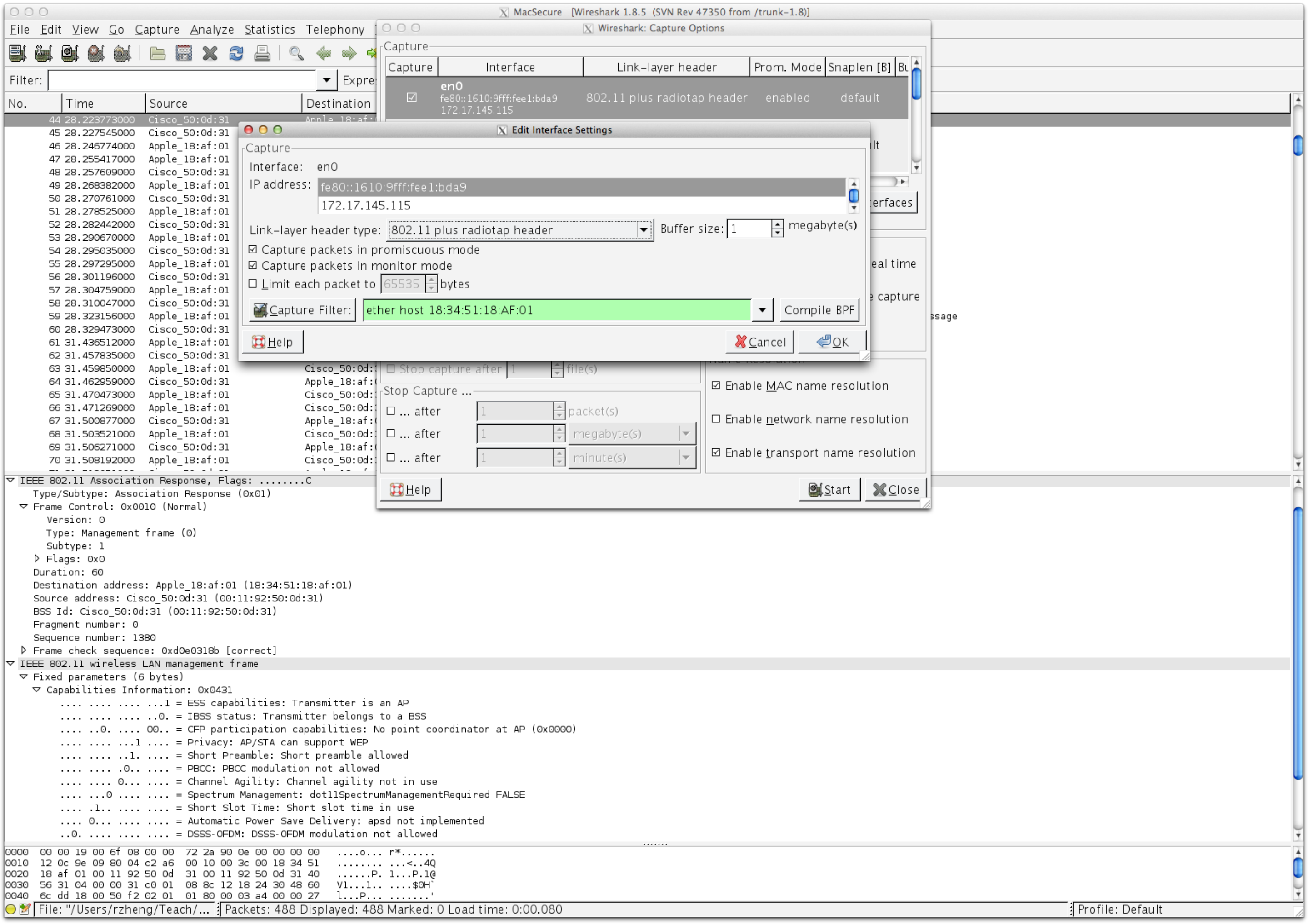
CAS765 Homework Assignment 2 – Trace analysis

Due date: September 30th, 2013

In this homework, you will be analyzing packet traces using the Wireshark software tool. Wireshark can be downloaded from http://www.wireshark.org/download.html. It is a tool for packet capture and analysis. A packet trace is a record of traffic at a location on the network. The packet trace records a timestamp for each packet, along with the bits that make up the packet, from the lower-layer headers to the higher-layer contents. To capture packet traces from a wireless network interface card (NIC), one needs to be put the NIC into promiscuous and monitoring modes. One can specify the capture filter to selectively capture interested packets (Figure 1). Since some NIC cards may not support the monitoring mode or users do not have the permission to do so, in this homework, two packet traces are provided and can be downloaded from the course page.

The two packet traces correspond to frames exchanged between a mobile device and wireless access points. In the first trace, the device connects to MacSecure; and in the second trace, the device connects to MacConnect. The MAC address of the mobile device is 18:34:51:18:AF:01 (Apple_18:af:01).


MacSecure [Wireshark 1.8.5 (SVN Rev 47350 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony
Filter:
Expre
Wireshark: Capture Options
Edit Interface Settings
Help
Cancel
OK
Compile BPF
Start
Close
Profile: Default

No.	Time	Source	Destination
44	28.223773000	Cisco_50:0d:31	Apple_18:af:
45	28.227545000	Cisco_50:0d:31	
46	28.246774000	Apple_18:af:01	
47	28.255417000	Apple_18:af:01	
48	28.257609000	Cisco_50:0d:31	
49	28.268382000	Apple_18:af:01	
50	28.270761000	Cisco_50:0d:31	
51	28.278525000	Apple_18:af:01	
52	28.282442000	Cisco_50:0d:31	
53	28.290670000	Apple_18:af:01	
54	28.295035000	Cisco_50:0d:31	
55	28.297295000	Apple_18:af:01	
56	28.301196000	Cisco_50:0d:31	
57	28.304759000	Apple_18:af:01	
58	28.310047000	Cisco_50:0d:31	
59	28.323156000	Apple_18:af:01	
60	28.329473000	Cisco_50:0d:31	
61	31.436512000	Apple_18:af:01	
62	31.457835000	Cisco_50:0d:31	
63	31.459850000	Apple_18:af:01	Cisco_50:0d:
64	31.462959000	Cisco_50:0d:31	Apple_18:af:
65	31.470473000	Apple_18:af:01	Cisco_50:0d:
66	31.471269000	Apple_18:af:01	Cisco_50:0d:
67	31.500877000	Cisco_50:0d:31	Apple_18:af:
68	31.503521000	Apple_18:af:01	Cisco_50:0d:
69	31.506271000	Cisco_50:0d:31	Apple_18:af:
70	31.508192000	Apple_18:af:01	Cisco_50:0d:

Wireshark: Capture Options — Capture

Capture	Interface	Link-layer header	Prom. Mode	Snaplen [B]	Bu
☑	en0 fe80::1610:9fff:fee1:bda9 172.17.145.115	802.11 plus radiotap header	enabled	default	

Edit Interface Settings — Capture

Interface: en0

IP address: fe80::1610:9fff:fee1:bda9
172.17.145.115

Link-layer header type: 802.11 plus radiotap header   Buffer size: 1 megabyte(s)

☑ Capture packets in promiscuous mode

☑ Capture packets in monitor mode

□ Limit each packet to 65535 bytes

Capture Filter: ether host 18:34:51:18:AF:01

□ Stop capture after 1 file(s)

Stop Capture ...

□ ... after 1 packet(s)

□ ... after 1 megabyte(s)

□ ... after 1 minute(s)

☑ Enable MAC name resolution

□ Enable network name resolution

☑ Enable transport name resolution

```
▽ IEEE 802.11 Association Response, Flags: ........C
    Type/Subtype: Association Response (0x01)
  ▽ Frame Control: 0x0010 (Normal)
      Version: 0
      Type: Management frame (0)
      Subtype: 1
    ▷ Flags: 0x0
    Duration: 60
    Destination address: Apple_18:af:01 (18:34:51:18:af:01)
    Source address: Cisco_50:0d:31 (00:11:92:50:0d:31)
    BSS Id: Cisco_50:0d:31 (00:11:92:50:0d:31)
    Fragment number: 0
    Sequence number: 1380
  ▷ Frame check sequence: 0xd0e0318b [correct]
▽ IEEE 802.11 wireless LAN management frame
  ▽ Fixed parameters (6 bytes)
    ▽ Capabilities Information: 0x0431
        .... .... .... ...1 = ESS capabilities: Transmitter is an AP
        .... .... .... ..0. = IBSS status: Transmitter belongs to a BSS
        .... ..0. .... 00.. = CFP participation capabilities: No point coordinator at AP (0x0000)
        .... .... ...1 .... = Privacy: AP/STA can support WEP
        .... .... ..1. .... = Short Preamble: Short preamble allowed
        .... .... .0.. .... = PBCC: PBCC modulation not allowed
        .... .... 0... .... = Channel Agility: Channel agility not in use
        .... ...0 .... .... = Spectrum Management: dot11SpectrumManagementRequired FALSE
        .... .1.. .... .... = Short Slot Time: Short slot time in use
        .... 0... .... .... = Automatic Power Save Delivery: apsd not implemented
        ..0. .... .... .... = DSSS-OFDM: DSSS-OFDM modulation not allowed
```

```
0000  00 00 19 00 6f 08 00 00  72 2a 90 0e 00 00 00 00   ....o... r*......
0010  12 0c 9e 09 80 04 c2 a6  00 10 00 3c 00 18 34 51   ........ ...<..4Q
0020  18 af 01 00 11 92 50 0d  31 00 11 92 50 0d 31 40   ......P. 1...P.1@
0030  56 31 04 00 00 31 c0 01  08 8c 12 18 24 30 48 60   V1...1.. ....$0H`
0040  6c dd 18 00 50 f2 02 01  01 80 00 03 a4 00 00 27   l...P... .......'
```

File: "/Users/rzheng/Teach/... Packets: 488 Displayed: 488 Marked: 0 Load time: 0:00.080

Fig. 1.   Wireshark screen capture

MacSecure trace: Open the file MacSecure.pcap in Wireshare (using "File" → "Open"). You will see a split screen with the top half showing the frames captured over time, and the bottom half showing the information of the highlighted frame in the top half. One can click the arrows on the left to expand for further information. Answer the following questions:

1) Can you guess what is the vendor (manufacture) of the APs for MacSecure?
2) What is the first frame (at time 0.0)? Why is the SSID set to "Broadcast"?

3) What are the frames numbered 2, 3, 4? What information can you deduce from these frames from the Radiotap header, and the IEEE 802.11 wireless LAN management frame?
4) Explain the frames 29 and 30.
5) What channel does the AP operate that the mobile is associated with?
6) Between frame 31 - 44, a number of association requests have been sent from the mobile device
7) Which extended authentication protocol(s) (EAP) is used by MacSecure (e.g., EAP-TTLS/MSCHAPv2, EAP-TTLS, etc.)
8) Which EAP is used in authenticating the mobile device?
9) Frame 71 indicates the success of authentication via 802.11X. Which frames correspond to the 4-way handshake for establishing pair-wise transient key? What are the nonces used by the AP and the mobile devices in the 4-way exchange?
10) Why cannot we see DHCP message exchanges in the trace for address allocation?

MacConnect trace: MacConnect provides unencrypted open access to campus WiFi. It uses web login to authenticate users.

1) Type “Bootp” in the filter field to display only DHCP related messages. A DHCP NAK message by the DHCP server is sent when a requested address is not available. From DHCP request message 77 - 101, what is the requested address by the mobile? What is the IP address allocated to the mobile eventually?
2) What is the purpose of the gratuitous ARP in frame 136?
3) Type “SSL” in the filter field to display SSL messages that are used to authenticate the user. From the frame 243 - 273, identify the type of messages exchanged and the values of the angle bracket (<>) in reference to Figure 2 that describes the connection setup process in SSL.

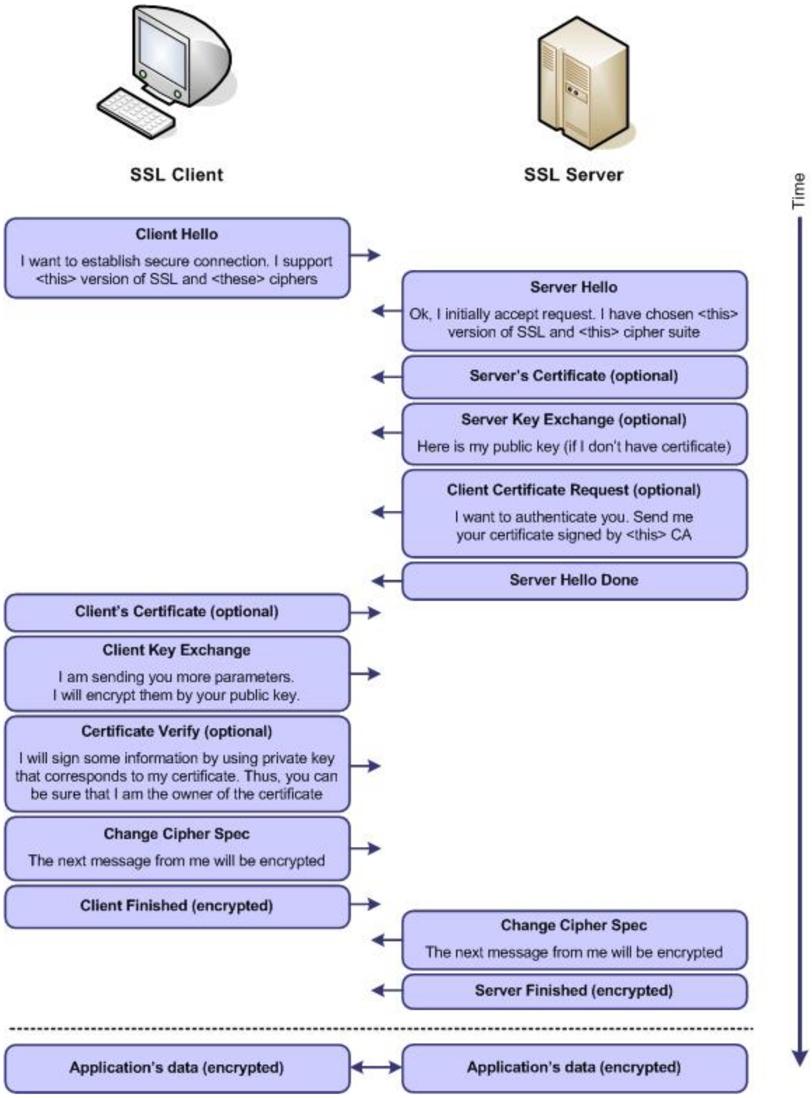

SSL Client
SSL Server
Time
Client Hello
I want to establish secure connection. I support <this> version of SSL and <these> ciphers
Server Hello
Ok, I initially accept request. I have chosen <this> version of SSL and <this> cipher suite
Server's Certificate (optional)
Server Key Exchange (optional)
Here is my public key (if I don't have certificate)
Client Certificate Request (optional)
I want to authenticate you. Send me your certificate signed by <this> CA
Server Hello Done
Client's Certificate (optional)
Client Key Exchange
I am sending you more parameters. I will encrypt them by your public key.
Certificate Verify (optional)
I will sign some information by using private key that corresponds to my certificate. Thus, you can be sure that I am the owner of the certificate
Change Cipher Spec
The next message from me will be encrypted
Client Finished (encrypted)
Change Cipher Spec
The next message from me will be encrypted
Server Finished (encrypted)
Application's data (encrypted)
Application's data (encrypted)

Fig. 2. SSL connection setup