

Wireless Security of Public Wi-Fi



...

CIT 460 - Wireless Security

Group 1:

Nathan Snyder, Alex Andrews, Adam Meyer, Thomas Wilson, Zach
Linderman, Keith Cornell

The Goals

Data Collection

How often are secure connections used on public Wi-Fi?

How do individuals and corporations use Public Wi-Fi?

How can it be made more secure?

What can people do to stay more secure on public Wi-Fi?

Conclusions

Class Discussion



Raspberry Pi v2 Model B



Features:

- 1 gig of ram
- 6x more powerful than previous version
- Quad-core Arm processor
- Powered from micro USB 5v
- 10/100 Ethernet
- HDMI output

Accessories:

- 7" touchscreen -- \$57
- Rii i18 touchpad 2.4ghz keyboard+Mouse -- \$22
- Anker Astro E1 5200MaH battery pack -- \$16
- Wifi Antenna 802.11 b/g/n usb adaptor
- Case for 7" screen -- \$28

Capturing more than broadcast packets with the Raspberry Pi..
Priceless

Raspberry Pi v2 model b App Installation

```
pi@raspberrypi:~$ sudo apt-get install aircrack-ng
E: Command line option 'n' from -ng is not known.
pi@raspberrypi:~$ sudo apt-get install aircrack-ng
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  iieee-data
The following NEW packages will be installed:
  aircrack-ng iieee-data
0 upgraded, 2 newly installed, 0 to remove and 134 not upgraded.
Need to get 1,222 kB of archives.
After this operation, 5,783 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://mirrordirector.raspbian.org/raspbian/ jessie/main aircrack-ng armhf
  1:1.2-0-beta3-4 [392 kB]
Get:2 http://mirrordirector.raspbian.org/raspbian/ jessie/main iieee-data all 201
  50531.1-deb8u2 [830 kB]
Fetched 1,222 kB in 2s (501 kB/s)
Selecting previously unselected package aircrack-ng.
(Reading database ... 123463 files and directories currently installed.)
Preparing to unpack .../aircrack-ng_1:1.2-0-beta3-4_armhf.deb ...
Unpacking aircrack-ng (1:1.2-0-beta3-4) ...
```

Installation of Aircrack

- Raspbian is debian based, so use 'apt-get'
- Other apps installed: tshark, nethogs, iperf

```
Setting up iperf (2.0.5+dfsg1-2) ...
pi@raspberrypi:~$ sudo apt-get install nmap
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  liblinear1 ndiff python-lxml
Suggested packages:
  liblinear-tools liblinear-dev python-lxml-dbg
The following NEW packages will be installed:
  liblinear1 ndiff nmap python-lxml
0 upgraded, 4 newly installed, 0 to remove and 1
Need to get 4,845 kB of archives.
After this operation, 20.5 MB of additional disk
Do you want to continue? [Y/n]
```

Installation of Nmap

Inspired by an article from *Network World*: <http://www.networkworld.com/article/2225683/cisco-subnet/cisco-subnet-raspberry-pi-as-a-network-monitoring-node.html>

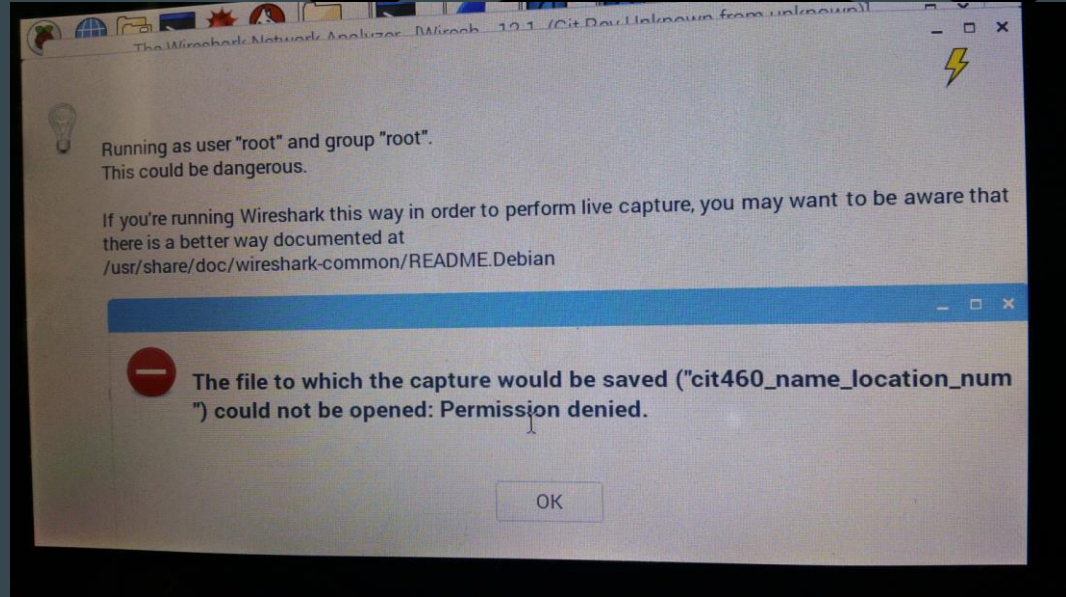
Raspberry Pi v2 model b App Installation

Things of note:

GUI gets in the way!

Must use cmd line

Needed to be self-contained



Data Collection Process

Hardware: Raspberry Pi 2 + ALFA network card

Tools: aircrack-ng suite, wireshark with tshark, macchanger

Shell script using BASH shell



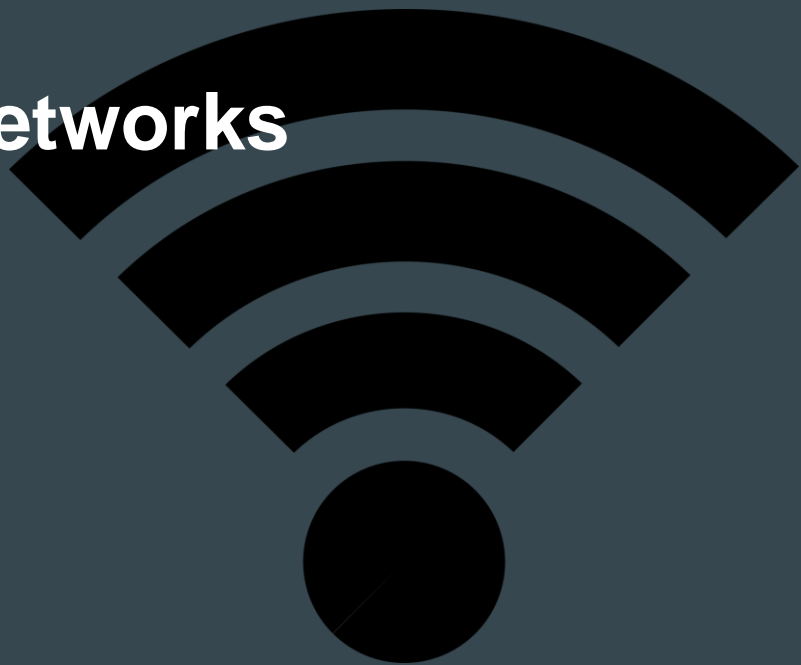
Corporate Public Guest Networks

Open or Shared secret

Credentials supplied with 802.1x

Internet access only

Segregated from internal network



The Problems

Legal

Contractor?

Inside?

Black box?

Ethical

Privacy concerns

Data management

Technical

Custom tool



Shell Script to Automate

Configure Raspberry Pi/Kali Linux

Setup the adapter

Monitor mode

Applications at the command line (tshark, macchanger, etc.)



Original Script

```
#!/bin/sh

#Bash Script for automation of wireless information gathering v1.3
#IUPUI CIT 460 Semester project
#Nathan Snyder, Alex Andrews
#Assumes you have aircrack-ng suite, macchanger, and wireshark installed

echo starting wireless packet capture...
sleep 3
#change mac address to hide real mac
echo changing mac address to hide real mac
sleep 3
sudo macchanger --mac 00:11:22:33:44:55 wlan0
sleep 3
echo hid that mac!
sleep 5
#start airmon on default wlan0, edit if different interface
sudo airmon-ng start wlan0
#log all traffic from nearby APs -I for monitor mode -k to start capture immediately -$
#edit after the -w for your specific capture, your name, location, and number if more $
sudo touch cit460_school_kali
sudo chmod o=rwx cit460_school_kali
sudo tshark -I -i mon0 -w cit460_school_kali
```

First Alteration to Script

```
#!/bin/sh

#Bash Script for automation of wireless information gathering v1.3
#IUPUI CIT 460 Semester project
#Nathan Snyder, Alex Andrews
#Assumes you have aircrack-ng suite, macchanger, and wireshark installed

echo starting wireless packet capture...
sleep 3
#change mac address to hide real mac
echo changing mac address to hide real mac
sleep 3
sudo macchanger --mac 00:11:22:33:44:55 wlan0
sleep 3
echo hid that mac!
sleep 5
#start airmon on default wlan0, edit if different interface
sudo airmon-ng start wlan0
#log all traffic from nearby APs -I for monitor mode -k to start capture immediately -$
#edit after the -w for your specific capture, your name, location, and number if more $
sudo touch cit460_school_kali
sudo chmod o=rwx cit460_school_kali
sudo tshark -I -i mon0 -w cit460_school_kali
```

Captured Files















Each Member collected data

Public Wifi

McDonalds

Starbucks

Home Guest Network

Name ▲	Date Created	Date Modified	Modified By	Size
 cit460_adam_brownsburg2	Sunday	Sunday	Adam Meyer	18.2 MB
 cit460_adam_home	Sunday	Sunday	Adam Meyer	9.4 MB
 cit460_adam_home2	Sunday	Sunday	Adam Meyer	4.9 MB
 cit460_adam_homeopen	Sunday	Sunday	Adam Meyer	2.7 MB
 cit460_adam_hometcpdump	Sunday	Sunday	Adam Meyer	70 KB
 cit460_name_location_num	Apr 14, 2017	Apr 14, 2017	Nathan Snyder	2.2 MB
 cit460_nathan_IUPUI_IT_1	Apr 14, 2017	Apr 14, 2017	Nathan Snyder	639 KB
 cit460_nathan_mcdnoblesville	Apr 14, 2017	Apr 14, 2017	Nathan Snyder	2.6 MB
 cit460_nathan_nbleteacof_1	Apr 14, 2017	Apr 14, 2017	Nathan Snyder	12.6 MB
 cit460_nathan_nbleteacof_2	Apr 14, 2017	Apr 14, 2017	Nathan Snyder	8.8 MB
 cit460_nathan_noblesvilledwntwn_1	Apr 14, 2017	Apr 14, 2017	Nathan Snyder	34.5 MB
 cit460_nathan_noblesvillemcdconnor_1	Apr 14, 2017	Apr 14, 2017	Nathan Snyder	219 KB
 cit460_nathan_noblesvillemcdconnor_2	Apr 14, 2017	Apr 14, 2017	Nathan Snyder	10.8 MB
 cit460_nathan_noblesvillestarbucks_1	Apr 14, 2017	Apr 14, 2017	Nathan Snyder	5.9 MB

Wireshark Results

Beacon Frames

Broadcast Packet

SSID : ATTQeHNqs2



No.	Time	Source	Destination	Protocol	Length	Info
64838	1464.538829	SophosLt_2d:06:11	Broadcast	802.11	210	Beacon frame, SN=3033, FN=0, Flags=....., BI=100, SSID=pvtntwrk
64839	1464.540592	SophosLt_2d:06:12	Broadcast	802.11	208	Beacon frame, SN=3034, FN=0, Flags=....., BI=100, SSID=PEDCOR
64840	1464.559294	ArrisGro_07:2b:a0	Broadcast	802.11	242	Beacon frame, SN=3102, FN=0, Flags=....., BI=100, SSID=ATT4n2B7B7
64841	1464.586993	ArrisGro_83:e7:d0	Broadcast	802.11	296	Beacon frame, SN=574, FN=0, Flags=....., BI=100, SSID=BHNDG1670AE7D2
64842	1464.587441	ArrisGro_83:e7:d7	IPv6mcast_01	802.11	162	Data, SN=3621, FN=0, Flags=-p...F.
64843	1464.601641	ArrisGro_3d:bc:30	Broadcast	802.11	242	Beacon frame, SN=3039, FN=0, Flags=....., BI=100, SSID=ATTQeHNqs2
64844	1464.637654	ArrisGro_b8:c6:00	Broadcast	802.11	278	Beacon frame, SN=1472, FN=0, Flags=....., BI=100, SSID=ATTRH5YZfi
64845	1464.639449	SophosLt_2d:06:10	Broadcast	802.11	212	Beacon frame, SN=3035, FN=0, Flags=....., BI=100, SSID=Wifi Guest
64846	1464.641223	SophosLt_2d:06:11	Broadcast	802.11	210	Beacon frame, SN=3036, FN=0, Flags=....., BI=100, SSID=pvtntwrk
64847	1464.642988	SophosLt_2d:06:12	Broadcast	802.11	208	Beacon frame, SN=3037, FN=0, Flags=....., BI=100, SSID=PEDCOR
64848	1464.647209	ArrisGro_75:04:00	Broadcast	802.11	247	Beacon frame, SN=3444, FN=0, Flags=....., BI=100, SSID=SuckDeeDeesNuts
64849	1464.661698	ArrisGro_07:2b:a0	Broadcast	802.11	242	Beacon frame, SN=3103, FN=0, Flags=....., BI=100, SSID=ATT4n2B7B7
64850	1464.689422	ArrisGro_83:e7:d0	Broadcast	802.11	296	Beacon frame, SN=575, FN=0, Flags=....., BI=100, SSID=BHNDG1670AE7D2
64851	1464.720083	BelkinIn_b9:31:9b	Broadcast	802.11	222	Beacon frame, SN=603, FN=0, Flags=....., BI=100, SSID=Socks
64852	1464.722236	0a:86:3b:b9:31:9c	Broadcast	802.11	246	Beacon frame, SN=604, FN=0, Flags=....., BI=100, SSID=socks
64853	1464.742046	SophosLt_2d:06:10	Broadcast	802.11	212	Beacon frame, SN=3038, FN=0, Flags=....., BI=100, SSID=Wifi Guest

▼ Frame 64853: 212 bytes on wire (1696 bits), 212 bytes captured (1696 bits) on interface 0
Interface id: 0 (mon0)
Encapsulation type: IEEE 802.11 plus radiotap radio header (23)
Arrival Time: Apr 12, 2017 02:52:08.078972000 Eastern Daylight Time

More Wireshark Results

No.	Time	Source	Destination	Protocol	Length	Info
2385	20.509107	ArubaNet_b8:57:c2	Broadcast	802.11	181	Beacon frame, SN=3895, FN=0, Flags=....., BI=10..
2386	20.519590	ArubaNet_b9:20:42	Broadcast	802.11	181	Beacon frame, SN=2209, FN=0, Flags=....., BI=10..
2387	20.564347	ArubaNet_b8:44:40	Broadcast	802.11	205	Beacon frame, SN=2021, FN=0, Flags=....., BI=10..
2388	20.565226	ArubaNet_b8:40:a0	Broadcast	802.11	205	Beacon frame, SN=3674, FN=0, Flags=....., BI=10..
2389	20.565800	ArubaNet_b8:40:a2	Broadcast	802.11	181	Beacon frame, SN=3674, FN=0, Flags=....., BI=10..
2390	20.579457	ArubaNet_b9:4a:e0	Broadcast	802.11	205	Beacon frame, SN=4039, FN=0, Flags=....., BI=10..
2391	20.579747	ArubaNet_b9:4a:e1	Broadcast	802.11	203	Beacon frame, SN=4039, FN=0, Flags=....., BI=10..
2392	20.580028	ArubaNet_b9:4a:e2	Broadcast	802.11	181	Beacon frame, SN=4039, FN=0, Flags=....., BI=10..
2393	20.622161	ArubaNet_b9:20:40	Broadcast	802.11	206	Beacon frame, SN=2210, FN=0, Flags=....., BI=10..
2394	20.656521	2a:0a:8f:b3:ee:9c	Broadcast	802.11	144	Probe Request, SN=1705, FN=0, Flags=....., SSID..
2395	20.666751	ArubaNet_b8:44:40	Broadcast	802.11	205	Beacon frame, SN=2022, FN=0, Flags=....., BI=10..
2396	20.667329	ArubaNet_b8:44:42	Broadcast	802.11	181	Beacon frame, SN=2022, FN=0, Flags=....., BI=10..
2397	20.667933	ArubaNet_b8:40:a1	Broadcast	802.11	203	Beacon frame, SN=3675, FN=0, Flags=....., BI=10..
2398	20.668201	ArubaNet_b8:40:a2	Broadcast	802.11	181	Beacon frame, SN=3675, FN=0, Flags=....., BI=10..
2399	20.681932	ArubaNet_b9:4a:e0	Broadcast	802.11	205	Beacon frame, SN=4040, FN=0, Flags=....., BI=10..

Tag: SSID parameter set: attwifi
 Tag Number: SSID parameter set (0)
 Tag length: 7
 SSID: attwifi

```

0030 00 00 64 00 21 04 00 07 51 7a 7d 77 69 65 65 01 ..d.1... attwifi.
0040 07 8c 18 24 30 48 60 6c 03 01 01 05 04 00 01 00 ..$.H!.....
0050 00 2a 01 00 2d 1a ed 11 1b ff ff ff 00 00 00 00 ..*.0.....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
  
```

No.	Time	Source	Destination	Protocol	Length	Info
2385	20.509107	ArubaNet_b8:57:c2	Broadcast	802.11	181	Beacon frame, SN=3895, FN=0, Flags=....., BI=10..
2386	20.519590	ArubaNet_b9:20:42	Broadcast	802.11	181	Beacon frame, SN=2209, FN=0, Flags=....., BI=10..
2387	20.564347	ArubaNet_b8:44:40	Broadcast	802.11	205	Beacon frame, SN=2021, FN=0, Flags=....., BI=10..
2388	20.565226	ArubaNet_b8:40:a0	Broadcast	802.11	205	Beacon frame, SN=3674, FN=0, Flags=....., BI=10..
2389	20.565800	ArubaNet_b8:40:a2	Broadcast	802.11	181	Beacon frame, SN=3674, FN=0, Flags=....., BI=10..
2390	20.579457	ArubaNet_b9:4a:e0	Broadcast	802.11	205	Beacon frame, SN=4039, FN=0, Flags=....., BI=10..
2391	20.579747	ArubaNet_b9:4a:e1	Broadcast	802.11	203	Beacon frame, SN=4039, FN=0, Flags=....., BI=10..
2392	20.580028	ArubaNet_b9:4a:e2	Broadcast	802.11	181	Beacon frame, SN=4039, FN=0, Flags=....., BI=10..
2393	20.622161	ArubaNet_b9:20:40	Broadcast	802.11	206	Beacon frame, SN=2210, FN=0, Flags=....., BI=10..
2394	20.656521	2a:0a:8f:b3:ee:9c	Broadcast	802.11	144	Probe Request, SN=1705, FN=0, Flags=....., SSID..
2395	20.666751	ArubaNet_b8:44:40	Broadcast	802.11	205	Beacon frame, SN=2022, FN=0, Flags=....., BI=10..
2396	20.667329	ArubaNet_b8:44:42	Broadcast	802.11	181	Beacon frame, SN=2022, FN=0, Flags=....., BI=10..
2397	20.667933	ArubaNet_b8:40:a1	Broadcast	802.11	203	Beacon frame, SN=3675, FN=0, Flags=....., BI=10..
2398	20.668201	ArubaNet_b8:40:a2	Broadcast	802.11	181	Beacon frame, SN=3675, FN=0, Flags=....., BI=10..
2399	20.681932	ArubaNet_b9:4a:e0	Broadcast	802.11	205	Beacon frame, SN=4040, FN=0, Flags=....., BI=10..

Tag: SSID parameter set: IU Secure
 Tag Number: SSID parameter set (0)
 Tag length: 9
 SSID: IU Secure

```

0030 00 00 64 00 31 04 00 09 49 55 20 53 65 63 75 72 ..d.1... IU Secur
0040 05 01 07 8c 18 24 30 48 60 6c 03 01 01 05 04 00 ..$.H!.....
0050 01 00 00 2a 01 02 30 14 01 00 0f ac 04 01 00 0f ..*.0.....
0060 00 0f ac 04 01 00 00 0f ac 01 28 00 2d 1a ed 11 ..*.0.....
0070 1b ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 ..*.0.....
0080 00 00 00 00 00 00 00 00 3d 16 01 00 19 00 00 00 .....
  
```

No.	Time	Source	Destination	Protocol	Length	Info
2314	19.894694	ArubaNet_b8:57:c2	Broadcast	802.11	181	Beacon frame, SN=3889, FN=0, Flags=....., BI=10..
2315	19.906768	ArubaNet_b9:20:40	Broadcast	802.11	206	Beacon frame, SN=2203, FN=0, Flags=....., BI=10..
2316	19.951834	ArubaNet_b8:40:a1	Broadcast	802.11	203	Beacon frame, SN=3668, FN=0, Flags=....., BI=10..
2317	19.954963	ArubaNet_b8:44:42	Broadcast	802.11	181	Beacon frame, SN=2015, FN=0, Flags=....., BI=10..
2318	19.966173	ArubaNet_b8:40:20	Broadcast	802.11	205	Beacon frame, SN=1038, FN=0, Flags=....., BI=10..
2319	19.966470	ArubaNet_b8:40:21	Broadcast	802.11	203	Beacon frame, SN=1038, FN=0, Flags=....., BI=10..
2320	19.966742	ArubaNet_b8:40:22	Broadcast	802.11	181	Beacon frame, SN=1038, FN=0, Flags=....., BI=10..
2321	19.978030	ArubaNet_b9:3b:e0	Broadcast	802.11	205	Beacon frame, SN=2604, FN=0, Flags=....., BI=10..
2322	19.978333	ArubaNet_b9:3b:e1	Broadcast	802.11	203	Beacon frame, SN=2604, FN=0, Flags=....., BI=10..
2323	19.978606	ArubaNet_b9:3b:e2	Broadcast	802.11	181	Beacon frame, SN=2604, FN=0, Flags=....., BI=10..
2324	19.982143	ArubaNet_b8:46:a2	Broadcast	802.11	181	Beacon frame, SN=4034, FN=0, Flags=....., BI=10..
2325	19.993774	ArubaNet_b9:4e:00	Broadcast	802.11	205	Beacon frame, SN=1898, FN=0, Flags=....., BI=10..
2326	19.994354	ArubaNet_b9:4e:02	Broadcast	802.11	181	Beacon frame, SN=1898, FN=0, Flags=....., BI=10..
2327	20.007009	ArubaNet_b9:20:40	Broadcast	802.11	206	Beacon frame, SN=2204, FN=0, Flags=....., BI=10..
2328	20.007311	ArubaNet_b9:20:41	Broadcast	802.11	203	Beacon frame, SN=2204, FN=0, Flags=....., BI=10..

Tag: SSID parameter set: eduroam
 Tag Number: SSID parameter set (0)
 Tag length: 7
 SSID: eduroam

```

0030 00 00 64 00 31 04 00 07 65 64 75 72 6f 61 6d 01 ..d.1... eduroam
0040 07 8c 18 24 30 48 60 6c 03 01 01 05 04 00 01 00 ..$.H!.....
0050 00 2a 01 02 30 14 01 00 0f ac 04 01 00 00 0f ..*.0.....
0060 ac 04 01 00 00 0f ac 01 28 00 2d 1a ed 11 1b ff ..*.0.....
0070 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..*.0.....
0080 00 00 00 00 00 00 00 00 3d 16 01 00 19 00 00 00 .....
  
```

Beacon Frames

SSIDs

Over 96,000 packets in 15 minutes

Address Resolution Protocol (ARP)

147 0.858034	ArrisGro_7b:72:a0	Broadcast	802.11	296 Beacon frame, SN=1406, FN=0, Flags=....., BI=100, SSID=BHNTG1672G72A2
148 0.865752	ArrisGro_78:5e:90	Broadcast	802.11	304 Beacon frame, SN=344, FN=0, Flags=....., BI=100, SSID=OGMAGG
149 0.876198	ArrisGro_a1:56:80	Broadcast	802.11	274 Beacon frame, SN=3065, FN=0, Flags=....., BI=100, SSID=BHNTG1682G5682
150 0.878387	IETF-VRRP-VRID_01	Broadcast	ARP	96 Gratuitous ARP for 192.168.128.1 (Request)
151 0.878600	IETF-VRRP-VRID_01	Broadcast	ARP	96 Gratuitous ARP for 192.168.128.1 (Request)
152 0.878736	IETF-VRRP-VRID_01	Broadcast	ARP	96 Gratuitous ARP for 192.168.128.1 (Request)
153 0.878924	IETF-VRRP-VRID_01	Broadcast	ARP	96 Gratuitous ARP for 192.168.128.1 (Request)
154 0.886958	ArrisGro_02:44:20	Broadcast	802.11	299 Beacon frame, SN=3909, FN=0, Flags=....., BI=100, SSID=BHNDG1670A4422
155 0.890010	Netgear_b8:d7:a8	Broadcast	802.11	314 Beacon frame, SN=1362, FN=0, Flags=....., BI=100, SSID=NETGEAR08
156 0.896040	86:15:44:50:42:b4	Broadcast	802.11	302 Beacon frame, SN=3616, FN=0, Flags=....., BI=100, SSID=Broadcast

Frame 150: 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface 0
Interface id: 0 (mon0)

ARP Table

Build/maintain mapping database Ethernet to IP address

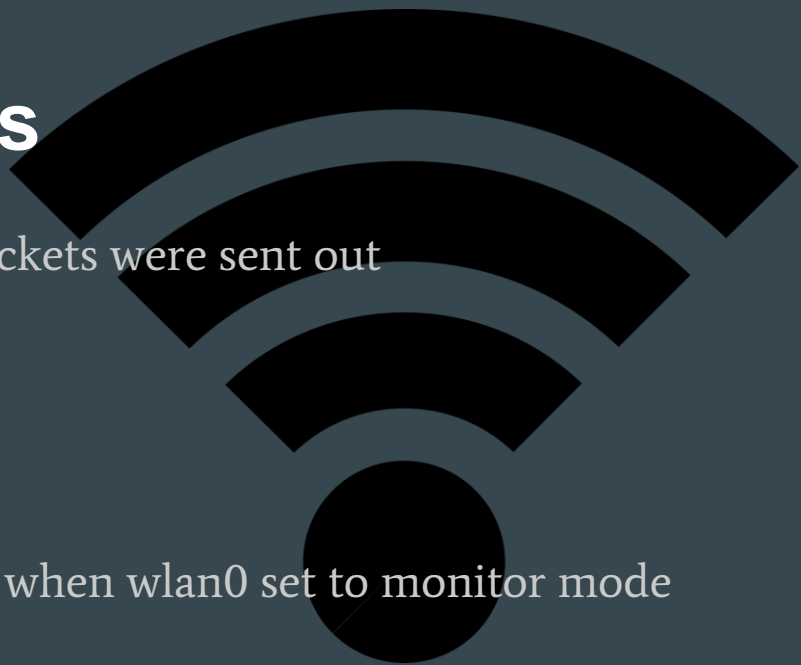
Layer 2 and Layer 3 addresses

ARP cached for 15 minutes

More Alterations and Tests

1. Not changing the MAC address, since no packets were sent out
2. Tried without “sleep” command
3. Used airodump-ng -w instead of tshark
4. Ensuring the interface name doesn't change when wlan0 set to monitor mode

Applying these changes, the results were similar...



Tried on Kali Linux (without Raspberry Pi)

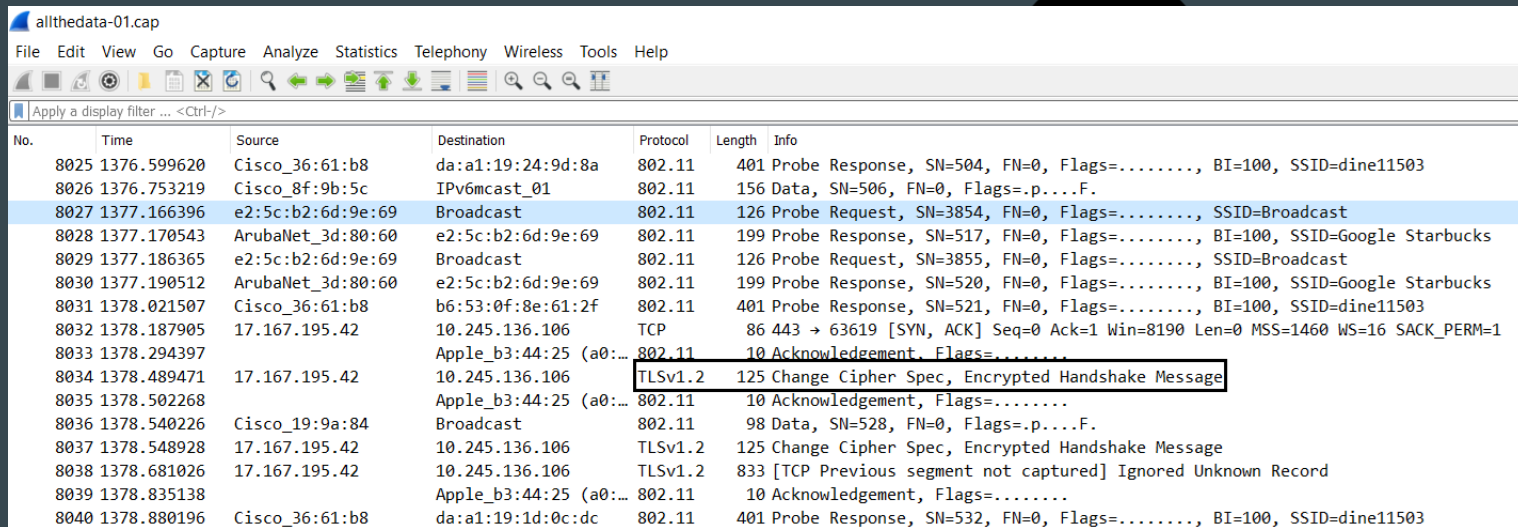
The image is a composite showing a Starbucks Coffee store on the left and a Wireshark network traffic capture window on the right. The Starbucks store is a two-story building with a stone and wood facade, featuring the 'STARBUCKS COFFEE' logo. The Wireshark window is titled 'Capturing from wlan0 [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]' and shows a list of captured packets. The filter is set to 'tcp'. The packet list includes various protocols such as SSL, TCP, and HTTPS. The hex dump at the bottom shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
17058	401.9599390	54.174.247.22	10.245.136.106	SSL	1574	[TCP Previous segment not captured] Continuation Data
17811	418.9530200	17.167.195.42	10.245.136.106	TCP	126	https > 63619 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1460 WS=16 SACK_PERM=1
17825	419.2543630	17.167.195.42	10.245.136.106	TLSv1.2	165	Change Cipher Spec, Encrypted Handshake Message
17832	419.3140490	17.167.195.42	10.245.136.106	TLSv1.2	165	Change Cipher Spec, Encrypted Handshake Message
17838	419.4464770	17.167.195.42	10.245.136.106	TLSv1.2	873	[TCP Previous segment not captured] Continuation Data
17854	419.7463610	17.167.195.44	10.245.136.106	TCP	120	https > 63622 [ACK] Seq=1 Ack=1 Win=2184 Len=0
17937	421.6734110	17.167.195.44	10.245.136.106	TCP	120	[TCP Previous segment not captured] https > 63622 [FIN, ACK] Seq=2271 Ack=910 Win=2559 Len=0
18391	432.8649840	54.174.247.22	10.245.136.106	TLSv1.2	157	[TCP Previous segment not captured] Encrypted Alert
19130	449.8200130	17.167.193.41	10.245.136.106	TCP	120	https > 63624 [ACK] Seq=1 Ack=1 Win=2184 Len=0
19132	449.8507290	17.167.193.41	10.245.136.106	TCP	120	https > 63624 [ACK] Seq=1 Ack=46 Win=2181 Len=0
19171	459.9735300	17.167.193.41	10.245.136.106	SSL	673	Continuation Data
19144	450.9625430	17.167.193.41	10.245.136.106	TLSv1.2	165	Change Cipher Spec, Encrypted Handshake Message
19193	451.2600710	17.167.193.41	10.245.136.106	TCP	120	[TCP Previous segment not captured] https > 63622 [FIN, ACK] Seq=2271 Ack=965 Win=2659 Len=0
19863	465.4165590	54.209.20.75	10.245.136.106	TCP	126	https > 63630 [ACK] Seq=1 Ack=1 Win=75 Len=0 TSval=57010654 TSecr=464659552
19875	465.6113630	54.209.20.75	10.245.136.106	TLSv1.2	265	[TCP Previous segment not captured] Application Data
19887	465.7943100	17.132.28.60	10.245.136.106	TCP	120	https > 63631 [ACK] Seq=1 Ack=1 Win=2671 Len=0

Expected Results

Captured TCP packets and TLSv1.2 “encrypted handshake message”

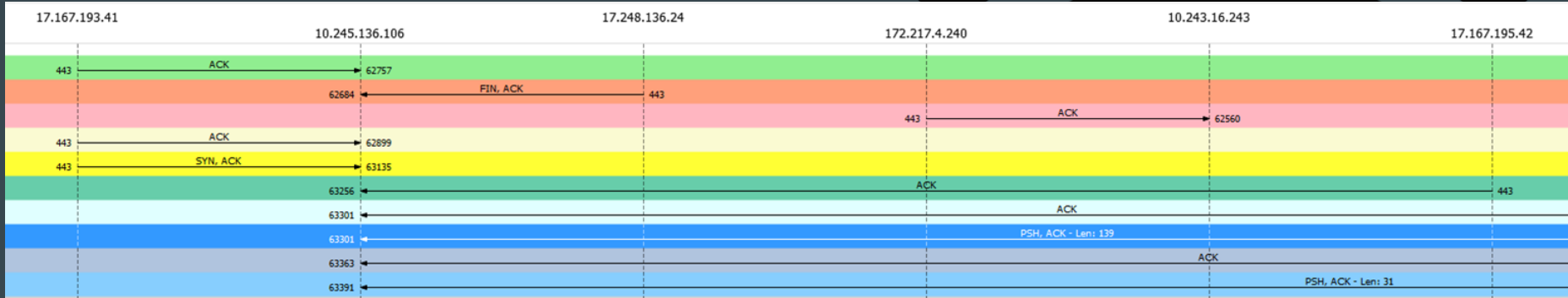
- Back to Starbucks
- Wireshark on Kali/Linux using Alfa network adapter
- Not using Raspberry Pi
- Monitor mode



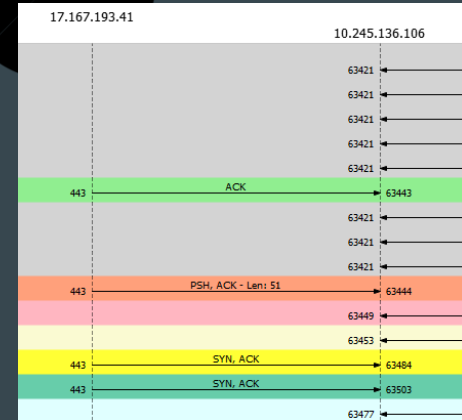
The image shows a Wireshark network traffic capture. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help), a toolbar with various icons, and a display filter field containing "Apply a display filter ... <Ctrl-/>". The main pane displays a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. Packet 8027 is highlighted in blue, showing a 126-byte Probe Request from source e2:5c:b2:6d:9e:69 to destination Broadcast. Packet 8028 is also highlighted, showing a 199-byte Probe Response from source ArubaNet_3d:80:60 to destination e2:5c:b2:6d:9e:69. Packet 8034 is highlighted and has a black box around its info field, showing a 125-byte Change Cipher Spec, Encrypted Handshake Message from source 17.167.195.42 to destination 10.245.136.106. Other packets include various Probe Responses, Acknowledgements, and Data packets.

No.	Time	Source	Destination	Protocol	Length	Info
8025	1376.599620	Cisco_36:61:b8	da:a1:19:24:9d:8a	802.11	401	Probe Response, SN=504, FN=0, Flags=....., BI=100, SSID=dine11503
8026	1376.753219	Cisco_8f:9b:5c	IPv6mcast_01	802.11	156	Data, SN=506, FN=0, Flags=.p....F.
8027	1377.166396	e2:5c:b2:6d:9e:69	Broadcast	802.11	126	Probe Request, SN=3854, FN=0, Flags=....., SSID=Broadcast
8028	1377.170543	ArubaNet_3d:80:60	e2:5c:b2:6d:9e:69	802.11	199	Probe Response, SN=517, FN=0, Flags=....., BI=100, SSID=Google Starbucks
8029	1377.186365	e2:5c:b2:6d:9e:69	Broadcast	802.11	126	Probe Request, SN=3855, FN=0, Flags=....., SSID=Broadcast
8030	1377.190512	ArubaNet_3d:80:60	e2:5c:b2:6d:9e:69	802.11	199	Probe Response, SN=520, FN=0, Flags=....., BI=100, SSID=Google Starbucks
8031	1378.021507	Cisco_36:61:b8	b6:53:0f:8e:61:2f	802.11	401	Probe Response, SN=521, FN=0, Flags=....., BI=100, SSID=dine11503
8032	1378.187905	17.167.195.42	10.245.136.106	TCP	86	443 → 63619 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1460 WS=16 SACK_PERM=1
8033	1378.294397	Apple_b3:44:25	(a0:...	802.11	10	Acknowledgement, Flags=.....
8034	1378.489471	17.167.195.42	10.245.136.106	TLSv1.2	125	Change Cipher Spec, Encrypted Handshake Message
8035	1378.502268	Apple_b3:44:25	(a0:...	802.11	10	Acknowledgement, Flags=.....
8036	1378.540226	Cisco_19:9a:84	Broadcast	802.11	98	Data, SN=528, FN=0, Flags=.p....F.
8037	1378.548928	17.167.195.42	10.245.136.106	TLSv1.2	125	Change Cipher Spec, Encrypted Handshake Message
8038	1378.681026	17.167.195.42	10.245.136.106	TLSv1.2	833	[TCP Previous segment not captured] Ignored Unknown Record
8039	1378.835138	Apple_b3:44:25	(a0:...	802.11	10	Acknowledgement, Flags=.....
8040	1378.880196	Cisco_36:61:b8	da:a1:19:1d:0c:dc	802.11	401	Probe Response, SN=532, FN=0, Flags=....., BI=100, SSID=dine11503

TCP Packets



- Using Wireshark's Flow Graph feature to view TCP flows
- Plot the traffic between 2 endpoints



Captured 1 HTTP Packet

8722 1499.585280000 184.50.239.16 10.243.16.243 HTTP 153	
+ Flags: 0x02 (Don't Fragment)	
Fragment offset: 0	
Time to live: 58	
Protocol: TCP (6)	
+ Header checksum: 0x6055 [correct]	
Source: 184.50.239.16 (184.50.239.16)	
Destination: 10.243.16.243 (10.243.16.243)	
[Source GeoIP: Unknown]	
[Destination GeoIP: Unknown]	
+ Transmission Control Protocol, Src Port: http (80), Dst Port: 62571 (62571), Seq: 1, Ack: 1, Len: 1448	
+ Hypertext Transfer Protocol	
0020 08 00 45 00 05 dc 17 9e 40 00 3a 06 60 55 38 32 ..E.....@...U	
0030 0a f3 10 f3 00 50 f4 6b 82 81 cd 75 7b 46 .P.....k...u(F	
0040 97 fd 80 10 03 ab af cc 00 00 01 01 08 0a a1 7b{	
0050 d0 52 50 bd 26 9e 56 72 4f 67 6e 54 37 76 2b 45 .RP.&.Vr OgnT7v+E	
0060 57 36 32 4e 72 48 71 31 39 64 42 65 68 34 36 45 w62NrHq1 9dBeh46E	
0070 4d 31 65 2f 54 50 64 32 57 63 6e 66 4c 53 7a 33 Mle/TPd2 WcnfLsz3	
0080 42 4a 35 4b 74 73 5a 41 47 64 55 30 55 32 54 59 BJ5KtsZA Gdu0U2TY	
0090 69 67 48 6e 73 58 31 74 71 30 73 6c 61 4c 38 6d igHhsX1t q0sLaL8m	
00a0 2b 6a 62 73 55 6d 32 47 6f 72 43 4c 58 64 2f 75 +jbsUm2G orCLXd/u	
00b0 44 66 6f 44 71 6b 65 71 41 7a 68 34 7a 35 72 41 DfoDqkeg Azh4z5FA	
00c0 73 66 64 33 6f 4c 32 2f 78 31 4e 35 37 68 7a 63 sfdSolZ/ xIN5Thzc	
00d0 31 6e 54 42 49 61 62 42 51 30 74 6f 2b 62 6d 59 lntBIab8 00to+bmY	
00e0 56 41 6e 66 2f 2b 57 77 33 67 48 31 39 61 65 56 VAnf/+Ww 3ghI9aeV	
00f0 75 71 6c 4e 62 68 74 56 6b 48 69 57 48 77 4f 4e uqLnbhtV kHiWhwON	
0100 65 42 6c 67 67 48 4f 63 78 30 4b 2b 65 6a 79 64 eBlggH0c x0K+ejyd	
0110 69 30 76 63 51 37 31 70 42 2f 3e 2f 63 59 64 77 iOvcQ71p B/6/cydw	
0120 54 52 45 57 41 6d 43 64 6e 48 45 51 72 54 6a 72 TREWAmCd nHEQTjr	
0130 42 67 62 63 54 6e 4f 62 72 48 5a 54 67 4c 55 77 BqbcTn0b rHZtqLUw	
0140 4b 4b 69 54 62 53 62 79 48 5a 2f 78 6a 61 61 67 KkiTb5by HZ/xjaaag	
0150 44 69 49 30 64 73 6d 73 4f 6a 6a 74 74 52 55 53 DiI0dms Oj1ttRUS	
0160 2b 50 65 42 55 62 4a 62 68 62 44 32 50 53 31 +PeBLUlj bhhd2PS1	
0170 67 2f 4e 78 73 59 4f 67 36 2b 35 4b 52 42 38 43 g/NxsY0g 6+SKFBGC	
0180 41 77 45 41 41 61 4f 43 41 59 30 77 67 67 4f 4a AwEAAaOC AY0wggBJ	
0190 4d 41 73 47 41 31 55 64 44 77 51 45 41 77 49 46 MasGA1UD DwQEAWIF	
01a0 6f 44 41 64 42 67 4e 56 48 53 55 45 46 6a 41 55 oDAdBgNV HSEFjAU	
01b0 42 67 67 72 42 67 45 46 42 51 63 44 41 51 59 49 BggrBgEF BQcDAQYI	
01c0 4b 77 59 42 42 51 55 48 41 77 49 77 4d 77 59 44 KwYBBQUH Aw1wMyYD	
01d0 56 52 30 66 42 43 77 7f 4b 6a 41 6f 6f 43 61 67 VROfBCw KJaoCag	
01e0 4a 49 59 69 61 48 52 30 63 44 8f 76 4c 32 4e 79 JIYi aHRO cDovL2Ny	
01f0 62 43 35 6c 62 6e 52 79 64 58 4e 30 4c 6d 35 6c bCSlnRy dXN0LmS1	
0200 64 43 39 73 5a 58 5a 6c 62 44 46 72 4c 6d 4e 79 dCSzXZL bDfRlMny	
0210 62 44 42 4c 42 67 4e 56 48 53 41 45 52 44 42 43 bDBLBNV HSAERDDB	
0220 4d 44 59 47 43 6d 43 47 53 41 47 47 2b 6d 77 4b MDYGcmCC SAGGmMk	
0230 41 51 55 77 4b 44 41 6d 42 67 67 72 42 67 45 46 AQUwKDAm BggrBgEF	
0240 42 51 63 43 41 52 59 61 61 48 52 30 63 44 6f 76 BQcCARYa ahR0cDov	
0250 4c 33 64 33 64 79 35 6c 62 6e 52 79 64 58 4e 30 L3d3dyS1 bnRyDXNO	
0260 4c 6d 35 6c 64 43 39 79 63 47 45 77 43 41 59 47 LmSLdC9y cGEwCAYG	

General IP Information

IP: 184.50.239.16

Decimal: 3090345744

Hostname: a184-50-239-16.deploy.static.akamaitechnologies.com

ASN: 20940

ISP: Akamai Technologies

Organization: Akamai Technologies

Services: None detected


Type: [Corporate](#)

Assignment: [Static IP](#)

Blacklist: [Blacklist Check](#)

Geolocation Information

Continent: North America

Country: United States 

State/Region: Massachusetts

City: Cambridge

Latitude: 42.3626 (42° 21' 45.36" N)

Longitude: -71.0843 (71° 5' 3.48" W)

Postal Code: 02142

802.11 Authentication

- Authentication:
A process that either accepts or rejects identity of NIC

4517	695.497174	Apple_c7:7e:cf	ArubaNet_3d:80:60	802.11	64 Authentication, SN=3499, FN=0, Flags=.....
4518	695.498198	Apple_c7:7e:cf	ArubaNet_3d:80:60	802.11	64 Authentication, SN=3499, FN=0, Flags=....R...
4519	695.522775	Apple_c7:7e:cf	ArubaNet_3d:80:60	802.11	64 Authentication, SN=3499, FN=0, Flags=....R...
4520	695.525334	Apple_c7:7e:cf	ArubaNet_3d:80:60	802.11	64 Authentication, SN=3499, FN=0, Flags=....R...
4521	695.542292	Apple_c7:7e:cf	ArubaNet_3d:80:60	802.11	64 Authentication, SN=3499, FN=0, Flags=....R...
4522	695.560197	Cisco_19:9a:84	Broadcast	802.11	98 Data, SN=3162, FN=0, Flags=-p....F.
4523	695.568911	Apple_c7:7e:cf	ArubaNet_3d:80:60	802.11	64 Authentication, SN=3499, FN=0, Flags=....R...
4524	695.569423		Broadcom_04:7e:cf (...)	802.11	10 Clear-to-send, Flags=.....
4525	695.592976	Apple_c7:7e:cf	ArubaNet_3d:80:60	802.11	64 Authentication, SN=3500, FN=0, Flags=.....
4526	695.593488	Apple_c7:7e:cf	ArubaNet_3d:80:60	802.11	64 Authentication, SN=3500, FN=0, Flags=....R...
4527	695.596560	Apple_c7:7e:cf	ArubaNet_3d:80:60	802.11	64 Authentication, SN=3500, FN=0, Flags=....R...
4528	695.598608	Apple_c7:7e:cf	ArubaNet_3d:80:60	802.11	64 Authentication, SN=3500, FN=0, Flags=....R...
4529	695.605778	Apple_c7:7e:cf	ArubaNet_3d:80:60	802.11	64 Authentication, SN=3500, FN=0, Flags=....R...
4530	695.612415	Apple_ca:a0:2f	ZebraTec_66:76:61	802.11	24 Null function (No data), SN=1596, FN=0, Flags=.....T
4531	695.612414	Apple_ca:a0:2f	ZebraTec_66:76:61	802.11	24 Null function (No data), SN=1596, FN=0, Flags=....R..T
4532	695.612415	Apple_ca:a0:2f	ZebraTec_66:76:61	802.11	24 Null function (No data), SN=1596, FN=0, Flags=....R..T
4533	695.612928	Apple_ca:a0:2f	ZebraTec_66:76:61	802.11	24 Null function (No data), SN=1596, FN=0, Flags=....R..T
4534	695.617535	Apple_ca:a0:2f	ZebraTec_66:76:61	802.11	24 Null function (No data), SN=1596, FN=0, Flags=....R..T

```
> Frame 4517: 64 bytes on wire (512 bits), 64 bytes captured (512 bits)
  IEEE 802.11 Authentication, Flags: .....
    Type/Subtype: Authentication (0x000b)
      > Frame Control Field: 0xb000
        .000 0000 0011 1100 = Duration: 60 microseconds
        Receiver address: ArubaNet_3d:80:60 (84:d4:7e:3d:80:60)
        Destination address: ArubaNet_3d:80:60 (84:d4:7e:3d:80:60)
        Transmitter address: Apple_c7:7e:cf (28:a0:2b:c7:7e:cf)
        Source address: Apple_c7:7e:cf (28:a0:2b:c7:7e:cf)
        BSS Id: ArubaNet_3d:80:60 (84:d4:7e:3d:80:60)
        .... .. 0000 = Fragment number: 0
        1101 1010 1011 .... = Sequence number: 3499
  IEEE 802.11 wireless LAN management frame
    Fixed parameters (6 bytes)
      Authentication Algorithm: Open System (0)
      Authentication SEQ: 0x0001
      Status code: Successful (0x0000)
    Tagged parameters (34 bytes)
```

Remaining Packets

Also, captured:

Beacon frames

Probe request frames

Acknowledgement (ACK) frames

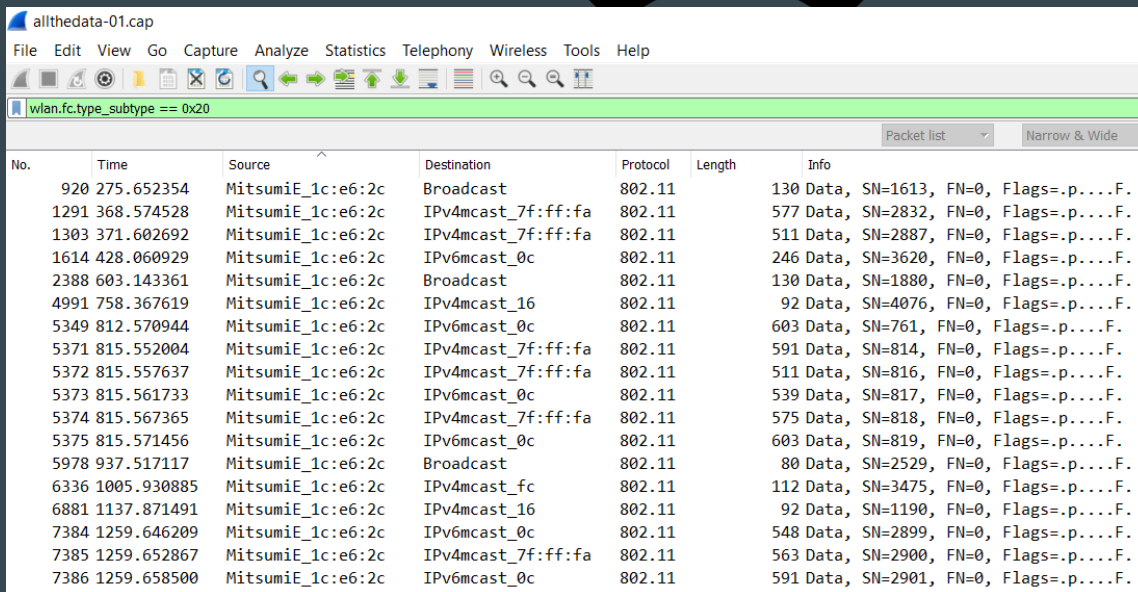
Data frames

Did not capture:

Deauthentication frames

Association frames

Data frames...



No.	Time	Source	Destination	Protocol	Length	Info
920	275.652354	MitsumiE_1c:e6:2c	Broadcast	802.11	130	Data, SN=1613, FN=0, Flags=.p....F.
1291	368.574528	MitsumiE_1c:e6:2c	IPv4mcast_7f:ff:fa	802.11	577	Data, SN=2832, FN=0, Flags=.p....F.
1303	371.602692	MitsumiE_1c:e6:2c	IPv4mcast_7f:ff:fa	802.11	511	Data, SN=2887, FN=0, Flags=.p....F.
1614	428.060929	MitsumiE_1c:e6:2c	IPv6mcast_0c	802.11	246	Data, SN=3620, FN=0, Flags=.p....F.
2388	603.143361	MitsumiE_1c:e6:2c	Broadcast	802.11	130	Data, SN=1880, FN=0, Flags=.p....F.
4991	758.367619	MitsumiE_1c:e6:2c	IPv4mcast_16	802.11	92	Data, SN=4076, FN=0, Flags=.p....F.
5349	812.570944	MitsumiE_1c:e6:2c	IPv6mcast_0c	802.11	603	Data, SN=761, FN=0, Flags=.p....F.
5371	815.552004	MitsumiE_1c:e6:2c	IPv4mcast_7f:ff:fa	802.11	591	Data, SN=814, FN=0, Flags=.p....F.
5372	815.557637	MitsumiE_1c:e6:2c	IPv4mcast_7f:ff:fa	802.11	511	Data, SN=816, FN=0, Flags=.p....F.
5373	815.561733	MitsumiE_1c:e6:2c	IPv6mcast_0c	802.11	539	Data, SN=817, FN=0, Flags=.p....F.
5374	815.567365	MitsumiE_1c:e6:2c	IPv4mcast_7f:ff:fa	802.11	575	Data, SN=818, FN=0, Flags=.p....F.
5375	815.571456	MitsumiE_1c:e6:2c	IPv6mcast_0c	802.11	603	Data, SN=819, FN=0, Flags=.p....F.
5978	937.517117	MitsumiE_1c:e6:2c	Broadcast	802.11	80	Data, SN=2529, FN=0, Flags=.p....F.
6336	1005.930885	MitsumiE_1c:e6:2c	IPv4mcast_fc	802.11	112	Data, SN=3475, FN=0, Flags=.p....F.
6881	1137.871491	MitsumiE_1c:e6:2c	IPv4mcast_16	802.11	92	Data, SN=1190, FN=0, Flags=.p....F.
7384	1259.646209	MitsumiE_1c:e6:2c	IPv6mcast_0c	802.11	548	Data, SN=2899, FN=0, Flags=.p....F.
7385	1259.652867	MitsumiE_1c:e6:2c	IPv4mcast_7f:ff:fa	802.11	563	Data, SN=2900, FN=0, Flags=.p....F.
7386	1259.658500	MitsumiE_1c:e6:2c	IPv6mcast_0c	802.11	591	Data, SN=2901, FN=0, Flags=.p....F.

Discussion: *Where did we go wrong?*

Can each group come up with one suggestion or recommendation on how to fix the “automation of wireless information gathering” script?

Assume aircrack-ng suite, macchanger, and wireshark are installed...

```
echo starting wireless packet capture...
sleep 3
#change mac address to hide real mac
echo changing mac address to hide real mac
sleep 3
macchanger --mac 00:11:22:33:44:55 wlan0
sleep 3
echo hid that mac!
sleep 5
#start airmon on default wlan0, edit if different interface
airmon-ng start wlan0
#log all traffic from nearby APs -I for monitor mode -k to start capture
immediately -w for outfile
#edit after the -w for your specific capture, your name, location, and
number if more than one
sudo touch cit460_name_location_num
sudo chmod o=rw cit460_name_location_num
sudo tshark -i wlan0 -w cit460_name_location_num
```

Recommendations

Make sure the connection is encrypted: use HTTPS when browsing

Enable “Secure Browsing” in the security settings

Avoid services that are not encrypted (e.g., FTP, HTTP)

Avoid submitting payment information or other sensitive/confidential data

Use a VPN (e.g., Opera VPN)



Sources and References

- Hogg, S. (2013). “Raspberry Pi as a Network Monitoring Mode”. Retrieved from Network World:
<http://www.networkworld.com/article/2225683/cisco-subnet/cisco-subnet-raspberry-pi-as-a-network-monitoring-node.html>
- Raspberrypi.org. (2016). “Network monitor”. Retrieved from Raspberrypi.org:
<https://www.raspberrypi.org/forums/viewtopic.php?t=145608&p=959758>
- Public Wi-Fi Security Explained by the US FTC. Retrieved from Consumer FTC:
<https://www.consumer.ftc.gov/articles/0014-tips-using-public-wi-fi-networks>
- Wireshark Wiki (2017) Retrieved from <https://wiki.wireshark.org/HowToDecrypt802.11>

