** – extended service set
  - cijela bežična mreža
  - Više AP-ova
    - spojenih kroz Distribution system (**DS**)
  - ESSID/SSID (Service Set Identifier)
    - ime mreže (npr. FERwlan)



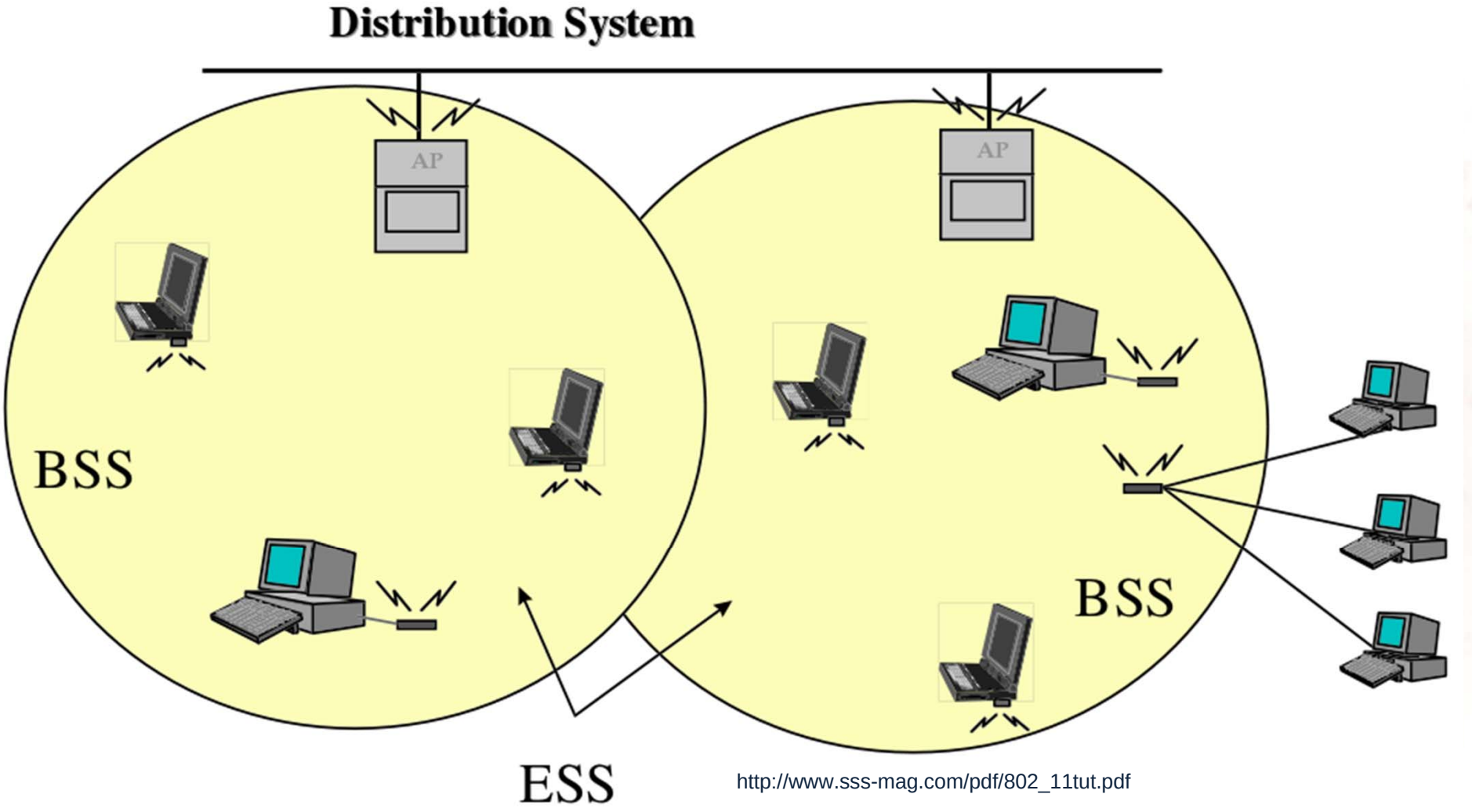


Bežična pristupna točka (AP)



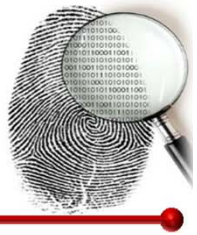
- Je zapravo samo Layer 2 hub
- Za forenzičke **istražitelje**, bitno je **razumijeti** da ako snimate promet bežične mreže
  - možda postoje **stanice** koje aktivno sudjeluju u mreži koje **nije moguće čuti** sa točke snimanja, zbog **slabe jačine signala**
- Ova jednostavna činjenica ima dalekosežne **posljedice** na protokole podatkovnog sloja i forenzičku analizu bežičnih **tragova**

802.11 osnove



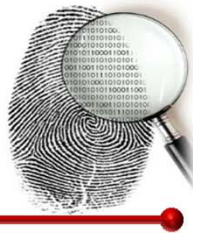
http://www.sss-mag.com/pdf/802_11tut.pdf

802.11 osnove – FERwlan primjer



- cijeli FER pokriven
  - pristupne točke (AP) u svakom hodniku
- Svi AP-ovi spojeni dalje na mrežu
  - žičanim Ethernet-om
- svaka stanica (PC, tablet, pametni telefon) može biti **bez prekida** spojena na FERwlan dok se fizički kreće kroz cijelu zgradu
  - samo mijenja AP-ove na koje je spojena (*roaming*)
- *Roaming* vrši stanica
  - neprekidno prati jačinu signala svih AP-ova u dosegu
  - i spaja se na onaj s najjačim signalom

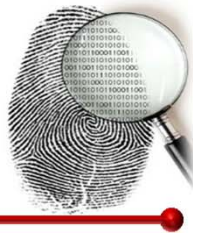
802.11 skup protokola



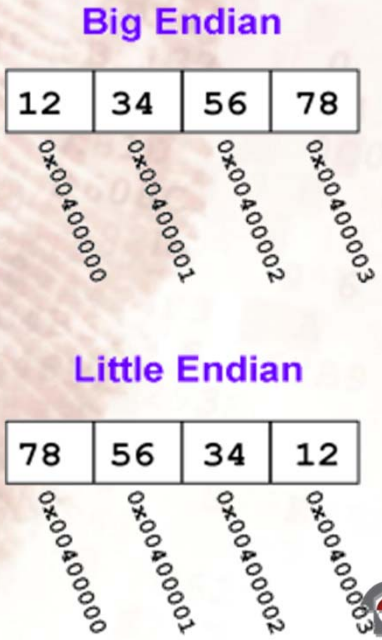
- standard za prijenos na **podatkovnom sloju** preko **bežičnog** fizičkog medija
  - uključujući radio i infracrveni spektar frekvencija

- 802.11 vrste okvira
  - **Upravljački** okviri
    - **upravljaju** komunikacijom između stanica
    - **osim** kontrole toka
  - **Kontrolni** okviri
    - **podržavaju** kontrolu toka
    - preko varijabilno dostupnog medija (kao što je RF)
  - **Podatkovni** okviri
    - **Enkapsuliraju** Layer 3+ podatke
    - koji se prenose između stanica aktivno prisutnih u komunikaciji na bežičnoj mreži

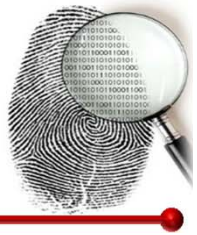
Endianness



- Kod **analize** snimljenog mrežnog **prometa**
  - kako znati koji bitovi odgovaraju kojim poljima protokola?
- Stanice mogu biti **konfigurirane** da prenose bitove **u različitim poretcima**, **ovisno** o korištenom protokolu podatkovnog sloja
  - ako su izvorišna i odredišna stanica sinkronizirane da interpretiraju i rekonstruiraju bitove po istom protokolu,
  - onda nema problema
- **poredak bitova** prijenosa
  - nije uvijek isti u 802.11 skupu protokola
- To može uzrokovati **netočne rezultate**
  - forenzičke analize



802.11 Endianness

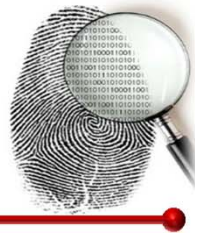


- U kontekstu mrežnih protokola
  - **big**-endian
    - ako je najznačajnija vrijednost prva poslana
  - **little**-endian
    - ako je najmanje značajna vrijednost prva poslana
  - **mixed**-endian ili **middle**-endian
    - ako je sustav kombinacija ovih metoda

- Istražitelji mrežne forenzike su naviknuti gledati snimljene bitove u **big-endian** obliku
  - **IP protokol** specificira **big-endian** za poredak bitova kada se šalju preko mreže
  - To se često naziva mrežnim poretkom byte-ova ("**network-byte order**")
- 802.11 je "mixed-endian"
  - dok je poredak bitova u svakom individualnom polju big-endian
  - sama polja se šalju u obrnutom pretku, unutar ograničenja byte-ova

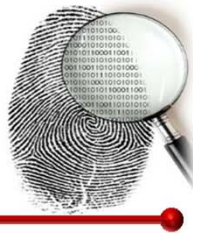
IEEE 802.11 Sigurnost & Enkripcija

802.11 sigurnosni protokoli



- **WEP**
  - Originalni sigurnosni protokol za 802.11, nesiguran
- **WPA**
  - Zamijenio WEP, isto nesiguran
  - **dva načina**
    - **PSK** – *pre-shared key* (jedna "lozinka" za spajanje)
    - Enterprise – *korisničko ime/lozinka* za spajanje
- **WPA2**
  - Smatra se sigurnim danas
  - PSK ili Enterprise

Wired Equivalent Privacy (WEP)

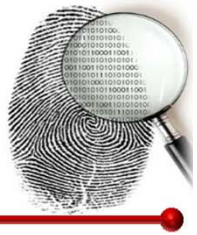


- dio 802.11 standarda

- ideja je bila da WAP (wireless access point) omogući "privatnu" mrežu
  - slično okolini/servisu
    koju žičani hub omogućuje
    zbog prirodnih ograničenja fizičkog medija

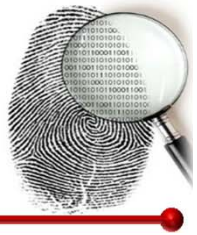
- Kako bi dobili pristup WEP-enkriptiranoj bežičnoj mreži, korisnici moraju znati "(pre)shared secret" ključ = PSK
  - kako bi dobili pristup Layer 2 bežičnom hub servisu

Probelmi sa WEP-om

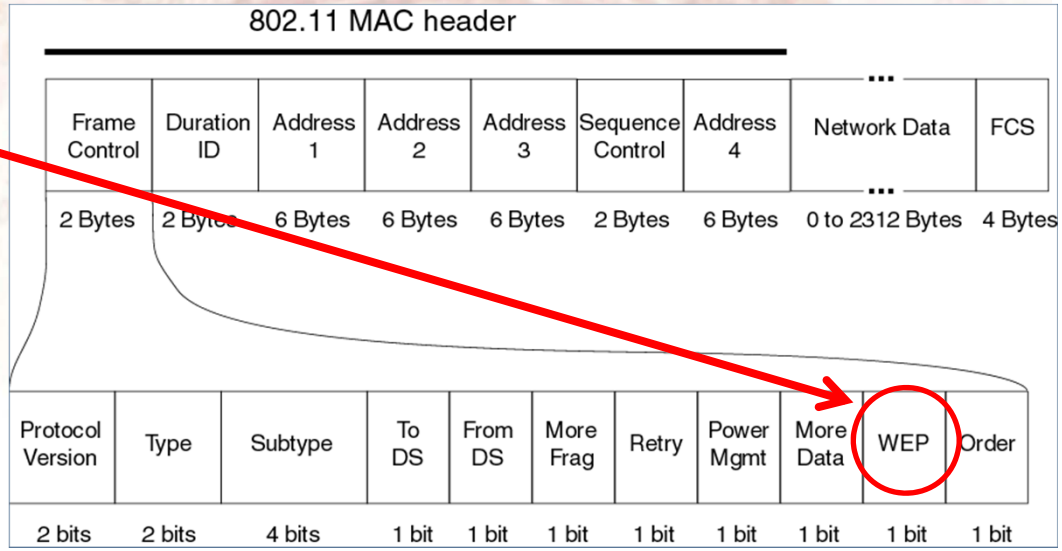


- Najvažnij **problem** WEP protokola:
  - dopušta **bilo kojoj stanici u dosegu** radio valova
    - **da sluša** radio promet
    - i tako **sakuplja nezaštičeni materijal ključa**
  - koji onda može biti korišten da se izvrši **brute-force** napad
    - i sazna enkripcijski ključ (PSK)
- **Rasprostranjeni alati**
  - kao što je “aircrack-ng”
  - omogućavaju čak i početnicima da krekiraju WEP ključeve
    - i pristupe “zaštičenim” bežičnim mrežama
- sve ovo je dovelo do toga da WEP bude **obustavljen**
  - u korist novih protokola bežične privatnosti
  - kao što su WPA i WPA2

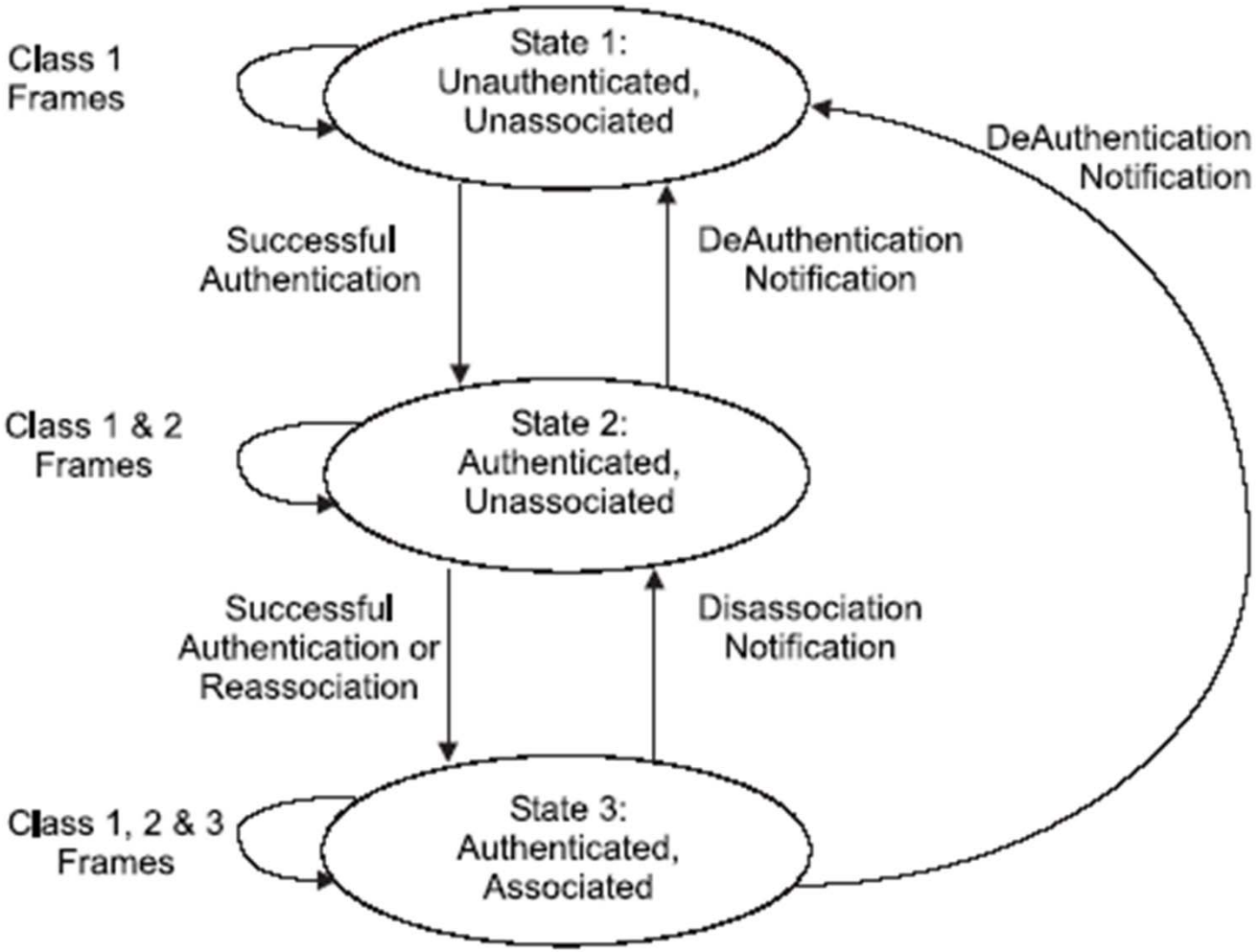
Enkripcija



- Kako znati je li bežična komunikacija enkriptirana?
  - ili snimka paketa ili tok paketa
- Korištenje PSK-a za autentikaciju
  - **NE** znači **automatski**
  - da je podatkovni **promet šifriran**, isto
- 802.11 upravljački okviri
  - imaju "**Privacy**" polje **postavljeno na "1"**
    - kada je tajnost podataka potrebna
    - za sve razmijenjene **podatkovne** vrste **okvira**
- 802.11 podatkovni okviri
  - imaju "Protected" bit
    - unutar prvog byte odmaka od 802.11 MAC uokviravanja
    - postavljen je na "1" kada se WEP, WPA ili WPA2 koristi



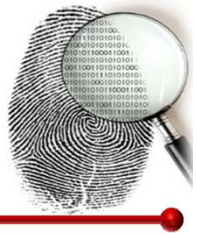
Autentikacija, asocijacija



http://cecs.wright.edu/~pmateti/InternetSecurity/Lectures/WirelessHacks/Mateti-WirelessHacks.htm

Denial of Service napadi

Autentikacija, asocijacija

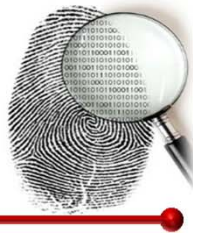


- **Autentikacija**
  - Otvorene mreže ili WEP zaštičene
  - **Ne** u WPA (802.1X)
    - ono se odvija kasnije (nakon asocijacije)
    - u tom slučaju ovaj korak koristi otvorenu autentikaciju
- **podatkovni** okviri mogu biti **slani** tek **nakon asocijacije**
  - i 802.1X autentikacije, ako je korištena
- Ovi ***upravljački*** okviri nisu nikada zaštičeni

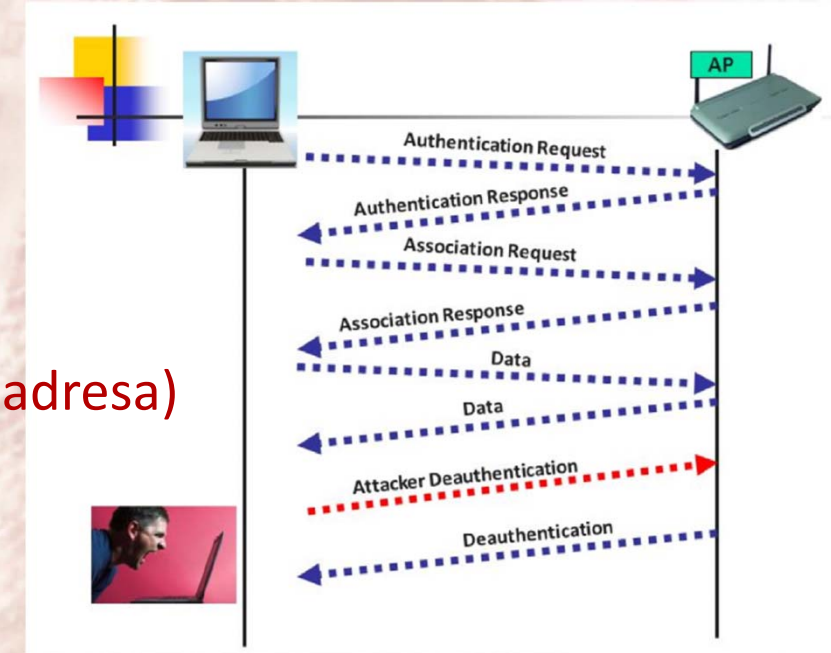
  => **lažiranje je moguće**!
    - Bitno (**opasno**) za deautentikaciju

https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/802.11_Association_process_explained

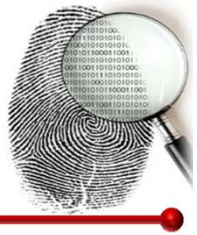
Deautentikacijski napad



- **Deautentikacija** može biti izvršena na dva načina:
  1. Stanica → AP: "Odlazim sa mreže" ili
  2. AP → stanica: "Odspajam te sa mreže jer:
     - si **neaktivan** ili
     - mreža se **gasi** ili
     - **nema razloga**
  - **Ciljana** deautentikacija:
    - AP → **jedna** stanica (njena MAC adresa)
  - **Broadcast** deautentikacija:
    - AP → **broadcast** MAC adresa
      - Odspaja **sve**
      - Neki klijenti ignoriraju broadcast deautentikaciju !!!

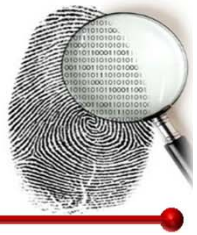


DoS – ciljana deautentikacija



- Napadač šalje deautentikacijske okvire sa **lažiranom** MAC adresom (žrtvinom)
  - Ovi okviri **nisu nikada zaštičeni**
    - zbog toga, **ništa ga ne spriječava** da to učini
- **ponovljeno** (često) šalje deautentikacijske okvire
  - **pravi se** da je legitimna **stanica** → šalje **AP-u**
  - pravi se da je legitiman **AP** → šalje **stanici**
- Stanica **se mora** autenticirati i asocirati **opet** nakon **svake** deautentikacije => zapinje u petlji!
  - zato, **ne može slati podatkovne** okvire
    - jer se nemože **nikada** u potpunosti **spojiti**

DoS – broadcast deautentikacija

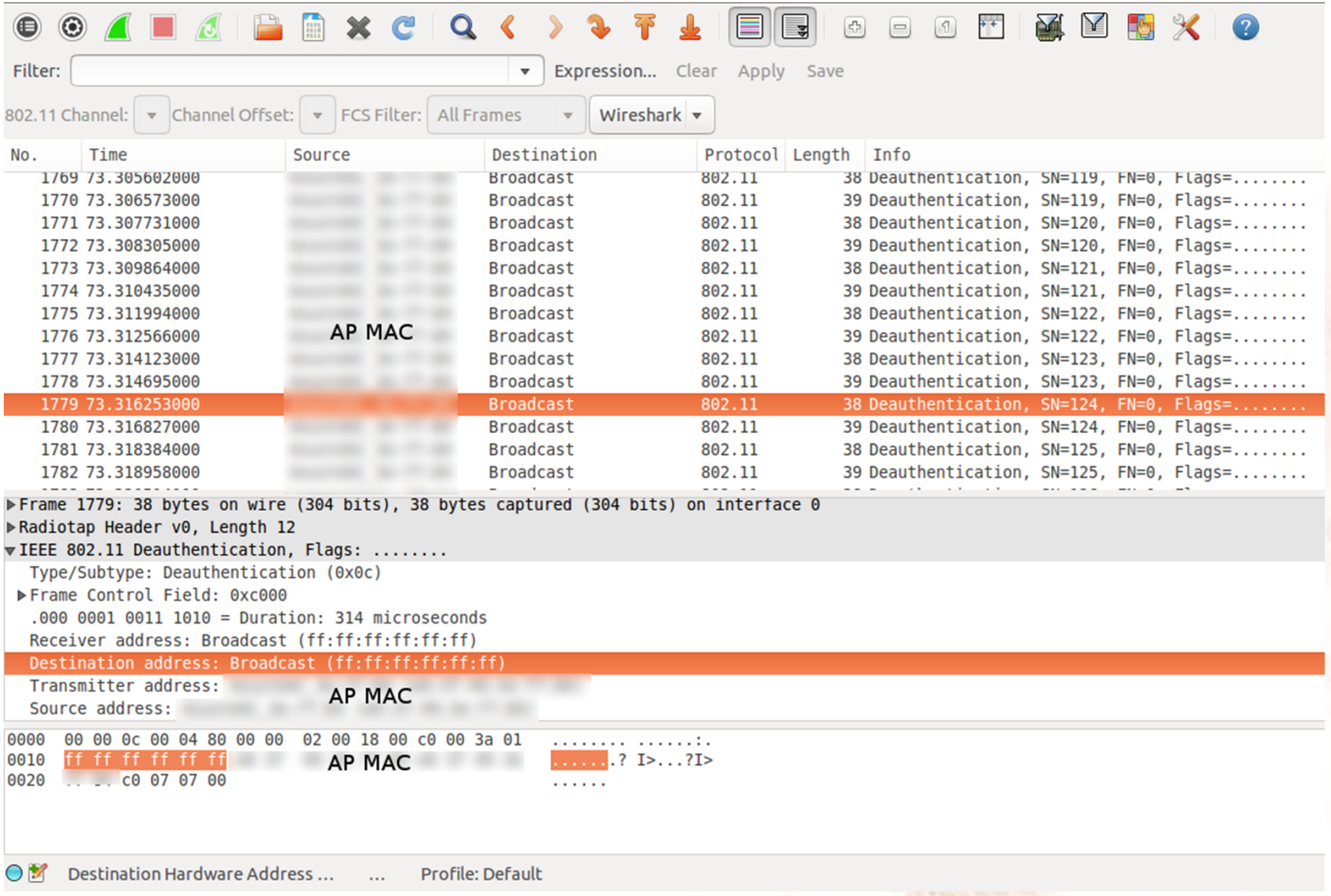


- Napadač šalje **broadcast** deautentikacijske okvire
  - pravi se da je legitiman **AP** → šalje **svim stanicama**
- **Sve stanice** se **neprekidno**
  - autenticiraju i asociraju!!! ☹
  - i postanu toliko zauzete da…
- **Nitko ne može** slati podatke

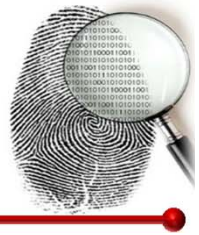
  => efektivno blokira **cijelu mrežu**

- Tako "pametni" Wi-Fi jammer-i rade
  - za razliku od onih koji samo **šalju puno šuma** na specifičnu frekvenciju
  - ali **moguće** ih **je detektirati** analizom mrežnog prometa (npr. u Wireshark-u)

DoS – broadcast deautentikacija



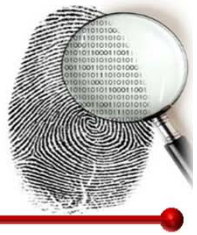
DoS deautentikacija – zanimljivost



- **Hotel** je **kažnjen** zbog korištenja ovih tehnika
  - **blokirali su** Wi-Fi mreže gostiju kako bi **morali koristiti** hotelsku **skupu** Wi-Fi mrežu
  - Netko je primijetio i prepoznao to, i prijavio ih ☺

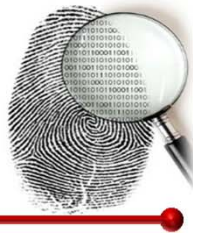
http://motherboard.vice.com/read/fcc-fines-freedom-hating-hotel-wi-fi-provider-for-blocking-personal-hotpsots

Dekriptiranje WPA i WEP PSK



- **podaci** poslani preko bežične mreže mogu biti **prisluškivani**
  - ako se WEP ili WPA/WPA2 koriste
  - i **PSK je poznat**
- za **pronaći PSK** -> za WEP potrebno je **snimiti legitimne** pakete
  - koji sadržavaju inicijalizacijske vektore (IVs)
  - koje AP generira kada komunicira sa ostalim klijentima
- za WPA/WPA2 **4-way EAPoL handshake** mora biti **snimljen**
  - odvija se odmah nakon asocijacije
- **napadač** ili
  - strpljivo **čeka** reasocijaciju (i handshake)
  - ili koristi **lažiranu** deautentikaciju
    - da odspoji žrtvu s mreže
    - i tako ju natjera da se ponovno spoji i izvrši handshake
- **žrtva nemože primijetiti** tako brzu deautentikaciju
  - stanica se ponovno spoji vrlo brzo, kao da se ništa nije dogodilo
  - ali, **može biti detektirano** kada se gleda mrežni promet
    - pomoću Wireshark-a, primjerice

4-way handshake



Filter: Expression... Clear Apply Save

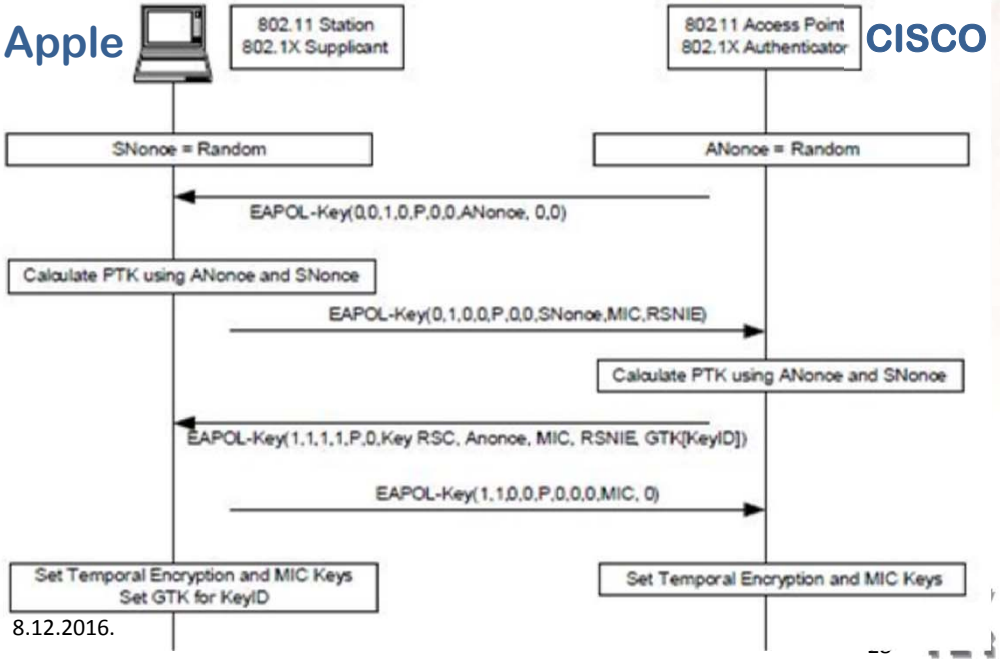
802.11 Channel: Channel Offset: FCS Filter: All Frames Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
85	5.647962		Cisco-Li_82:b2:55 (RA)	802.11	38	Acknowledgement, Flags=.....C
86	5.648961		Cisco-Li_82:b2:55 (RA)	802.11	38	Clear-to-send, Flags=.....C
87	5.649953	Cisco-Li_82:b2:55	Apple_82:36:3a	EAPOL	181	Key (Message 1 of 4)
88	5.649964		Cisco-Li_82:b2:55 (RA)	802.11	38	Acknowledgement, Flags=.....C
89	5.650959	Apple_82:36:3a	Cisco-Li_82:b2:55	EAPOL	181	Key (Message 2 of 4)
90	5.650970		Apple_82:36:3a (RA)	802.11	38	Acknowledgement, Flags=.....C
91	5.654947		Cisco-Li_82:b2:55 (RA)	802.11	38	Clear-to-send, Flags=.....C
92	5.655957	Cisco-Li_82:b2:55	Apple_82:36:3a	EAPOL	239	Key (Message 3 of 4)
93	5.655968		Cisco-Li_82:b2:55 (RA)	802.11	38	Acknowledgement, Flags=.....C
94	5.655973	Apple_82:36:3a	Cisco-Li_82:b2:55	EAPOL	159	Key (Message 4 of 4)
95	5.656951		Apple_82:36:3a (RA)			
96	5.734961	Cisco-Li_82:b2:55	Broadcast			
97	5.837942	Cisco-Li_82:b2:55	Broadcast			
98	5.842998		Apple_82:36:3a (RA)			

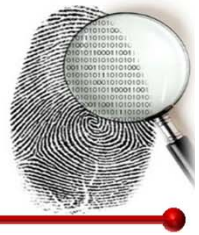
▶ Logical-Link Control
▼ 802.1X Authentication
  Version: 802.1X-2004 (2)
  Type: Key (3)
  Length: 117
  Key Descriptor Type: EAPOL RSN Key (2)
▼ Key Information: 0x008a
    .... .010 = Key Descriptor Version: AES Cipher, HMAC-SHA1 MI
    .... 1... = Key Type: Pairwise Key
    ....00 .... = Key Index: 0

```
0030  aa aa 03 00 00 00 88 8e  02 03 00 75 02 00 8a 00   ........ ...u....
0040  10 00 00 00 00 00 00 00  00 3e 8e 96 7d ac d9 60   ........ .>..}..`
0050  32 4c ac 5b 6a a7 21 23  5b f5 7b 94 97 71 c8 67   2L.[j.!# [.{..q.g
0060  98 9f 49 d0 4e d4 7c 69  33 00 00 00 00 00 00 00   ..I.N.|i 3.......
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```

802.1X Authentication (eapol), ... Profile: Default

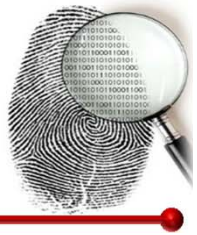


Bruteforce – WEP



- WEP je izrazito nesiguran
  - moguć je bruteforce
  - sa umjerenom količinom snimljenog mrežnog prometa
- ako nema mrežnog prometa na mreži
  - postoje različite tehnike kako ga umjetno generirati
  - ovisno o okolnostima

Bruteforce – WPA PSK

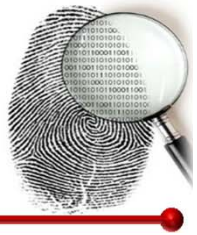


- Izrazito **spor**
  - moguć u praksi samo korištenjem riječnika očekivanih lozinki
  - bruteforce moguć samo kada je lozinka slaba (česta/predvidljiva)
- 4-way handshake je potreban
  - moguće ga je dobiti deautentikacijom žrtve
  - ili strpljivim čekanjem
- potrebno je stvoriti ***rainbow tablice***
  - zbog dizajna algoritma
  - za kombinacije SSID-a i lozinke
  - I dalje korisne za česte kombinacije SSID-eva i lozinka
    - npr. default postavke neke opreme

http://www.renderlab.net/projects/WPA-tables/

Prisluškivanje prometa

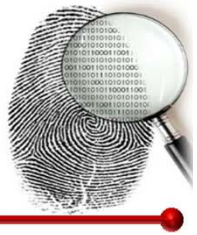
802.11 prisluškivanje prometa



- Postaviti sučelje u ***monitor mode***
- **Slušati** na ispravnom kanalu
- **Dešifrirati** promet ako je potrebno
- Napredne tehnike:
  - **Više** AP-ova na **različitim** kanalima
  - **Rekonstrukcija** mrežnog prometa *roaming* stanice
  - **procjena** fizičke lokacije stanica/AP-ova
    - snimanjem jačine njihovih signala
  - **automatska analiza** prometa
    - korištenjem specijaliziranih **alata**
    - kako bi znali na koje dijelove prometa se fokusirati

Lažna pristupna točka

Lažna bežična pristupna točka

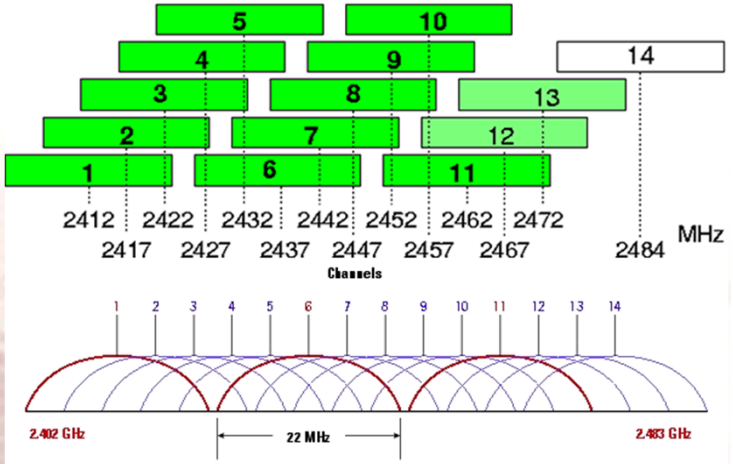


- Neautorizirana/**lažna** pristupna točka u bežičnoj mreži
  - tipično postavljena od napadača
    - kako bi **prisluškivali** žrtvine podatke dok se prenose
    - ili **oteli** korisničku sjednicu (man in the middle napad)

- **Detekcija** lažnih pristupnih točaka
  - istražitelj prvo treba detektirati sve pristupne točke
  - kako bi verificirao je li ili nije pristupna točka lažna
    - provjeravanjem:
      - MAC, SSID, Proizvođača, vrste medija, kanala

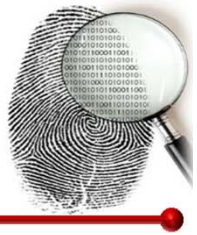
Mijenjanje kanala

- Korištene frekvencije
  - Sjedinjene Američke Države
    - 11 kanala za 802.11b/g/n,
    - frekvencije do 2.412 GHz do 2.462 GHz
  - Većina europe dopušta 13 kanala
    - do 2.472 GHz
  - Japan
    - dopušta 802.11b skroz do kanala 14, ili 2.484 GHz



- Mijenjanje kanala
  - Kartice proizvedene u SAD-u često ne podržavaju kanal 14
    - jer je ilegalno komunicirati na toj frekvenciji
  - Postoji preklapanje između kanala, ali na 2.484 GHz, kanal 14 je dovoljno daleko od kanala 11 da mrežne kartice namještene na kanal 11 vjerojatno neće pokupiti nikakav signal sa kanala 14
  - Zato ako napadač ilegalno komunicira na kanalu 14
    - sigurnosi timovi koji prate SAD kanale ga vjerojatno ne bi nikada detektirali

802.11n Greenfield način

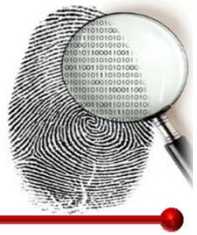


- 802.11n (“MIMO”-bazirana) specifikacija
  - omogućava puno veću propusnost od 802.11a/b/g
    - 100Mbps ili više !!! (54-600)

do 4 antene

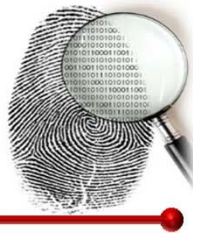
- 802.11n standard specificira dva načina:
  - Miješani način
    - koji dopušta da radi sa starim 802.11a/b/g mrežama
  - Greenfield (GF) ili “samo visokopropusni” način
    - koji **u potpunosti koristi** pojačanu propusnost
    - ali **nije vidljiv** 802.11a/b/g uređajima
    - Stariji (802.11a/b/g) uređaji će viditi GF promet samo **kao šum**
      - skeniranjem zraka sa 802.11a/b/g karticom **nije moguće** vidjeti 802.11n uređaje koji rade u Greenfield (GF) načinu

Zli Blizanac



- napadač **postavlja** WAP
  - sa **istim SSID-om** kao onim koji koristi mreža žrtve
    - **obično** sa ciljem izvršavanja **man-in-the-middle** napada
- komercijalni 802.11 klijenti se **asociraju** sa SSID-om
  - koji im njihovi operateri kažu
- Ako postoji **više od jednog** WAP sa istim SSID-om
  - kao što je slučaj sa većinom centralno upravljanih bežičnih mreža
    - ili tvrtkinih ili od Wi-Fi "hotspot-a"
- onda će se klijent asocirati sa WAP
  - koji daje **najjači signal**
- Ako je **signal zlog blizanca jači**
  - od **legitimnog** WAP-a
  - 802.11 **klijenti** će se **asocirati** sa **Zlim Blizancem**

Hole196 u WPA2

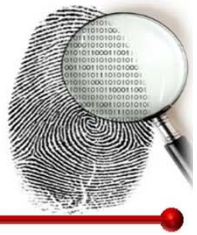


- Komunikacija između stanica i AP-a
  - koristi PTK (Pairwise Transient Key), jedinstven za svaku stanicu
- Broadcast komunikacija kroz BSS
  - koristi GTK (Group Temporal Key), isti za sve stanice
  - čak ga i napadač posjeduje
- stoga, napadač spojen na mrežu
  - može lažirati AP broadcast-ove svim stanicama
  - jer posjeduje GTK (svi ga posjeduju)
- Posaljedice:
  - **ARP spoof** (MITM)
  - **Port scan**, daljinska eksploatacija itd. koja zaobilazi izolaciju klijenata

http://www.airtightnetworks.com/WPA2-Hole196

Lociranje bežičnih uređaja

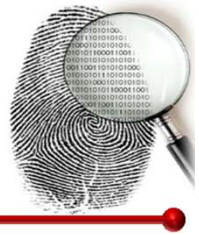
Lociranje bežičnih uređaja



- Najizazovniji aspekt forenzike bežičnih mreža
  - je težina **fizičkog lociranja** zanimljivih uređaja
    - **kompromitirani** laptop **se može fizički kretati** kroz mrežu tvrtke
    - **lažni** WAP **može biti sakriven** na lukava mjesta kao što je ispod ploča stropa
      - ili vani **na ulici**, u parku, …

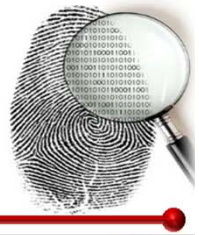
- Strategije za lociranje bežičnih uređaja uključuju:
  - **sakupljanje** opisnika stanica, kao što su MAC adrese
  - za klijente, **identifikacija** AP-ovog SSID-a s kojim je stanica asocirana
  - uzastopno **mjerenje** jačine signala uređaja
    - **micanje mjernog uređaja** na razne lokacije
    - i **triangulacijom** signala

Jačina signala

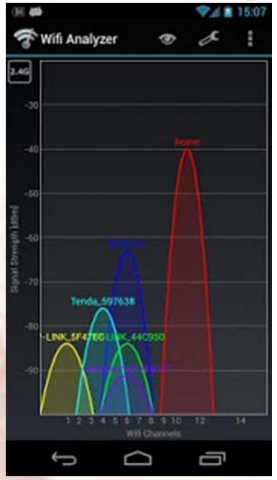


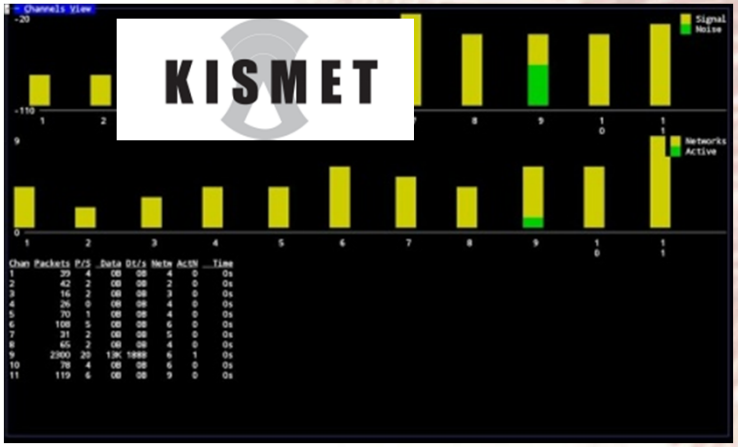
- **obližnji** WAP-ovi mogu biti **detektirani**
  - sa raznim alatima
    - koji pokazuju njihovu **relativnu jačinu signala**
    - i **smjer**
- često je moguće **locirati** bežični uređaj samo gledanjem **jačine signala**
  - i hodanjem u smjeru pojačavanja jačine signala
    - ako stanica koju tražimo nije mobilna
- Received Signal Strength Indication (RSSI)
  - **ponekad** je moguće **vidjeti**
    - the IEEE 802.11 (RSSI) i
    - Transmit (Tx) Rate informacije
  - kada gledamo snimak paketa
    - ako alat koji je snimio pakete opskrbljuje te podate u svojim dodatnim okvirima
  - **802.11** specifikacija jednostavno **ne sadržava** takve informacije u zaglavlju **podatkovnog sloja**

Primjer alata



- Za **analizu** WAP-ova moguće je koristiti:
  - aplikacije za **mobilne** telefone
    - Wi-Fi Analyzer
    - Wi-Fi finder
    - Wi-Fi radar
  - NetStumbler
    - point-and-click alat za **Windows**
  - Kismet
  - Mnogo, **mnogo više**...

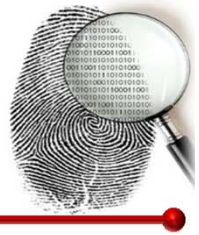




MS-Windows dnevnici

korisni u forenzici bežičnih mreža

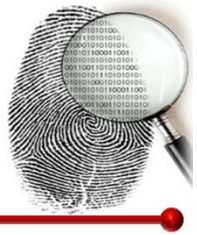
Bežične mreže i Windows Registry



- Windows prati **sve** što radite na sustavu
  - što imate **spojeno** na računalo
  - i što ste **koristili** na sustavu

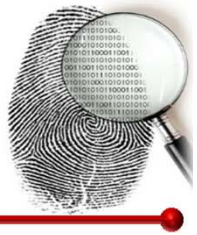
- Znajući **gdje tražiti** ove informacije
  - i što one govore
  - je jedan od velikih izazova
  - koji imaju istražitelji incidenata
  - kada pretražuju računala

Mrežna sučelja

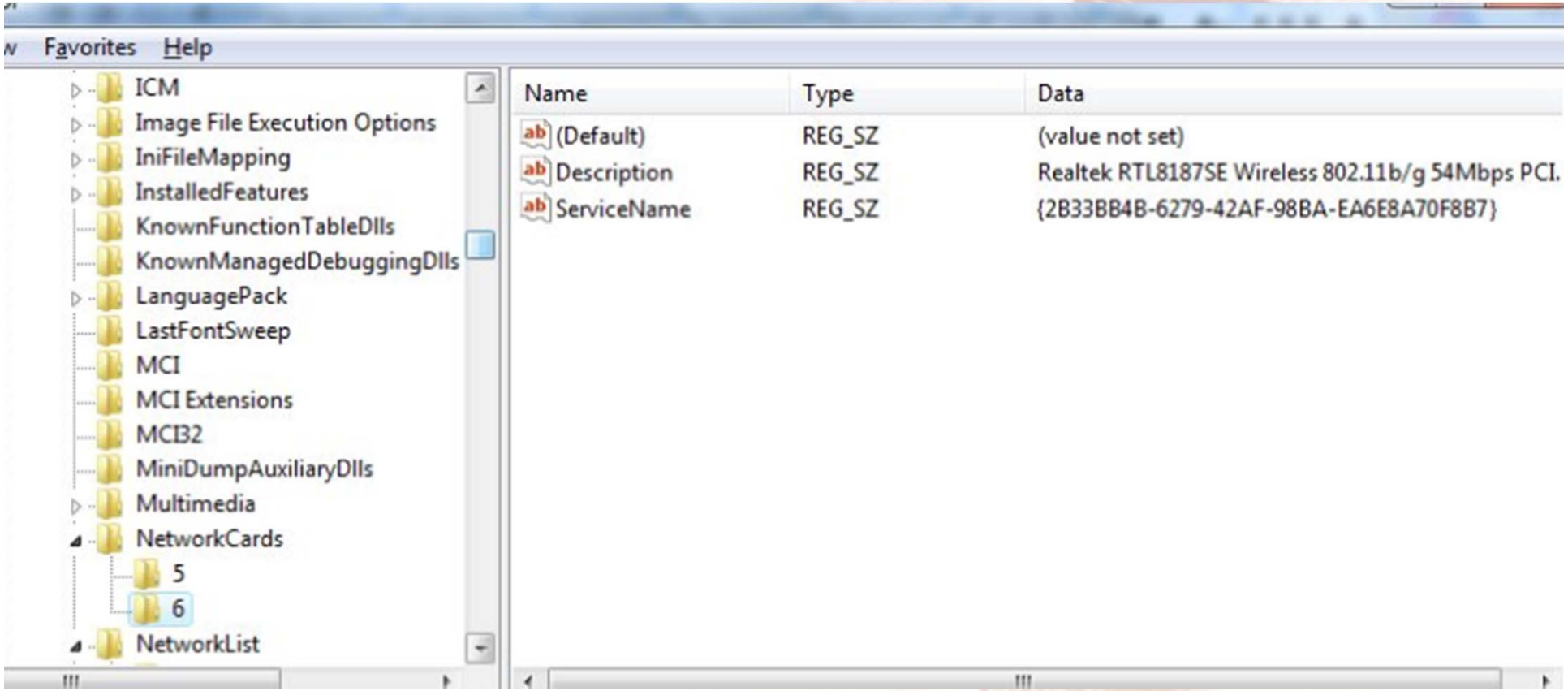


- Windows **Vista** sprema
  - mrežne postavke i konfiguracije
  - u više odvojenih lokacija
- Prva informacija za pronalazak bežičnih informacija
  - je **registry key** koji sprema podatke vezane uz kontrolere mrežnih sučelja (NIC's)
  - Ove informacije se nalaze na sljedećoj lokaciji:
    - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkCards

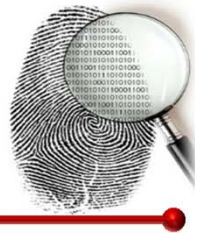
Mrežna sučelja - primjer



HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkCards



Interface information



HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{GUID}

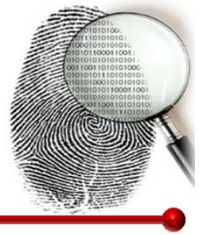
Editor

View Favorites Help

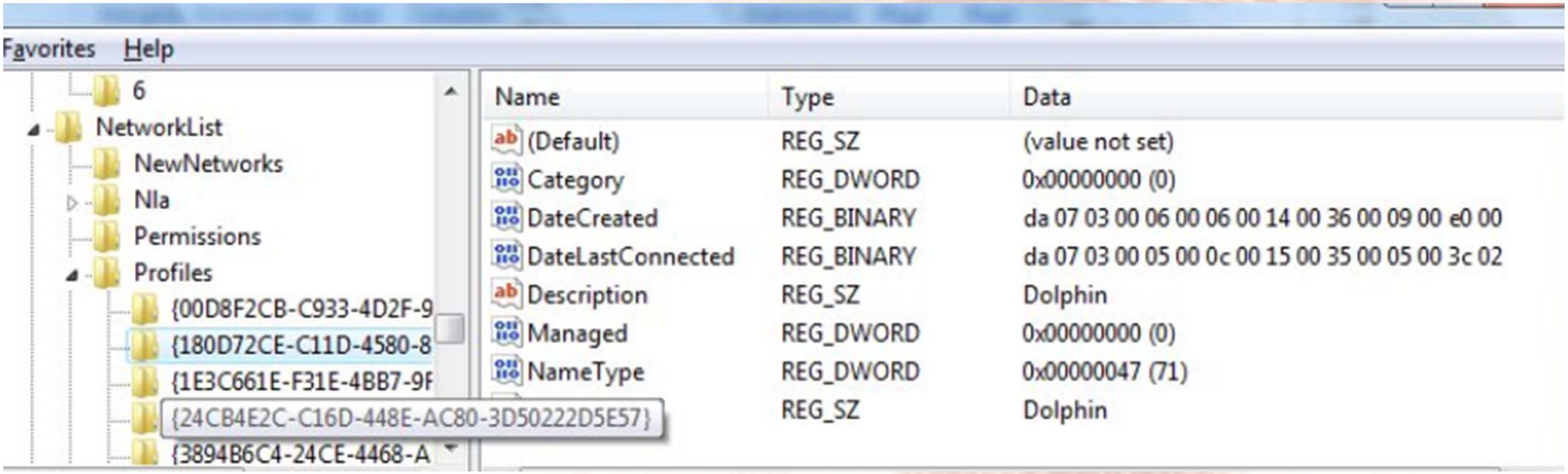
- Enum
- Linkage
- Parameters
  - Adapters
    - {2B33BB4B-6279-42AF-9
    - {3F6294EC-1674-4618-BF
    - {55A30E48-C84D-40D1-8
    - {6B6B4C5D-AA03-41A2-
    - {CE422ED5-F1D2-4411-B
  - DNSRegisteredAdapters
  - Interfaces
    - {2B33BB4B-6279-42AF-9
    - {3F6294EC-1674-4618-BF
    - {55A30E48-C84D-40D1-8
    - {6B6B4C5D-AA03-41A2-
    - {CE422ED5-F1D2-4411-B
  - PersistentRoutes
  - Winsock
- Performance
- ServiceProvider
- Tcpip6

Name	Type	Data
(Default)	REG_SZ	(value not set)
AddressType	REG_DWORD	0x00000000 (0)
DhcpConnForceBro...	REG_DWORD	0x00000001 (1)
DhcpDefaultGateway	REG_MULTI_SZ	172.19.5.244
DhcpDomain	REG_SZ	gateway.2wire.net
DhcpInterfaceOptions	REG_BINARY	2e 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 03
DhcpIPAddress	REG_SZ	172.19.5.5
DhcpNameServer	REG_SZ	172.19.5.244
DhcpServer	REG_SZ	172.19.5.244
DhcpSubnetMask	REG_SZ	255.255.255.0
DhcpSubnetMaskOpt	REG_MULTI_SZ	255.255.255.0
Domain	REG_SZ	
EnableDeadGWDetect	REG_DWORD	0x00000001 (1)
EnableDHCP	REG_DWORD	0x00000001 (1)
IsServerNapAware	REG_DWORD	0x00000000 (0)
Lease	REG_DWORD	0x00015180 (86400)
LeaseObtainedTime	REG_DWORD	0x4c233a83 (1277377155)
LeaseTerminatesTime	REG_DWORD	0x4c26ac03 (1277602819)
NameServer	REG_SZ	

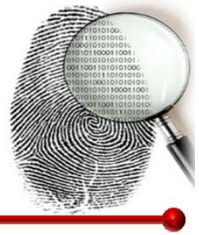
Korišteni AP-ovi



- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\
  - *Dolphin* –SSID mreže



Forenzika bežičnih mreža



- IEEE 802.11 osnove
- DoS slanjem **deautentikacijskih** okvira
- Sigurnost & enkripcija
- Prisluškivanje prometa
- **Lažne** pristupne točke
- detektiranje **fizičke lokacije** AP-a
- MS-Windows **registry** informacije


RacFor.zesoi.fer.hr
RacFor@zesoi.fer.hr