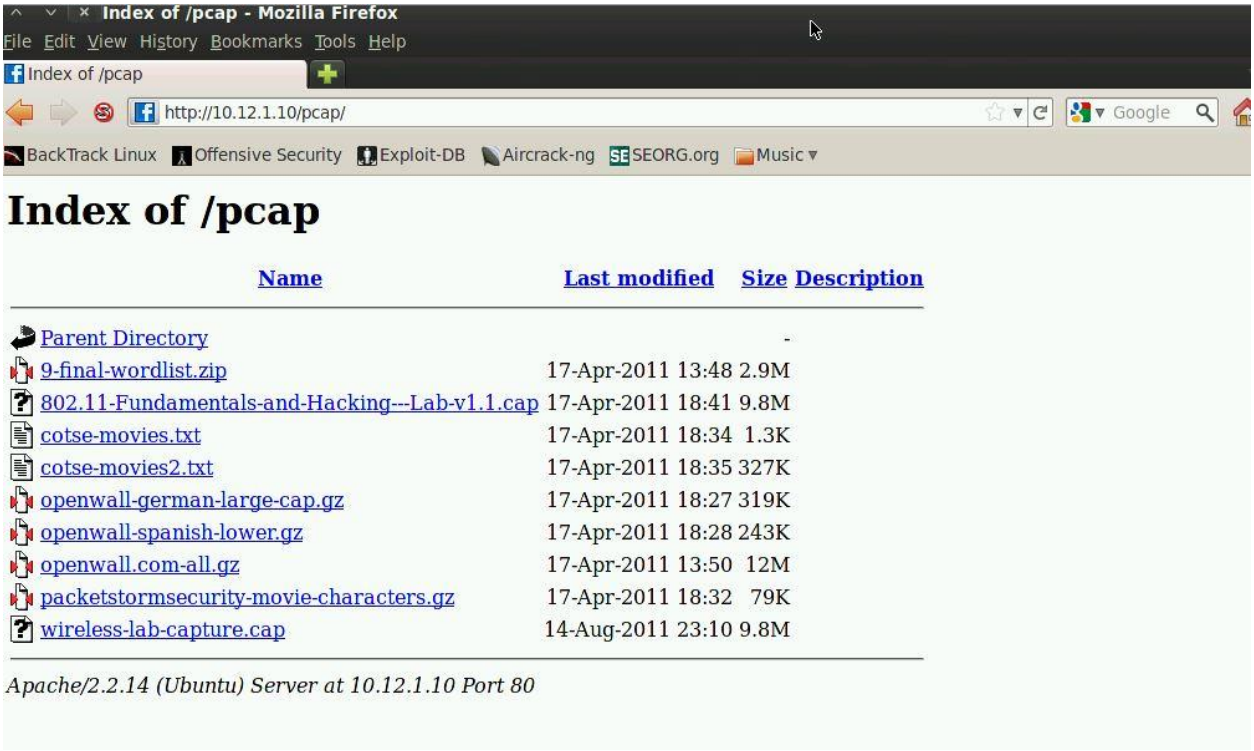
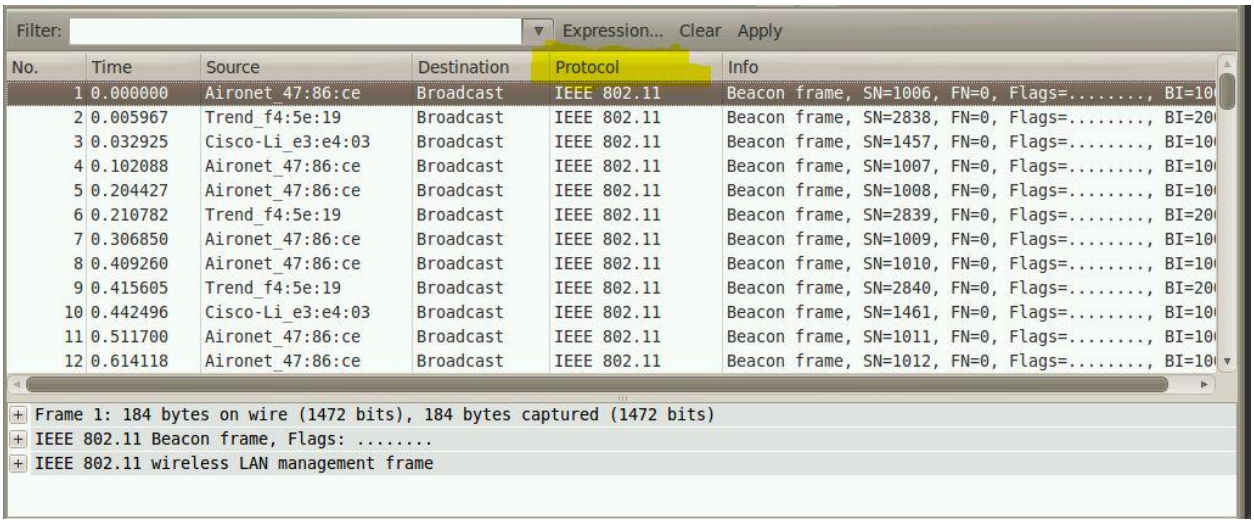
Vikash Kumar Deo
N15708475
Lab 6 – Wireless

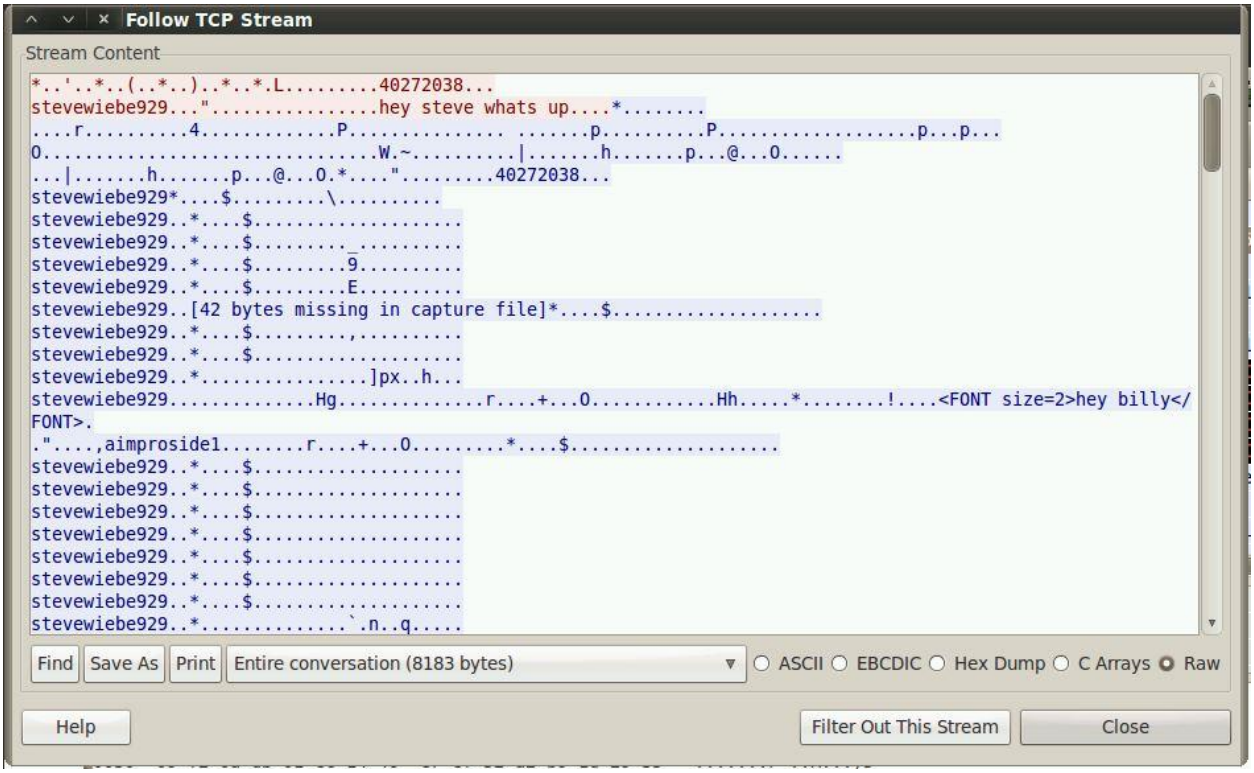
2. The following capture file was downloaded from the webpage.



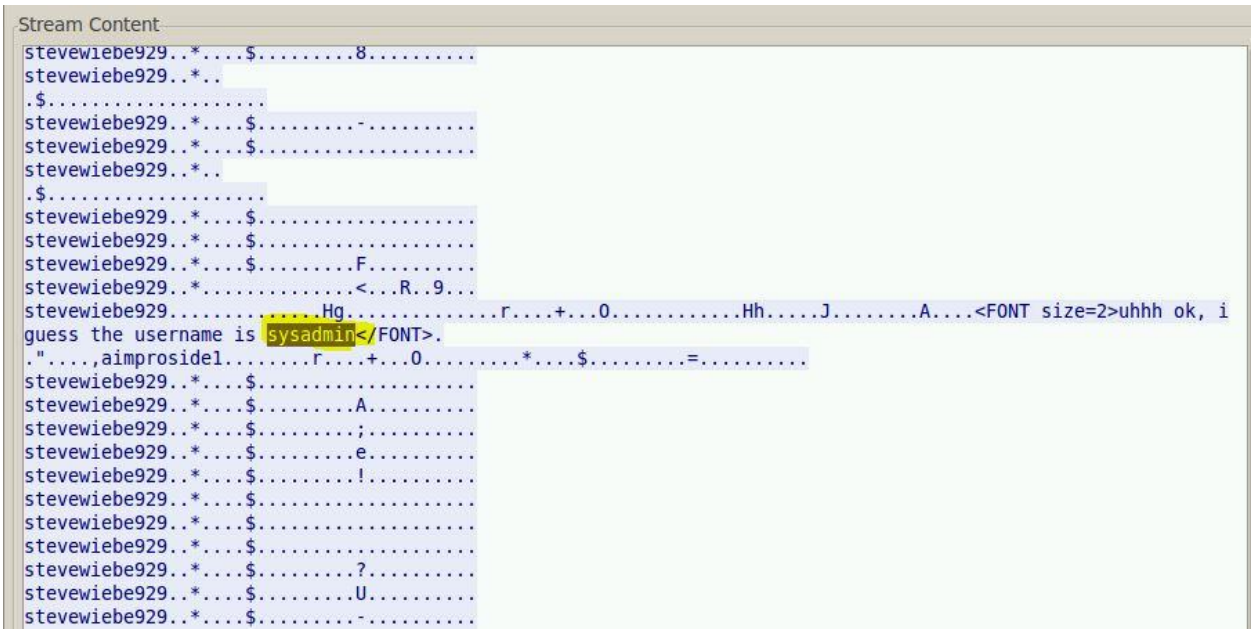
The file was opened in Wireshark and we can see the protocol as **IEEE 802.11 WLAN**.

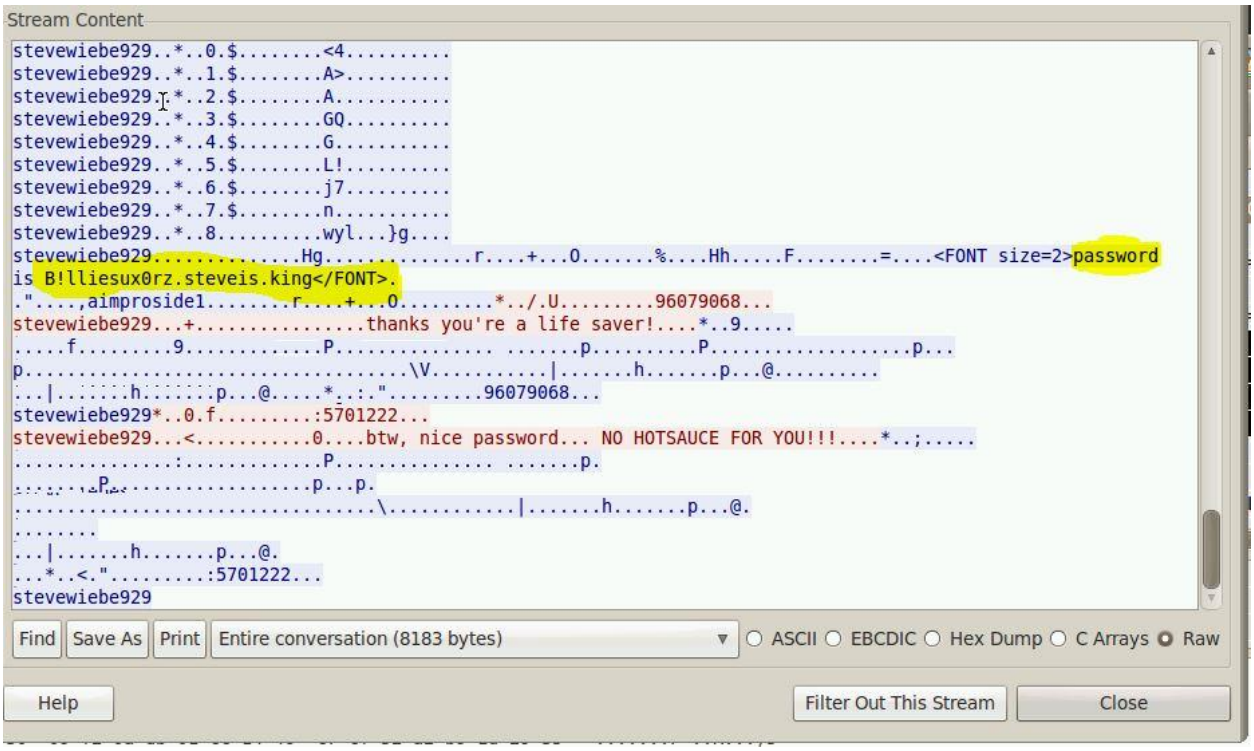


A TCP packet is selected by applying filter and it is opened in ‘follow TCP stream’ using “Analyze” option and then, the conversation is observed.



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

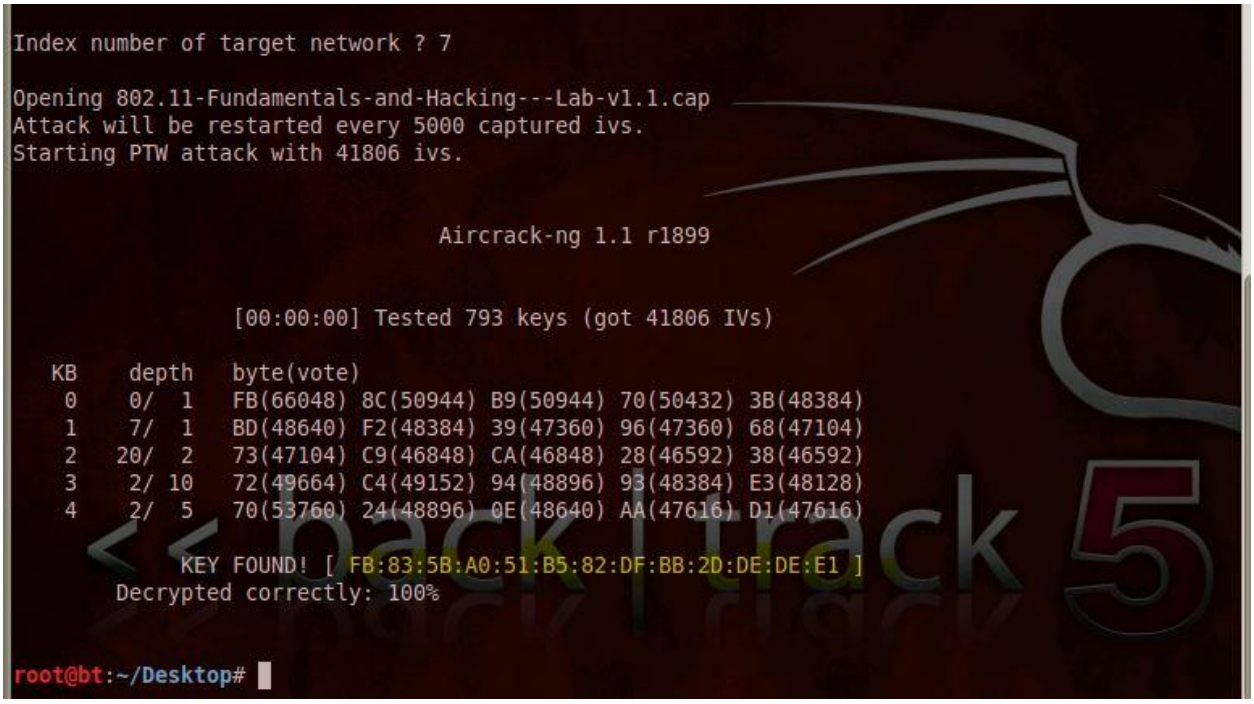




Primary plaintext communication protocol used here is "IEEE 802.11 WLAN".
The Conversation is about "twin galaxy servers".
Administrator's user name is "sysadmin".
Password is "B!lliesux0rz.steveis.king".

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.

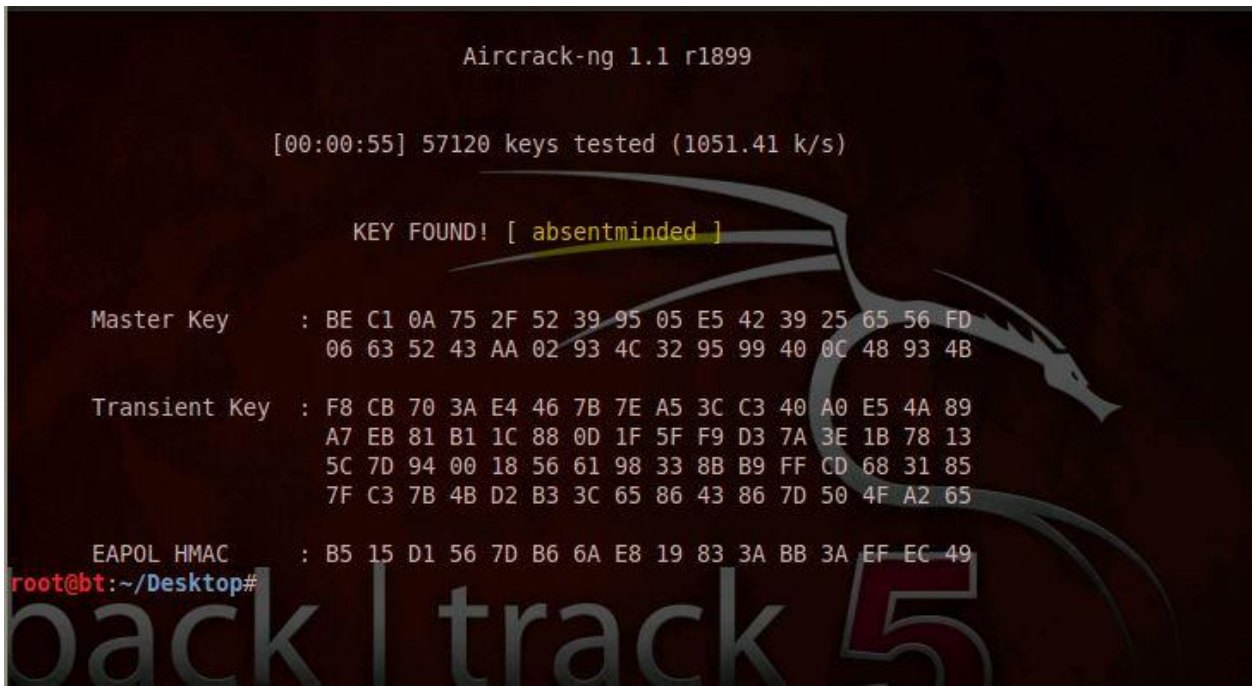


WEP Key for "CrackSmack" is "FB:83:5B:A0:51:82:DF:BB:2D:DE:DE:E1".

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.



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:            8846f7eaee8fb117ad06bdd830b7586c
        password:           password
root@bt:~/Desktop#
```

The Password is “password”.