Identifying and Responding to Wireless Attacks

Chris Hurley (roamer)

roamer@securitytribe.com

Contents

- A brief history of wireless security and attacks
- Attacks against WEP
- Attacks against WPA
- Attacks against VPN
- Man in the Middle Attacks
- Identifying and responding to these attacks

A brief history of wireless security and attacks

- Wired Equivalent Privacy (WEP) was the original security mechanism for 802.11 networks.
- Scott Fluhrer, Itsik Mantin, and Adi Shamir discovered that WEP was flawed in their paper “Weaknesses in the Key Scheduling Algorithm of RC4”

A brief history of wireless security and attacks

- Attacks based on Fluhrer, Mantin, and Shamir's paper have come to be known as "FMS Attacks"
- Shortly after the FMS paper was released tools to automate WEP cracking were developed
  - WEPCrack
  - AirSnort

A brief history of wireless security and attacks

- In response to the weaknesses in WEP new security mechanisms were developed.
  - Cisco developed the Lightweight Extensible Authentication Protocol (LEAP)
  - WiFi Protected Access (WPA) was developed to replace WEP
    - WPA-PSK (Pre-Shared Key)
    - WPA-RADIUS

A brief history of wireless security and attacks

- In March, 2003, Joshua Wright disclosed that LEAP was vulnerable to a dictionary attack
- A short time later Wright released ASLEAP, a tool to automate attacks against LEAP.
- Cisco released EAP-FAST as a replacement for LEAP about a year after Wright's initial disclosure to them.

A brief history of wireless security and attacks

- In November 2003 Robert Moskowitz of ISCA Labs detailed potential problems with WPA when deployed using a Pre-Shared Key in his paper “Weakness in Passphrase Choice in WPA Interface”

A brief history of wireless security and attacks

- In November 2004 Joshua Wright released CoWPAtty.
- CoWPAtty automated the dictionary attack process against WPA-PSK networks.

A brief history of wireless security and attacks

- Despite excessive cries to the contrary, WEP was still relatively safe to use in some environments.
- Cracking a WEP key was so time consuming that it was often not feasible.
- Regular rotation of WEP keys could render FMS attacks ineffective on most networks.

A brief history of wireless security and attacks

- After the release of the FMS paper, h1kari of Dachboden Labs released a paper detailing ways to more effectively crack WEP.
- In 2004 new tools based on a Chopping attack were released

A brief history of wireless security and attacks

- Chopping attacks take a WEP packet and “chop” off the last byte.
- This breaks the CRC/ICV.
- If the last byte was 0, xor last the last 4 bytes with a certain value to make a valid CRC.
- Retransmit the packet.

A brief history of wireless security and attacks

- This attack methodology significantly reduced the amount of time required to crack WEP keys.
- Made a largely theoretical attack (FMS) realistic
- Tools
  - Aircrack
  - weplab

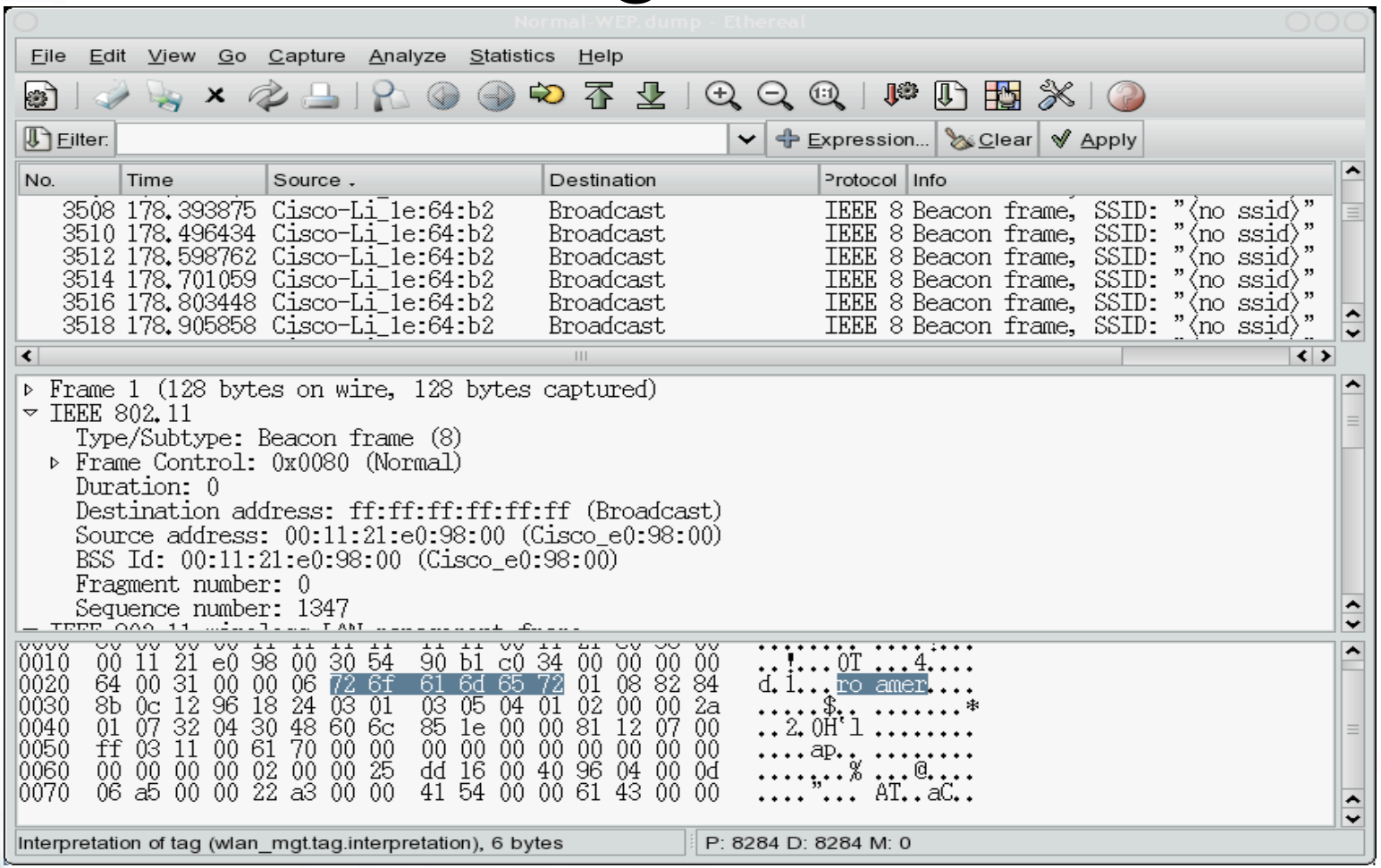
A brief history of wireless security and attacks

- Where are we now?
  - Can wireless networks be deployed in a corporate environment securely?
  - Is wireless intrusion detection viable?
  - Can attacks against wireless networks be observed and reacted to in real time?

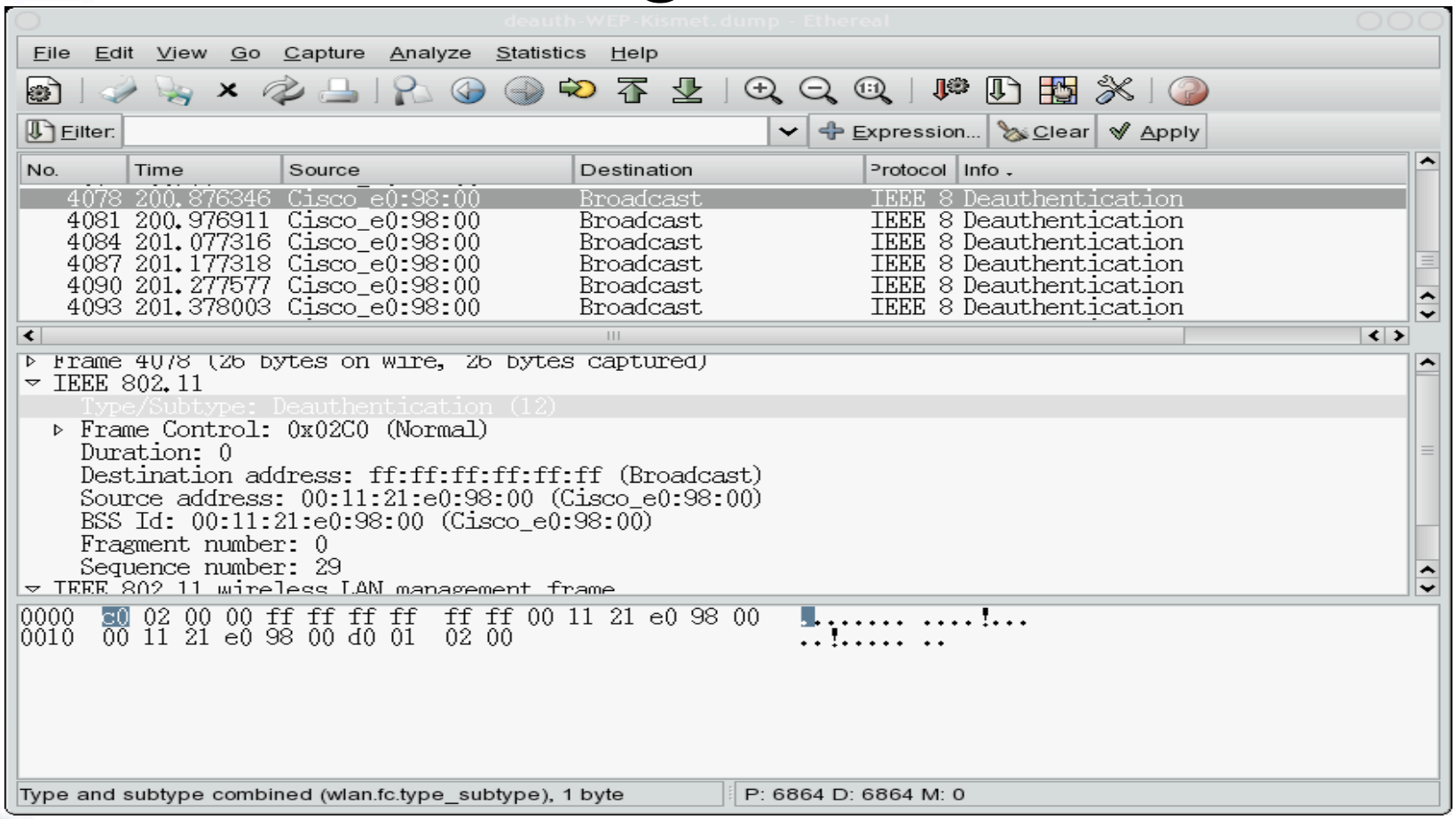
Attacks Against WEP

- Even with chopping attacks, a large number of packets still need to be captured by an attacker
- The easiest way to do this is by reinjecting packets back into the network to generate unique initialization vectors.

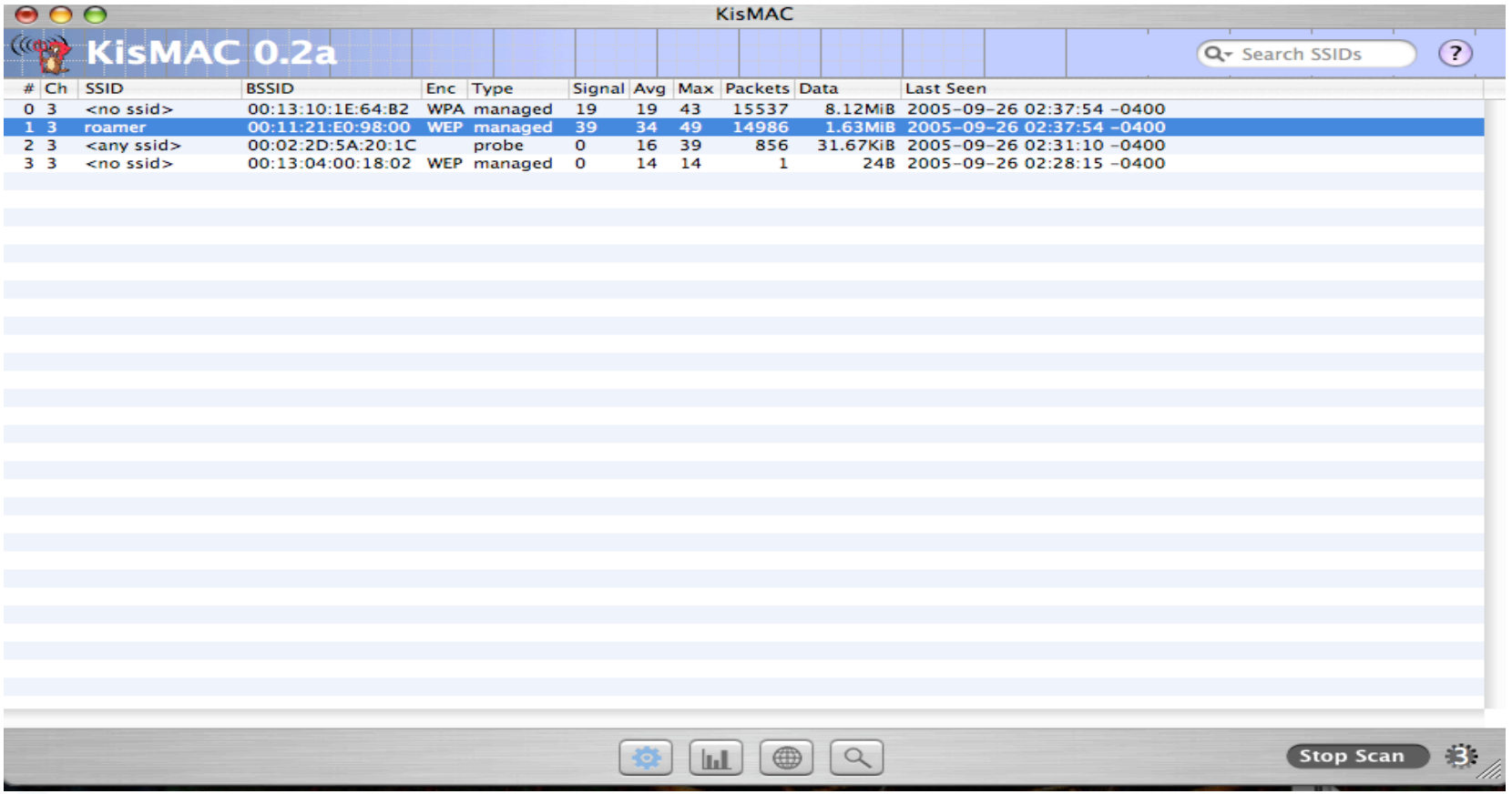
Attacks Against WEP



Attacks Against WEP

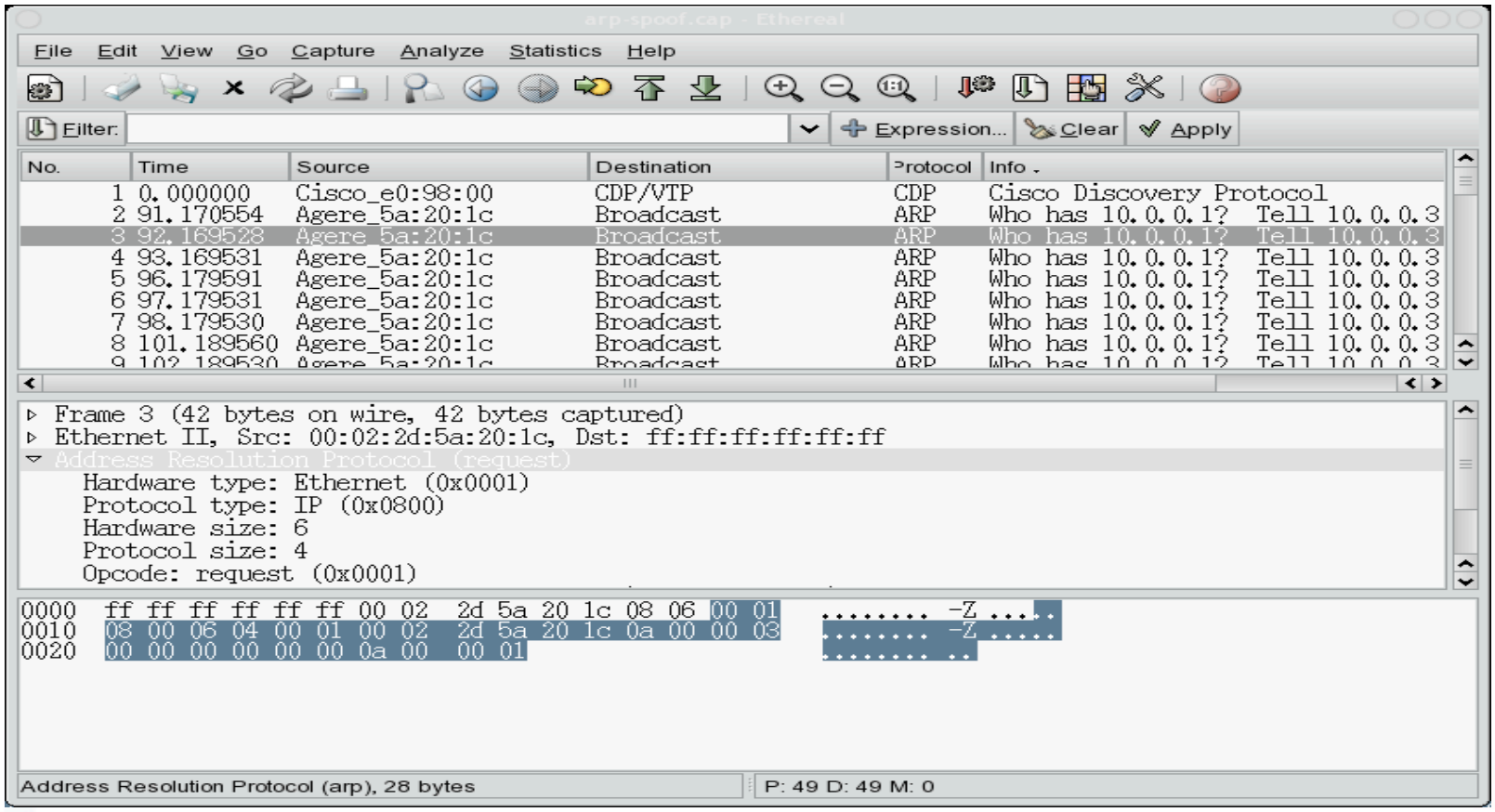


Attacks Against WEP



#	Ch	SSID	BSSID	Enc	Type	Signal	Avg	Max	Packets	Data	Last Seen
0	3	<no ssid>	00:13:10:1E:64:B2	WPA	managed	19	19	43	15537	8.12MiB	2005-09-26 02:37:54 -0400
1	3	roamer	00:11:21:E0:98:00	WEP	managed	39	34	49	14986	1.63MiB	2005-09-26 02:37:54 -0400
2	3	<any ssid>	00:02:2D:5A:20:1C		probe	0	16	39	856	31.67KiB	2005-09-26 02:31:10 -0400
3	3	<no ssid>	00:13:04:00:18:02	WEP	managed	0	14	14	1	24B	2005-09-26 02:28:15 -0400

Attacks Against WEP



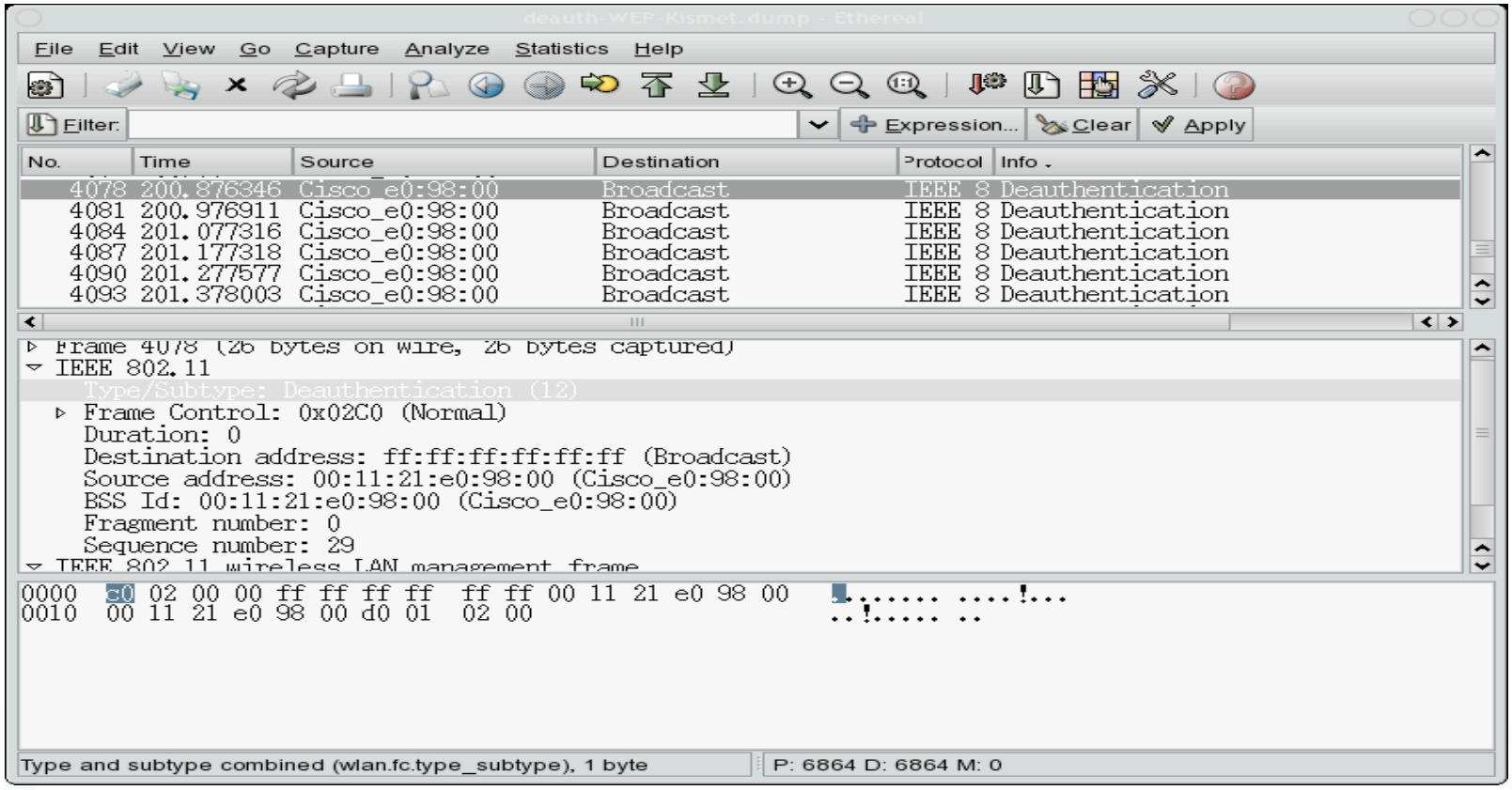
Responding to Attacks Against WEP

- An attack against WEP is in progress
  - Deauthentication block
  - ARP Injection block
    - ARP Injection is easy to identify
    - Understand the approximate number of ‘normal’ ARP packets seen on your network
  - Rotate WEP keys
  - LAST RESORT: Shut down the WLAN

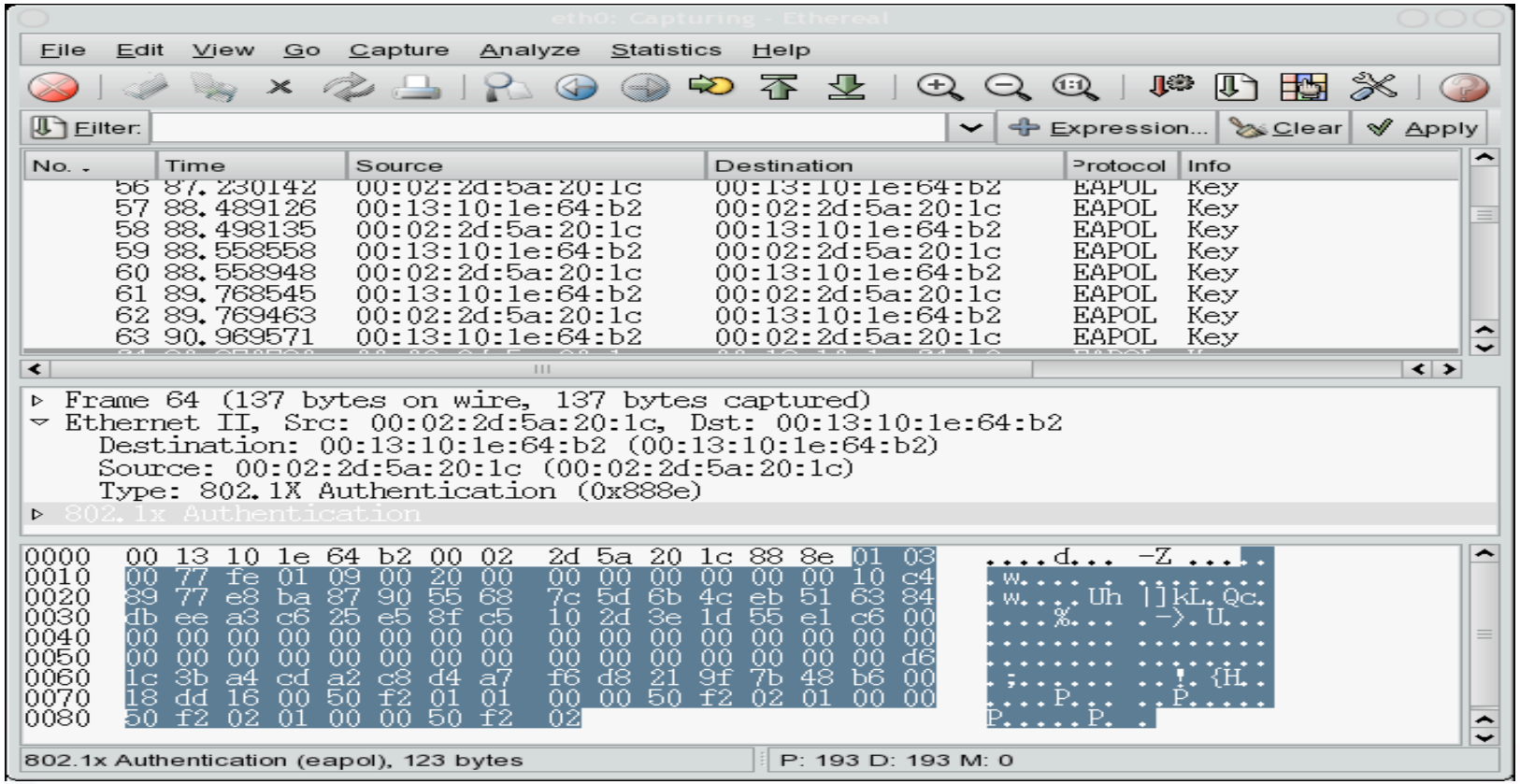
Attacks Against WPA

- WPA Pre Shared Keys with passphrases shorter than 21 characters are vulnerable to dictionary attacks
- This is an offline attack and not as easy to identify in real time as attacks against WEP

Attacks Against WPA



Attacks Against WPA



Responding to Attacks Against WPA

- Unlike WEP attacks by the time you can take action, it is likely too late
- If your WPA passphrase is more than 21 characters, no action is necessary
- If it is shorter than 21 characters, immediately change to a passphrase longer than 21 characters
- Use WPA with RADIUS or some other form of secondary authentication. Preferably two factor authentication

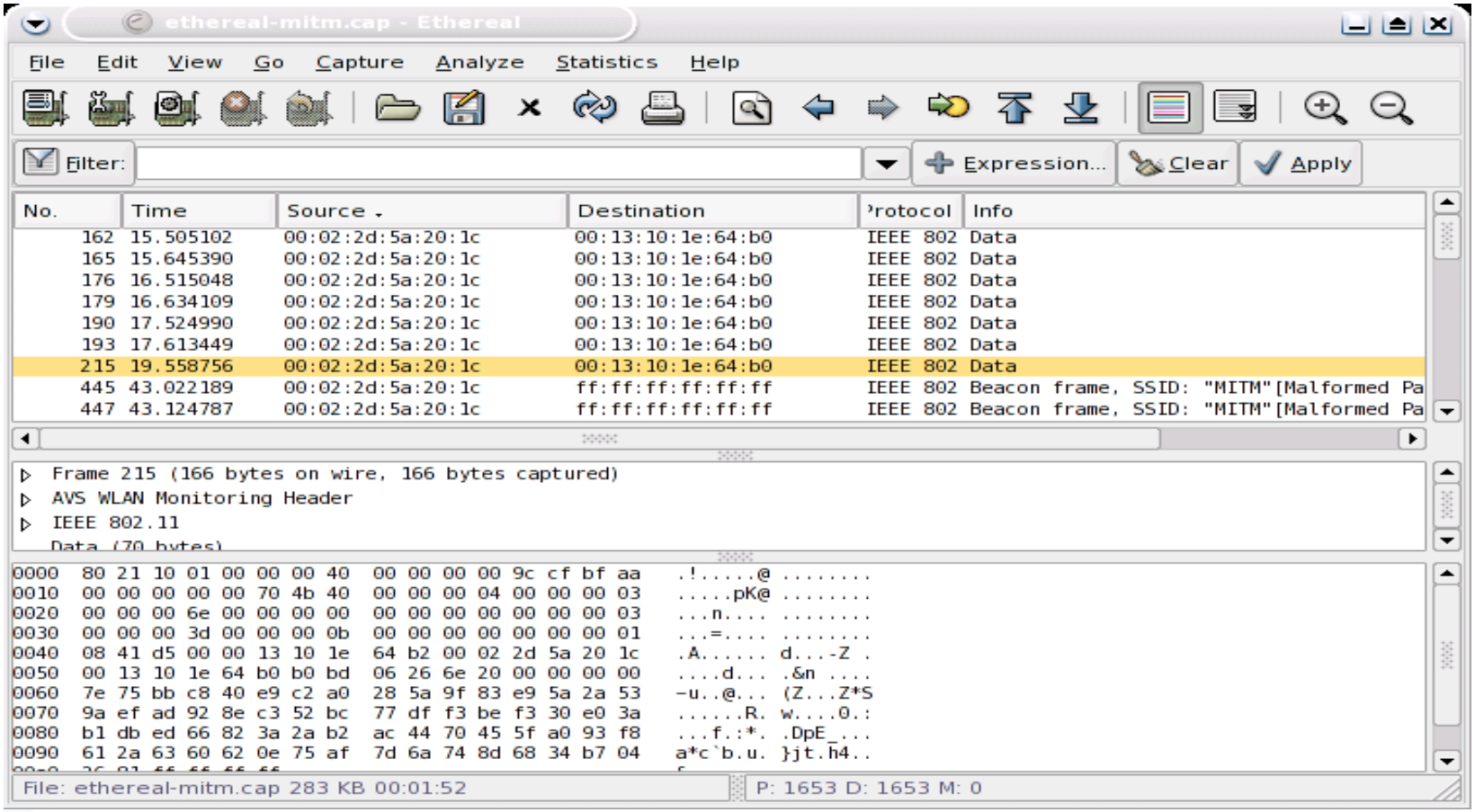
Man in the Middle Attacks

- Attempt to have clients authenticate to an access point that is not a legitimate AP.
- Capture cleartext traffic to glean usernames, passwords, and other sensitive information

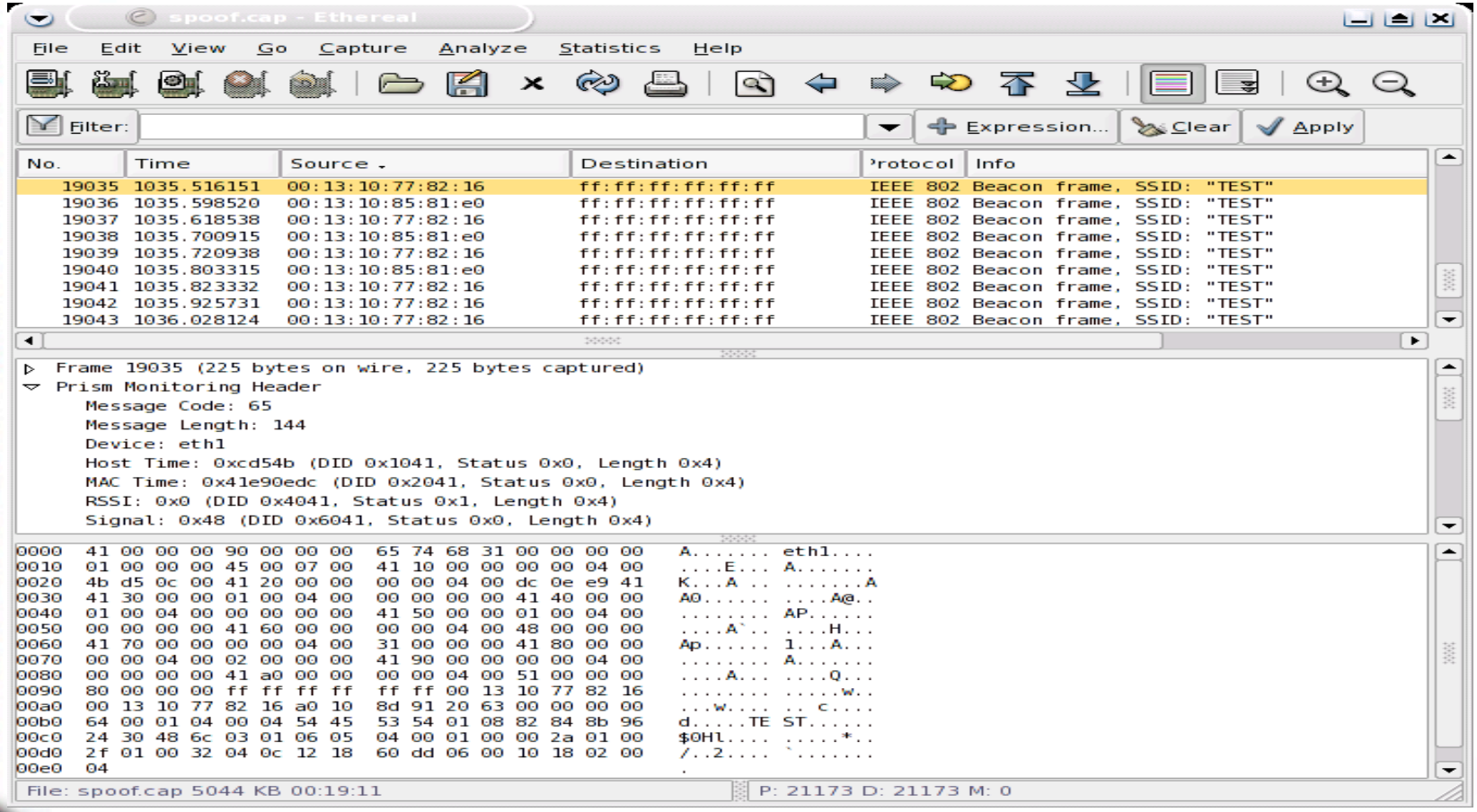
Man in the Middle Attacks

- Client based MITM attack
  - Use a client card configured in HOSTAP mode to act as an access point
  - Use a client card configured in HOSTAP mode to spoof a legitimate access point
- Access Point based MITM attack
  - Use an access point with custom firmware to spoof a legitimate access point

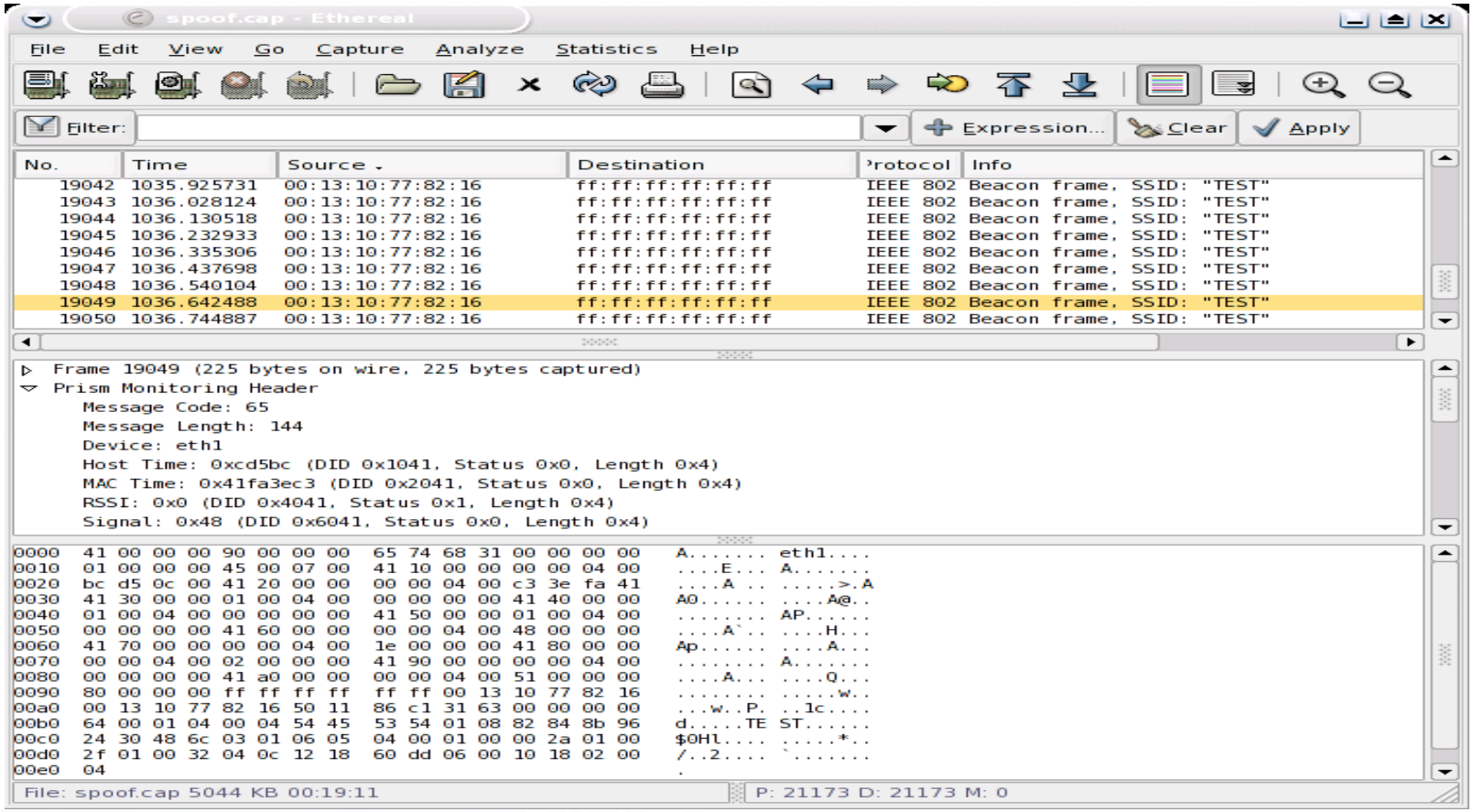
Man in the Middle Attacks



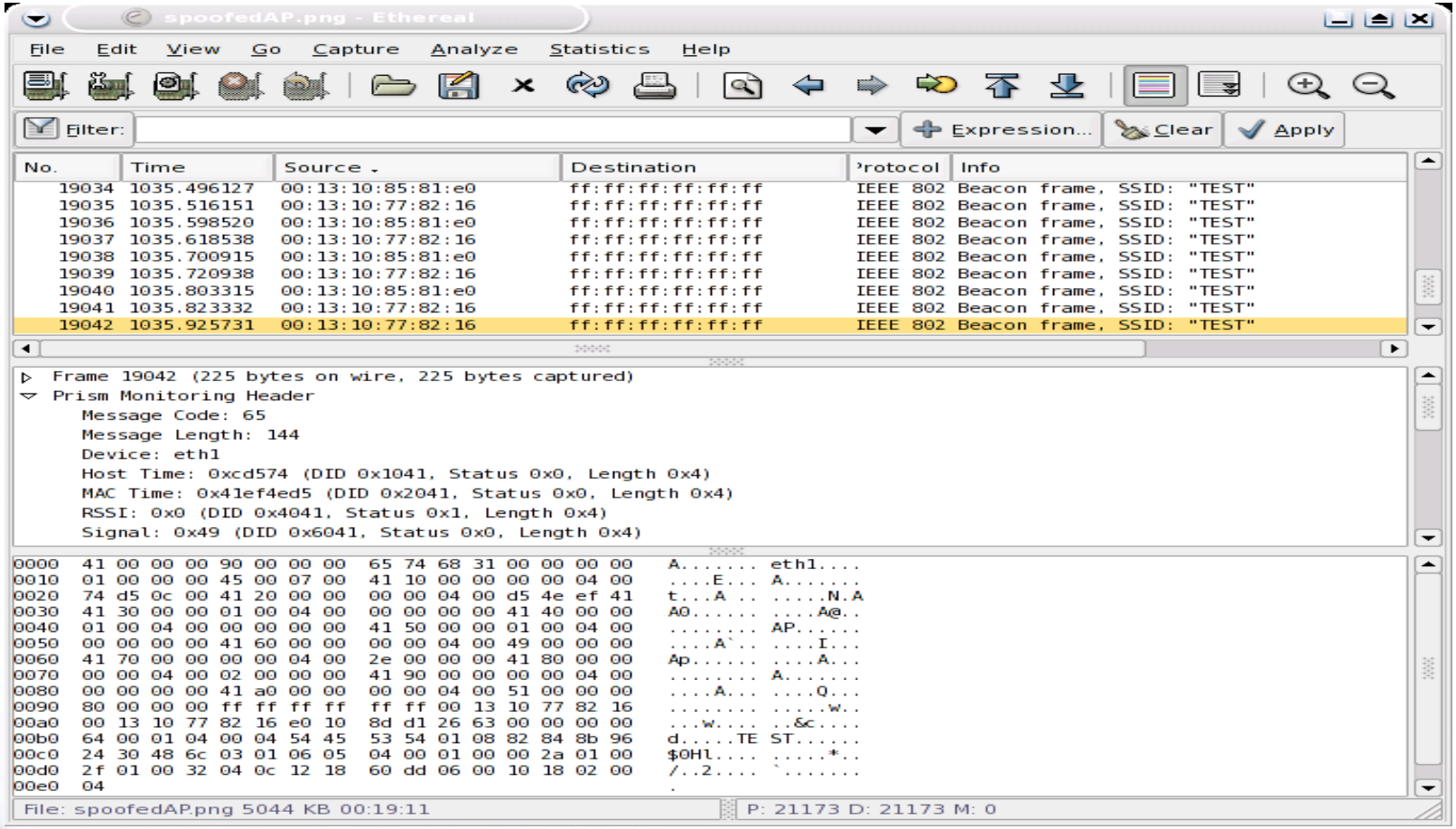
Man in the Middle Attacks



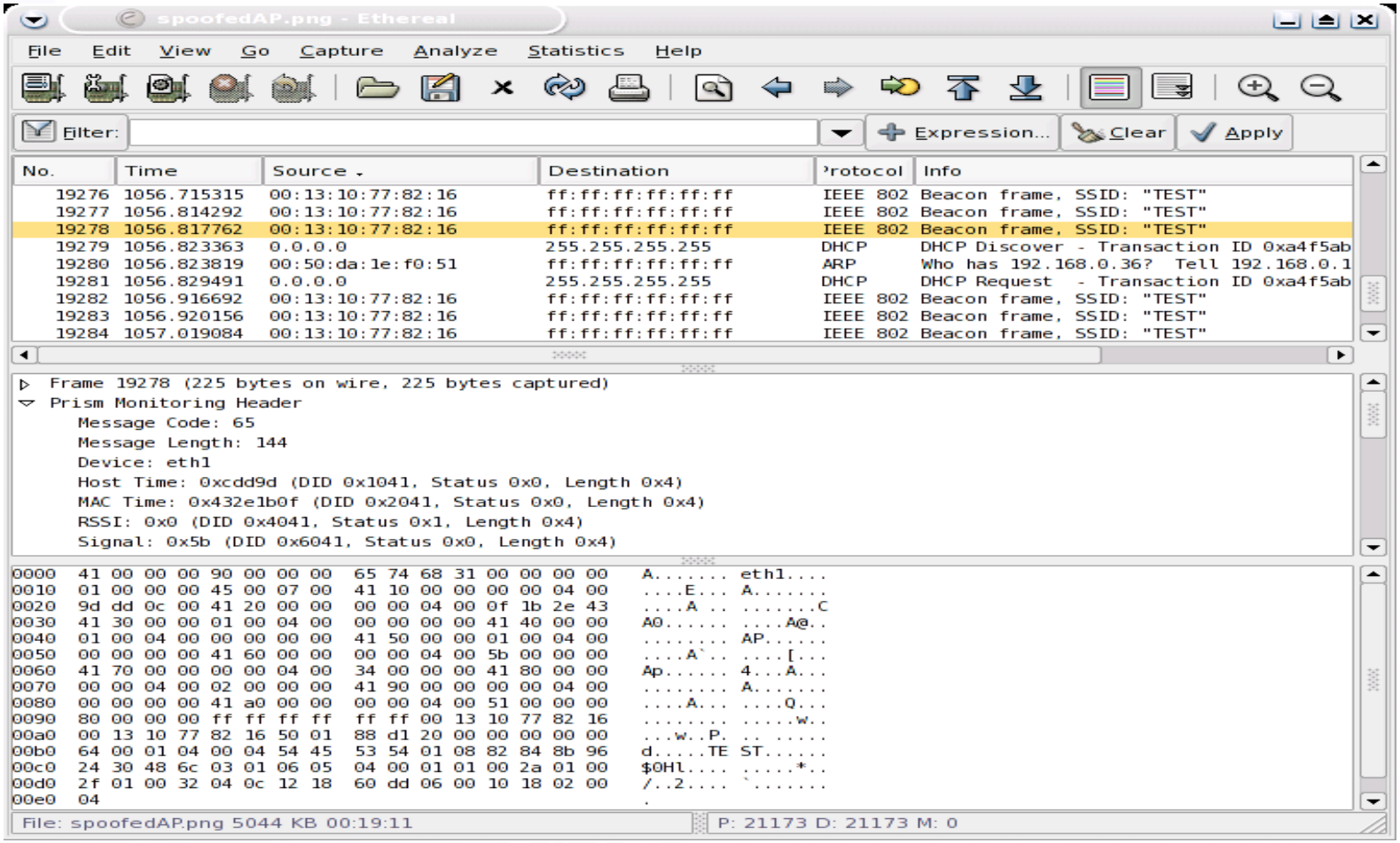
Man in the Middle Attacks



Man in the Middle Attacks



Man in the Middle Attacks



Responding to Man in the Middle Attacks

- Real time response to Man in the Middle Attacks is difficult.
- Preventative measures should be in place prior to a Man in the Middle attack commencing.

Responding to Man in the Middle Attacks

- Always require authentication to the network over an encrypted channel
- Use two factor authentication
- Treat the WLAN as a DMZ host with no network privileges without authentication
- Utilize wireless network equipment that actively responds to these type of events

Conclusion

- Wireless attacks have evolved significantly over the years
- As attacks have evolved, so have the tools available to administrators to respond to attacks
- No tool is a substitute for well trained, vigilant Administrators

Questions?

- roamer@securitytribe.com
- chris@goons.org