ıssignment 7

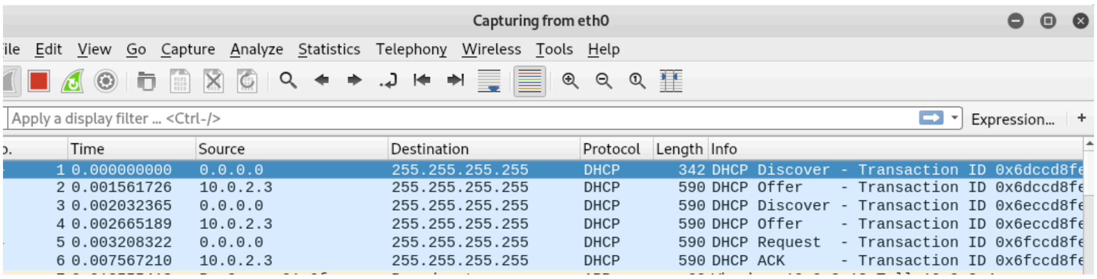
)1)

) The 4 messages in a DHCP sequence, **Discover**, **Offer**, **Request**, **Acknowledge** are each sent s (Layer-2) unicast or broadcast packets?

: can be either unicast or broadcast packets and can be also both. But since unicast is onsidered to be better than broadcast most clients will prefer a unicast reply that matches their ıyer two address.

)2)

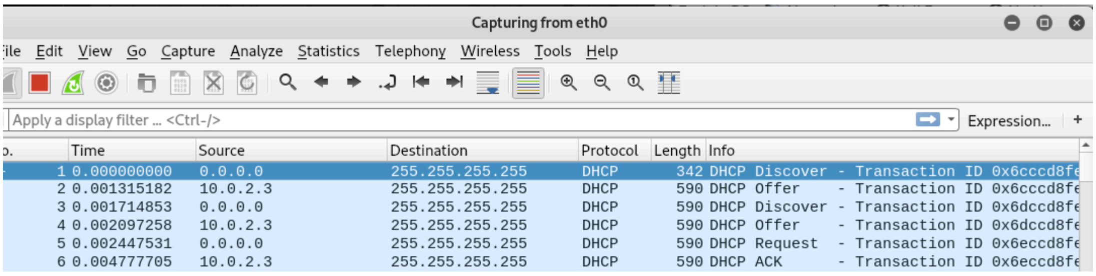
or this question I will first change the Network setting to Promiscuous Mode = Allow Any on oth Kali and DSL. Then I will run kali on eth0 and restart DSL and capture packets



Capturing from eth0
ile Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
).      Time         Source        Destination       Protocol  Length Info
      1 0.000000000  0.0.0.0       255.255.255.255   DHCP        342 DHCP Discover - Transaction ID 0x6dccd8fe
      2 0.001561726  10.0.2.3      255.255.255.255   DHCP        590 DHCP Offer    - Transaction ID 0x6dccd8fe
      3 0.002032365  0.0.0.0       255.255.255.255   DHCP        590 DHCP Discover - Transaction ID 0x6eccd8fe
      4 0.002665189  10.0.2.3      255.255.255.255   DHCP        590 DHCP Offer    - Transaction ID 0x6eccd8fe
      5 0.003208322  0.0.0.0       255.255.255.255   DHCP        590 DHCP Request  - Transaction ID 0x6fccd8fe
      6 0.007567210  10.0.2.3      255.255.255.255   DHCP        590 DHCP ACK      - Transaction ID 0x6fccd8fe
```

'hen i changed the network permission to deny and follow the same step as above and capture he packets.

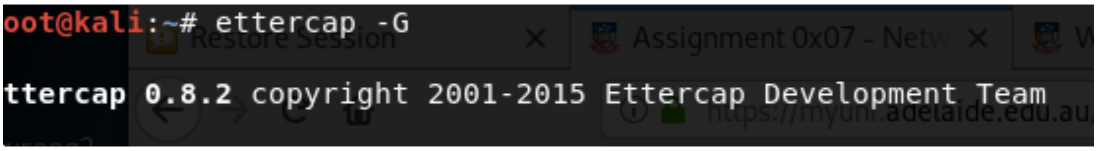


Capturing from eth0
ile Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

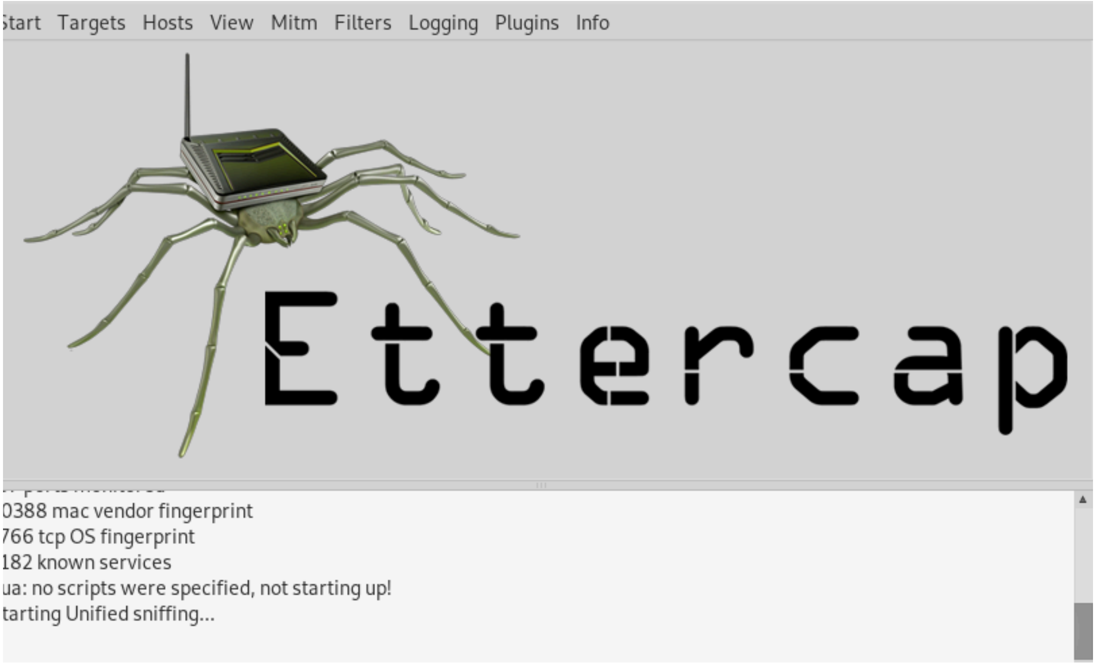
```
).      Time         Source        Destination       Protocol  Length Info
      1 0.000000000  0.0.0.0       255.255.255.255   DHCP        342 DHCP Discover - Transaction ID 0x6cccd8fe
      2 0.001315182  10.0.2.3      255.255.255.255   DHCP        590 DHCP Offer    - Transaction ID 0x6cccd8fe
      3 0.001714853  0.0.0.0       255.255.255.255   DHCP        590 DHCP Discover - Transaction ID 0x6dccd8fe
      4 0.002097258  10.0.2.3      255.255.255.255   DHCP        590 DHCP Offer    - Transaction ID 0x6dccd8fe
      5 0.002447531  0.0.0.0       255.255.255.255   DHCP        590 DHCP Request  - Transaction ID 0x6eccd8fe
      6 0.004777705  10.0.2.3      255.255.255.255   DHCP        590 DHCP ACK      - Transaction ID 0x6eccd8fe
```

)3)

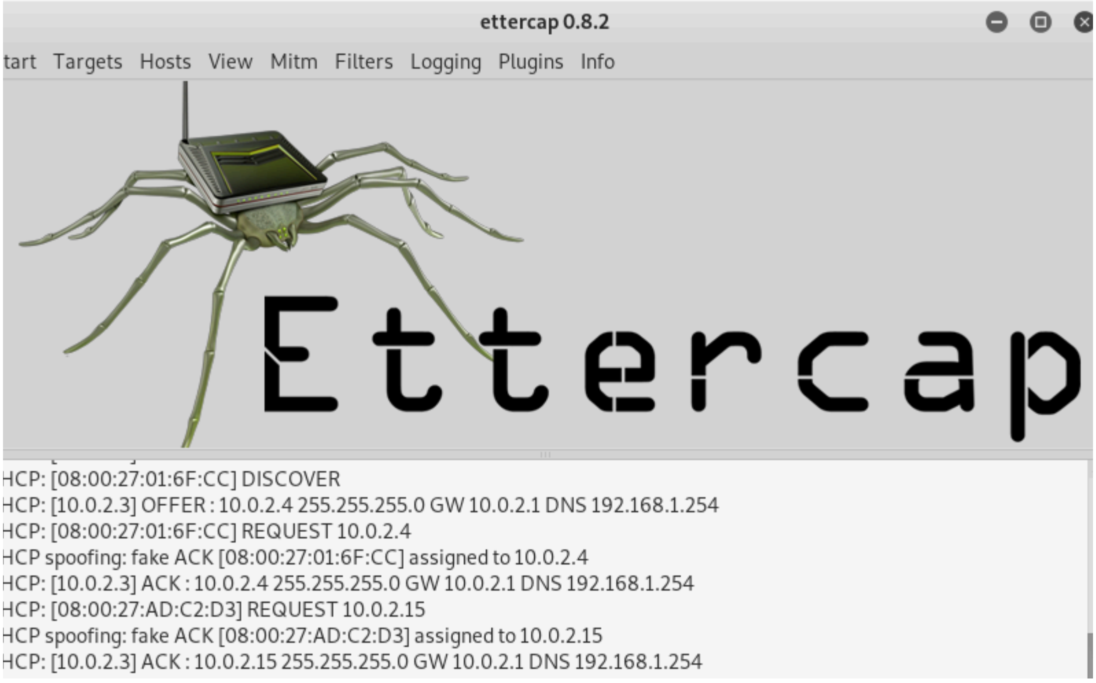
used the command ettercap -G and did the step as the asssignmnet sheet.



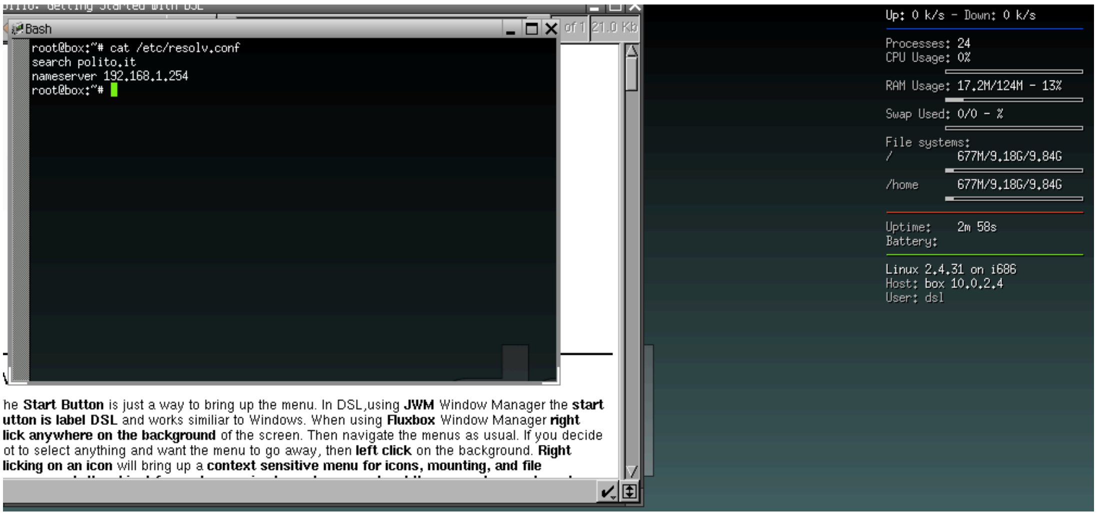
```
oot@kali:~# ettercap -G

ttercap 0.8.2 copyright 2001-2015 Ettercap Development Team
```



```
0388 mac vendor fingerprint
766 tcp OS fingerprint
182 known services
ua: no scripts were specified, not starting up!
tarting Unified sniffing...
```



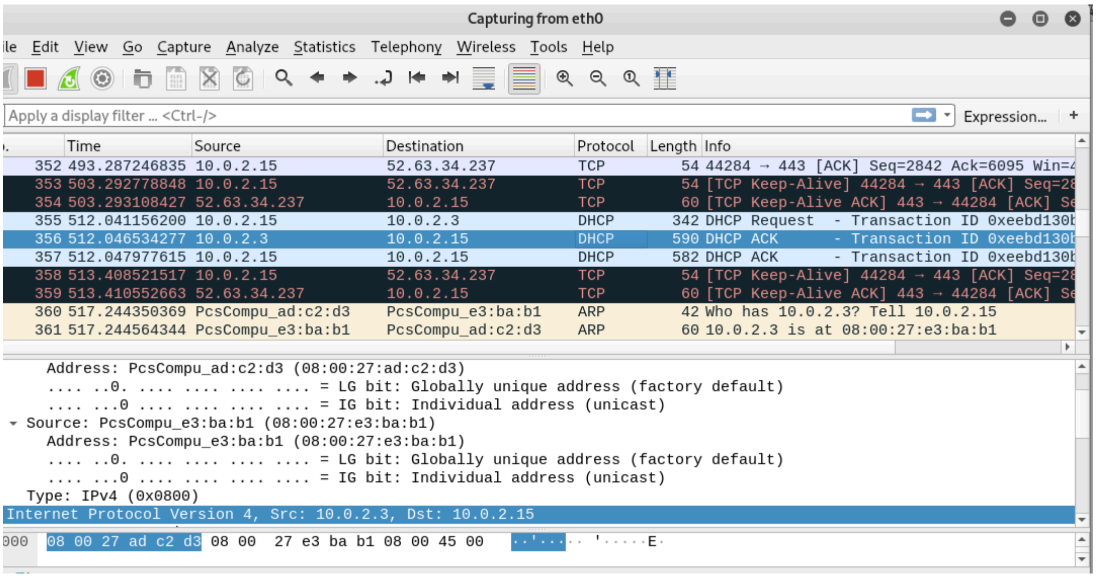
```
HCP: [08:00:27:01:6F:CC] DISCOVER
HCP: [10.0.2.3] OFFER : 10.0.2.4 255.255.255.0 GW 10.0.2.1 DNS 192.168.1.254
HCP: [08:00:27:01:6F:CC] REQUEST 10.0.2.4
HCP spoofing: fake ACK [08:00:27:01:6F:CC] assigned to 10.0.2.4
HCP: [10.0.2.3] ACK : 10.0.2.4 255.255.255.0 GW 10.0.2.1 DNS 192.168.1.254
HCP: [08:00:27:AD:C2:D3] REQUEST 10.0.2.15
HCP spoofing: fake ACK [08:00:27:AD:C2:D3] assigned to 10.0.2.15
HCP: [10.0.2.3] ACK : 10.0.2.15 255.255.255.0 GW 10.0.2.1 DNS 192.168.1.254
```



```
root@box:~# cat /etc/resolv.conf
search polito.it
nameserver 192.168.1.254
root@box:~#
```

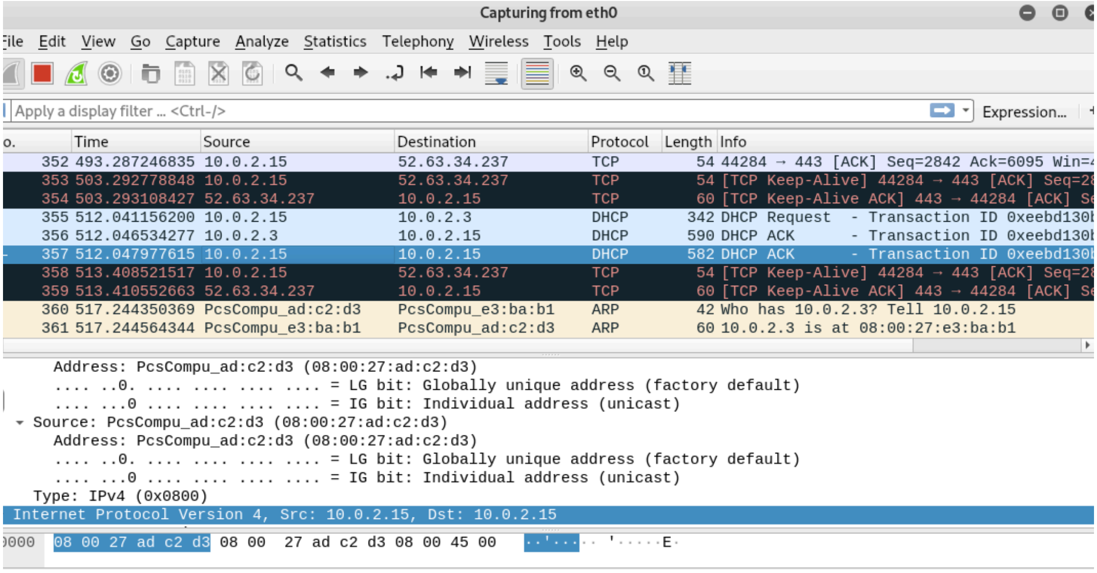
```
Up: 0 k/s - Down: 0 k/s
Processes: 24
CPU Usage: 0%
RAM Usage: 17.2M/124M - 13%
Swap Used: 0/0 - %
File systems:
/          677M/9.18G/9.84G
/home      677M/9.18G/9.84G
Uptime:    2m 58s
Battery:
Linux 2.4.31 on i686
Host: box 10.0.2.4
User: dsl
```

he **Start Button** is just a way to bring up the menu. In DSL,using **JWM** Window Manager the **start utton is label DSL** and works similiar to Windows. When using **Fluxbox** Window Manager **right lick anywhere on the background** of the screen. Then navigate the menus as usual. If you decide ot to select anything and want the menu to go away, then **left click** on the background. **Right licking on an icon** will bring up a **context sensitive menu for icons, mounting, and file**



```
.    Time           Source              Destination         Protocol Length Info
 352 493.287246835 10.0.2.15           52.63.34.237        TCP         54 44284 → 443 [ACK] Seq=2842 Ack=6095 Win=4
 353 503.292778848 10.0.2.15           52.63.34.237        TCP         54 [TCP Keep-Alive] 44284 → 443 [ACK] Seq=28
 354 503.293108427 52.63.34.237        10.0.2.15           TCP         60 [TCP Keep-Alive ACK] 443 → 44284 [ACK] Se
 355 512.041156200 10.0.2.15           10.0.2.3            DHCP       342 DHCP Request  - Transaction ID 0xeebd130b
 356 512.046534277 10.0.2.3            10.0.2.15           DHCP       590 DHCP ACK      - Transaction ID 0xeebd130b
 357 512.047977615 10.0.2.15           10.0.2.15           DHCP       582 DHCP ACK      - Transaction ID 0xeebd130b
 358 513.408521517 10.0.2.15           52.63.34.237        TCP         54 [TCP Keep-Alive] 44284 → 443 [ACK] Seq=28
 359 513.410552663 52.63.34.237        10.0.2.15           TCP         60 [TCP Keep-Alive ACK] 443 → 44284 [ACK] Se
 360 517.244350369 PcsCompu_ad:c2:d3   PcsCompu_e3:ba:b1   ARP         42 Who has 10.0.2.3? Tell 10.0.2.15
 361 517.244564344 PcsCompu_e3:ba:b1   PcsCompu_ad:c2:d3   ARP         60 10.0.2.3 is at 08:00:27:e3:ba:b1

    Address: PcsCompu_ad:c2:d3 (08:00:27:ad:c2:d3)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: PcsCompu_e3:ba:b1 (08:00:27:e3:ba:b1)
    Address: PcsCompu_e3:ba:b1 (08:00:27:e3:ba:b1)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.0.2.3, Dst: 10.0.2.15

000  08 00 27 ad c2 d3 08 00  27 e3 ba b1 08 00 45 00   ··'···· '·····E·
```

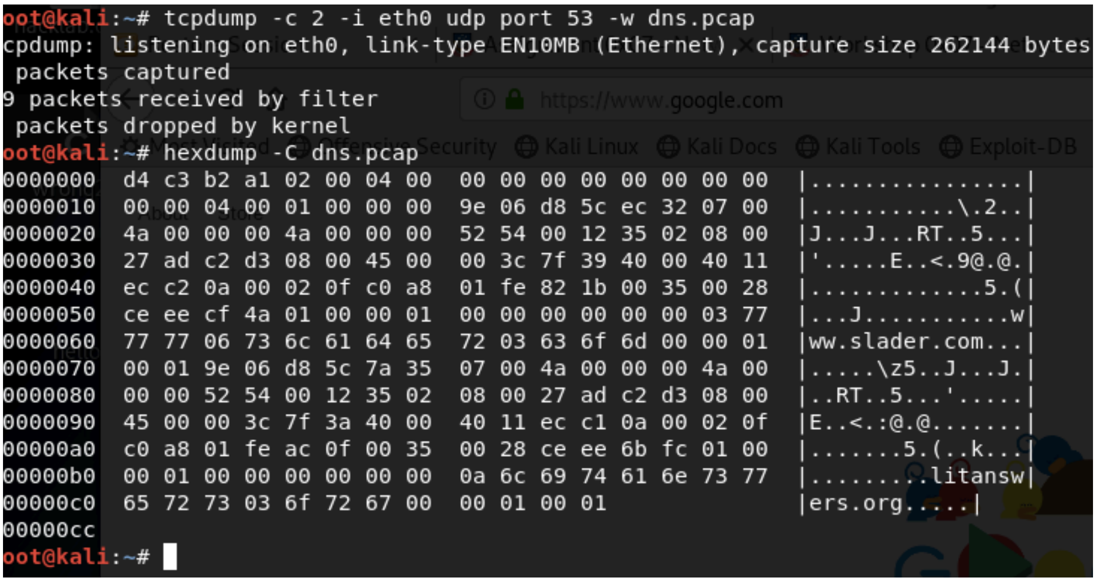
ake ACKcoming from source 10.0.2.15



```
o.   Time           Source              Destination         Protocol Length Info
 352 493.287246835 10.0.2.15           52.63.34.237        TCP         54 44284 → 443 [ACK] Seq=2842 Ack=6095 Win=4
 353 503.292778848 10.0.2.15           52.63.34.237        TCP         54 [TCP Keep-Alive] 44284 → 443 [ACK] Seq=28
 354 503.293108427 52.63.34.237        10.0.2.15           TCP         60 [TCP Keep-Alive ACK] 443 → 44284 [ACK] Se
 355 512.041156200 10.0.2.15           10.0.2.3            DHCP       342 DHCP Request  - Transaction ID 0xeebd130b
 356 512.046534277 10.0.2.3            10.0.2.15           DHCP       590 DHCP ACK      - Transaction ID 0xeebd130b
 357 512.047977615 10.0.2.15           10.0.2.15           DHCP       582 DHCP ACK      - Transaction ID 0xeebd130b
 358 513.408521517 10.0.2.15           52.63.34.237        TCP         54 [TCP Keep-Alive] 44284 → 443 [ACK] Seq=28
 359 513.410552663 52.63.34.237        10.0.2.15           TCP         60 [TCP Keep-Alive ACK] 443 → 44284 [ACK] Se
 360 517.244350369 PcsCompu_ad:c2:d3   PcsCompu_e3:ba:b1   ARP         42 Who has 10.0.2.3? Tell 10.0.2.15
 361 517.244564344 PcsCompu_e3:ba:b1   PcsCompu_ad:c2:d3   ARP         60 10.0.2.3 is at 08:00:27:e3:ba:b1

    Address: PcsCompu_ad:c2:d3 (08:00:27:ad:c2:d3)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: PcsCompu_ad:c2:d3 (08:00:27:ad:c2:d3)
    Address: PcsCompu_ad:c2:d3 (08:00:27:ad:c2:d3)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.15

0000 08 00 27 ad c2 d3 08 00  27 ad c2 d3 08 00 45 00   ··'···· '·····E·
```

'he real and fake DHCP ACK is in the screenshots above.

4)



```
oot@kali:~# tcpdump -c 2 -i eth0 udp port 53 -w dns.pcap
cpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
 packets captured
9 packets received by filter
 packets dropped by kernel
oot@kali:~# hexdump -C dns.pcap
0000000  d4 c3 b2 a1 02 00 04 00  00 00 00 00 00 00 00 00  |................|
0000010  00 00 04 00 01 00 00 00  9e 06 d8 5c ec 32 07 00  |...........\.2..|
0000020  4a 00 00 00 4a 00 00 00  52 54 00 12 35 02 08 00  |J...J...RT..5...|
0000030  27 ad c2 d3 08 00 45 00  00 3c 7f 39 40 00 40 11  |'.....E..<.9@.@.|
0000040  ec c2 0a 00 02 0f c0 a8  01 fe 82 1b 00 35 00 28  |.............5.(|
0000050  ce ee cf 4a 01 00 00 01  00 00 00 00 00 00 03 77  |...J...........w|
0000060  77 77 06 73 6c 61 64 65  72 03 63 6f 6d 00 00 01  |ww.slader.com...|
0000070  00 01 9e 06 d8 5c 7a 35  07 00 4a 00 00 00 4a 00  |.....\z5..J...J.|
0000080  00 00 52 54 00 12 35 02  08 00 27 ad c2 d3 08 00  |..RT..5...'.....|
0000090  45 00 00 3c 7f 3a 40 00  40 11 ec c1 0a 00 02 0f  |E..<.:@.@.......|
00000a0  c0 a8 01 fe ac 0f 00 35  00 28 ce ee 6b fc 01 00  |.......5.(..k...|
00000b0  00 01 00 00 00 00 00 00  0a 6c 69 74 61 6e 73 77  |.........litansw|
00000c0  65 72 73 03 6f 72 67 00  00 01 00 01              |ers.org.....|
00000cc
oot@kali:~#
```