Caffé Latte with a Free Topping of Cracked WEP

Retrieving WEP Keys From Road-Warriors

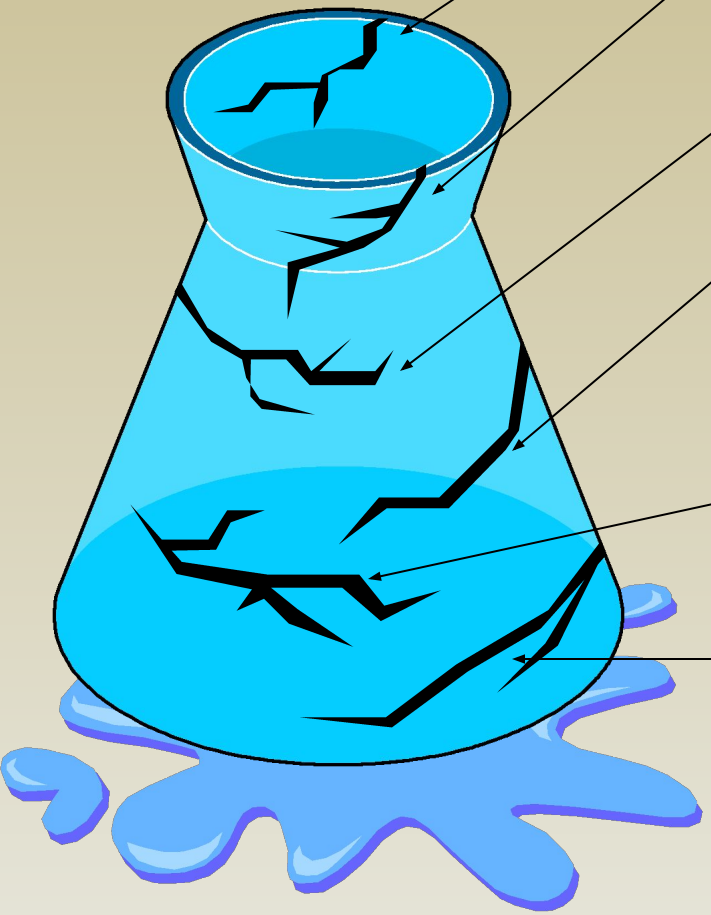
- Vivek Ramachandran
- MD Sohail Ahmad

AirTight® NETWORKS

www.airtightnetworks.net

Cracks in WEP -- Historic Evolution

IEEE WG admitted that WEP cannot hold any water. Recommended users to upgrade to WPA, WPA2



2001 - The insecurity of 802.11, Mobicom, July 2001
N. Borisov, I. Goldberg and D. Wagner.

2001 - Weaknesses in the key scheduling algorithm of RC4.
S. Fluhrer, I. Mantin, A. Shamir. Aug 2001.

2002 - Using the Fluhrer, Mantin, and Shamir Attack to Break WEP
A. Stubblefield, J. Ioannidis, A. Rubin.

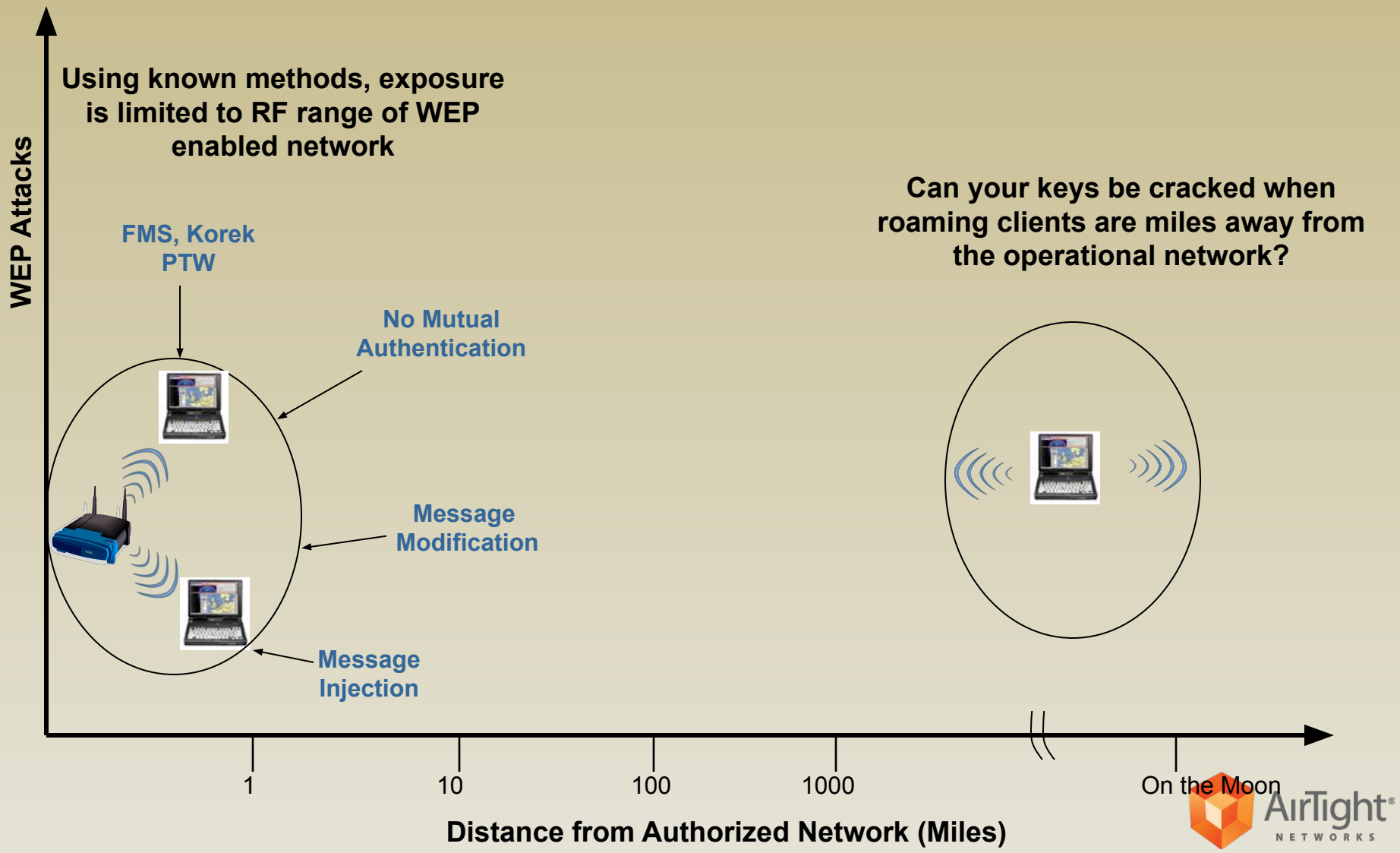
2004 – KoreK, improves on the above technique and reduces the complexity of WEP cracking. We now require only around 500,000 packets to break the WEP key.

2005 – Adreas Klein introduces more correlations between the RC4 key stream and the key.

2007 – PTW extend Andreas technique to further simplify WEP Cracking. Now with just around 60,000 – 90,000 packets it is possible to break the WEP key.

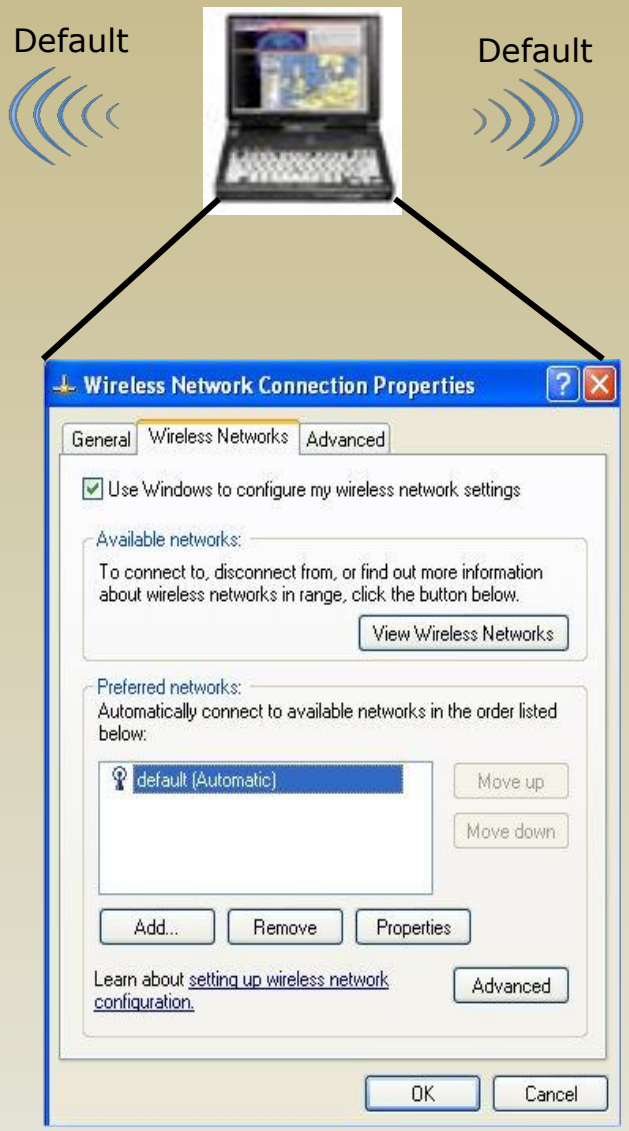
AirTight® NETWORKS

WEP Attacks – exposure area



AirTight NETWORKS

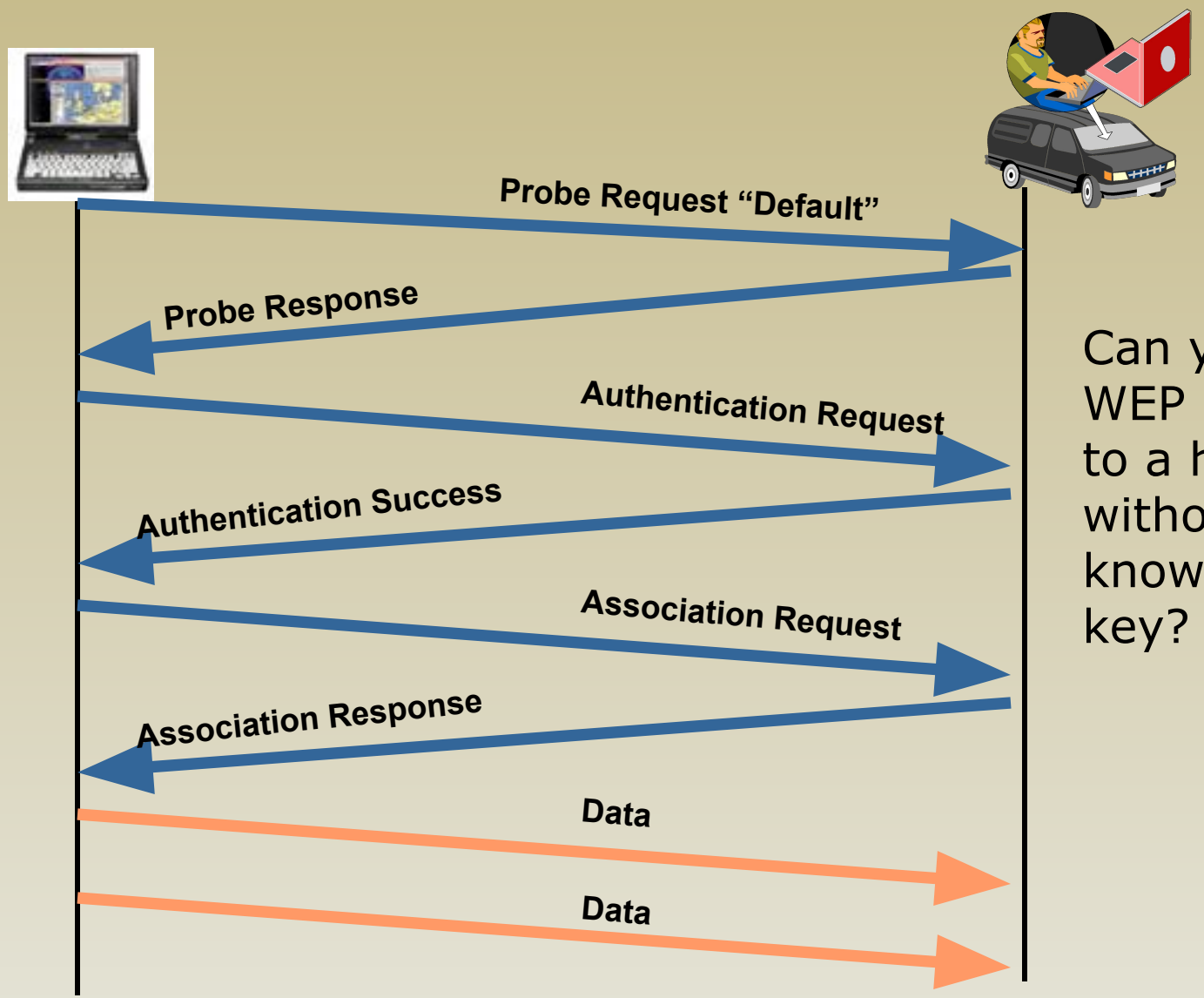
Observation #1



- Can we somehow have an isolated Client generate WEP encrypted data packets using the authorized network's key?
- Windows caches the WEP key of networks in its PNL
- To crack WEP all we need is encrypted data packets
  - 80K for PTW attack
  - 500K for KoreK attack
- It does not matter if these packets come from the AP or the Client

Airlight NETWORKS

Observation #2



Can you force a WEP client connect to a honey pot without having knowledge of the key?

AirTight NETWORKS

Caffé Latte – Attack timelines

- Every spoofed Association gives us encrypted data packets (either DHCP or ARP)
- Send a De-auth, process repeats, keep collecting the trace
- Timelines for cracking the WEP key for various network configurations assuming 500k packets is as follows:

Network Configuration	Approximate Cracking time
Shared + DHCP	3 days
Shared + Static IP	1.5 days
Open + DHCP	6 days
Open + Static IP	2 days

AirTight NETWORKS

Can we speed it up?

DAYS

HOURS

MINUTES

AirTight NETWORKS

Problem Formulation

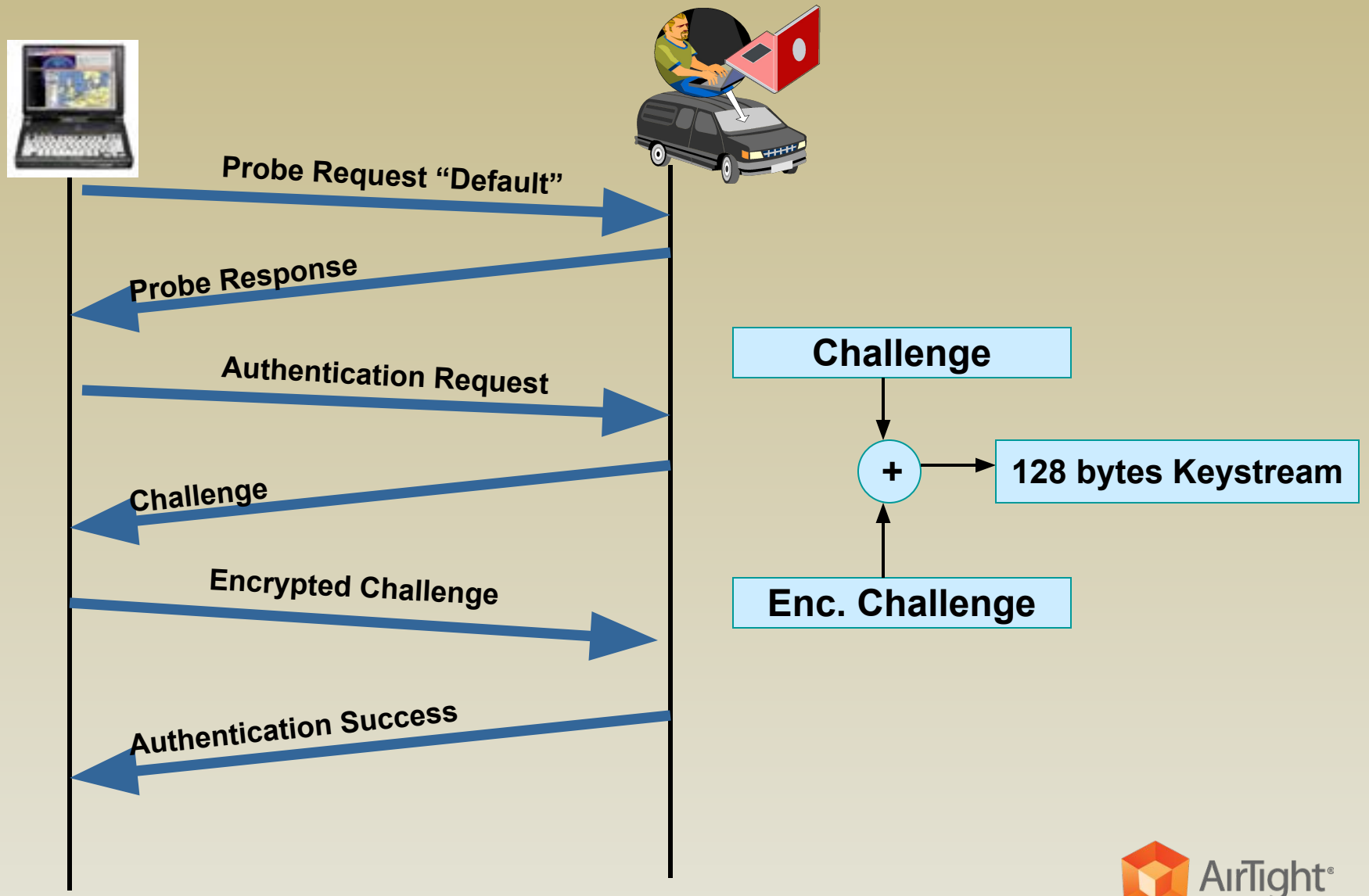
Network Configuration	Approximate Cracking time
Shared + DHCP	3 days
Shared + Static IP	1.5 days
Open + DHCP	6 days
Open + Static IP	2 days

A solution is complete **Only if**:

- Solve for all network configurations
- Key cracking should be done by the time a user finishes sipping a cup of coffee

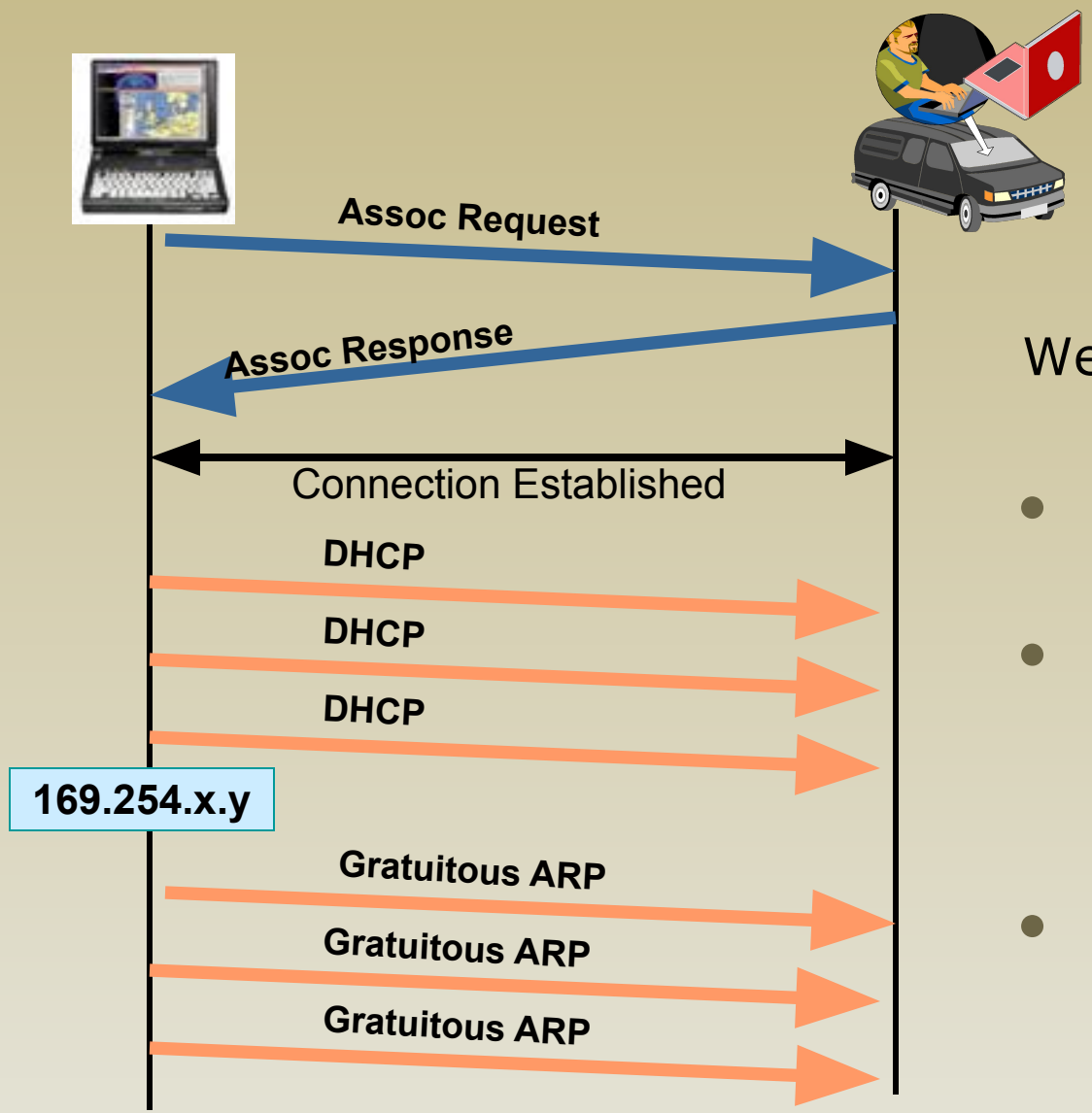
AirTight® NETWORKS

Caffé latte – Shared + DHCP



AirTight NETWORKS

Caffe latte – Shared + DHCP (2)

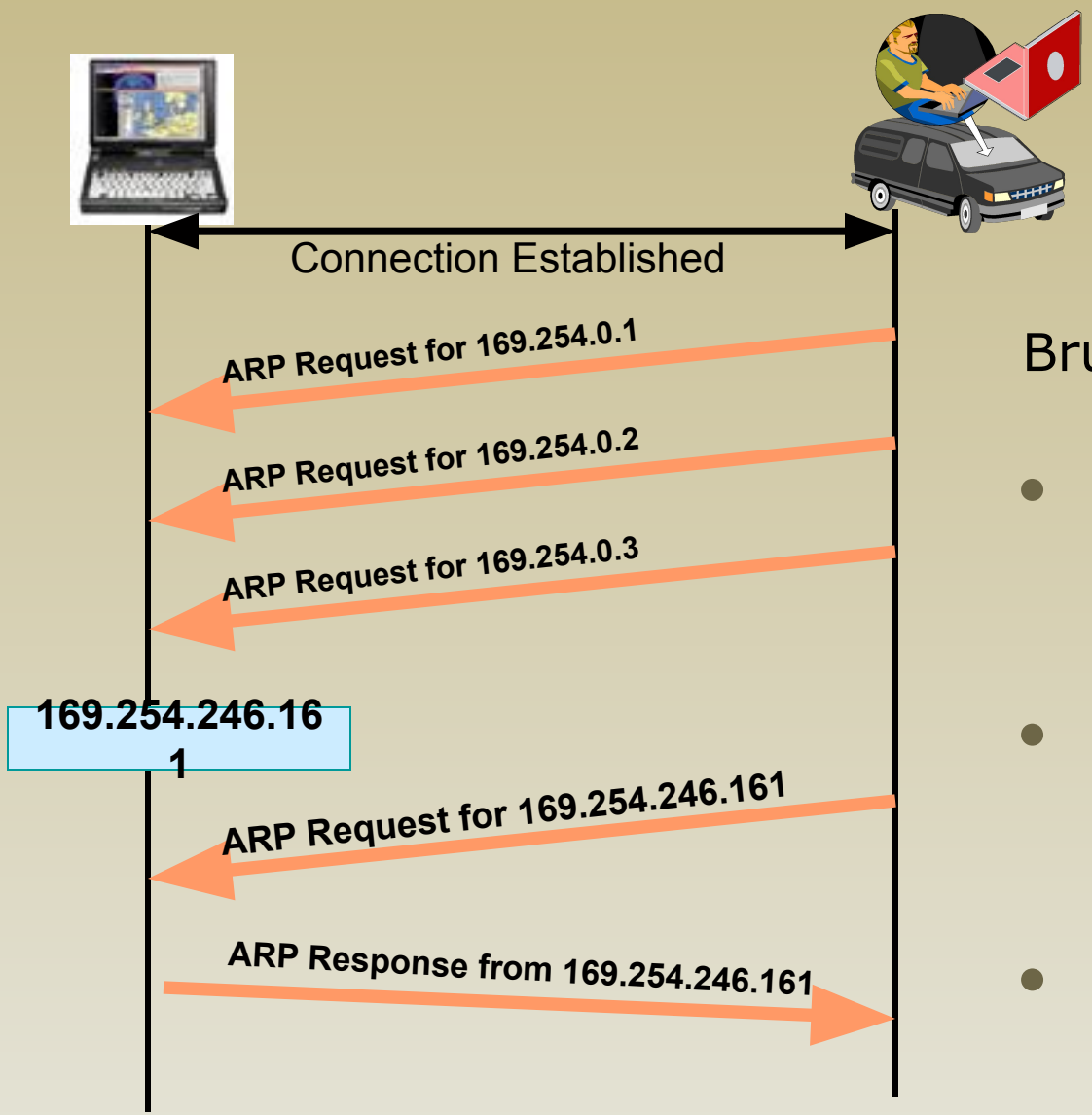


We now have:

- 128 bytes of keystream
- Client IP is somewhere between 169.254.0.0 – 169.254.255.255
- Can we find the Client IP?

AirTight NETWORKS

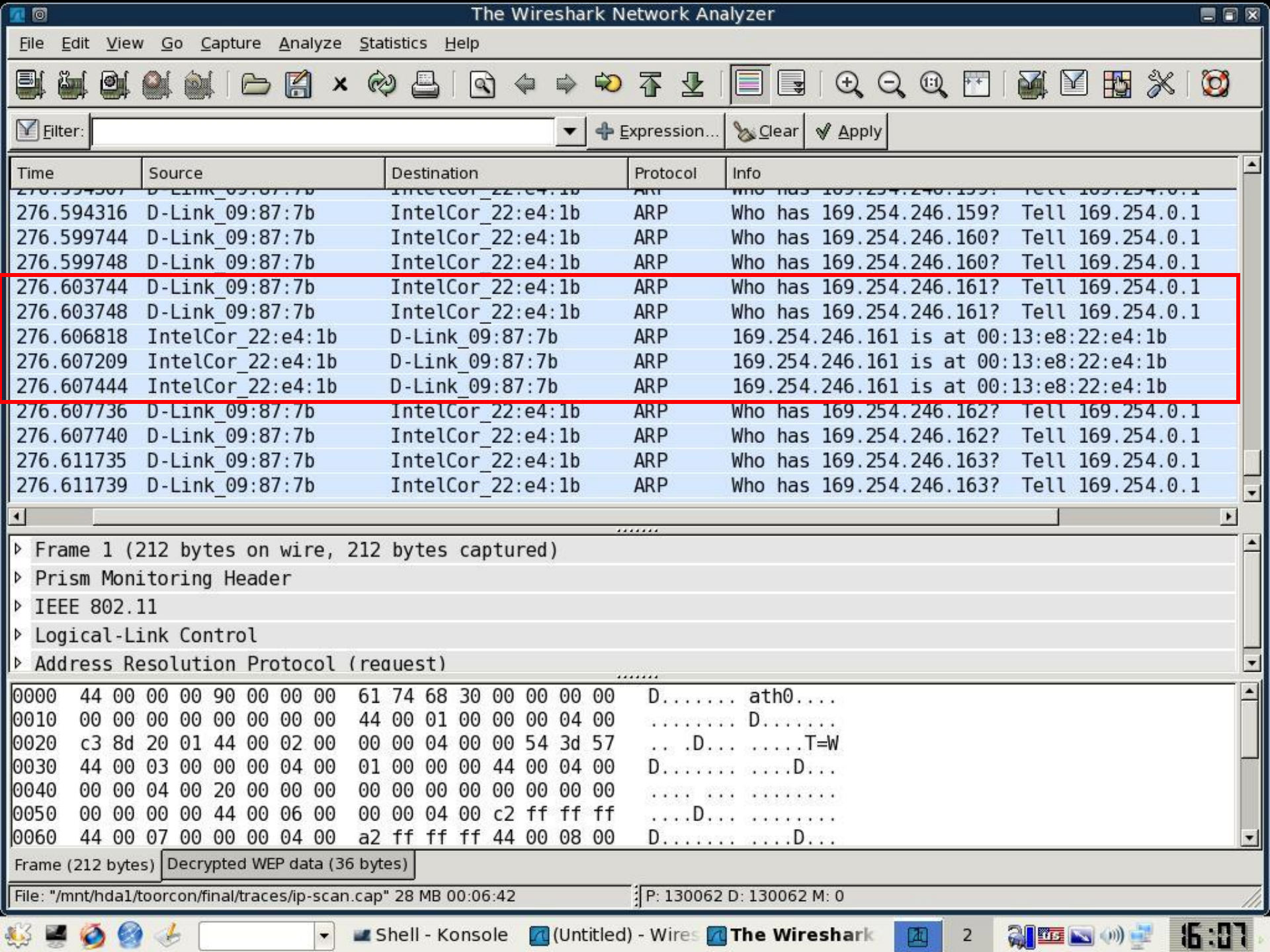
Caffe latte – Shared + DHCP (3)



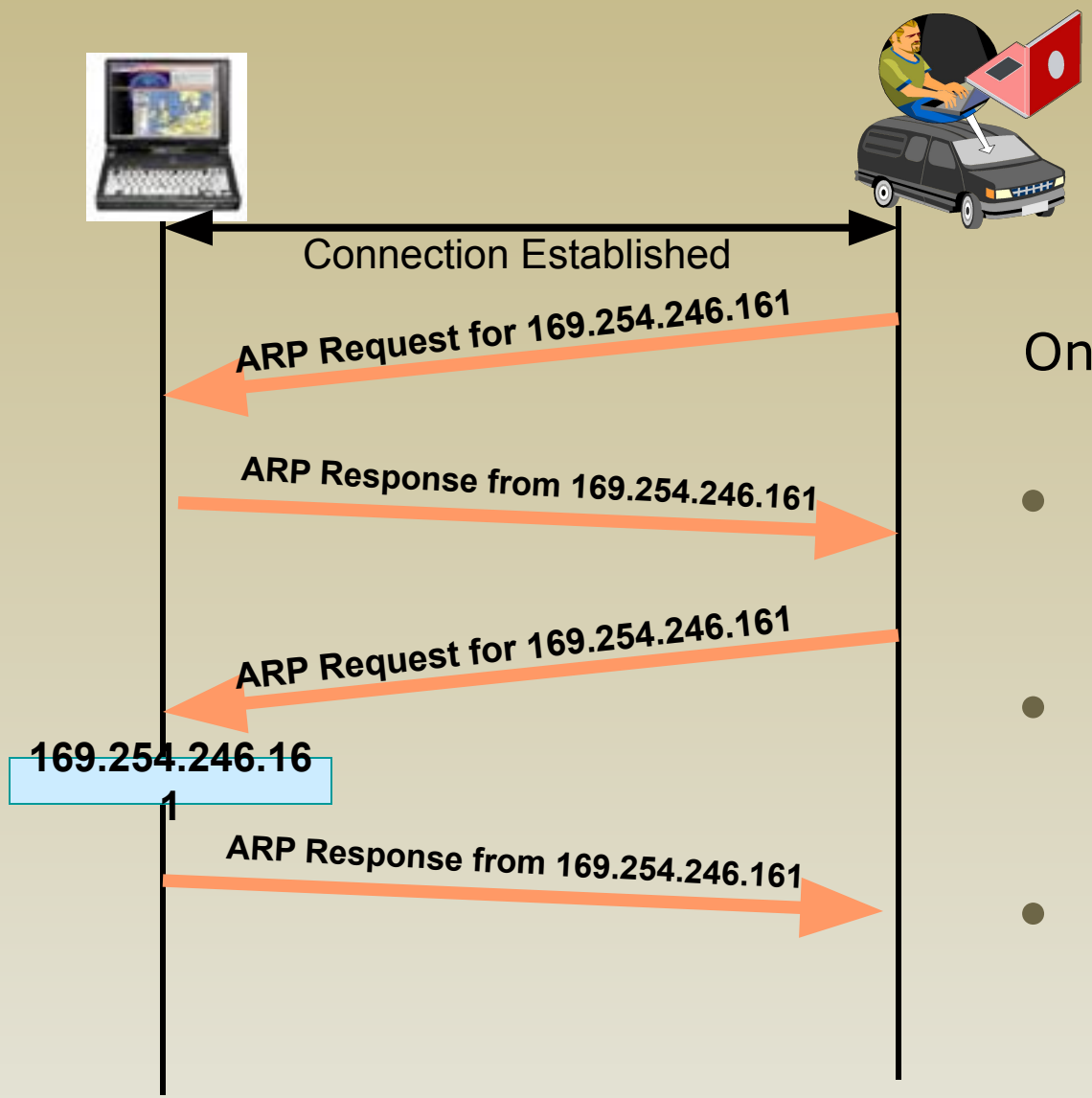
Brute force the Client IP

- 169.254.0.0 – 169.254.255.255 is ~65,000 space
- ARP Request on wireless is 40 bytes (LLC + ARP +ICV)
- We have a 128 byte key stream from the previous step

AirTight NETWORKS


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
Time Source Destination Protocol Info
276.594316 D-Link_09:87:7b IntelCor_22:e4:1b ARP Who has 169.254.246.159? Tell 169.254.0.1
276.599744 D-Link_09:87:7b IntelCor_22:e4:1b ARP Who has 169.254.246.160? Tell 169.254.0.1
276.599748 D-Link_09:87:7b IntelCor_22:e4:1b ARP Who has 169.254.246.160? Tell 169.254.0.1
276.603744 D-Link_09:87:7b IntelCor_22:e4:1b ARP Who has 169.254.246.161? Tell 169.254.0.1
276.603748 D-Link_09:87:7b IntelCor_22:e4:1b ARP Who has 169.254.246.161? Tell 169.254.0.1
276.606818 IntelCor_22:e4:1b D-Link_09:87:7b ARP 169.254.246.161 is at 00:13:e8:22:e4:1b
276.607209 IntelCor_22:e4:1b D-Link_09:87:7b ARP 169.254.246.161 is at 00:13:e8:22:e4:1b
276.607444 IntelCor_22:e4:1b D-Link_09:87:7b ARP 169.254.246.161 is at 00:13:e8:22:e4:1b
276.607736 D-Link_09:87:7b IntelCor_22:e4:1b ARP Who has 169.254.246.162? Tell 169.254.0.1
276.607740 D-Link_09:87:7b IntelCor_22:e4:1b ARP Who has 169.254.246.162? Tell 169.254.0.1
276.611735 D-Link_09:87:7b IntelCor_22:e4:1b ARP Who has 169.254.246.163? Tell 169.254.0.1
276.611739 D-Link_09:87:7b IntelCor_22:e4:1b ARP Who has 169.254.246.163? Tell 169.254.0.1
Frame 1 (212 bytes on wire, 212 bytes captured)
Prism Monitoring Header
IEEE 802.11
Logical-Link Control
Address Resolution Protocol (request)
0000 44 00 00 00 90 00 00 00 61 74 68 30 00 00 00 00 D....... ath0....
0010 00 00 00 00 00 00 00 00 44 00 01 00 00 00 04 00 .... D.......
0020 c3 8d 20 01 44 00 02 00 00 00 04 00 00 54 3d 57 .. .D... .....T=W
0030 44 00 03 00 00 00 04 00 01 00 00 00 44 00 04 00 D....... ....D...
0040 00 00 04 00 20 00 00 00 00 00 00 00 00 00 00 00 ....
0050 00 00 00 00 44 00 06 00 00 00 04 00 c2 ff ff ff ....D... ....
0060 44 00 07 00 00 00 04 00 a2 ff ff ff 44 00 08 00 D....... ....D...
Frame (212 bytes)
Decrypted WEP data (36 bytes)
File: "/mnt/hda1/toorcon/final/traces/ip-scan.cap" 28 MB 00:06:42
P: 130062 D: 130062 M: 0
Shell - Konsole
(Untitled) - Wires
The Wireshark
2
16:07

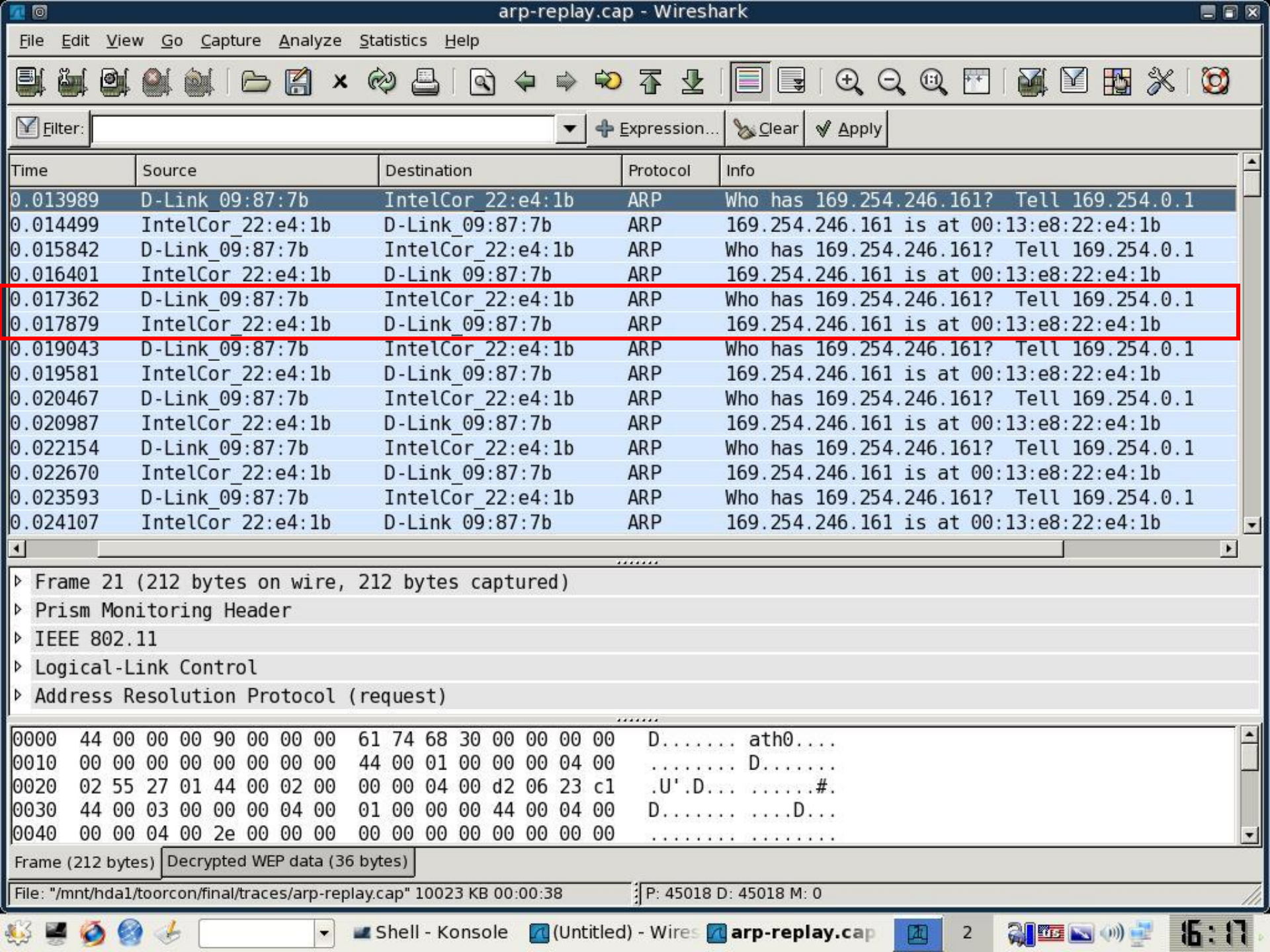
Caffe latte – Shared + DHCP (4)



Once the Client IP is known

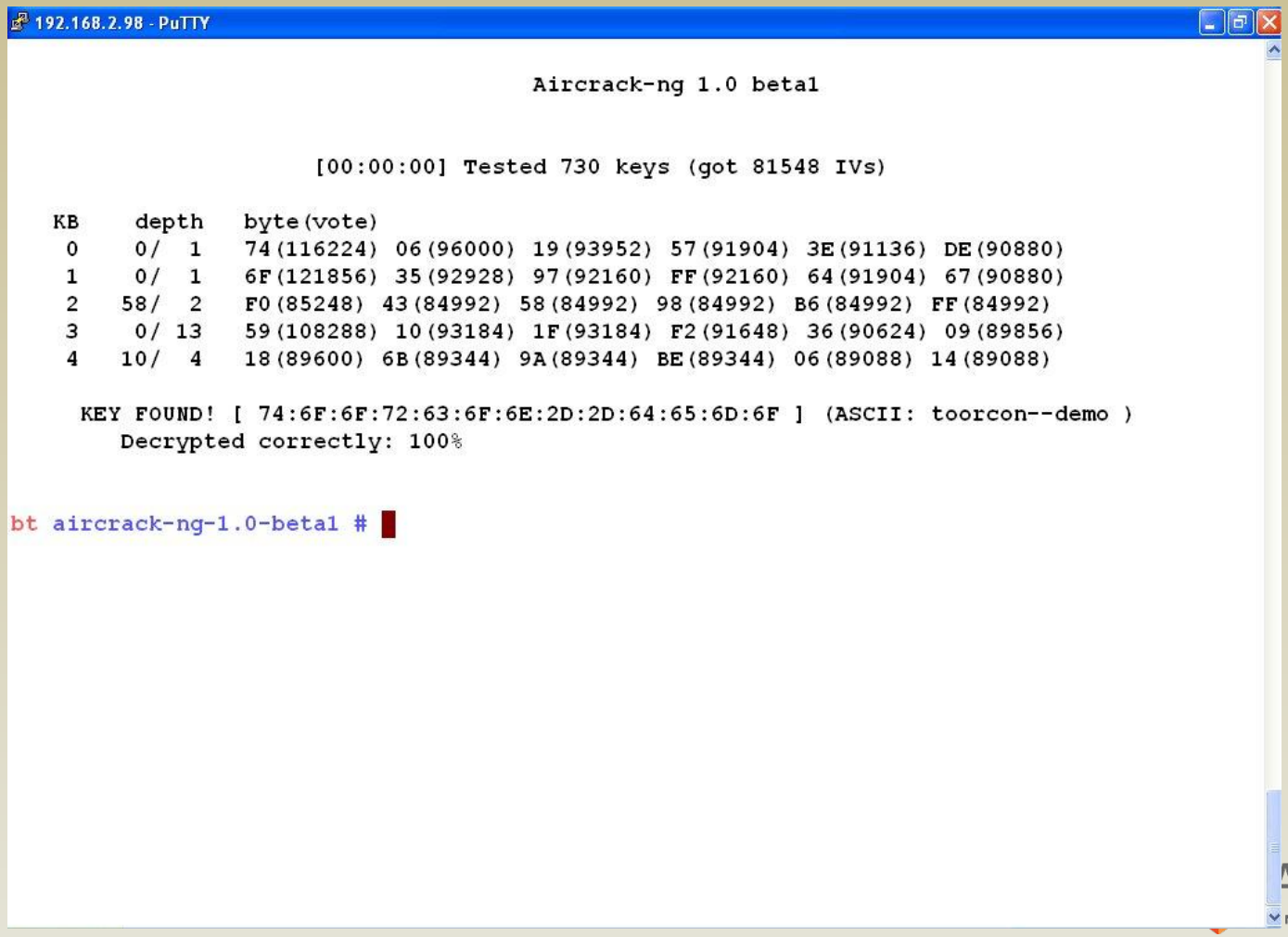
- Send a flood of ARP Requests
- Client will reply back with ARP Responses
- Start trace collection and run the PTW attack ☺

AirTight NETWORKS


arp-replay.cap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
Time Source Destination Protocol Info
0.013989 D-Link_09:87:7b IntelCor_22:e4:1b ARP Who has 169.254.246.161? Tell 169.254.0.1
0.014499 IntelCor_22:e4:1b D-Link_09:87:7b ARP 169.254.246.161 is at 00:13:e8:22:e4:1b
0.015842 D-Link_09:87:7b IntelCor_22:e4:1b ARP Who has 169.254.246.161? Tell 169.254.0.1
0.016401 IntelCor_22:e4:1b D-Link_09:87:7b ARP 169.254.246.161 is at 00:13:e8:22:e4:1b
0.017362 D-Link_09:87:7b IntelCor_22:e4:1b ARP Who has 169.254.246.161? Tell 169.254.0.1
0.017879 IntelCor_22:e4:1b D-Link_09:87:7b ARP 169.254.246.161 is at 00:13:e8:22:e4:1b
0.019043 D-Link_09:87:7b IntelCor_22:e4:1b ARP Who has 169.254.246.161? Tell 169.254.0.1
0.019581 IntelCor_22:e4:1b D-Link_09:87:7b ARP 169.254.246.161 is at 00:13:e8:22:e4:1b
0.020467 D-Link_09:87:7b IntelCor_22:e4:1b ARP Who has 169.254.246.161? Tell 169.254.0.1
0.020987 IntelCor_22:e4:1b D-Link_09:87:7b ARP 169.254.246.161 is at 00:13:e8:22:e4:1b
0.022154 D-Link_09:87:7b IntelCor_22:e4:1b ARP Who has 169.254.246.161? Tell 169.254.0.1
0.022670 IntelCor_22:e4:1b D-Link_09:87:7b ARP 169.254.246.161 is at 00:13:e8:22:e4:1b
0.023593 D-Link_09:87:7b IntelCor_22:e4:1b ARP Who has 169.254.246.161? Tell 169.254.0.1
0.024107 IntelCor_22:e4:1b D-Link_09:87:7b ARP 169.254.246.161 is at 00:13:e8:22:e4:1b
Frame 21 (212 bytes on wire, 212 bytes captured)
Prism Monitoring Header
IEEE 802.11
Logical-Link Control
Address Resolution Protocol (request)
0000 44 00 00 00 90 00 00 00 61 74 68 30 00 00 00 00 D....... ath0....
0010 00 00 00 00 00 00 00 00 44 00 01 00 00 00 04 00 .... D.......
0020 02 55 27 01 44 00 02 00 00 00 04 00 d2 06 23 c1 .U'.D... ......#.
0030 44 00 03 00 00 00 04 00 01 00 00 00 44 00 04 00 D....... ....D...
0040 00 00 04 00 2e 00 00 00 00 00 00 00 00 00 00 00 ....
Frame (212 bytes) Decrypted WEP data (36 bytes)
File: "/mnt/hda1/toorcon/final/traces/arp-replay.cap" 10023 KB 00:00:38
P: 45018 D: 45018 M: 0
Shell - Konsole (Untitled) - Wires arp-replay.cap 2 16:17

Caffé latte – Shared + DHCP (5)

- Once we have around 80,000 ARP Response packets: ☺ ☺ ☺



AirTight NETWORKS

Caffé Latte for Shared Auth + DHCP - Analysis

- Client IP Discovery phase: 3-4 minutes (send 2 packets for each IP)
- ARP Request/Response Flood: 4-5 minutes (to get around 80,000 packets)
- Key cracking with Aircrack-ng: ~1 minute

Can this technique be used for the other configurations as well?

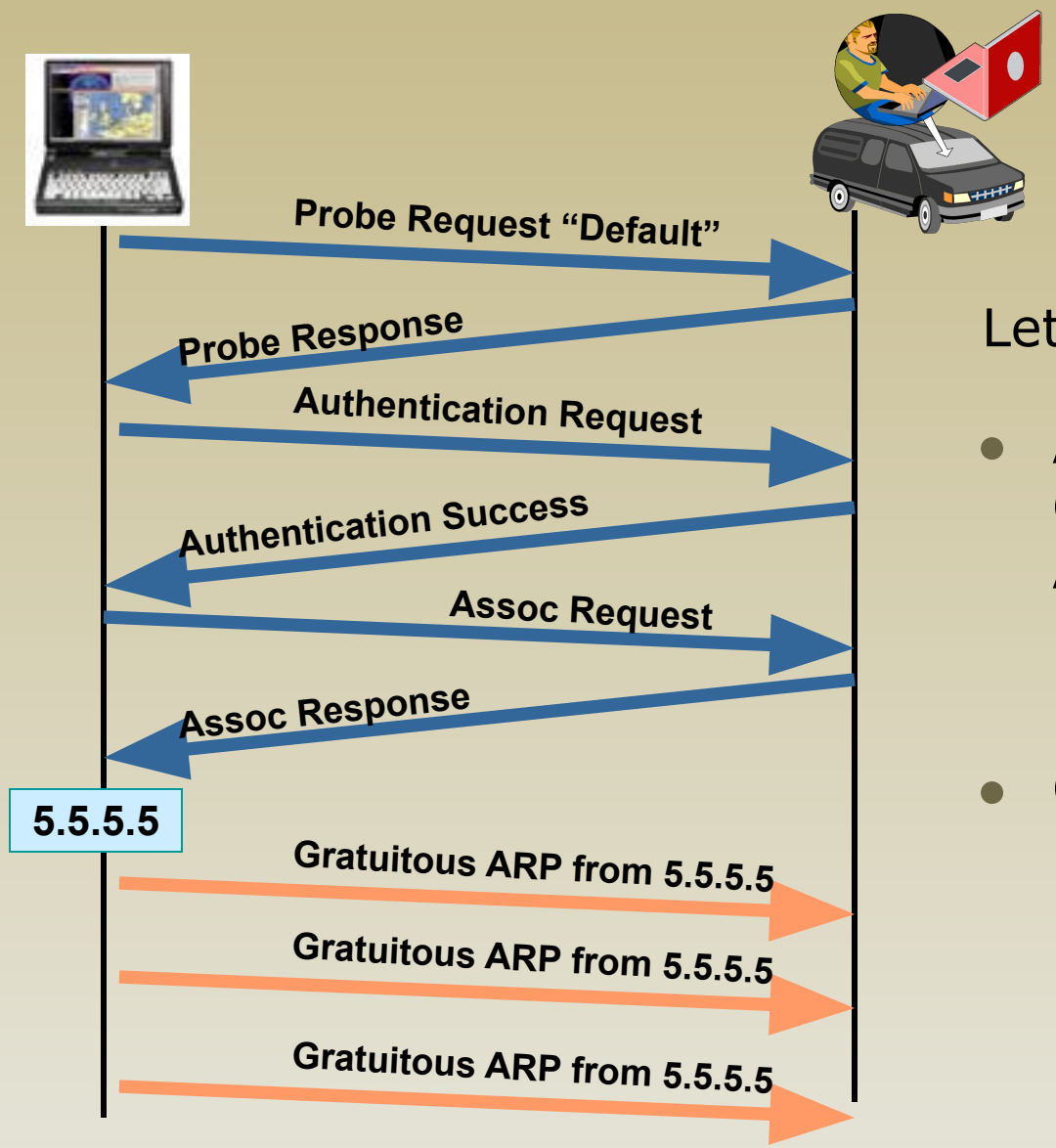
Network Configuration	Approximate Cracking time
Shared + DHCP	~ 10 mins
Shared + Static IP	1.5 days
Open + DHCP	6 days
Open + Static IP	2 days

Is there a more general solution to the problem ?

Lets look at the Open + Static IP case

AirTight NETWORKS

Caffé latte – Open + Static IP



Lets say Client IP is 5.5.5.5

- After Association, the Client sends Gratuitous ARP for 5.5.5.5

- Can we use this ARP packet somehow?

AirTight NETWORKS

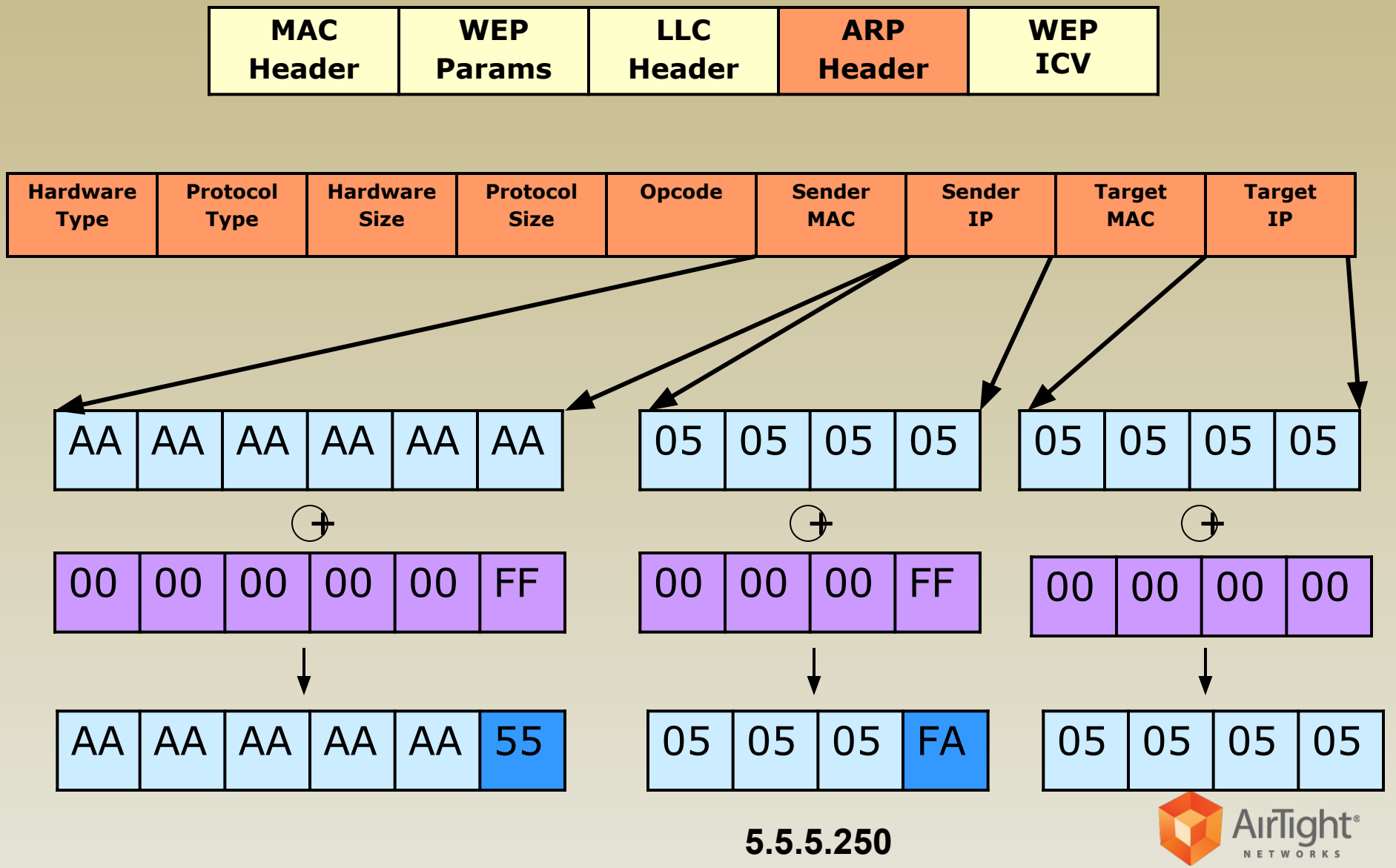
Using flaws in WEP – Message Modification and Message Replay

$$
\begin{aligned}
C' &= C \oplus \langle \Delta, c(\Delta) \rangle \\
&= \mathrm{RC4}(v,k) \oplus \langle M, c(M) \rangle \oplus \langle \Delta, c(\Delta) \rangle \\
&= \mathrm{RC4}(v,k) \oplus \langle M \oplus \Delta, c(M) \oplus c(\Delta) \rangle \\
&= \mathrm{RC4}(v,k) \oplus \langle M', c(M \oplus \Delta) \rangle \\
&= \mathrm{RC4}(v,k) \oplus \langle M', c(M') \rangle .
\end{aligned}
$$

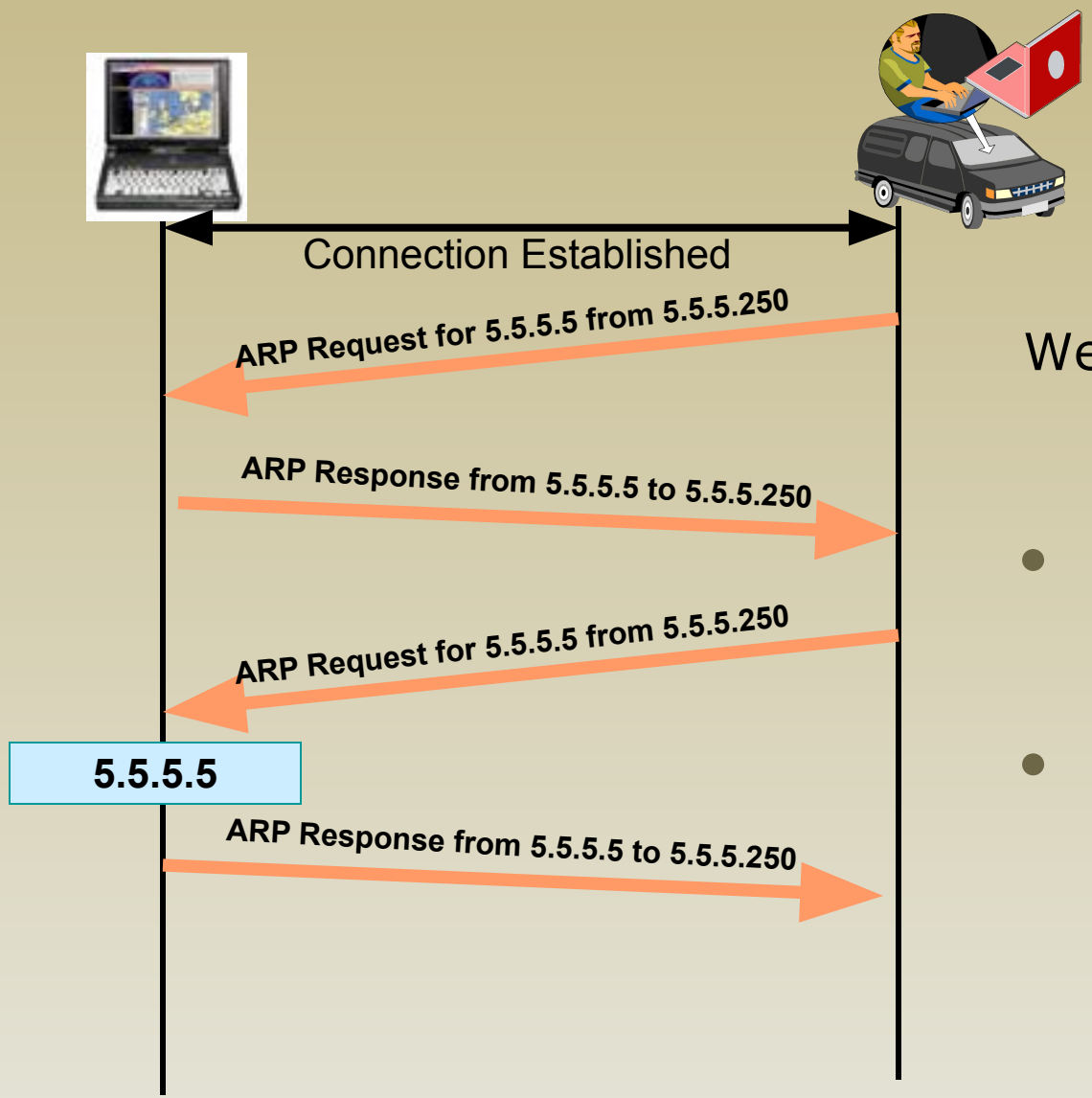
- First mention in "Intercepting Mobile Communication: The Insecurity of 802.11" – Nikita, Ian and David, UC Berkley
- It's possible to flip bits in a WEP encrypted packet and adjust the ICV to make the packet valid
- This packet can now be replayed back into the air and will be accepted by WEP devices
- Using this technique we can convert a Gratuitous ARP request into an ARP request destined for the Client coming from a different IP address

AirTight® NETWORKS

Applying Bit Flipping to an Encrypted ARP packet



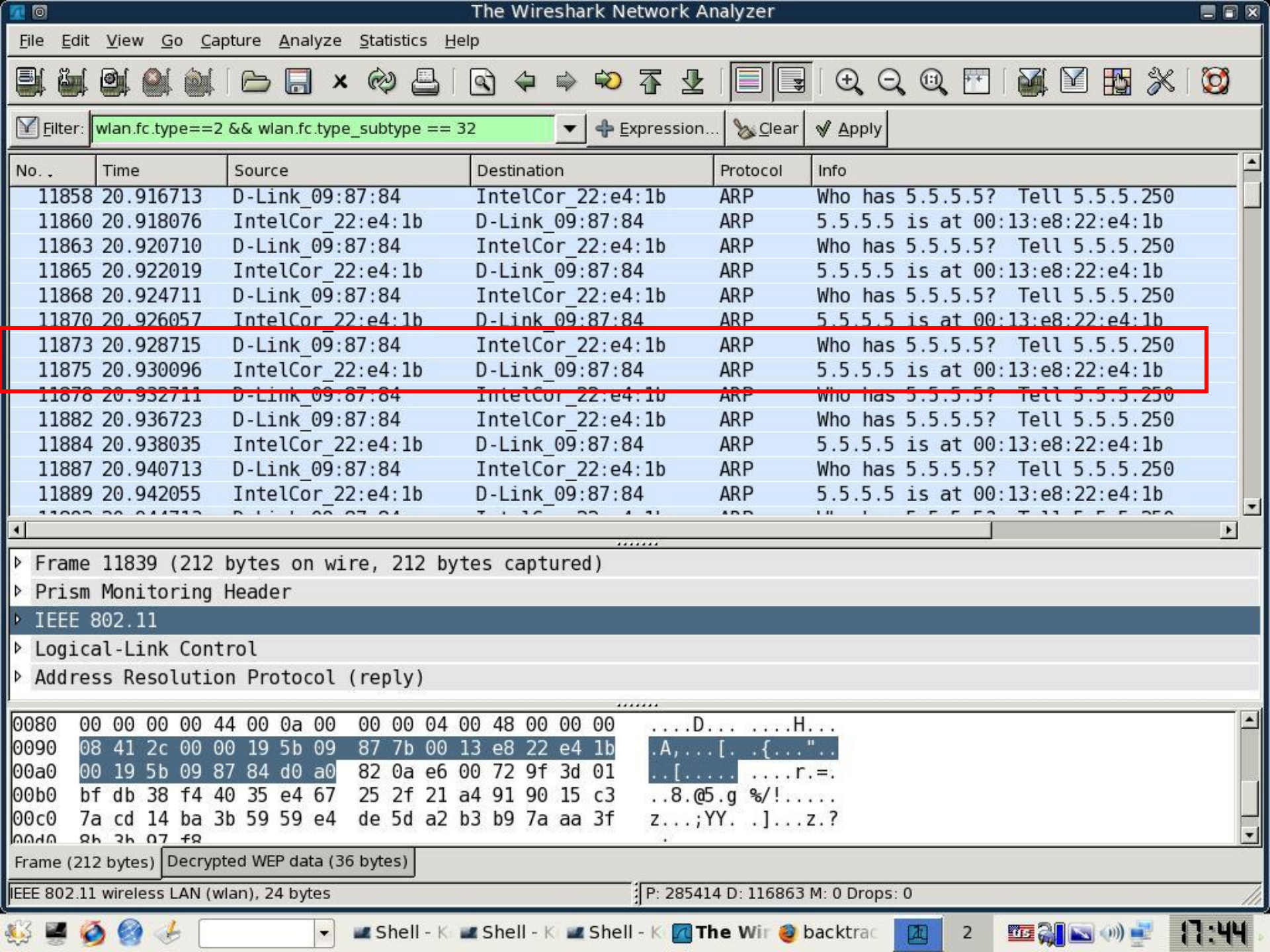
Caffe latte – Open + Static IP (2)



We send this bit flipped ARP packet to the Client

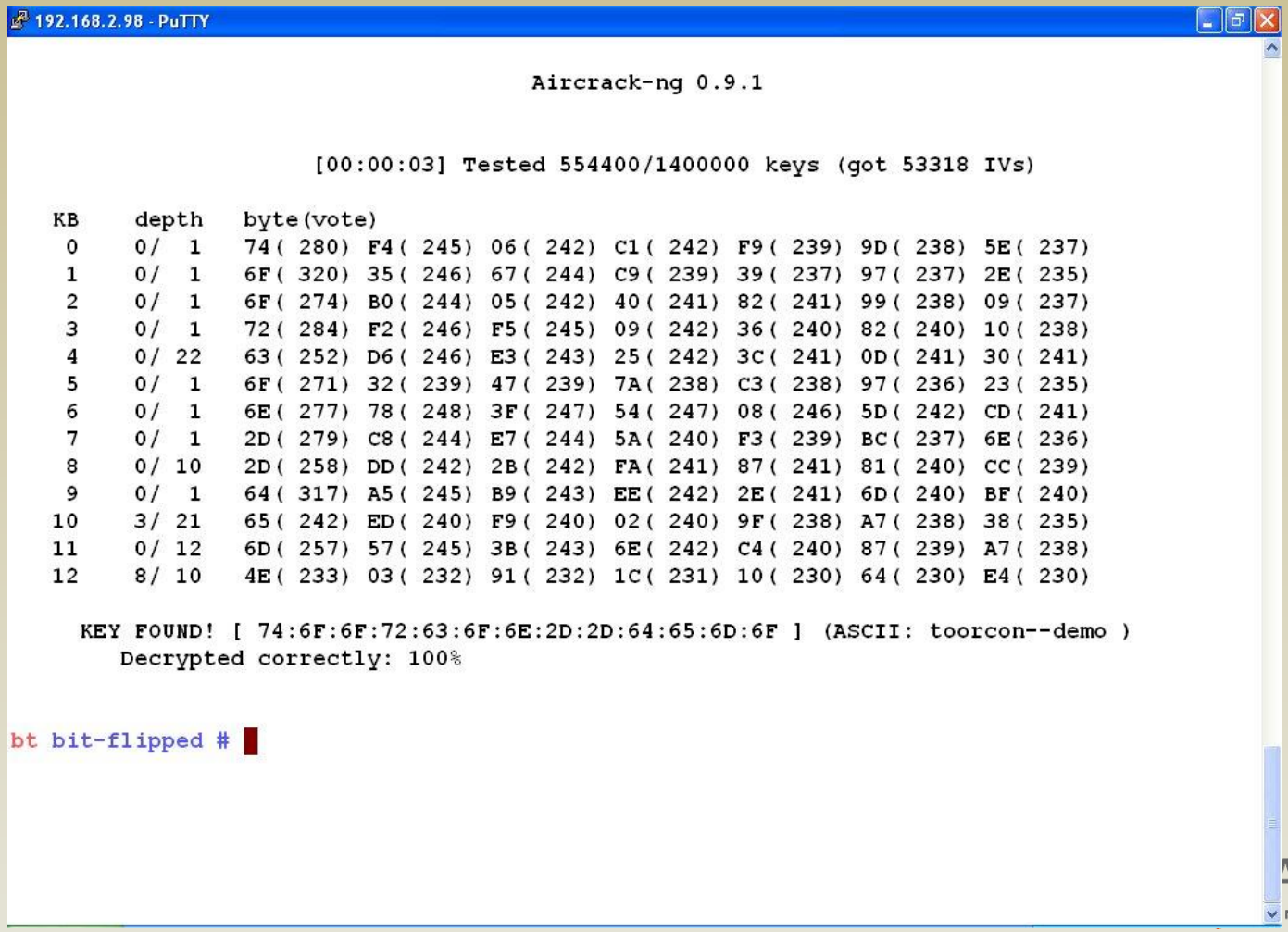
- We don't really care what the bit flipped IP was ☺
- Collect the ARP responses and fire up Aircrack-ng ☺

AirTight NETWORKS


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Help
Filter: wlan.fc.type==2 && wlan.fc.type_subtype == 32
Expression... Clear Apply
No. Time Source Destination Protocol Info
11858 20.916713 D-Link_09:87:84 IntelCor_22:e4:1b ARP Who has 5.5.5.5? Tell 5.5.5.250
11860 20.918076 IntelCor_22:e4:1b D-Link_09:87:84 ARP 5.5.5.5 is at 00:13:e8:22:e4:1b
11863 20.920710 D-Link_09:87:84 IntelCor_22:e4:1b ARP Who has 5.5.5.5? Tell 5.5.5.250
11865 20.922019 IntelCor_22:e4:1b D-Link_09:87:84 ARP 5.5.5.5 is at 00:13:e8:22:e4:1b
11868 20.924711 D-Link_09:87:84 IntelCor_22:e4:1b ARP Who has 5.5.5.5? Tell 5.5.5.250
11870 20.926057 IntelCor_22:e4:1b D-Link_09:87:84 ARP 5.5.5.5 is at 00:13:e8:22:e4:1b
11873 20.928715 D-Link_09:87:84 IntelCor_22:e4:1b ARP Who has 5.5.5.5? Tell 5.5.5.250
11875 20.930096 IntelCor_22:e4:1b D-Link_09:87:84 ARP 5.5.5.5 is at 00:13:e8:22:e4:1b
11878 20.932711 D-Link_09:87:84 IntelCor_22:e4:1b ARP Who has 5.5.5.5? Tell 5.5.5.250
11882 20.936723 D-Link_09:87:84 IntelCor_22:e4:1b ARP Who has 5.5.5.5? Tell 5.5.5.250
11884 20.938035 IntelCor_22:e4:1b D-Link_09:87:84 ARP 5.5.5.5 is at 00:13:e8:22:e4:1b
11887 20.940713 D-Link_09:87:84 IntelCor_22:e4:1b ARP Who has 5.5.5.5? Tell 5.5.5.250
11889 20.942055 IntelCor_22:e4:1b D-Link_09:87:84 ARP 5.5.5.5 is at 00:13:e8:22:e4:1b
Frame 11839 (212 bytes on wire, 212 bytes captured)
Prism Monitoring Header
IEEE 802.11
Logical-Link Control
Address Resolution Protocol (reply)
0080 00 00 00 00 44 00 0a 00 00 00 04 00 48 00 00 00 ....D... ....H...
0090 08 41 2c 00 00 19 5b 09 87 7b 00 13 e8 22 e4 1b .A,...[. .{..."..
00a0 00 19 5b 09 87 84 d0 a0 82 0a e6 00 72 9f 3d 01 ..[..... ....r.=.
00b0 bf db 38 f4 40 35 e4 67 25 2f 21 a4 91 90 15 c3 ..8.@5.g %/!.....
00c0 7a cd 14 ba 3b 59 59 e4 de 5d a2 b3 b9 7a aa 3f z...;YY. .]...z.?
Frame (212 bytes)
Decrypted WEP data (36 bytes)
IEEE 802.11 wireless LAN (wlan), 24 bytes
P: 285414 D: 116863 M: 0 Drops: 0
Shell - K
Shell - K
Shell - K
The Wir
backtrac
2
17:44

Caffé latte – Open + Static IP (3)

- Once we have around 60,000 ARP Response packets: ☺ ☺ ☺



AirTight NETWORKS

Caffé Latte for Open + Static IP - Analysis

- Capturing an ARP packet and bit flipping it: ~1 msec ☺
- ARP Request/Response Flood: 4-5 minutes (to get around 80,000 packets)
- Key cracking with Aircrack-ng: ~1 minute

Bit Flipping works for all the cases

Network Configuration	Approximate Cracking time
Shared + DHCP	~ 6 minutes
Shared + Static IP	~ 6 minutes
Open + DHCP	~ 6 minutes
Open + Static IP	~ 6 minutes

Implications of Caffé Latte

Risk is higher than previously perceived:

- WEP keys can now be cracked remotely, putting your enterprise at risk
- WEP Honey-pots are now possible

Few hours before our talk we came to know that a tool WEPOff had taken a stab at attacking isolated clients using a different technique (fragmentation) and only for a limited set of network configurations (DHCP). Also due to the nature of the fragmentation attack, it has to send 9 times the number of packets.

http://www.darknet.org.uk/2007/01/wep0ff-wireless-wep-key-cracker-tool/

Advisory

- Yet another reason to upgrade to WPA/WPA2
- Road warriors need to be careful even more now:
  - Exercise caution when using public hotspots
  - Upgrade your wireless drivers regularly
  - Switch off wireless when not in use
  - …
  - …

  Too many best practices to remember!

  Use a freely available wireless security agent on your laptop

- If you are using legacy WEP, do not build your enterprise defenses assuming the WEP key cannot be broken

Questions?

Vivek.Ramachandran@airtightnetworks.net

Md.Ahmad@airtightnetworks.net

Airtight Networks

www.AirTightNetworks.net

Acknowledgements: Amit Vartak

(amit.vartak@airtightnetworks.net)