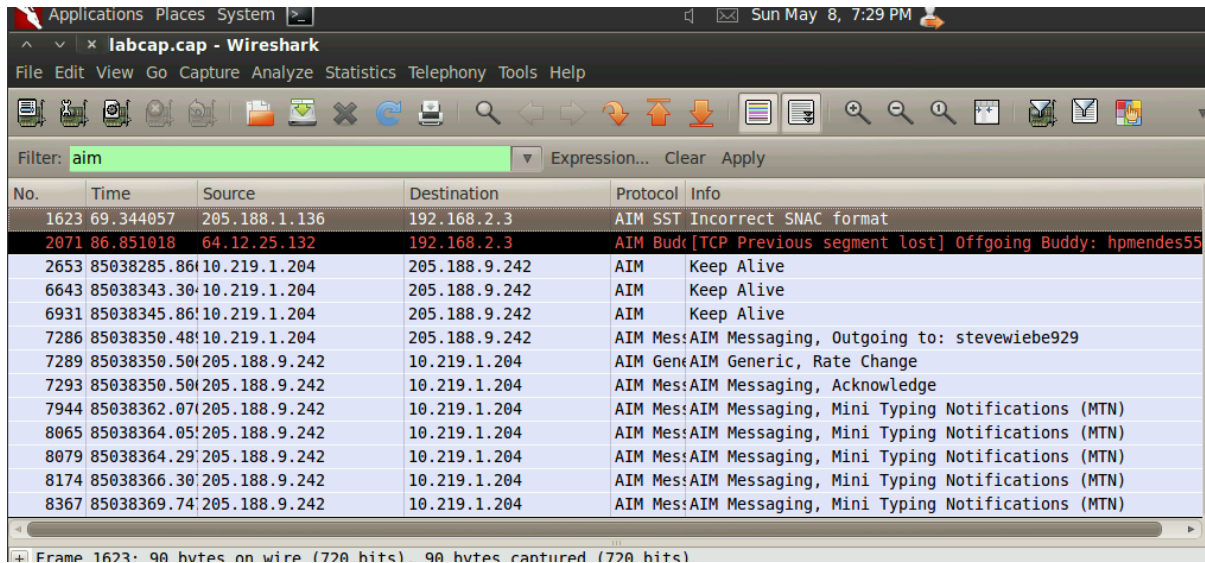


ACTIVITY - 1

1. What primary plaintext communication protocol is being used within the capture? (Hint: not TCP)

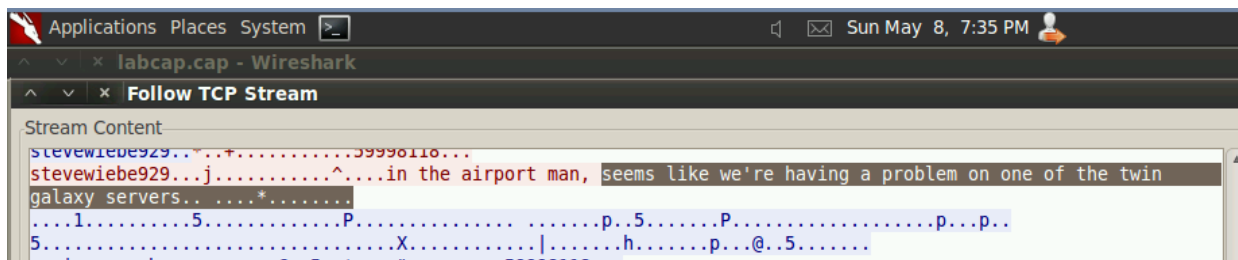
Ans: AIM Protocol 5190 port



No.	Time	Source	Destination	Protocol	Info
1623	69.344057	205.188.1.136	192.168.2.3	AIM SST	Incorrect SNAC format
2071	86.851018	64.12.25.132	192.168.2.3	AIM Buds	[TCP Previous segment lost] Offgoing Buddy: hpmendes55
2653	85038285.86	10.219.1.204	205.188.9.242	AIM	Keep Alive
6643	85038343.30	10.219.1.204	205.188.9.242	AIM	Keep Alive
6931	85038345.86	10.219.1.204	205.188.9.242	AIM	Keep Alive
7286	85038350.48	10.219.1.204	205.188.9.242	AIM Mes	AIM Messaging, Outgoing to: stevewiebe929
7289	85038350.50	205.188.9.242	10.219.1.204	AIM Gen	AIM Generic, Rate Change
7293	85038350.50	205.188.9.242	10.219.1.204	AIM Mes	AIM Messaging, Acknowledge
7944	85038362.07	205.188.9.242	10.219.1.204	AIM Mes	AIM Messaging, Mini Typing Notifications (MTN)
8065	85038364.05	205.188.9.242	10.219.1.204	AIM Mes	AIM Messaging, Mini Typing Notifications (MTN)
8079	85038364.29	205.188.9.242	10.219.1.204	AIM Mes	AIM Messaging, Mini Typing Notifications (MTN)
8174	85038366.30	205.188.9.242	10.219.1.204	AIM Mes	AIM Messaging, Mini Typing Notifications (MTN)
8367	85038369.74	205.188.9.242	10.219.1.204	AIM Mes	AIM Messaging, Mini Typing Notifications (MTN)

2. Whose server's is the conversation about?

Ans: Galaxy Server



Stream Content

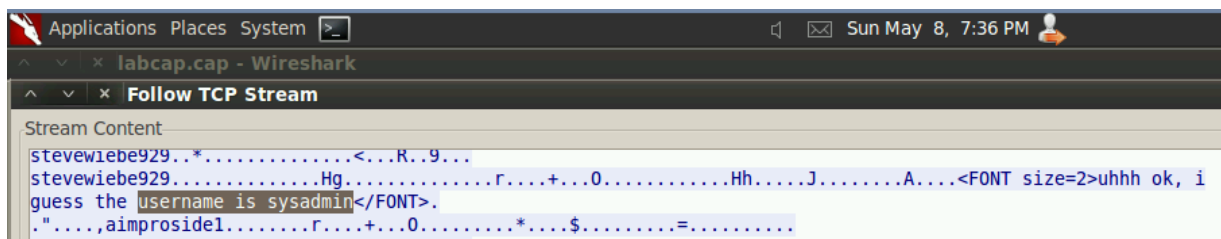
stevewiebe929...j.....^....in the airport man, seems like we're having a problem on one of the twin galaxy servers... ..*.....

...1.....5.....P.....p..5.....P.....p...p..

5.....X.....|.....h.....p...@..5.....

3. What is the administrator username?

Ans: sysadmin



Stream Content

stevewiebe929...<...R..9...

stevewiebe929.....Hg.....r...+...0.....Hh.....J.....A...uhhh ok, i guess the username is sysadmin.

.....aimprosidel.....r...+...0.....*.....\$.....=.....

4. What is the password?

Ans: B!lliesux0rz.steveis.king

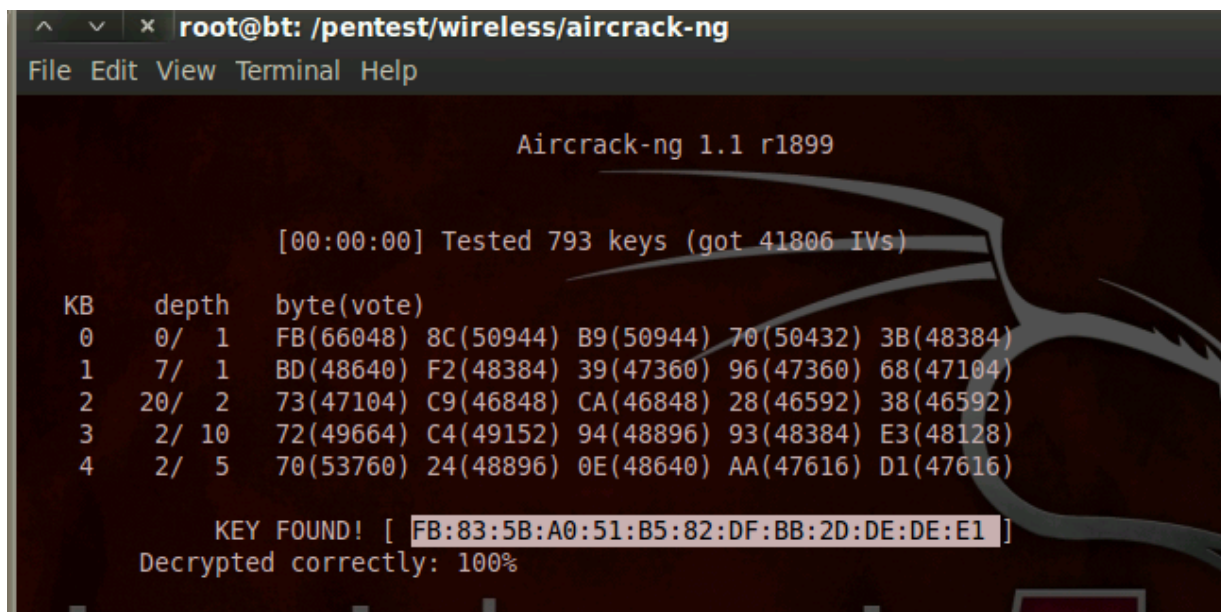


The image shows a Wireshark packet capture window titled 'labcap.cap - Wireshark'. The 'Follow TCP Stream' pane is active, displaying the stream content. The content is a series of lines, each starting with 'steviewiebe929...' followed by a sequence of characters. The last line of the stream is 'is B!lliesux0rz.steveis.king.' which is highlighted in blue. The word 'password' is visible in the background of the stream content.

ACTIVITY – 2

5. What is the WEP key?

Ans: FB:83:5B:A0:51:B5:82:DF:BB:2D:DE:DE:E1



The image shows a terminal window titled 'root@bt: /pentest/wireless/aircrack-ng'. The terminal displays the output of the Aircrack-ng 1.1 r1899 program. It shows a list of keys and their corresponding IVs, with the key 'FB:83:5B:A0:51:B5:82:DF:BB:2D:DE:DE:E1' highlighted in blue. The terminal also shows the message 'KEY FOUND!' and 'Decrypted correctly: 100%'.

ACTIVITY – 3

6. What is the pre-shared key?

Ans: absentminded



```
root@bt: /pentest/wireless/aircrack-ng
File Edit View Terminal Help

Aircrack-ng 1.1 r1899

[00:00:40] 57120 keys tested (1433.90 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:/pentest/wireless/aircrack-ng#
```

7. Which wordlist did you use?

Ans. final-wordlist.txt

8. How long did it take?

Ans: 40 seconds

ACTIVITY – 4

9. What was the user's password?

Ans: password

```
root@bt: ~/Desktop
File Edit View Terminal Help
root@bt:~/Desktop# asleap -r labcap.cap -W /pentest/passwords/wordlists/darkcode.lst
asleap 2.2 - actively recover LEAP/PPTP passwords. <jwright@hasborg.com>
Using wordlist mode with "/pentest/passwords/wordlists/darkcode.lst".

Captured LEAP exchange information:
  username:      jwright
  challenge:     ceb69885c656590c
  response:      7279f65aa49870f45822c89dcbbd73c1b89d377844caead4
  hash bytes:    586c
  NT hash:       8846f7eaae8fb117ad06bdd830b7586c
  password:      password
root@bt:~/Desktop#
```