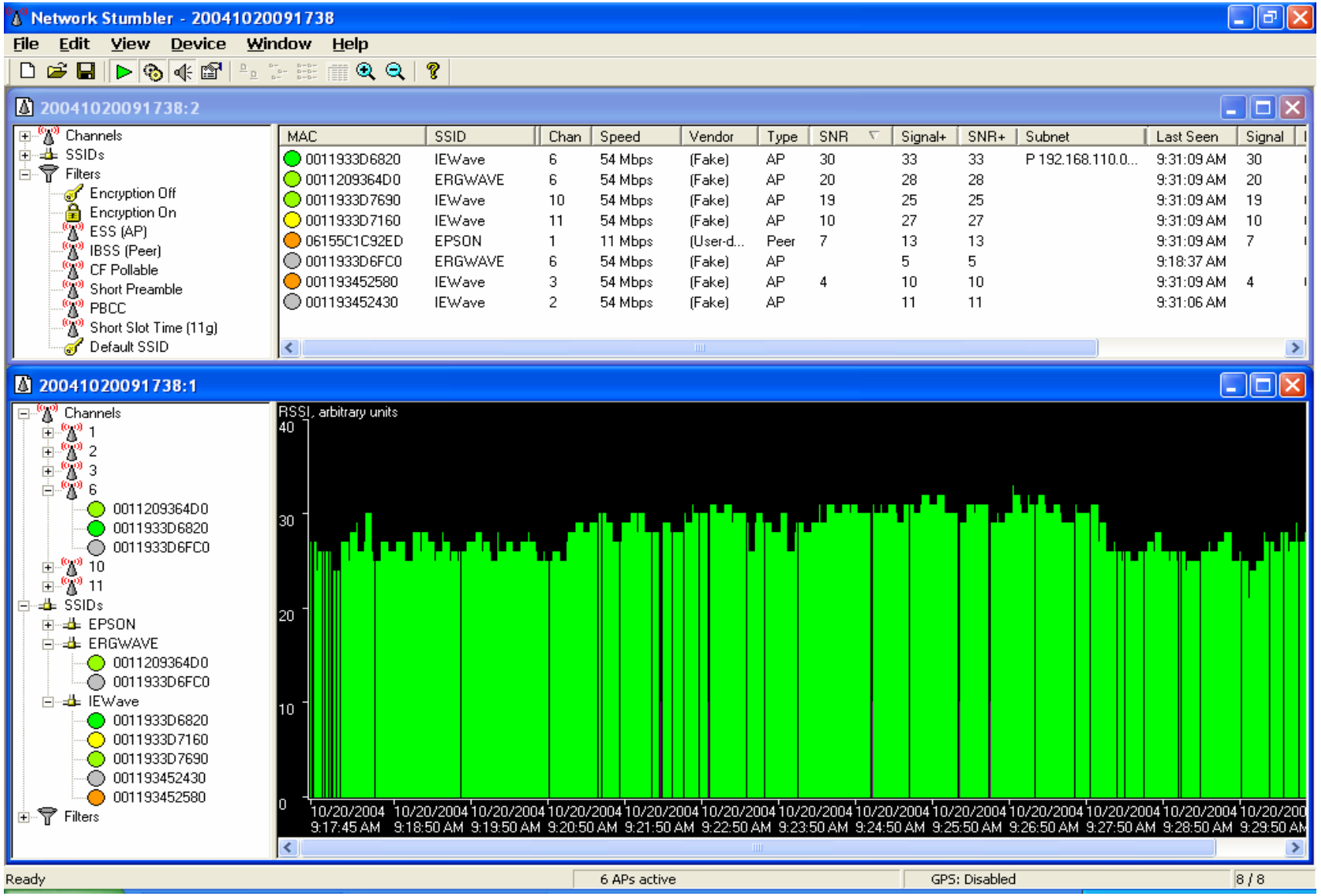
WLAN Sniffing and WEP Cracking

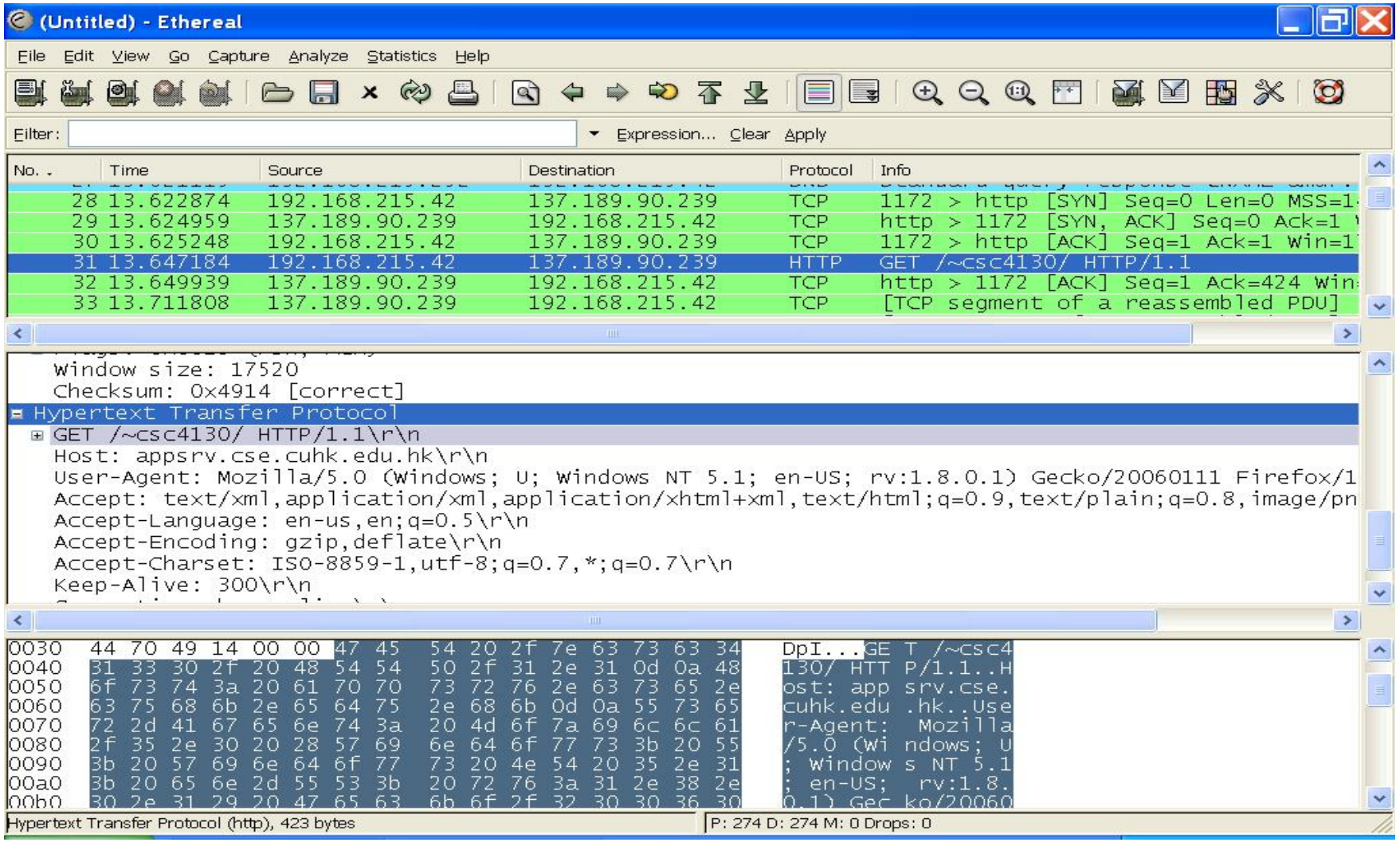
WLAN War Driving Survey 2004-05 Hong Kong by PISA,WTIA

	2002	2003	2004	2005
Date	07-Jul-02	05-Oct-03	28-Nov-04	04-Dec-05
Day	Sunday morning			
Weather	occasional light shower	sunny	sunny	sunny
Route	Kennedy Town - Causeway Bay			
No. of AP	187	474	926	1576
% of WEP/WPA disabled	77%	69%	60%	46%
% of factory default SSID	51%	39%	44%	39%
% of 802.11g AP			8.32%	68.15%

WLAN Monitoring by Network Stumbler



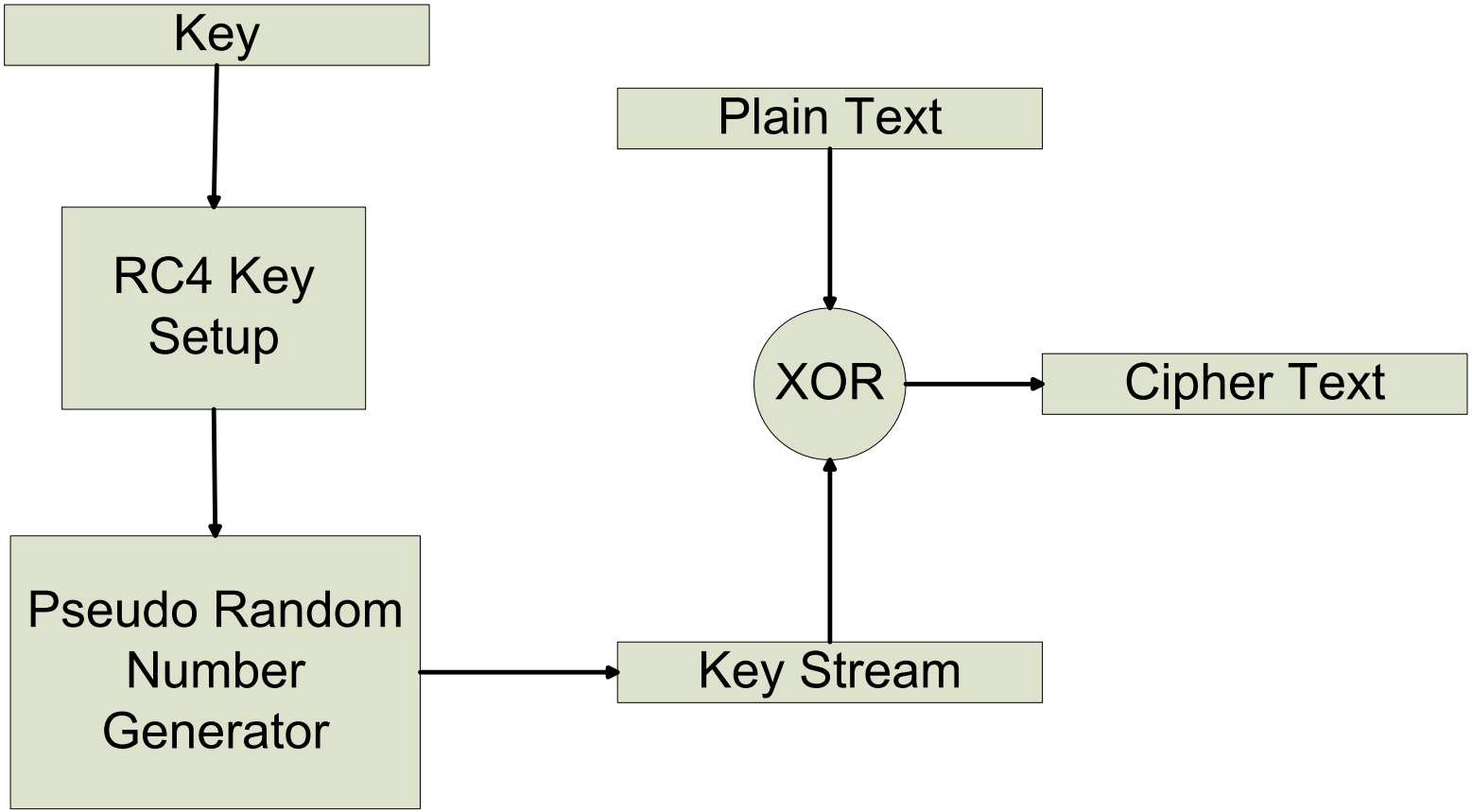
WLAN Traffic Captured by Ethereal



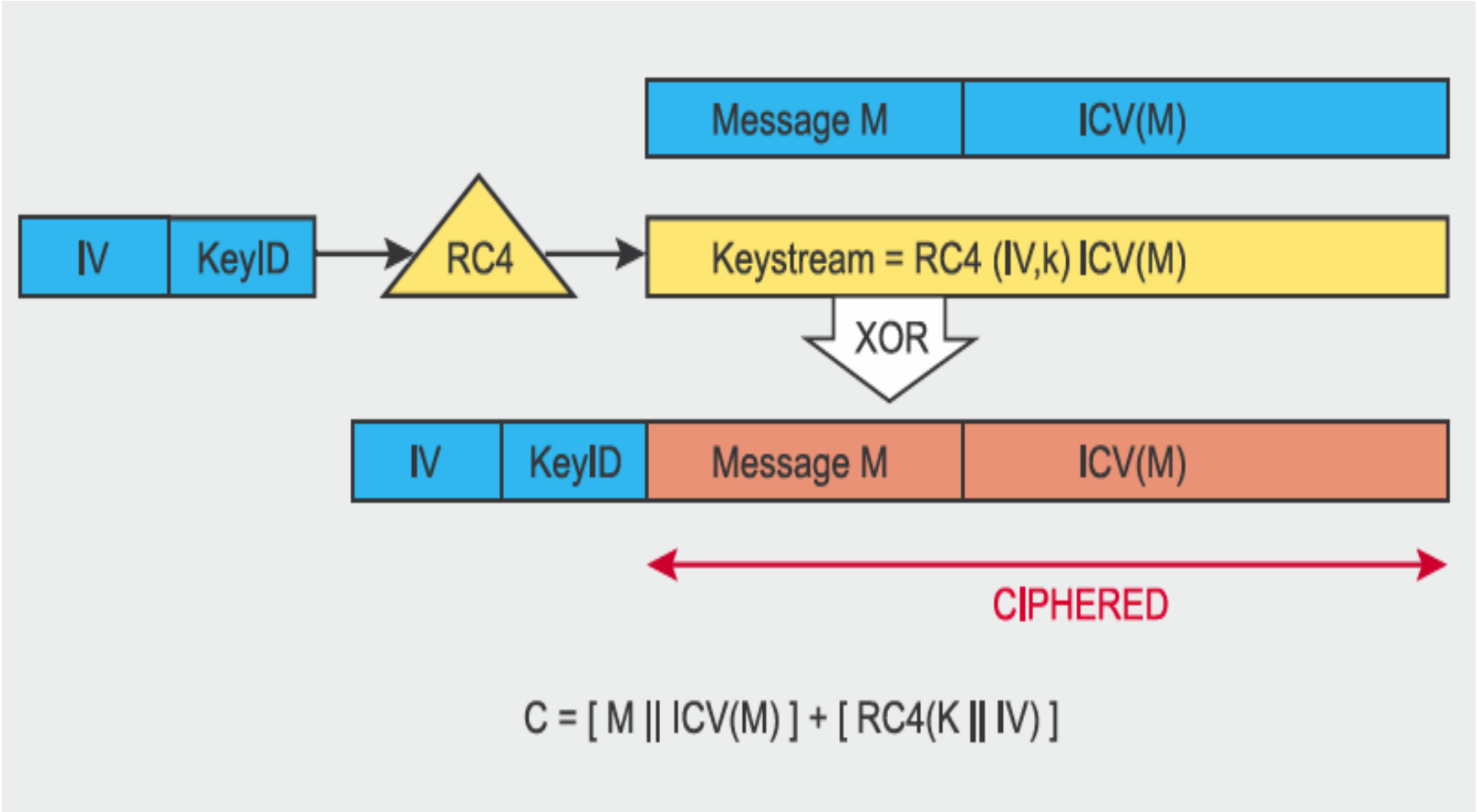
WEP Cracking

- Use RC4 encryption algorithm
- Shared (but static) secret 64 or 128-bit key to encrypt and decrypt the data (Symmetric Key)
- 24-bit ‘Initialization Vector’ (IV) leaving only 40 or 104 bits as the ‘real key’
- To protect the encrypted data, IV must be different for every message transmitted
- If Access Point transmits at 11 Mbps, all IVs are exhausted in roughly 5 hours

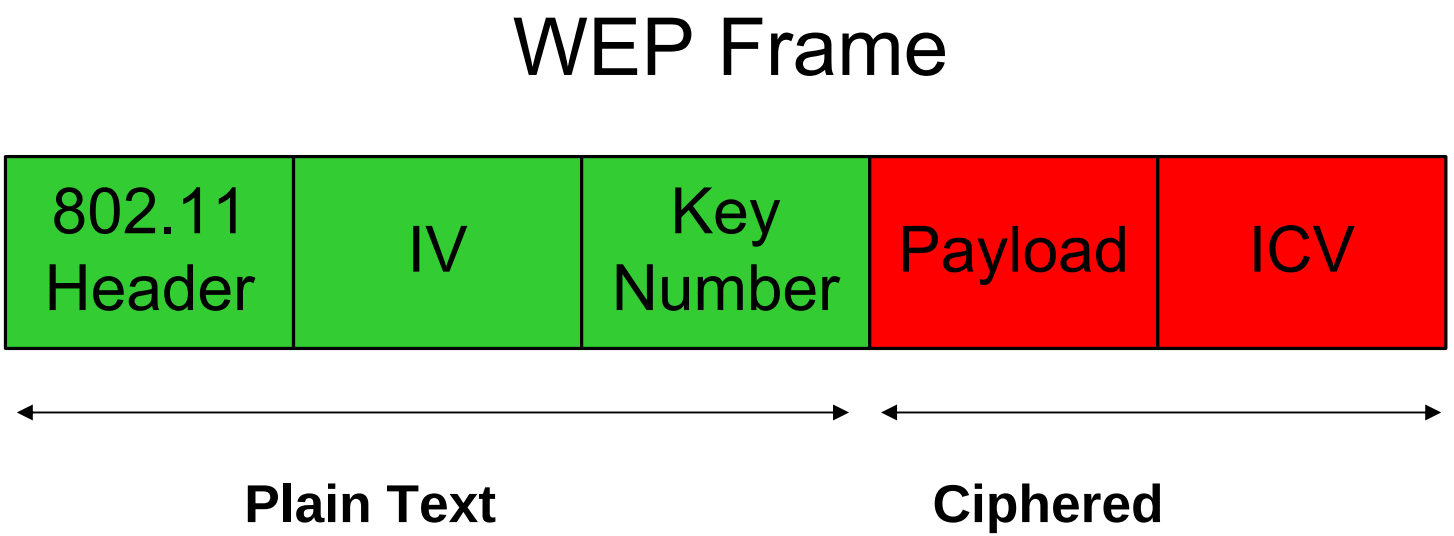
RC4 Stream Cipher



WEP Encryption Protocol



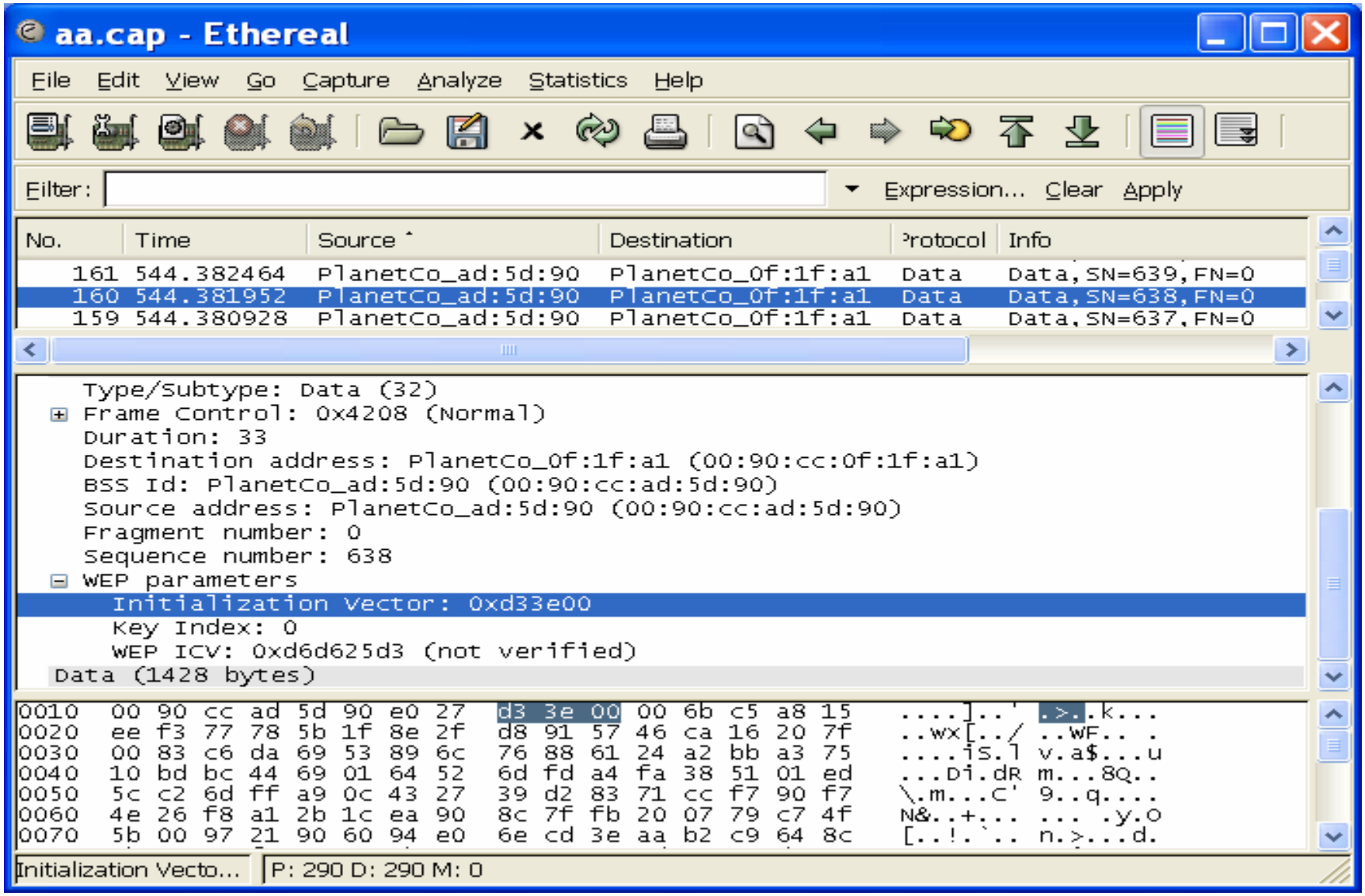
WEP Frame


WEP Frame
802.11 Header
IV
Key Number
Payload
ICV
Plain Text
Ciphered

Flaw in IV

- When enough packets have been collected (about 150,000 for 64 bit keys and 500,000-1M for 128 bit keys) software can be used to crack the WEP key
- Some IVs leak information about a certain byte of the key, thus statistically the correct key emerges when a sufficient number of IVs have been collected.
- At a recent Information Systems Security Association Meeting a small team of FBI agents demonstrated this technique and found a key real-time during the presentation in 3 minutes

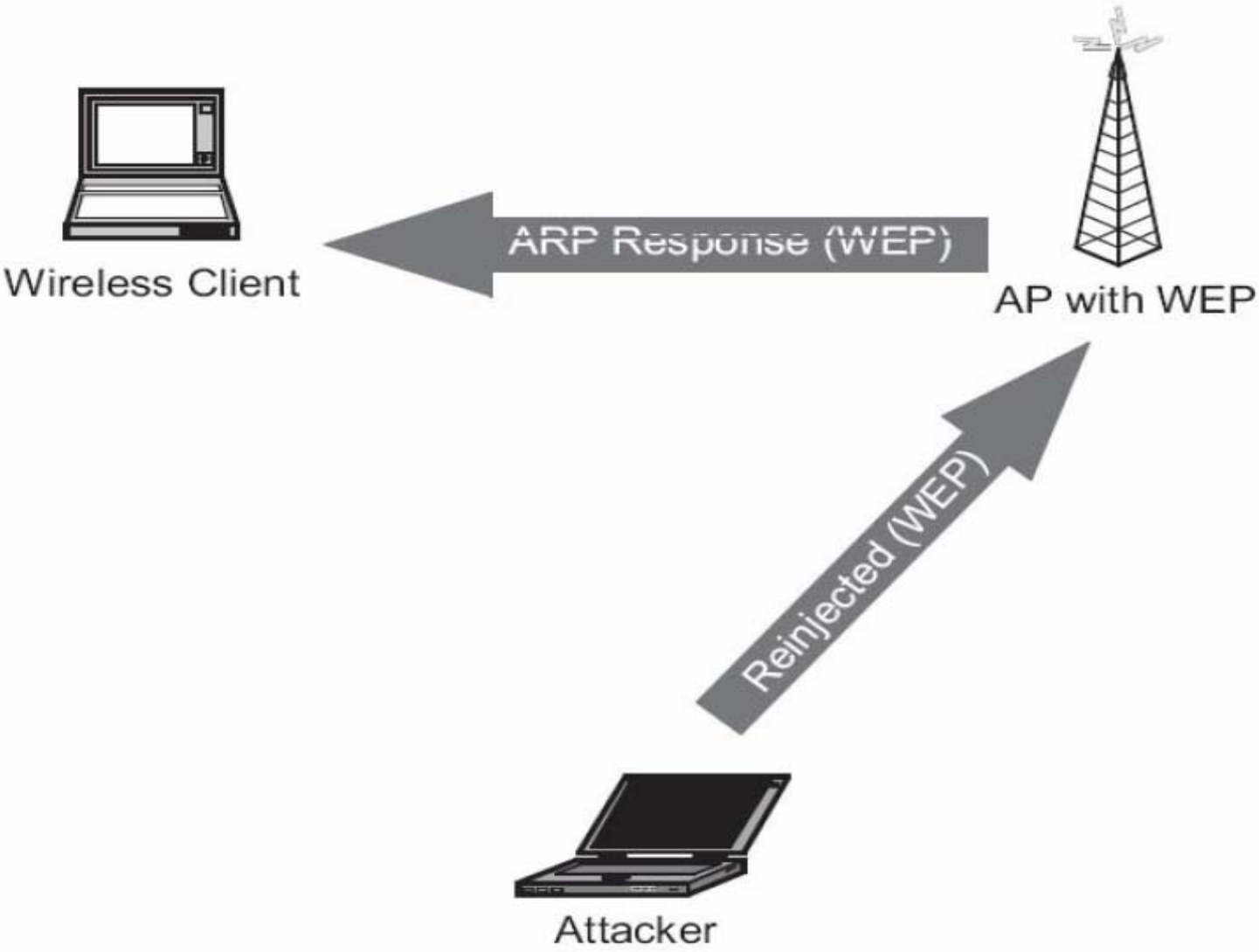
802.11 frame releases the IV information



Message Injection

- Hacker can listen to authentication process and determine a key stream for a particular IV
- Using this key stream, hacker can create packets and inject them into the network
- Collecting ARP packets (predictable size 28 bytes), and retransmitting them to AP
- WEP allows for IVs to be reused without triggering an alarm

ARP Replay Attack



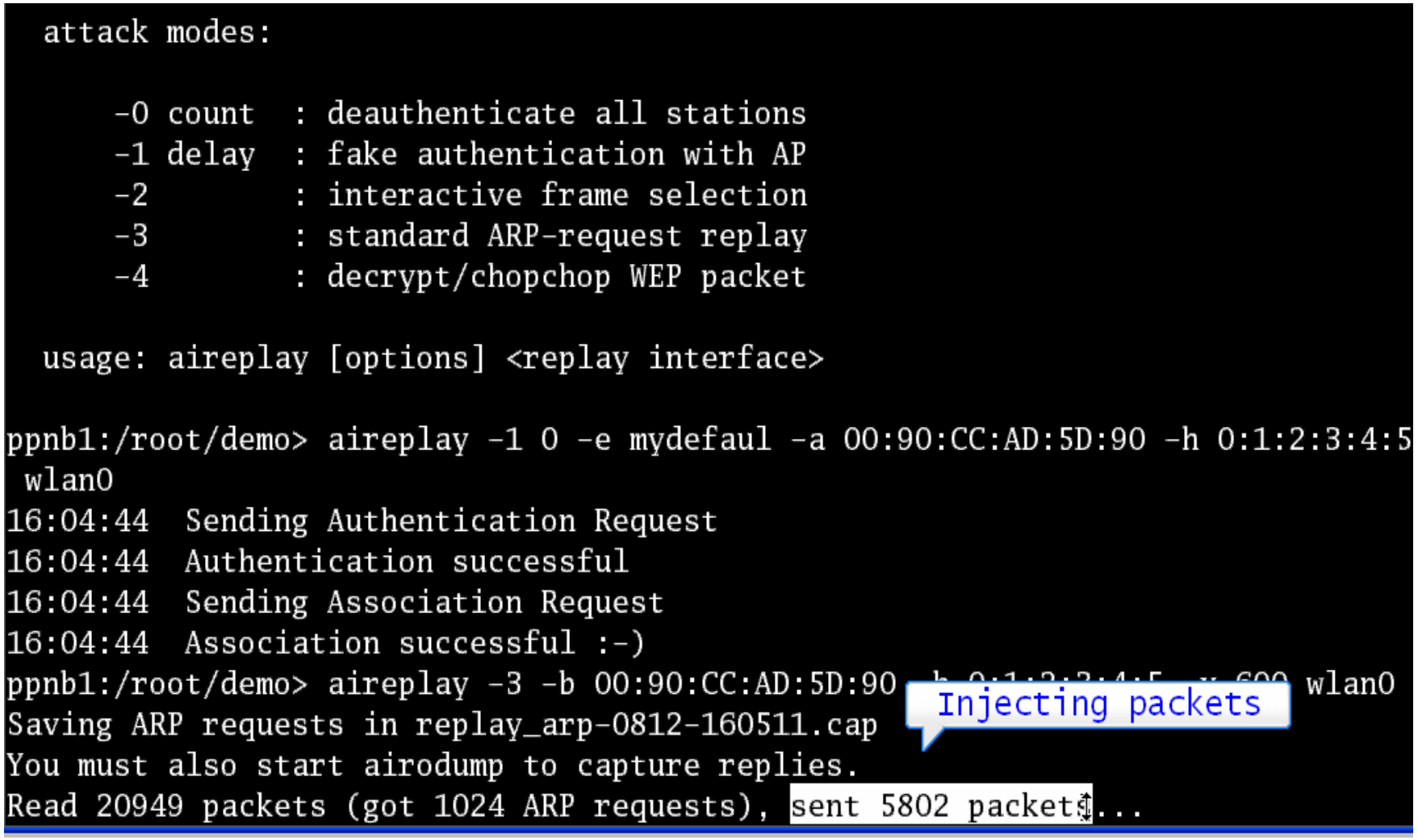
Forcing ARP packet to be generated

- Hacker sends a *deauthentication* frame to knock the client off the network and then require reauthentication.
- This process will often generate an ARP packet.
- After one or more ARP packets have been collected, they can then be retransmitted or reinjected into the network repeatedly until enough packets have been generated to supply the required number of unique IVs.

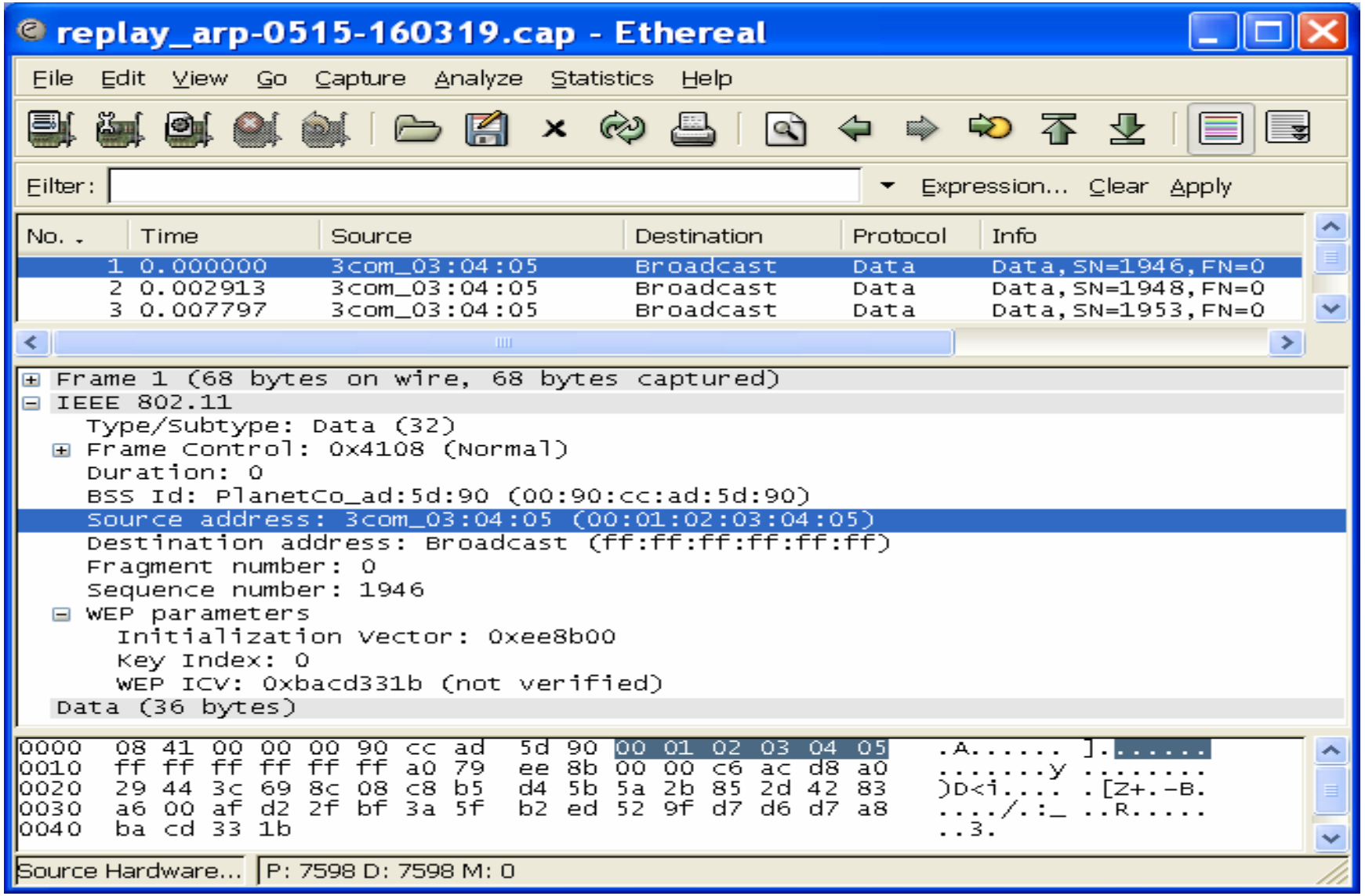
Fake authentication

- In open authentication, any client can be authenticated and associated with the access point, but the access point will drop any packets not encrypted with the correct WEP key.
- Hacker fakes an authentication and association request for a SSID with a spoofed MAC address (e.g. airplay in aircrack tool)

Packets Injection by aireplay



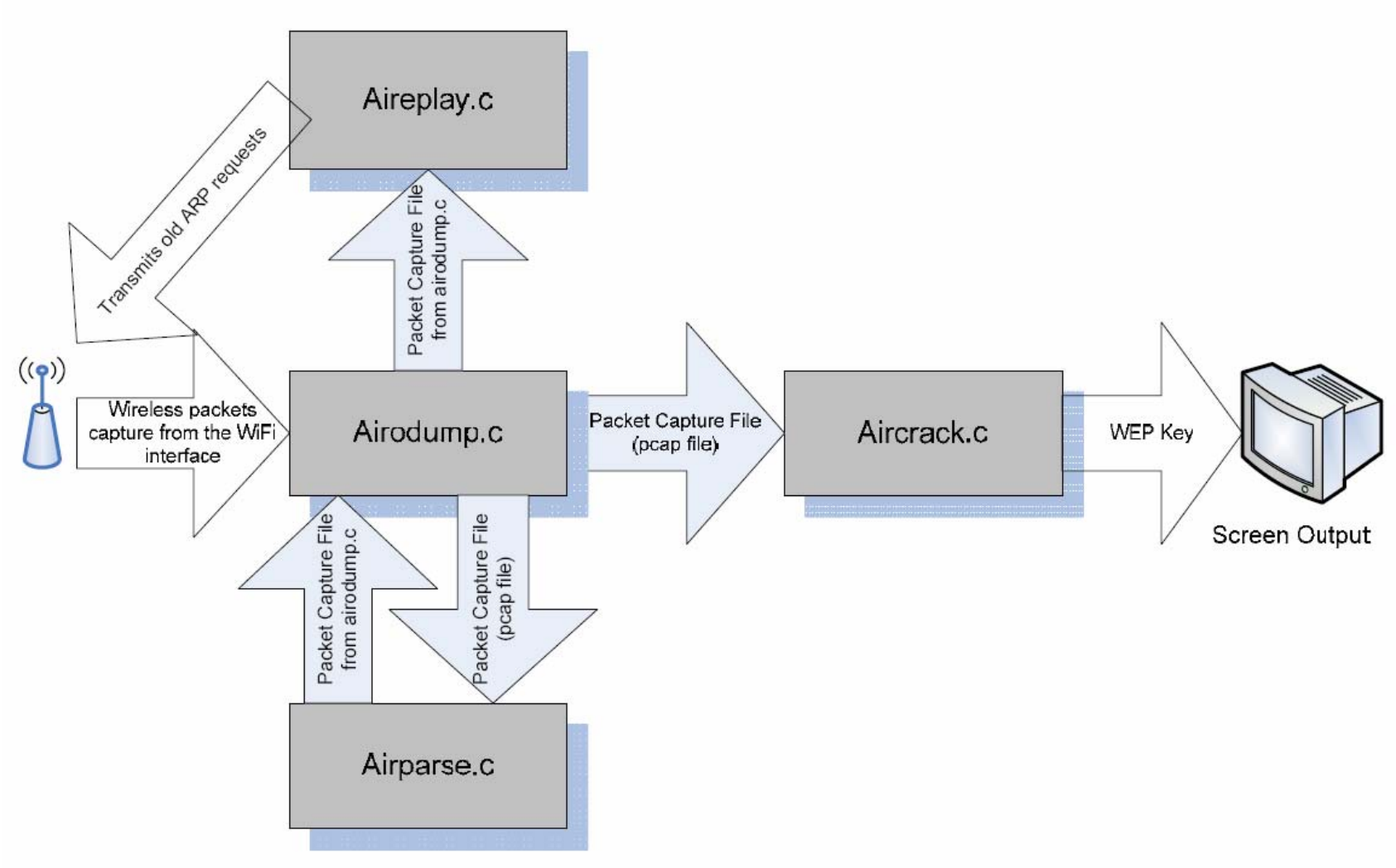
ARP Packets Replay with a spoofed MAC address



Cracking WEP with Aircrack

- Airodump collects packets
- Aircrack is used on the output file from Airodump
- It uses unique IVs to break the WEP key
- ~330,000 unique IVs and Aircrack broke the key in 1 second
- ~100,000 and it took 21 seconds

Aircrack Work Flow



WEP Crack Demo