Alexander Cannell

3/8/13

Professor Robertson

CSIS 4700

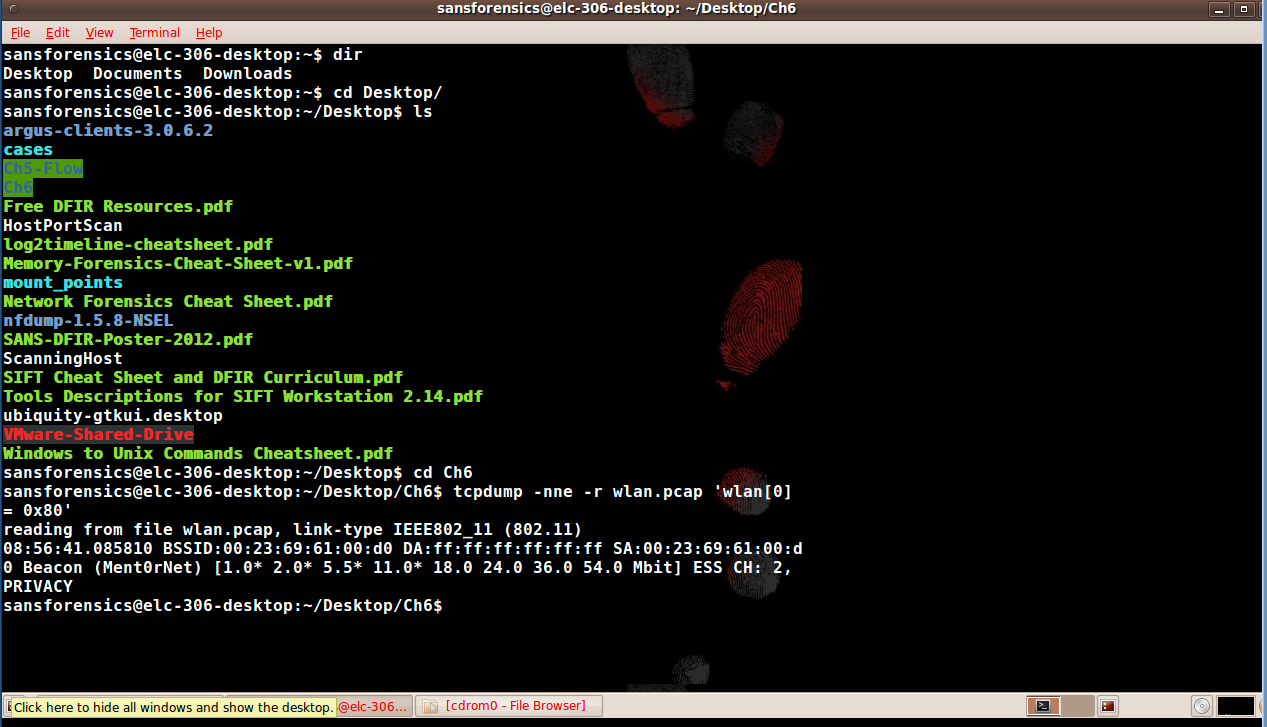
CASE STUDY: HackMe, Inc.

Introduction:

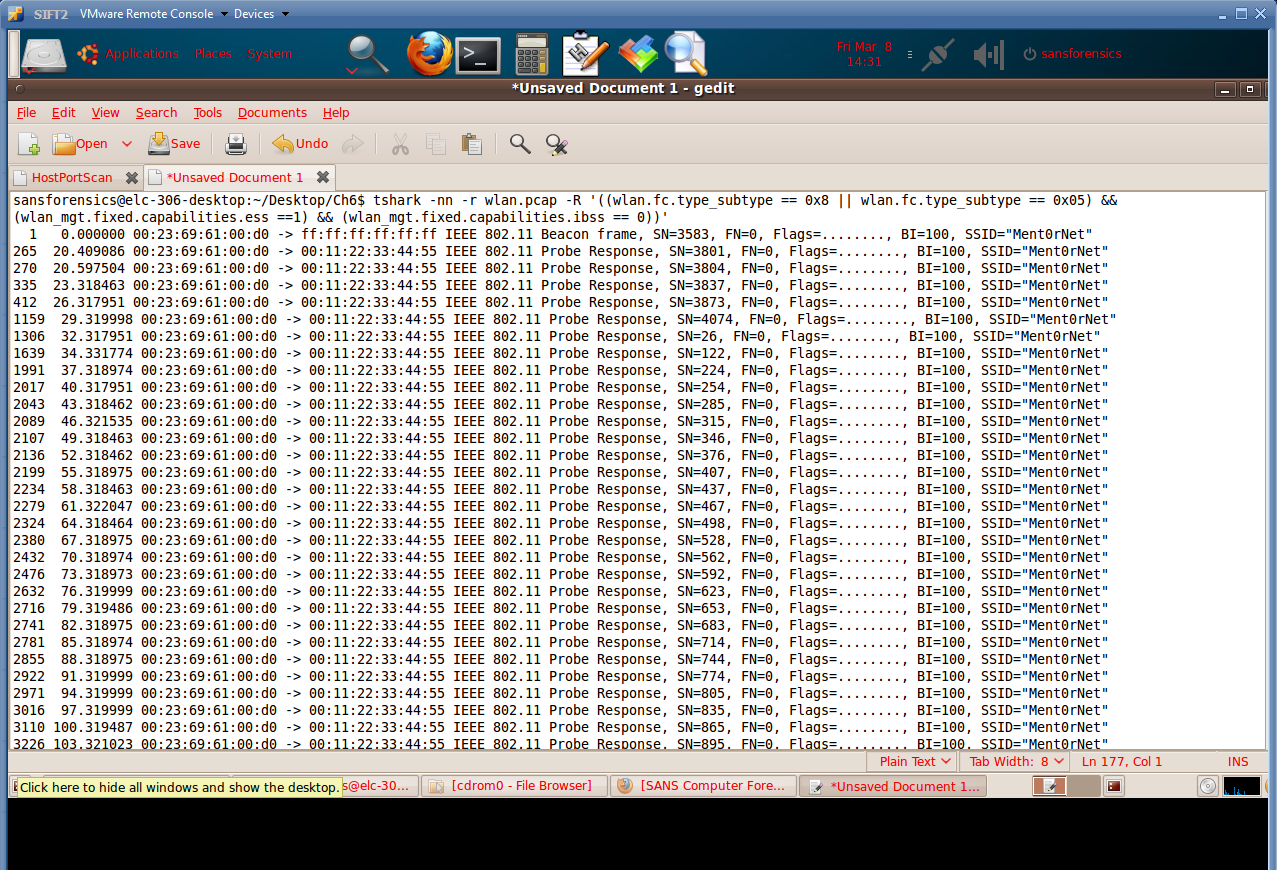
On September 17th, 2010, InterOptic is on the lam and is pinned down. The area is crawling with cops, and so he must stay put. But he also desperately needs to be able to get a message out to Ann and Mr x Lucky for him , he detects a wireless access point which is using a WAP encryption on their network. The tools we use are wireshark, tcpdump, and tshark.

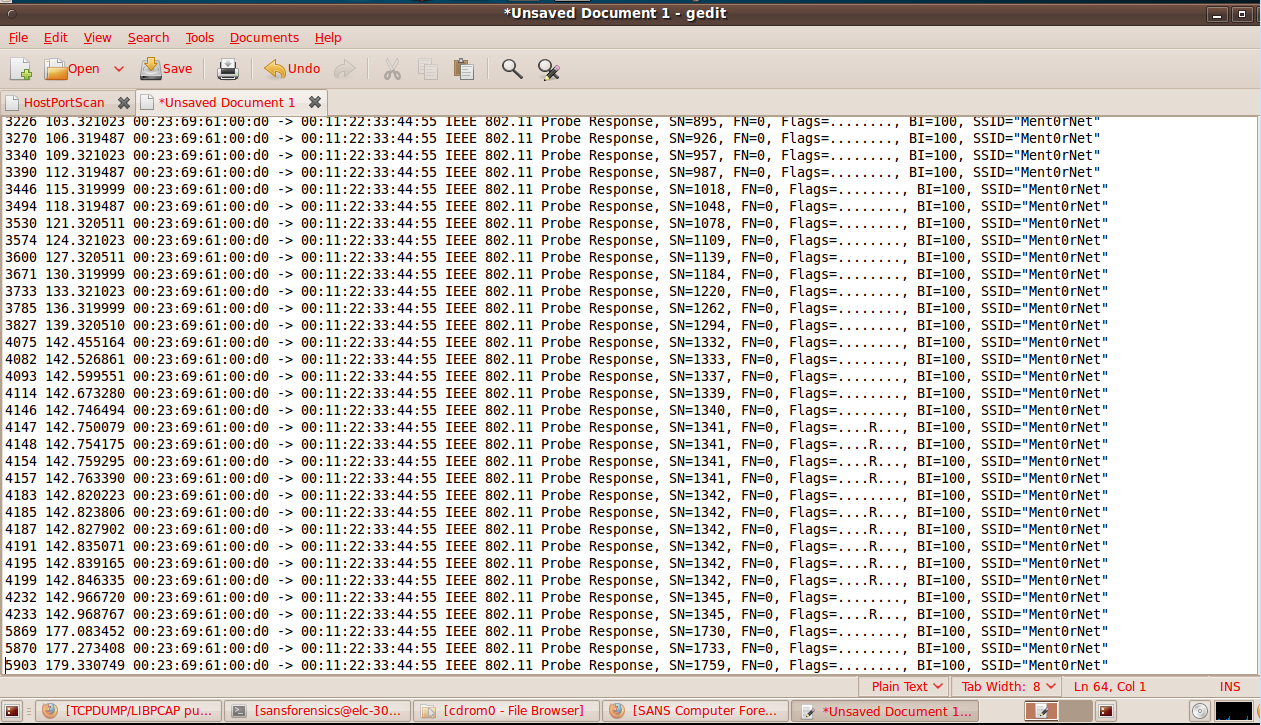
Supporting Documentation:

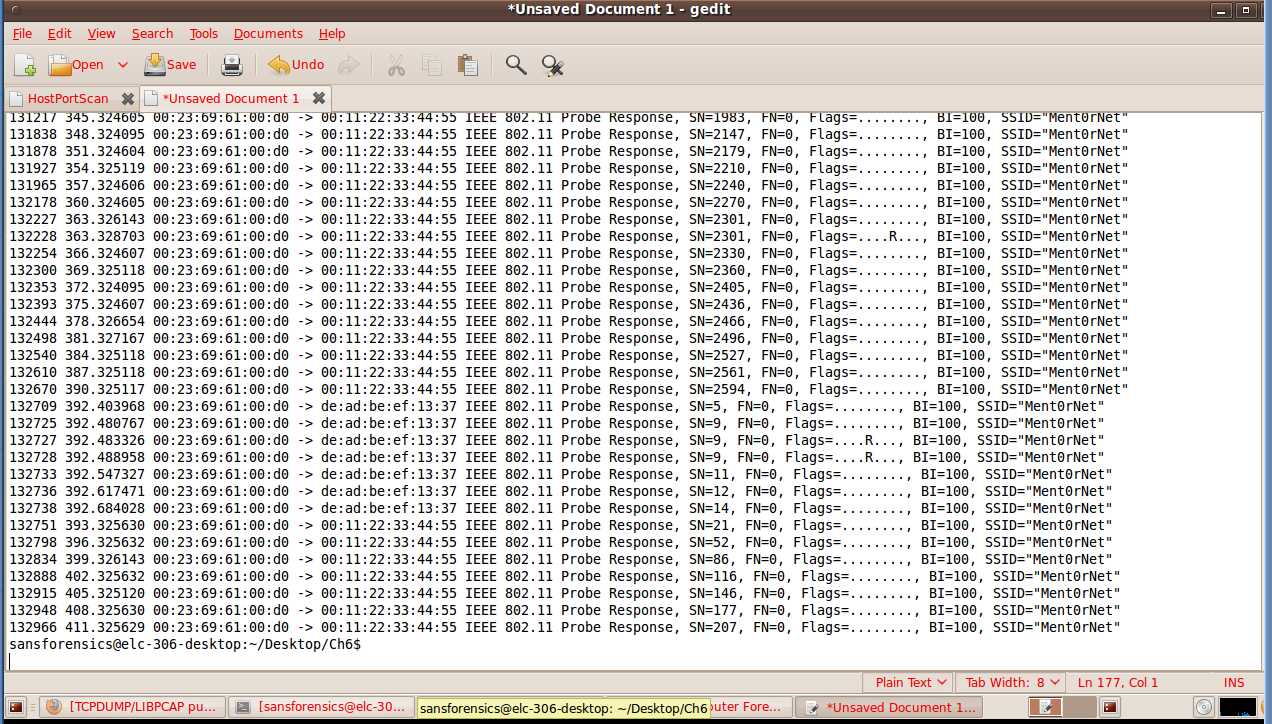
Using tcpdump to analyze the capture, also seeing the beacons frames.



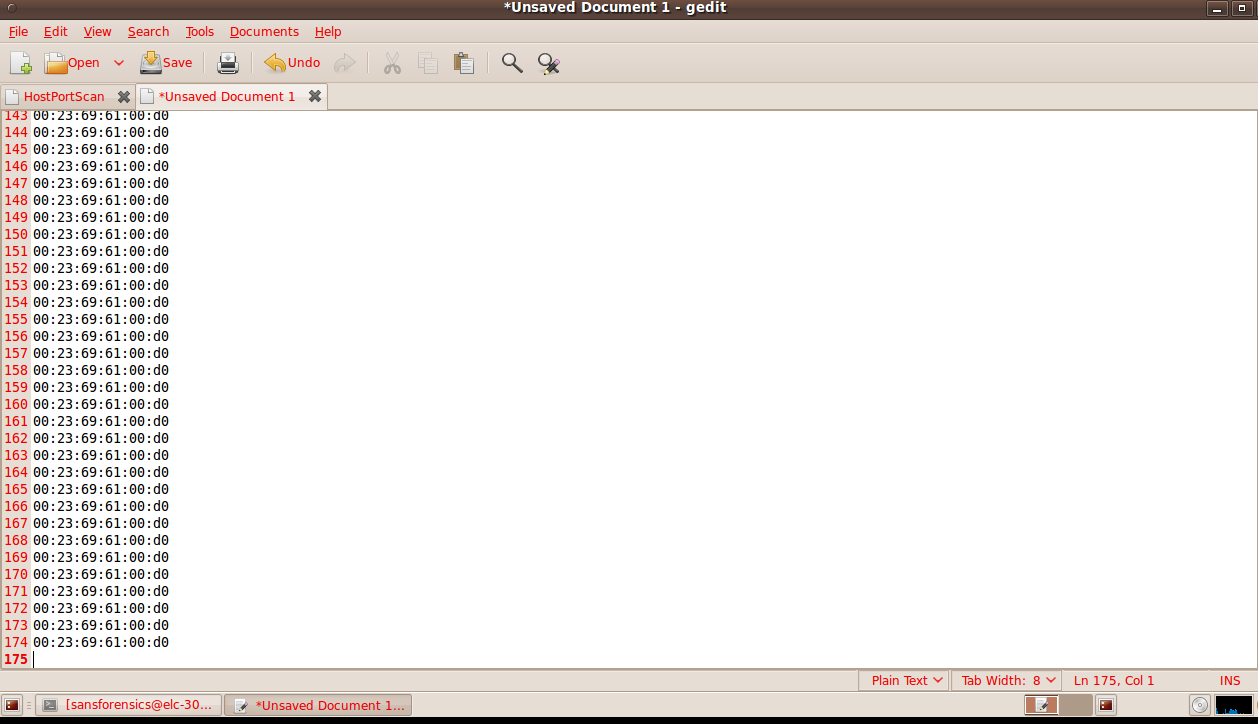
Using tshark to analyze the wireless capture, most specifically filtering WAP Announcing Management Frames.



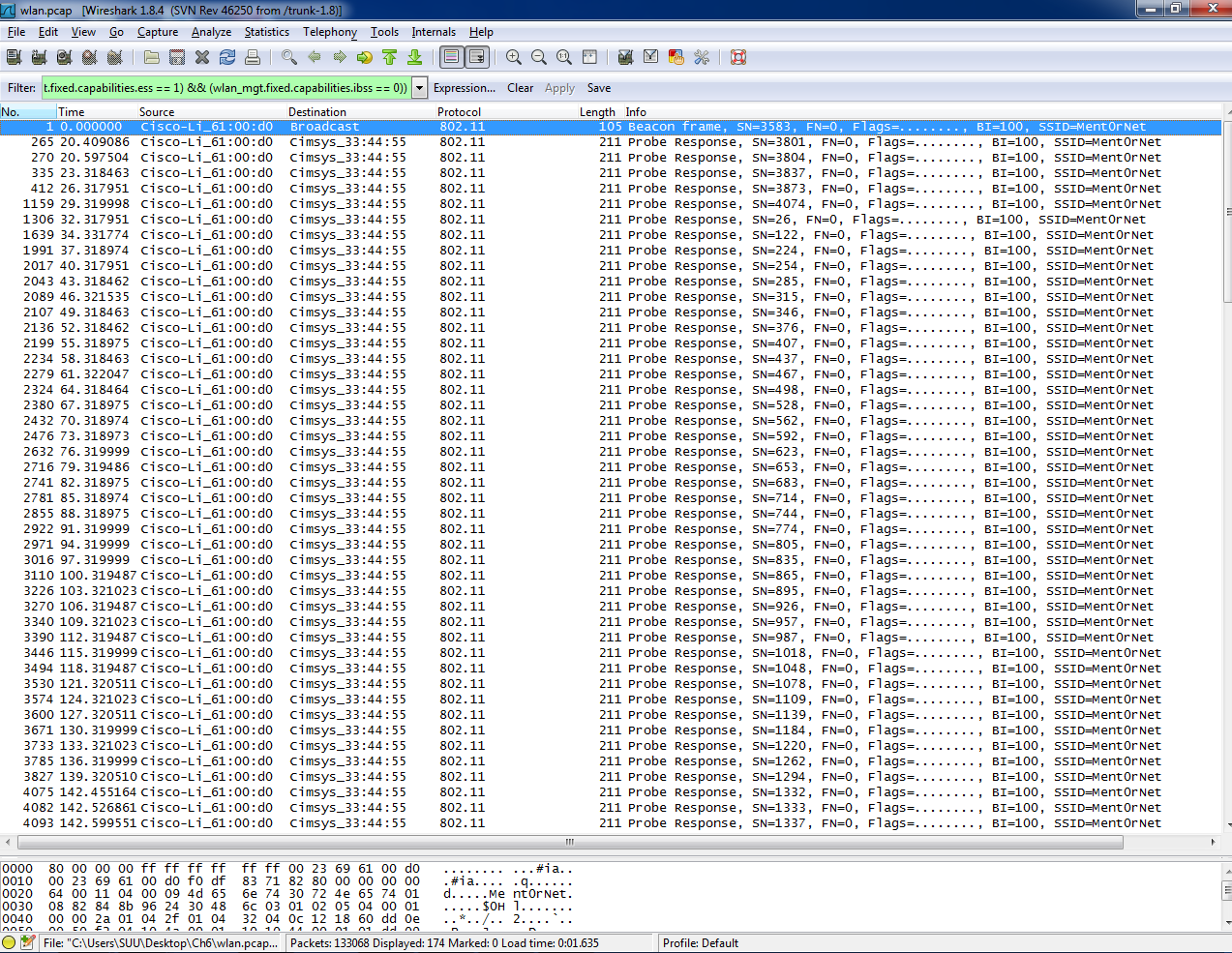




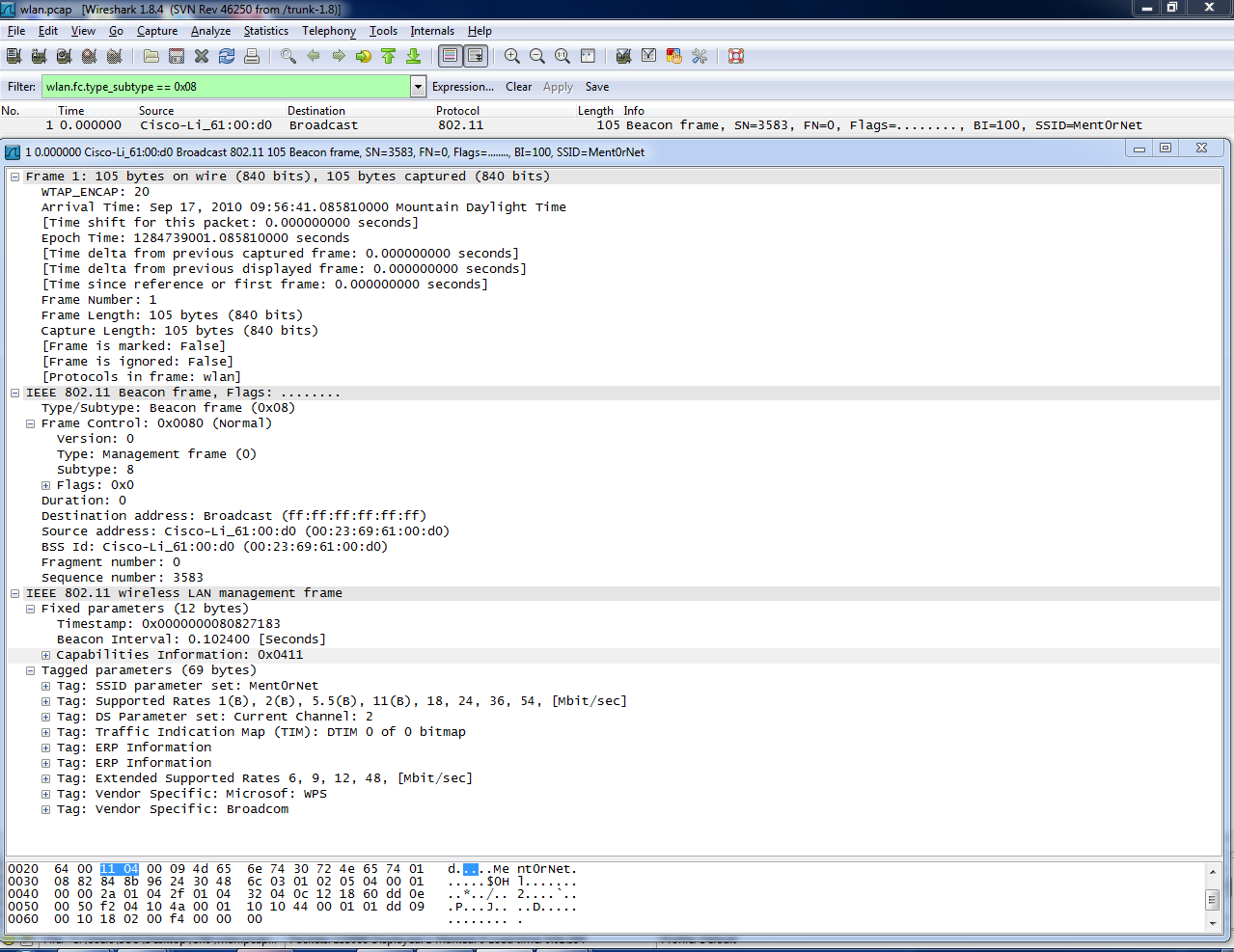
The uniq tool didn’t work on my SIFT, but I was able to get the mac address 00:23:69:61:00:d0 frames and copy those frames into notepad and get the line numbers for each of those frames. You can see there is 174 frames of 00:23:69:61:00:d0. ((wlan.fc.type\_subtype == 0x08 || wlan.fc.type\_subtype == 0x05) && (wlan\_mgt.fixed.capabilities.ess == 1) && (wlan\_mgt.fixed.capabilities.ibss == 0))



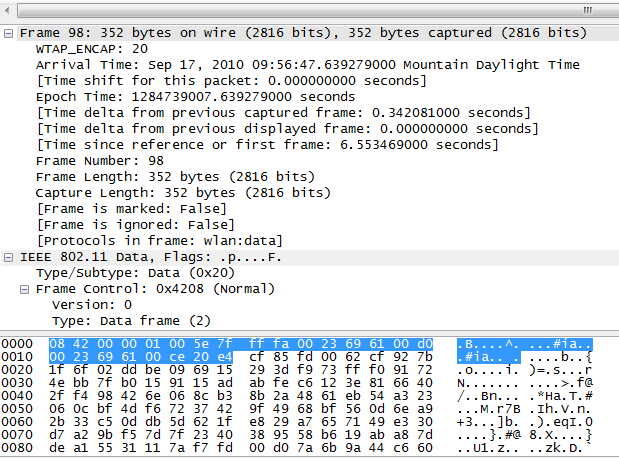
Wireshark verson of ((wlan.fc.type\_subtype == 0x08 || wlan.fc.type\_subtype == 0x05) && (wlan\_mgt.fixed.capabilities.ess == 1) && (wlan\_mgt.fixed.capabilities.ibss == 0))

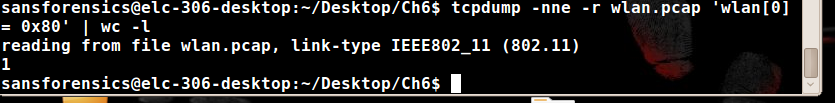


Now looking at just beacon frame 0x08 by using the wlan.fc.type\_subtype == 0x08 filter.

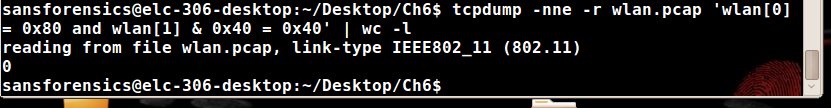


Now we are looking for the WLAN Encryption we can see the encryption flag .p….F. I used wlan.fc.type\_subtype == 0x20 to find this.

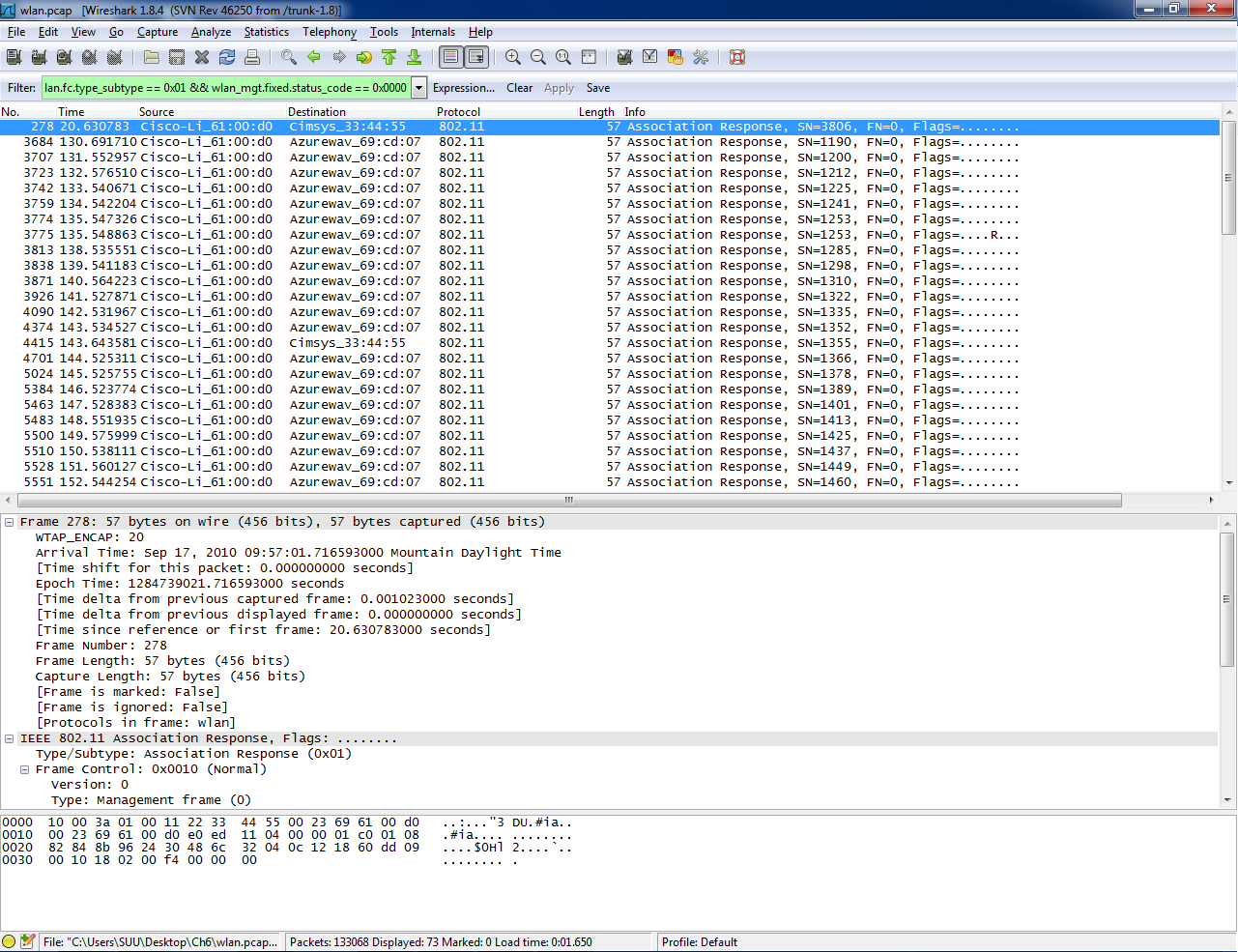


Now using tcpdump sending the output to the wc command to count the lines, but I only got one when I did this. 

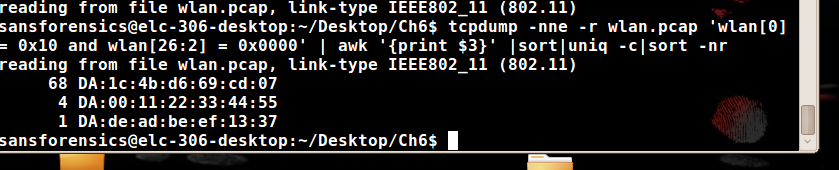
This shows the protected bit frames, but it didn’t quite work on mine I got 0.



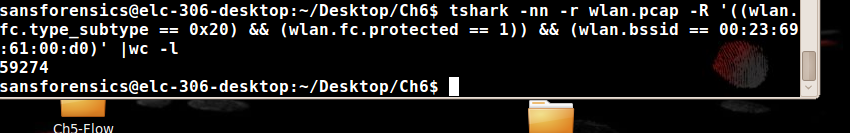
Wireshark is used to filter the association response subtype of the management frames. By wlan.fc.type\_subtype == 0x01 && wlan\_mgt.fixed.status\_code == 0x0000



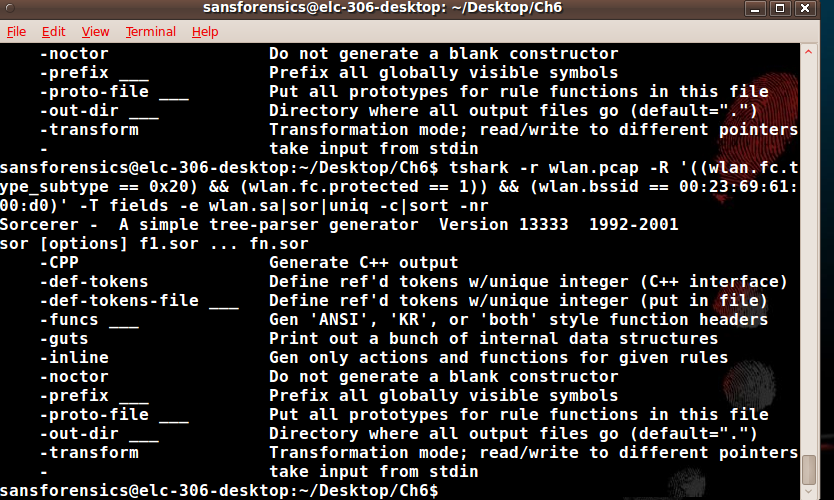
Tcpdump –nne –r wlan.pcap ‘wlan[0] = 0x10 and wlan[26:2] = 0x0000’|awk ‘{print $3}’ |sort|uniq –c|sort -nr



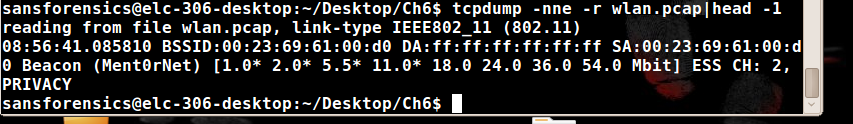
Now we use tshark to see the people who are in the neighborhood. Total frame captures.

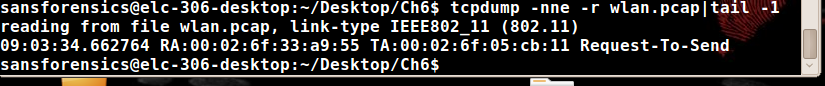


Number of each mac addresses encryption. This is what I get when I do this command, But I should have gotten different mac addresses. My -T fields doesn’t work.

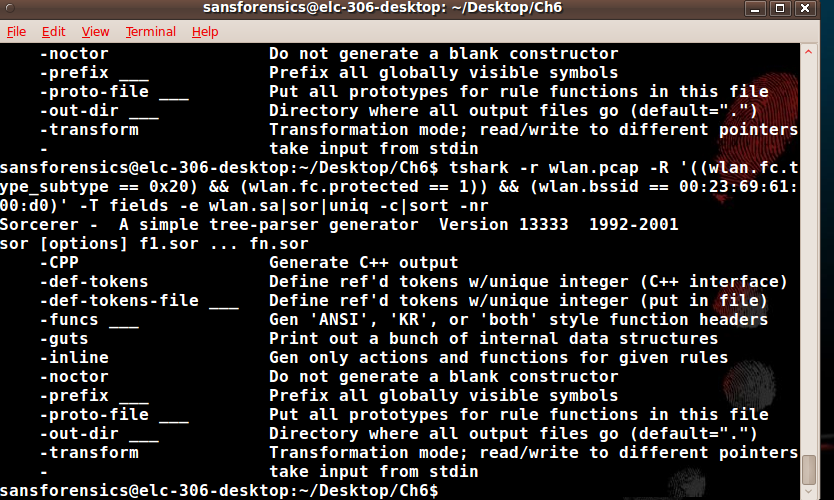


Using tcpdump to print the first/head and last/tail frame, and timestamp.

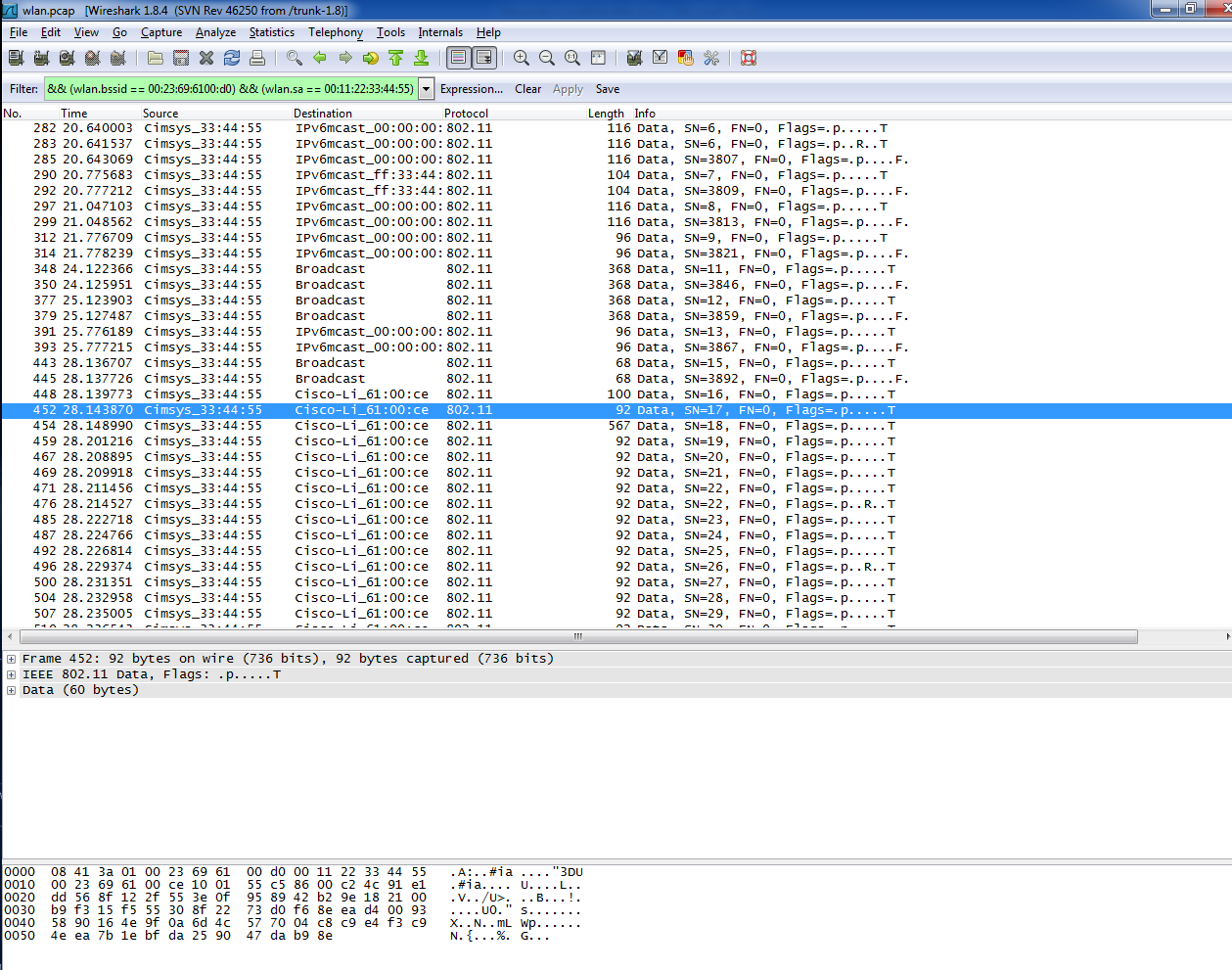




Number of each mac addresses encryption. This is what I get when I do this command, But I should have gotten different mac addresses. My -T fields doesn’t work.



This is my wireshark capture of the packets.



Examination:

1. What are the BSSID and SSID of the WAP of interest?

We can see that the Basic Service Set Identifier (BSSID) is 00:23:69:61:00:d0, and the Service Set Identifier (SSID) is MentOrNet.

1. Is the WAP of interest using encryption?

We can see that yes that the targeted WAP is encrypted because we inspected the frames and got .P….F.

1. What stations are interacting with the WAP and/or other stations on the WLAN?

We can see that there is three MAC addresses that are interacting with that WAP these are 00:11:22:33:44:55, 1c:4b:d6:69:cd:07, and de:ad:be:ef:13:37(HAHA Dead Beef LEET or 1337)

1. Are there patterns of activity that seem anomalous?

The data frames coming from a several unknown nods that have a unique IV’s being sent out from the WAP. It didn’t last for very long period of time; but appeared to be successfully.

1. How are they anomalous: Consistent with malfunction? Consistent with maliciousness?

You can use WEP crack attack, which targets the layer 2 broadcast address that came from the first node. But the attacker needs to collect large amounts of packets, and data from the network to retrieve the WEP key.

1. Can we identify any potentially bad actors?

We can see that the attack came from de:ad:be:ef:13:37 because 1c:4b:d6:69:cd:07 sent large amounts of frames to layer two and an unknown MAC came in and preformed a WEP attack successfully.

1. Can we determine if a bad actor successfully executed an attack?

The one way to make sure that the WEP Attack was successful would be to preform a aircrack –ng – 00:23:69:61:00:d0 wlan.pcap this will determine if the WEP crack Attack worked on this machine.

Conclusion:

We can see that the 1c:4b:d6:69:cd:07 computer begins to send authentication and association requests to layer two. Large amount of data is broadcast, we can see this through frames. The WEP crack was performed on the network to gain access, producing a WEP key. We can see the malicious traffic of de:ad:be:ef:13:37 and authenticate that it was InterOptic. I would say through this that InterOptic gained access to the WEP Key and to the network. We now need to see what message he sent on the network to MR x and ANN.