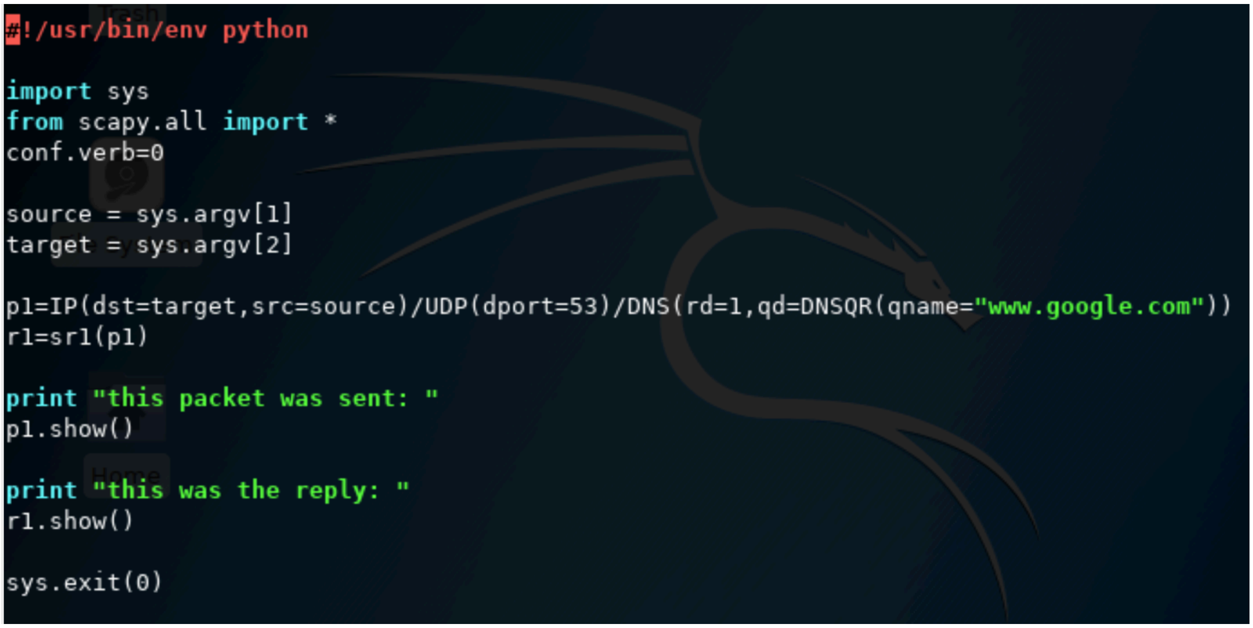
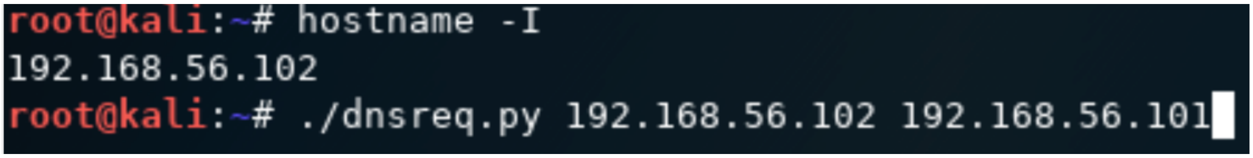
Willis Allstead
2/25/19
CS 445

SCAPY

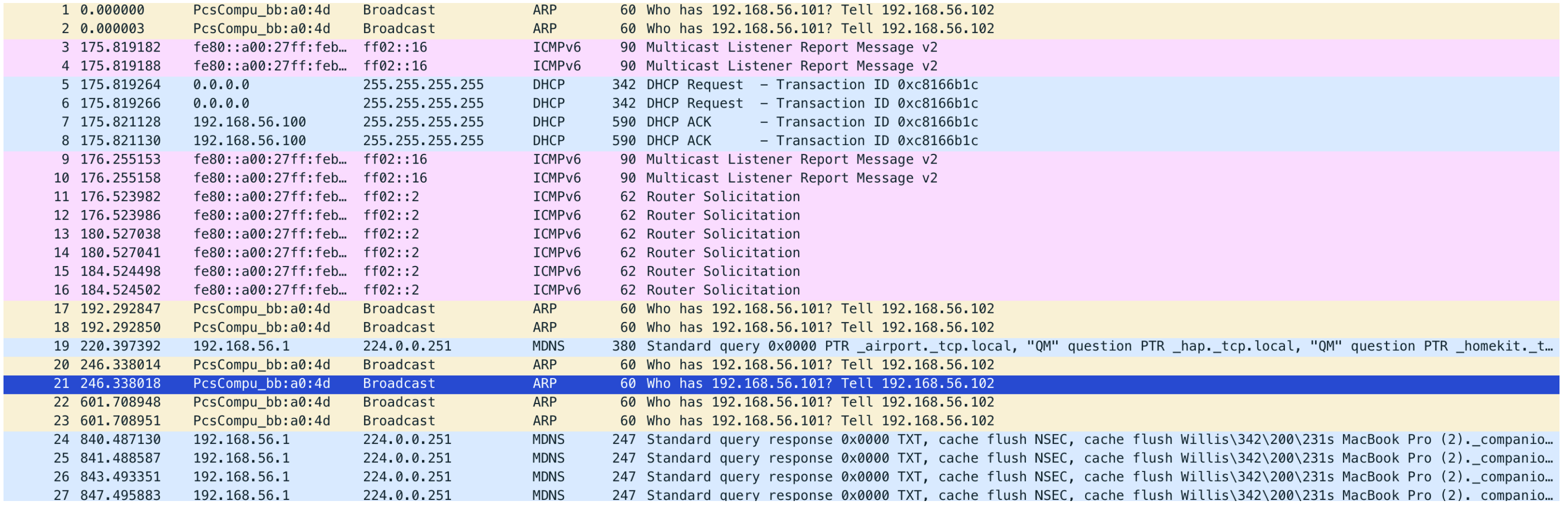


```
#!/usr/bin/env python

import sys
from scapy.all import *
conf.verb=0

source = sys.argv[1]
target = sys.argv[2]

p1=IP(dst=target,src=source)/UDP(dport=53)/DNS(rd=1,qd=DNSQR(qname="www.google.com"))
r1=sr1(p1)

print "this packet was sent: "
p1.show()

print "this was the reply: "
r1.show()

sys.exit(0)
```



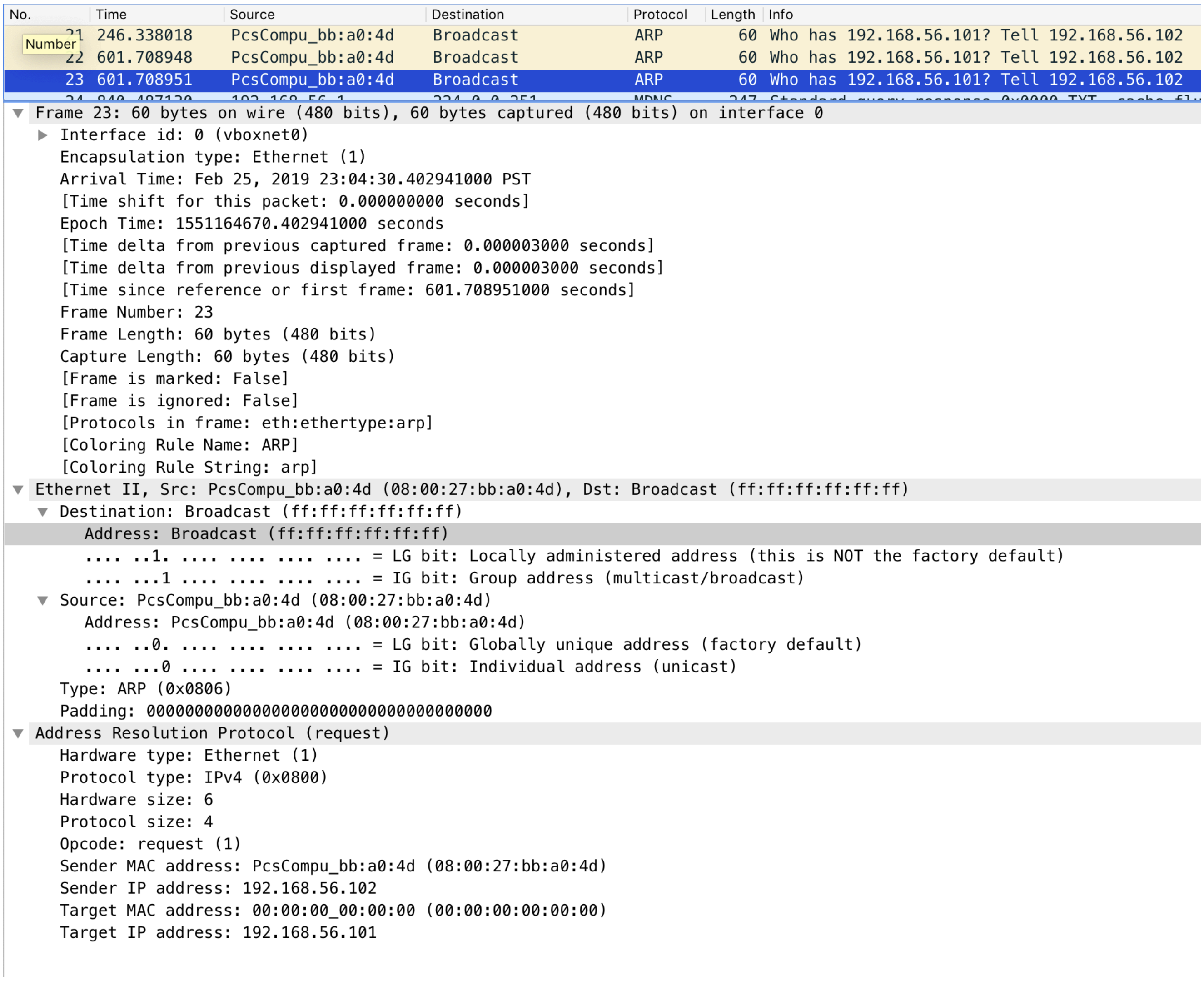
```
root@kali:~# hostname -I
192.168.56.102
root@kali:~# ./dnsreq.py 192.168.56.102 192.168.56.101
```

Upon connecting to the host-only adapter and running that script, with another VM running with IP address 192.168.56.101, the following packets are shown passing through the host-only adapter:



```
 1 0.000000     PcsCompu_bb:a0:4d    Broadcast        ARP       60 Who has 192.168.56.101? Tell 192.168.56.102
 2 0.000003     PcsCompu_bb:a0:4d    Broadcast        ARP       60 Who has 192.168.56.101? Tell 192.168.56.102
 3 175.819182   fe80::a00:27ff:feb…  ff02::16         ICMPv6    90 Multicast Listener Report Message v2
 4 175.819188   fe80::a00:27ff:feb…  ff02::16         ICMPv6    90 Multicast Listener Report Message v2
 5 175.819264   0.0.0.0              255.255.255.255  DHCP     342 DHCP Request  - Transaction ID 0xc8166b1c
 6 175.819266   0.0.0.0              255.255.255.255  DHCP     342 DHCP Request  - Transaction ID 0xc8166b1c
 7 175.821128   192.168.56.100       255.255.255.255  DHCP     590 DHCP ACK      - Transaction ID 0xc8166b1c
 8 175.821130   192.168.56.100       255.255.255.255  DHCP     590 DHCP ACK      - Transaction ID 0xc8166b1c
 9 176.255153   fe80::a00:27ff:feb…  ff02::16         ICMPv6    90 Multicast Listener Report Message v2
10 176.255158   fe80::a00:27ff:feb…  ff02::16         ICMPv6    90 Multicast Listener Report Message v2
11 176.523982   fe80::a00:27ff:feb…  ff02::2          ICMPv6    62 Router Solicitation
12 176.523986   fe80::a00:27ff:feb…  ff02::2          ICMPv6    62 Router Solicitation
13 180.527038   fe80::a00:27ff:feb…  ff02::2          ICMPv6    62 Router Solicitation
14 180.527041   fe80::a00:27ff:feb…  ff02::2          ICMPv6    62 Router Solicitation
15 184.524498   fe80::a00:27ff:feb…  ff02::2          ICMPv6    62 Router Solicitation
16 184.524502   fe80::a00:27ff:feb…  ff02::2          ICMPv6    62 Router Solicitation
17 192.292847   PcsCompu_bb:a0:4d    Broadcast        ARP       60 Who has 192.168.56.101? Tell 192.168.56.102
18 192.292850   PcsCompu_bb:a0:4d    Broadcast        ARP       60 Who has 192.168.56.101? Tell 192.168.56.102
19 220.397392   192.168.56.1         224.0.0.251      MDNS     380 Standard query 0x0000 PTR _airport._tcp.local, "QM" question PTR _hap._tcp.local, "QM" question PTR _homekit._t…
20 246.338014   PcsCompu_bb:a0:4d    Broadcast        ARP       60 Who has 192.168.56.101? Tell 192.168.56.102
21 246.338018   PcsCompu_bb:a0:4d    Broadcast        ARP       60 Who has 192.168.56.101? Tell 192.168.56.102
22 601.708948   PcsCompu_bb:a0:4d    Broadcast        ARP       60 Who has 192.168.56.101? Tell 192.168.56.102
23 601.708951   PcsCompu_bb:a0:4d    Broadcast        ARP       60 Who has 192.168.56.101? Tell 192.168.56.102
24 840.487130   192.168.56.1         224.0.0.251      MDNS     247 Standard query response 0x0000 TXT, cache flush NSEC, cache flush Willis\342\200\231s MacBook Pro (2)._companio…
25 841.488587   192.168.56.1         224.0.0.251      MDNS     247 Standard query response 0x0000 TXT, cache flush NSEC, cache flush Willis\342\200\231s MacBook Pro (2)._companio…
26 843.493351   192.168.56.1         224.0.0.251      MDNS     247 Standard query response 0x0000 TXT, cache flush NSEC, cache flush Willis\342\200\231s MacBook Pro (2)._companio…
27 847.495883   192.168.56.1         224.0.0.251      MDNS     247 Standard query response 0x0000 TXT, cache flush NSEC, cache flush Willis\342\200\231s MacBook Pro (2)._companio…
```

Whenever I run the script, more ARP broadcasts show up instantly. I was expecting to see plain DNS requests but I am not. Here is one of the ARP requests in more detail:



```
No.    Time        Source               Destination   Protocol  Length  Info
   21  246.338018  PcsCompu_bb:a0:4d    Broadcast     ARP           60  Who has 192.168.56.101? Tell 192.168.56.102
   22  601.708948  PcsCompu_bb:a0:4d    Broadcast     ARP           60  Who has 192.168.56.101? Tell 192.168.56.102
   23  601.708951  PcsCompu_bb:a0:4d    Broadcast     ARP           60  Who has 192.168.56.101? Tell 192.168.56.102
   24  840.487130  192.168.56.1         224.0.0.251   MDNS         247  Standard query response 0x0000 TXT, cache fl…
```

```
▼ Frame 23: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
  ▶ Interface id: 0 (vboxnet0)
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb 25, 2019 23:04:30.402941000 PST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1551164670.402941000 seconds
    [Time delta from previous captured frame: 0.000003000 seconds]
    [Time delta from previous displayed frame: 0.000003000 seconds]
    [Time since reference or first frame: 601.708951000 seconds]
    Frame Number: 23
    Frame Length: 60 bytes (480 bits)
    Capture Length: 60 bytes (480 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:arp]
    [Coloring Rule Name: ARP]
    [Coloring Rule String: arp]
▼ Ethernet II, Src: PcsCompu_bb:a0:4d (08:00:27:bb:a0:4d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▼ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Address: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  ▼ Source: PcsCompu_bb:a0:4d (08:00:27:bb:a0:4d)
      Address: PcsCompu_bb:a0:4d (08:00:27:bb:a0:4d)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
▼ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: PcsCompu_bb:a0:4d (08:00:27:bb:a0:4d)
    Sender IP address: 192.168.56.102
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.56.101
```

I have a feeling I did something wrong in the setup, or possibly in writing the script. I do believe I should be seeing plain DNS requests in wireshark, but I am not. If I remember correctly from previous classes, ARP requests map IP addresses to MAC addresses. Maybe because the VMs are not actually connected to external global internet, they cannot successfully pass DNS requests to each other?