IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

Foundational Packetry

Using SCAPY to understand
the foundations of the internet.

IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

Matt Erasmus

- An “enthusiastic amateur”
- Tinkerer
- Short attention spanner
- Or just a spanner

IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

Éireann Leverett

- Primarily Matt's sidekick
- Sometimes I get to turn the slides too!
- OK, I once slew the air-gap in SCADA, but I had had coffee.

Why?

"You know you have a distributed system when the crash of a computer you've never heard of stops you from getting any work done."

—LESLIE LAMPORT

DAFUQ?

We’re going to understand the distributed computing of the internet.

To do that we’re going to study some simple protocols you THINK you understand.

ARP

DNS

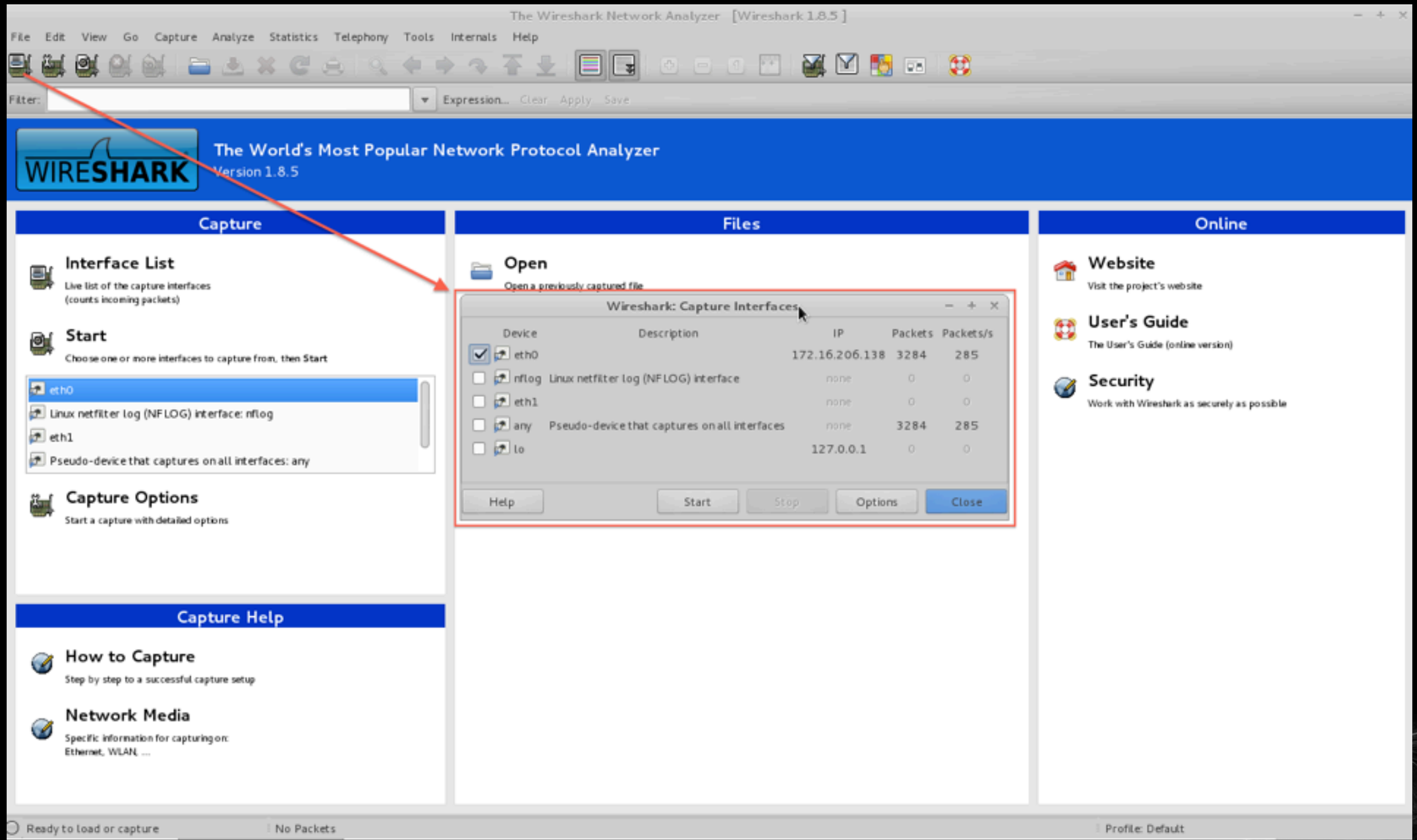
DHCP

HTTP

When you’re done you’ll be better at SCAPY, and at foundational networking.

IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

Wireshark is installed


The Wireshark Network Analyzer [Wireshark 1.8.5]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Version 1.8.5
Capture
Interface List
Live list of the capture interfaces
(counts incoming packets)
Start
Choose one or more interfaces to capture from, then Start
eth0
Linux netfilter log (NFLOG) interface: nflog
eth1
Pseudo-device that captures on all interfaces: any
Capture Options
Start a capture with detailed options
Files
Open
Open a previously captured file
Wireshark: Capture Interfaces
Device Description IP Packets Packets/s
eth0 172.16.206.138 3284 285
nflog Linux netfilter log (NFLOG) interface none 0 0
eth1 none 0 0
any Pseudo-device that captures on all interfaces none 3284 285
lo 127.0.0.1 0 0
Help Start Stop Options Close
Online
Website
Visit the project's website
User's Guide
The User's Guide (online version)
Security
Work with Wireshark as securely as possible
Capture Help
How to Capture
Step by step to a successful capture setup
Network Media
Specific information for capturing on:
Ethernet, WLAN, ...
Ready to load or capture
No Packets
Profile: Default

IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

How to Install SCAPY

Making packet porn easier

```
tcpdump
graphviz
imagemagick
gnuplot
python-gnuplot
python-crypto
python-pyx
```

man SCAPY

IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

lsc()

ls(TCP)

send() / sendp()

sr() / srp()

a = rdpcap(“~/pkts/dhcp.pcap”)

a.summary()

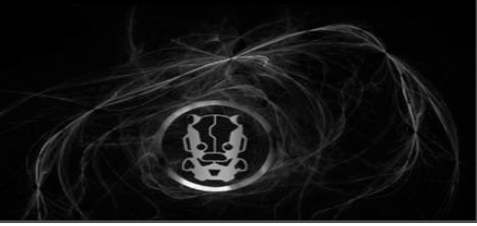
a[3].show()

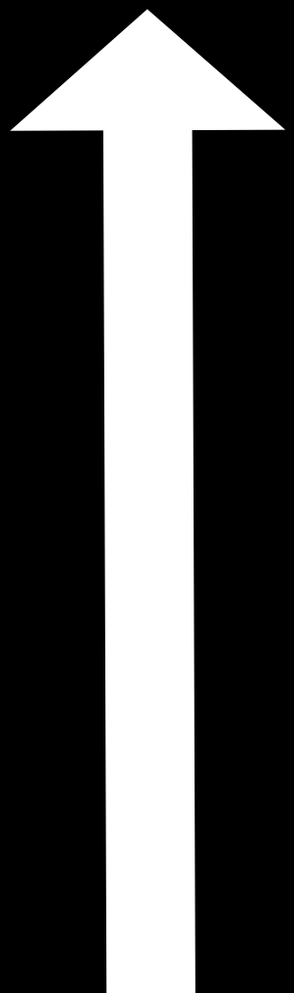
a.psdump("~/pkts/dhcp.eps", layer_shift=1)

a.pdfdump(“~/pkts/dhcp.pdf”, layer_shift=1)

wrpcap(“/pkts/dhcp.pcap”, packets)

wireshark(a)





```
 .d8b.  d8888b. d8888b. db      d888888b  .o88b.  .d8b.  d888888b d888888b  .d88b.  d8b   db
d8' `8b 88  `8D 88  `8D 88        `88'   d8P  Y8 d8' `8b `~~88~~'   `88'   .8P  Y8. 888o  88
88ooo88 88oodD' 88oodD' 88         88    8P      88ooo88    88       88    88    88 88V8o 88
88~~~88 88~~~   88~~~   88         88    8b      88~~~88    88       88    88    88 88 V8o88
88   88 88      88      88booo.   .88.   Y8b  d8 88   88    88      .88.   `8b  d8' 88  V888
YP   YP 88      88      Y88888P Y888888P  `Y88P' YP   YP    YP    Y888888P  `Y88P'  VP   V8P

d8888b. d8888b. d88888b .d8888. d88888b d8b   db d888888b  .d8b.  d888888b d888888b  .d88b.  d8b   db
88  `8D 88  `8D 88'     88'  YP 88'     888o  88 `~~88~~' d8' `8b `~~88~~'    `88'   .8P  Y8. 888o  88
88oodD' 88oobY' 88ooooo `8bo.   88ooooo 88V8o 88    88    88ooo88    88       88    88    88 88V8o 88
88~~~   88`8b   88~~~~~   `Y8b. 88~~~~~ 88 V8o88    88    88~~~88    88       88    88    88 88 V8o88
88      88 `88. 88.     db   8D 88.     88  V888    88    88   88    88      .88.   `8b  d8' 88  V888
88      88   YD Y88888P `8888Y' Y88888P VP   V8P    YP    YP   YP    YP    Y888888P  `Y88P'  VP   V8P

.d8888. d88888b .d8888. .d8888. d888888b  .d88b.  d8b   db
88'  YP 88'     88'  YP 88'  YP   `88'   .8P  Y8. 888o  88
`8bo.   88ooooo `8bo.   `8bo.     88    88    88 88V8o 88
  `Y8b. 88~~~~~   `Y8b.   `Y8b.   88    88    88 88 V8o88
db   8D 88.     db   8D db   8D  .88.   `8b  d8' 88  V888
`8888Y' Y88888P `8888Y' `8888Y' Y888888P  `Y88P'  VP   V8P

d888888b d8888b.  .d8b.  d8b   db .d8888. d8888b.  .d88b.  d8888b. d888888b
`~~88~~' 88  `8D d8' `8b 888o  88 88'  YP 88  `8D .8P  Y8. 88  `8D `~~88~~'
   88    88oobY' 88ooo88 88V8o 88 `8bo.   88oodD' 88    88 88oobY'    88
   88    88`8b   88~~~88 88 V8o88   `Y8b. 88~~~   88    88 88`8b      88
   88    88 `88. 88   88 88  V888 db   8D 88      `8b  d8' 88 `88.    88
   YP    88   YD YP   YP VP   V8P `8888Y' 88       `Y88P'  88   YD    YP

d8b   db d88888b d888888b db   d8b   db  .d88b.  d8888b. db   dD
888o  88 88'     `~~88~~' 88   I8I   88 .8P  Y8. 88  `8D 88 ,8P'
88V8o 88 88ooooo    88    88   I8I   88 88    88 88oobY' 88,8P
88 V8o88 88~~~~~    88    Y8   I8I   88 88    88 88`8b   88`8b
88  V888 88.        88    `8b d8'8b d8' `8b  d8' 88 `88. 88 `88.
VP   V8P Y88888P    YP     `8b8' `8d8'   `Y88P'  88   YD YP   YD

d8888b.  .d8b.  d888888b  .d8b.    db      d888888b d8b   db db   dD
88  `8D d8' `8b `~~88~~' d8' `8b   88        `88'   888o  88 88 ,8P'
88   88 88ooo88    88    88ooo88   88         88    88V8o 88 88,8P
88   88 88~~~88    88    88~~~88   88         88    88 V8o88 88`8b
88  .8D 88   88    88    88   88   88booo.   .88.   88  V888 88 `88.
Y8888D' YP   YP    YP    YP   YP   Y88888P Y888888P VP   V8P YP   YD

d8888b. db   db db    db .d8888. d888888b  .o88b.  .d8b.  db
88  `8D 88   88 `8b  d8' 88'  YP   `88'   d8P  Y8 d8' `8b 88
88oodD' 88ooo88  `8bd8'  `8bo.      88    8P      88ooo88 88
88~~~   88~~~88    88      `Y8b.    88    8b      88~~~88 88
88      88   88    88    db   8D   .88.   Y8b  d8 88   88 88booo.
88      YP   YP    YP    `8888Y' Y888888P  `Y88P' YP   YP Y88888P
```

send() and sr()

sendp() and srp()

Ether / ARP Who-has

Ether / ARP Is-at

Ether / IP / UDP / BOOTP / DHCP Discover

Ether / IP / UDP / BOOTP / DHCP Offer

Ether / IP / UDP / DHCP Request

Ether / IP / UDP / DHCP Ack

Ether / IP / UDP / DNS Query

Ether / IP / UDP / DNS Response

Ether / IP / TCP / HTTP GET

Ether / IP / TCP / HTTP RESPONSE

Enough, let's sling packets

```
ip = IP(dst="8.8.8.8")
ip.show()

ping = ICMP()
ping.show()
packet = ip/ping
packet.show()

fling = sr1(packet)
fling.show() or fling.summary()
```

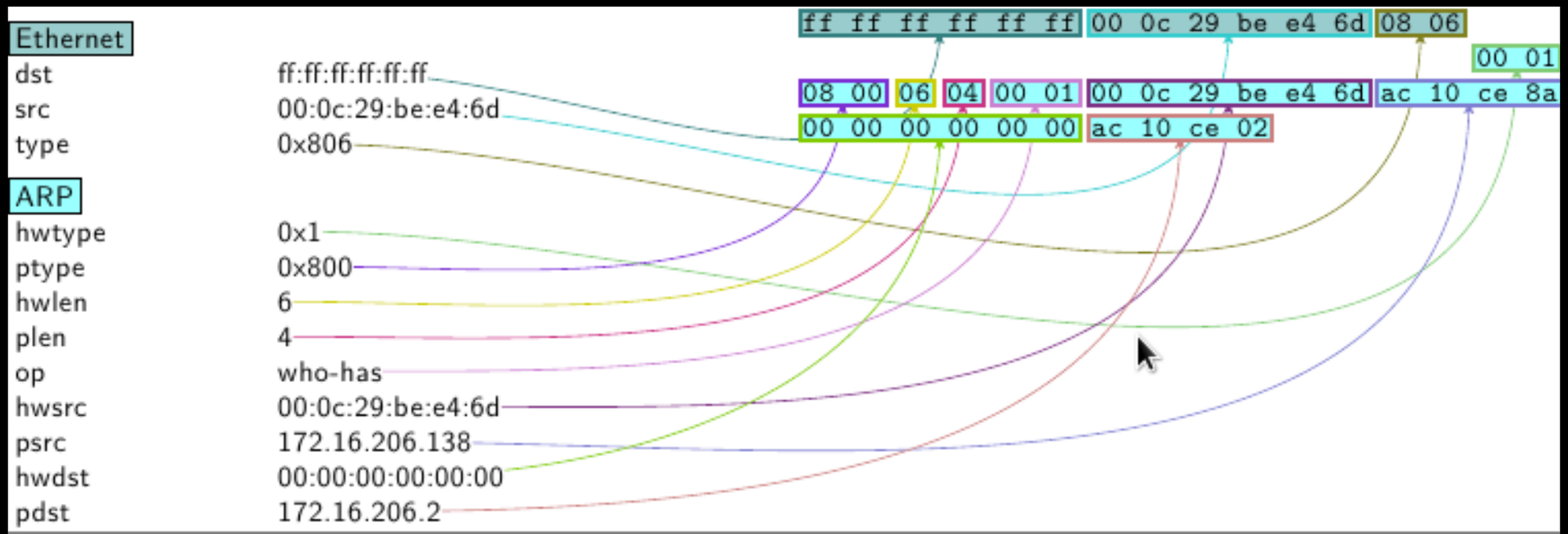
ARP Explanation

Message Types:

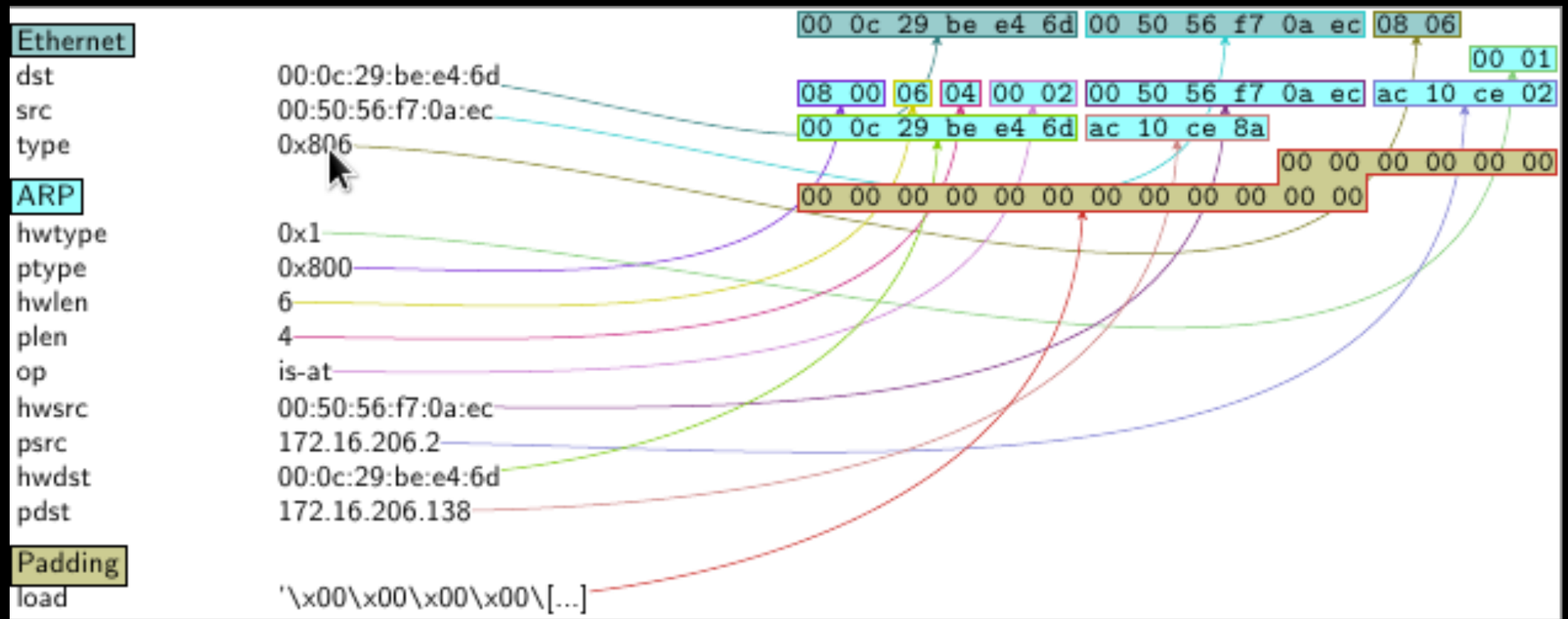
- Probes
- Announcements
  - Request (who-has)
  - Reply (is-at)

Resolves network layer addresses into link layer addresses

ARP who-has


Ethernet
dst
src
type
ff:ff:ff:ff:ff:ff
00:0c:29:be:e4:6d
0x806
ARP
hwtype
ptype
hwlen
plen
op
hwsrc
psrc
hwdst
pdst
0x1
0x800
6
4
who-has
00:0c:29:be:e4:6d
172.16.206.138
00:00:00:00:00:00
172.16.206.2
ff ff ff ff ff ff
00 0c 29 be e4 6d
08 06
00 01
08 00
06
04
00 01
00 0c 29 be e4 6d
ac 10 ce 8a
00 00 00 00 00 00
ac 10 ce 02

ARP is-at


Ethernet
dst
src
type
00:0c:29:be:e4:6d
00:50:56:f7:0a:ec
0x806
ARP
hwtype
ptype
hwlen
plen
op
hwsrc
psrc
hwdst
pdst
0x1
0x800
6
4
is-at
00:50:56:f7:0a:ec
172.16.206.2
00:0c:29:be:e4:6d
172.16.206.138
Padding
load
'\x00\x00\x00\x00\[...]
00 0c 29 be e4 6d 00 50 56 f7 0a ec 08 06
00 01
08 00 06 04 00 02 00 50 56 f7 0a ec ac 10 ce 02
00 0c 29 be e4 6d ac 10 ce 8a
00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00

ARP Solution

IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

```
e = Ether()
e.dst=”ff:ff:ff:ff:ff:ff”
e.type=0x806
a = ARP()
a.hwtype=0x1
a.op="who-has"
a.hwsrc="00:0c:29:be:e4:6d"
a.hwdst="00:00:00:00:00:00"
a.pdst="172.16.206.2"
packet = e/a

ans,unans = srp(packet, iface="eth0")
for snd,rcv in ans:
    macaddy = rcv.sprintf(r"%Ether.src%")

print "MAC address for: " + a.pdst + “is “ + macaddy
```

DNS Explanation

Given a domain get an IP address.

Can also do reverse DNS

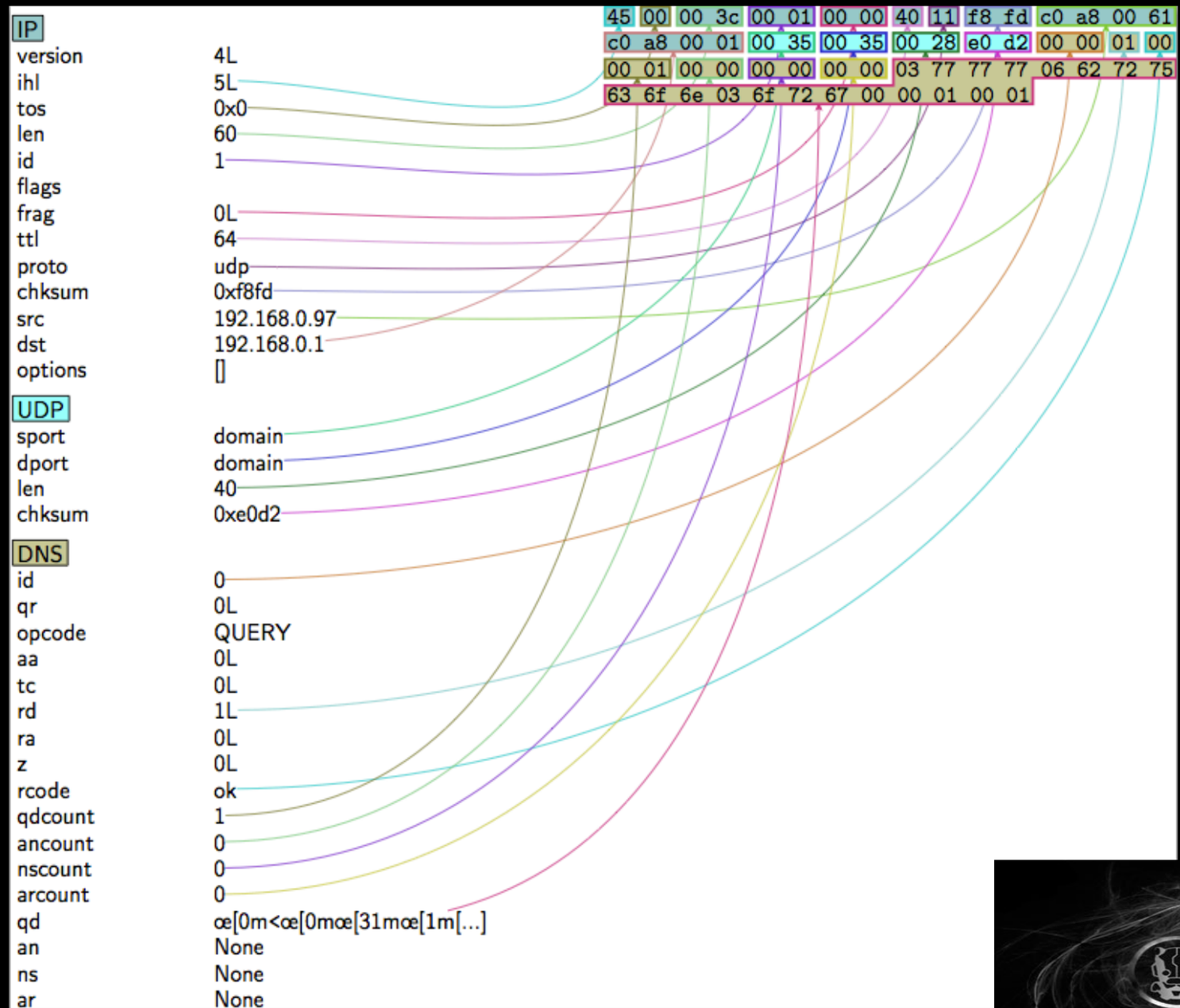
Sometimes used for other things

Simple query -> response format

IP / UDP / DNS

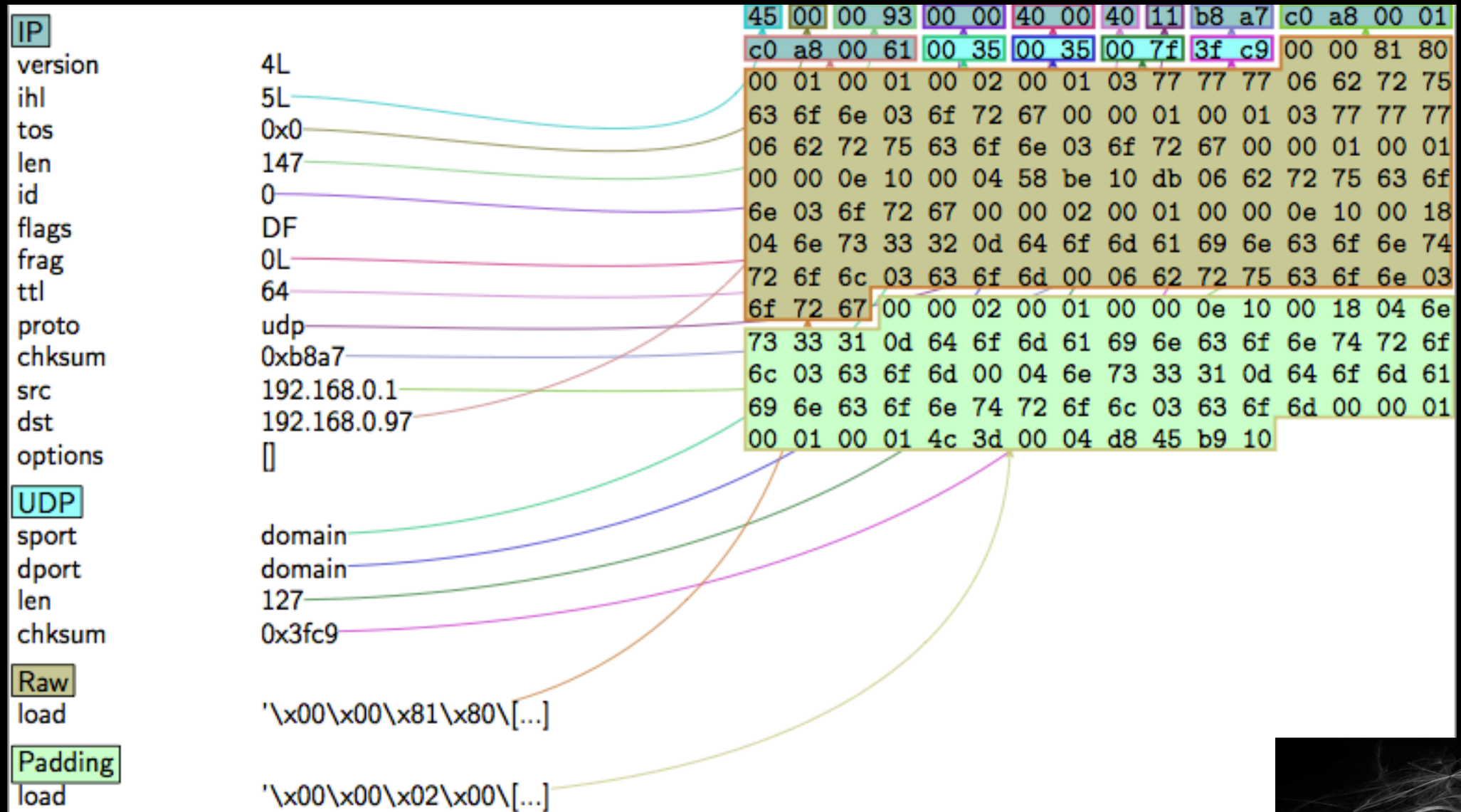
DNS is considered Application Layer

DNS query


45 00 00 3c 00 01 00 00 40 11 f8 fd c0 a8 00 61
c0 a8 00 01 00 35 00 35 00 28 e0 d2 00 00 01 00
00 01 00 00 00 00 00 00 03 77 77 77 06 62 72 75
63 6f 6e 03 6f 72 67 00 00 01 00 01
IP
version 4L
ihl 5L
tos 0x0
len 60
id 1
flags
frag 0L
ttl 64
proto udp
chksum 0xf8fd
src 192.168.0.97
dst 192.168.0.1
options []
UDP
sport domain
dport domain
len 40
chksum 0xe0d2
DNS
id 0
qr 0L
opcode QUERY
aa 0L
tc 0L
rd 1L
ra 0L
z 0L
rcode ok
qdcount 1
ancount 0
nscount 0
arcount 0
qd œ[0m<œ[0mœ[31mœ[1m[...]
an None
ns None
ar None

DNS Response

IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES



DNS Solution

```
i = IP(dst=”8.8.8.8”)
u = UDP()
d = DNS(rd=1,qd=DNSQR(qname="www.brucon.org"))

packet = i/u/d

x = sr1(packet)
x.display()
```

DHCP Explanation

Message Types:

- Discover (Client)
- Offer (Server)
- Request (Client)
- Ack (Server)
- Info (Client)
- Release (Client)

Also called BOOTP

STACK:

Ether()/

IP()/

UDP()/

BOOTP()/

DHCP()

DHCP Addressing

Stop and think about this.

You have no address.
And you have no default gateway.

How does this conversation happen ?

DHCP Gotchas

Disable DHCP on the interface you will use

Run i(f||p)config & note your MAC address

Now set a variable in SCAPY:

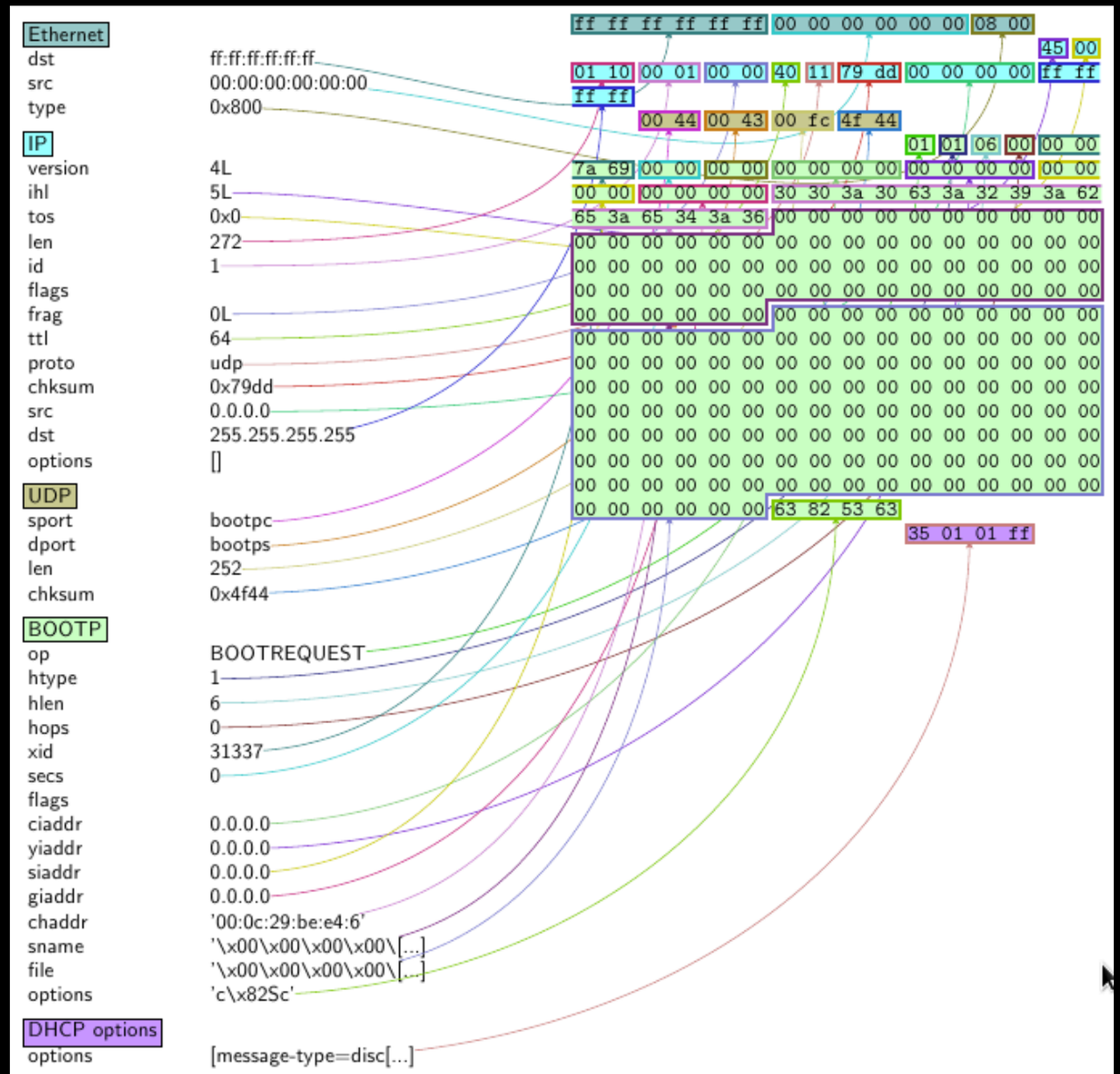
hw = '2b:42:31:5c:2a:73'

Filter on BOOTP in wireshark

Disable IP checking in SCAPY:

Conf.checkIPaddr = False

DHCP Discover

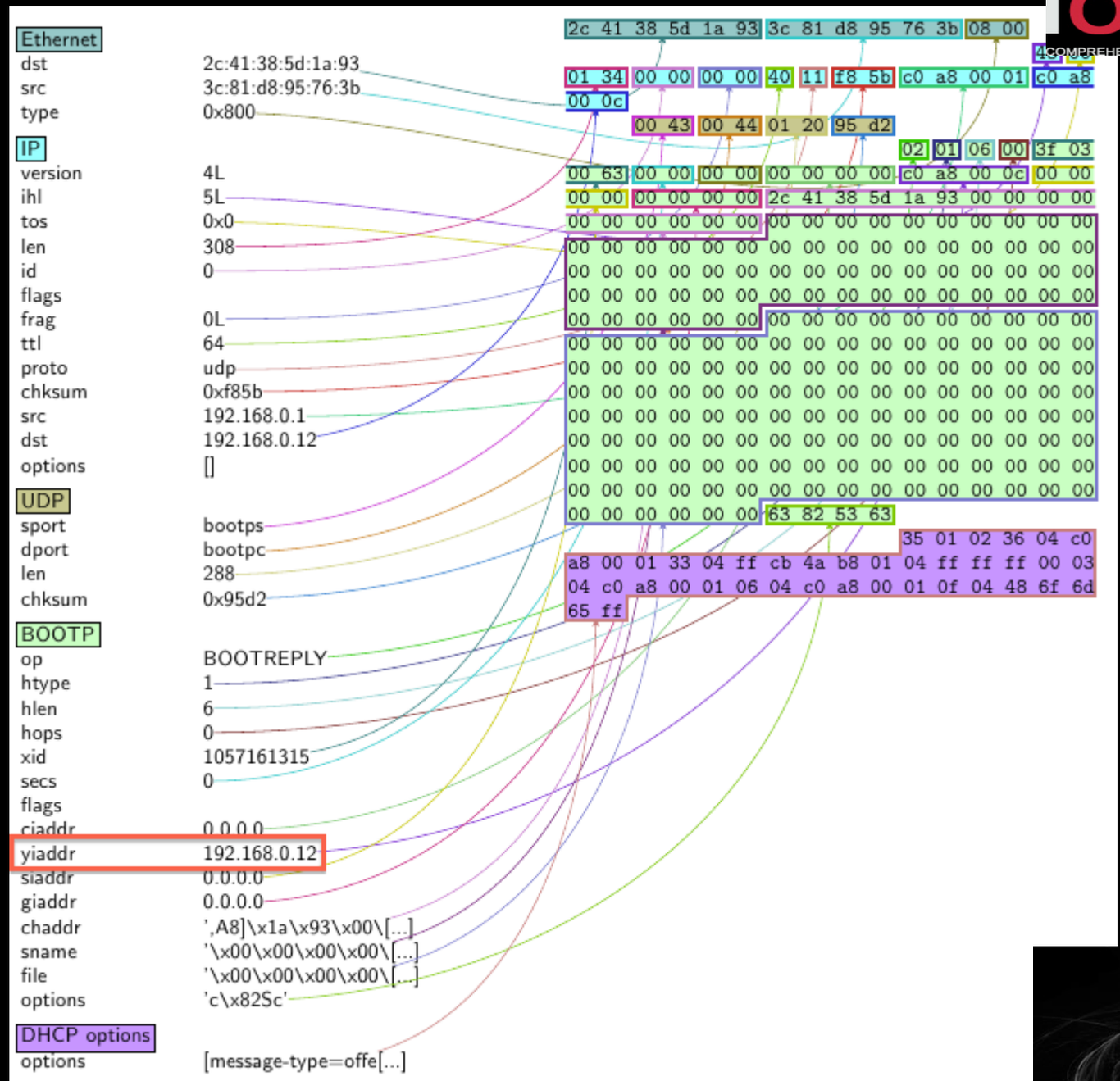


DHCP Discover

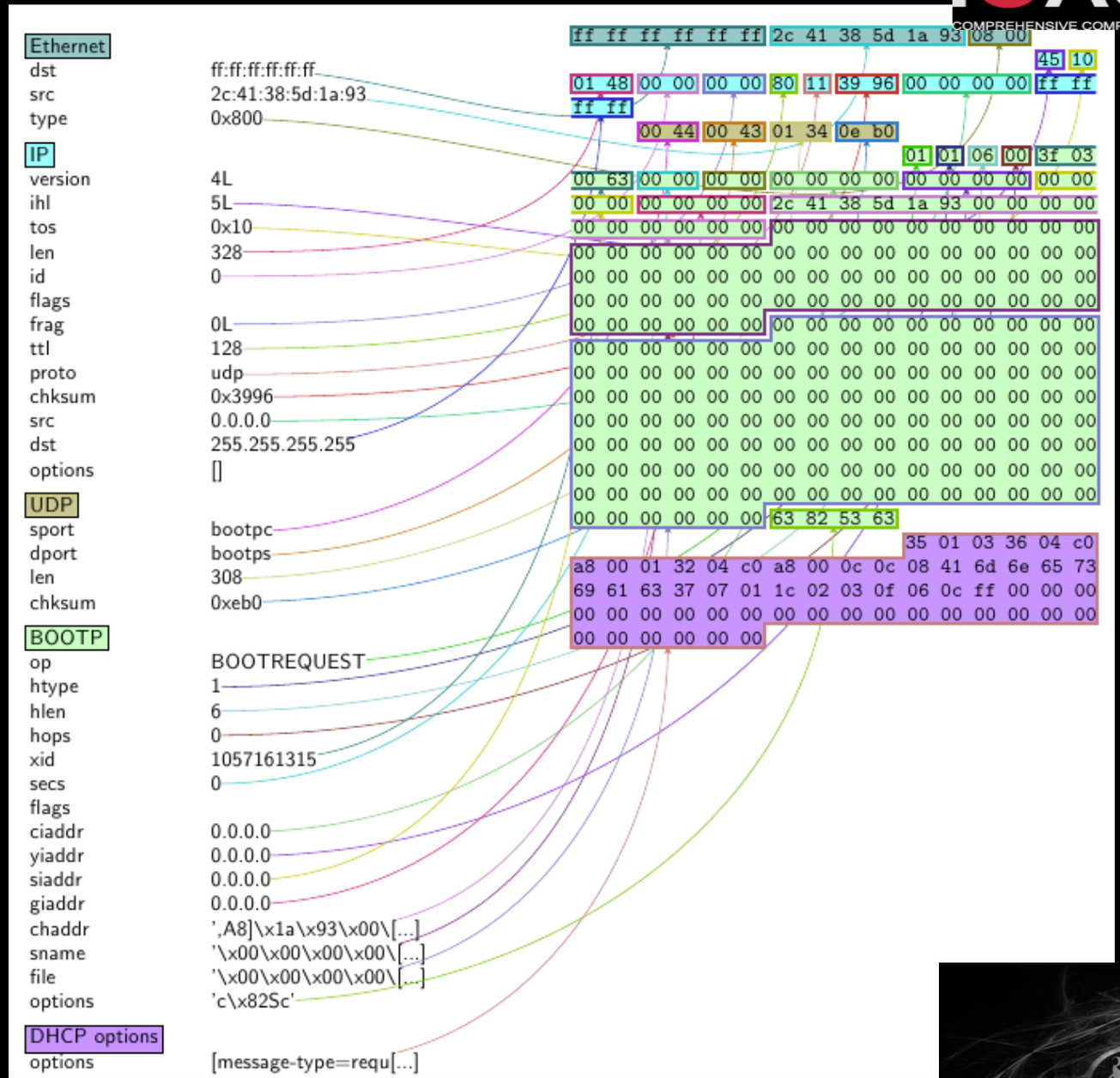
IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

```
conf.checkIPaddr = False
hw="00:0c:29:be:e4:6d"

e = Ether(dst="ff:ff:ff:ff:ff:ff")
i = IP(src="0.0.0.0",dst="255.255.255.255")
u = UDP(sport=68,dport=67)
b = BOOTP(chaddr=hw,xid=31337)
d = DHCP(options=[("message-type","discover"),"end"])

packet = e/i/u/b/d

srp(packet, iface="eth0", timeout=3)

# Why is there no reply to this packet ?
```

DHCP Offer



DHCP Request



DHCP Request

```
hw="00:0c:29:be:e4:6d"
e = Ether(dst="ff:ff:ff:ff:ff:ff")
i = IP(src="0.0.0.0",dst="255.255.255.255")
u = UDP(sport=68,dport=67)
b = BOOTP(chaddr=hw,xid=31337)
d = DHCP(options=[("message-type","request"),IPField("requested_addr","172.16.206.138"),"end"])

packet = e/i/u/b/d

srp(packet, iface="eth0")

# Use wireshark or pkt.display() in scapy to get your answer!
```

DHCP Ack

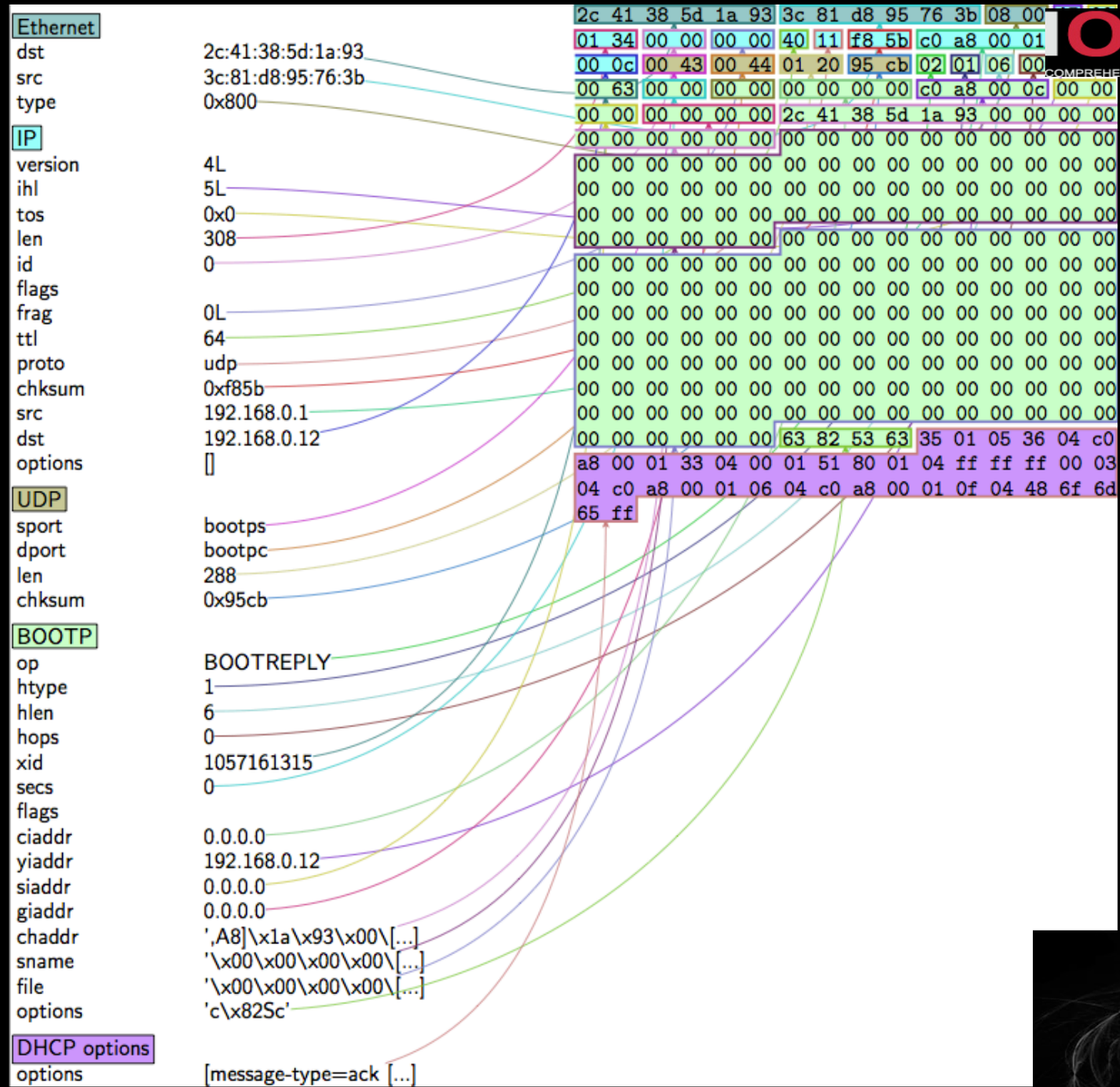
Then check wireshark/scapy for the ack. This should contain a number of fields for you to consume:

- Address
- Lease time
- DNS server
- Domain name
- Subnet

Now set up your machine with this info and continue!

Resolv.conf & i(f||p)config

DHCP Ack



Conf.checkIPaddr = True

HTTP Explanation

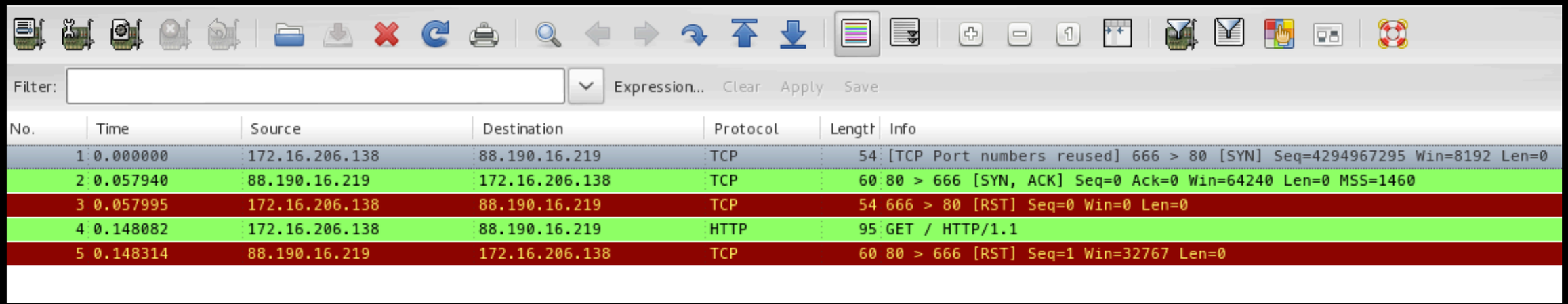
HTTP Requests:

- GET
- POST
- PUT
- DELETE
- OPTIONS
- etc. etc.

Application Level Protocol

* Stateless
* Request <-> Response
* Plaintext
* Much simpler

(not quite)



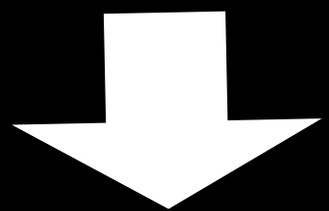
Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.206.138	88.190.16.219	TCP	54	[TCP Port numbers reused] 666 > 80 [SYN] Seq=4294967295 Win=8192 Len=0
2	0.057940	88.190.16.219	172.16.206.138	TCP	60	80 > 666 [SYN, ACK] Seq=0 Ack=0 Win=64240 Len=0 MSS=1460
3	0.057995	172.16.206.138	88.190.16.219	TCP	54	666 > 80 [RST] Seq=0 Win=0 Len=0
4	0.148082	172.16.206.138	88.190.16.219	HTTP	95	GET / HTTP/1.1
5	0.148314	88.190.16.219	172.16.206.138	TCP	60	80 > 666 [RST] Seq=1 Win=32767 Len=0

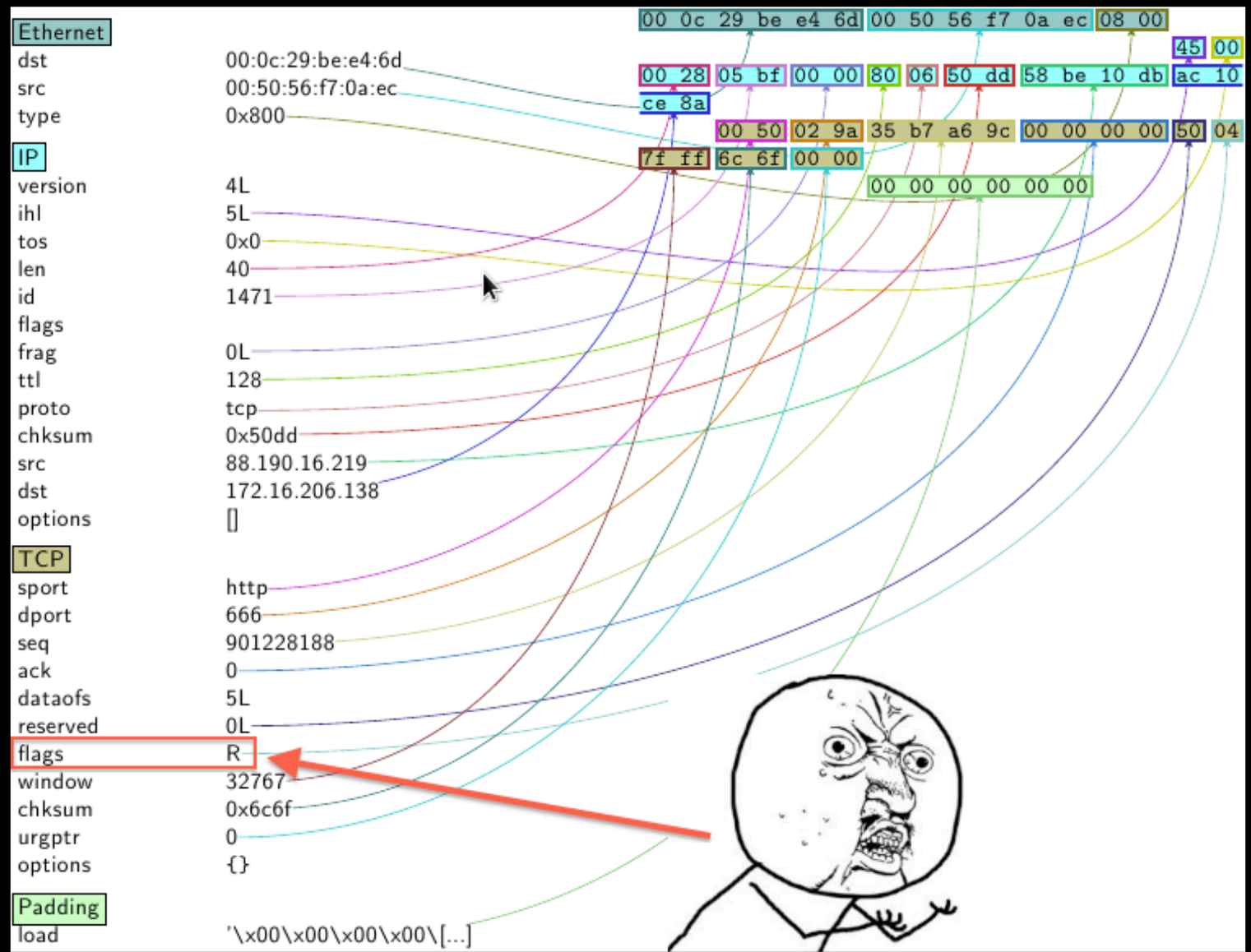
IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

HTTP Gotchas

TCP handshark fights will cause you headaches



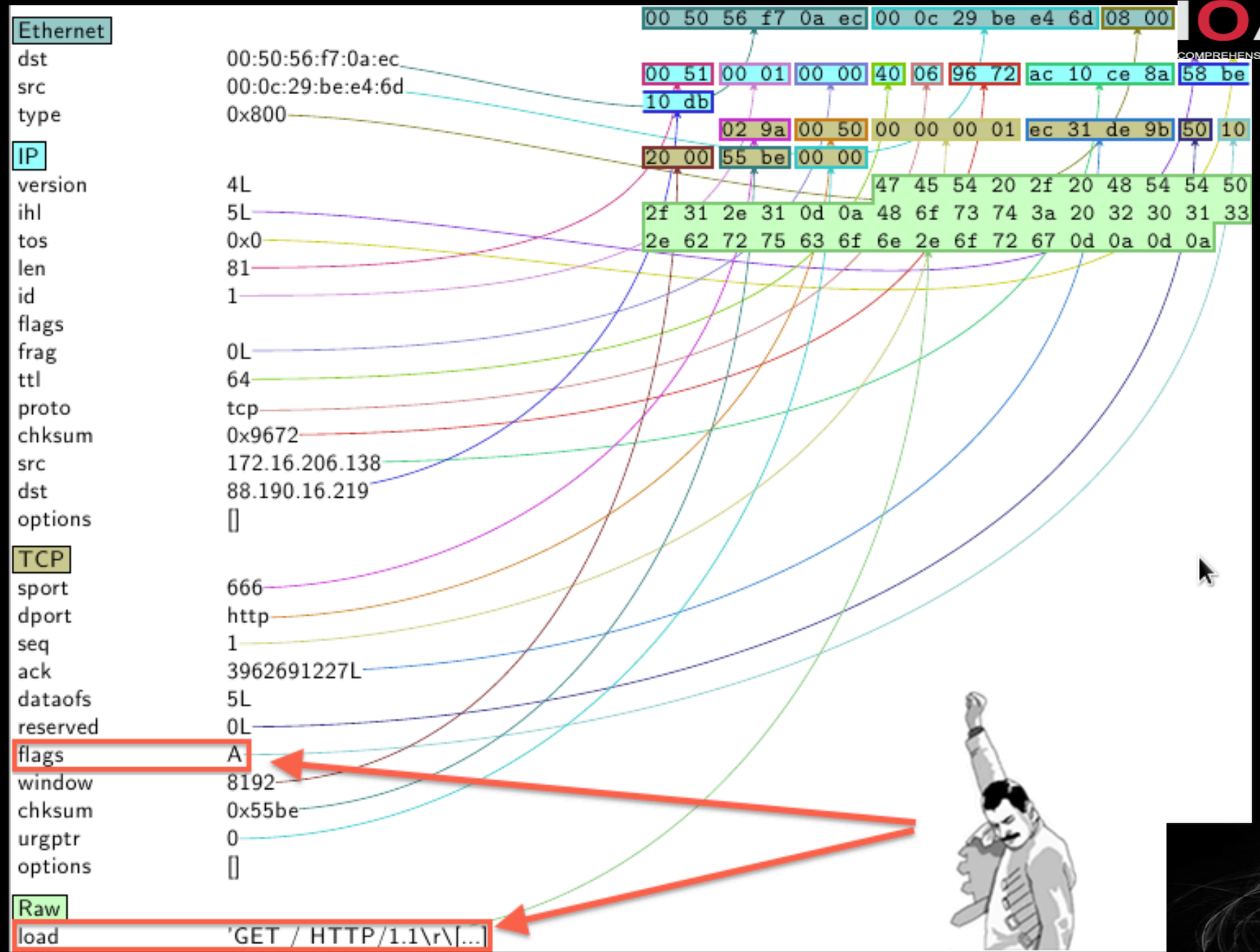
Operating System Handshake vs Scapy Handshake

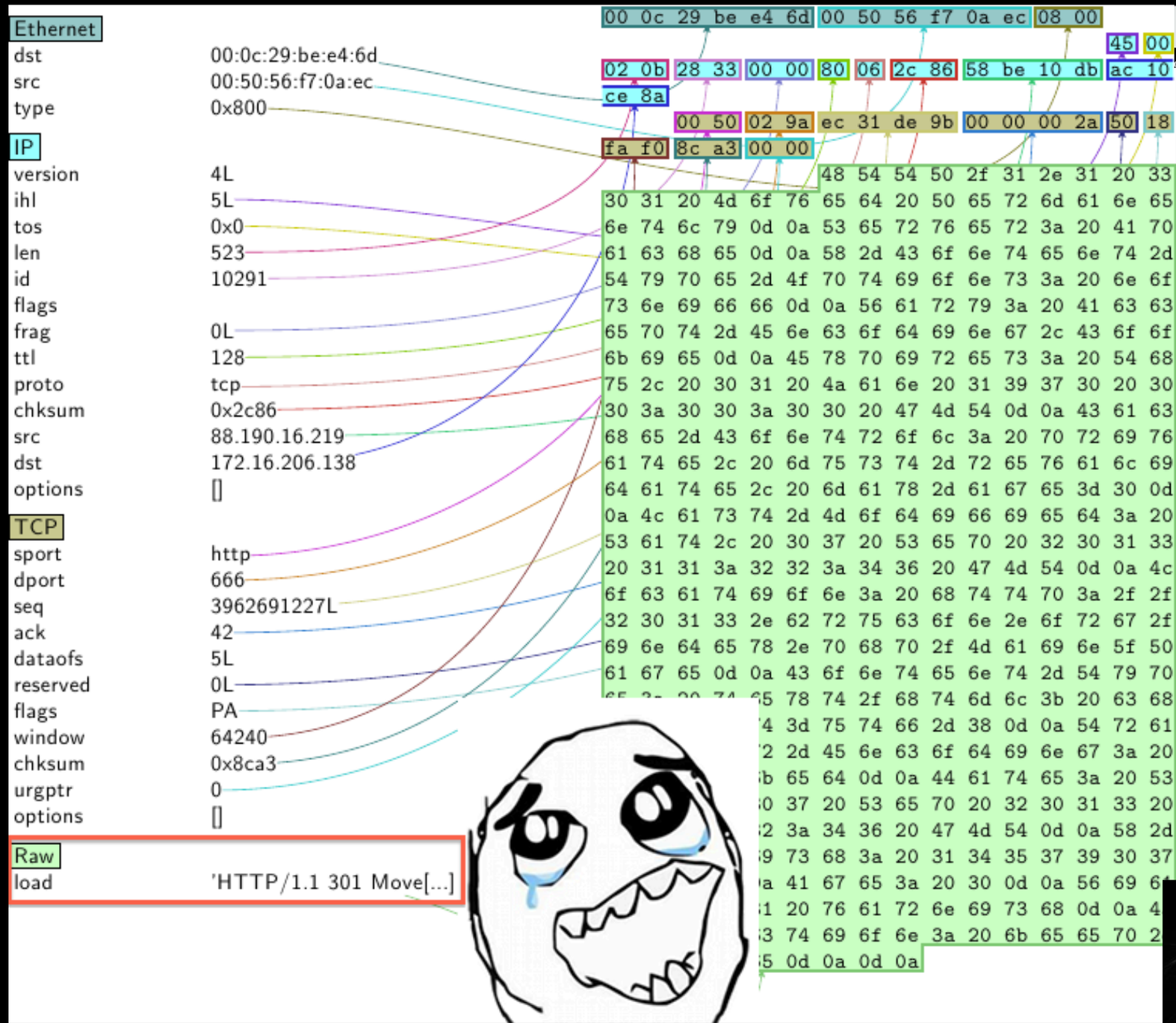

Ethernet
dst 00:0c:29:be:e4:6d
src 00:50:56:f7:0a:ec
type 0x800
IP
version 4L
ihl 5L
tos 0x0
len 40
id 1471
flags
frag 0L
ttl 128
proto tcp
chksum 0x50dd
src 88.190.16.219
dst 172.16.206.138
options []
TCP
sport http
dport 666
seq 901228188
ack 0
dataofs 5L
reserved 0L
flags R
window 32767
chksum 0x6c6f
urgptr 0
options {}
Padding
load '\x00\x00\x00\x00\[...]
00 0c 29 be e4 6d 00 50 56 f7 0a ec 08 00
45 00
00 28 05 bf 00 00 80 06 50 dd 58 be 10 db ac 10
ce 8a
00 50 02 9a 35 b7 a6 9c 00 00 00 00 50 04
7f ff 6c 6f 00 00
00 00 00 00 00 00

```
iptables
-A OUTPUT
-p tcp
-d 88.190.16.219
-s 172.16.206.138
--dport 80
--tcp-flags RST RST
-j DROP
```

IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

netsh for Windows firewalls


Ethernet
dst 00:50:56:f7:0a:ec
src 00:0c:29:be:e4:6d
type 0x800
IP
version 4L
ihl 5L
tos 0x0
len 81
id 1
flags
frag 0L
ttl 64
proto tcp
chksum 0x9672
src 172.16.206.138
dst 88.190.16.219
options []
TCP
sport 666
dport http
seq 1
ack 3962691227L
dataofs 5L
reserved 0L
flags A
window 8192
chksum 0x55be
urgptr 0
options []
Raw
load 'GET / HTTP/1.1\r\[...]
00 50 56 f7 0a ec 00 0c 29 be e4 6d 08 00
00 51 00 01 00 00 40 06 96 72 ac 10 ce 8a 58 be
10 db
02 9a 00 50 00 00 00 01 ec 31 de 9b 50 10
20 00 55 be 00 00
47 45 54 20 2f 20 48 54 54 50
2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 32 30 31 33
2e 62 72 75 63 6f 6e 2e 6f 72 67 0d 0a 0d 0a


Ethernet
dst 00:0c:29:be:e4:6d
src 00:50:56:f7:0a:ec
type 0x800
IP
version 4L
ihl 5L
tos 0x0
len 523
id 10291
flags
frag 0L
ttl 128
proto tcp
chksum 0x2c86
src 88.190.16.219
dst 172.16.206.138
options []
TCP
sport http
dport 666
seq 3962691227L
ack 42
dataofs 5L
reserved 0L
flags PA
window 64240
chksum 0x8ca3
urgptr 0
options []
Raw
load 'HTTP/1.1 301 Move[...]
00 0c 29 be e4 6d 00 50 56 f7 0a ec 08 00
45 00
02 0b 28 33 00 00 80 06 2c 86 58 be 10 db ac 10
ce 8a
00 50 02 9a ec 31 de 9b 00 00 00 2a 50 18
fa f0 8c a3 00 00
48 54 54 50 2f 31 2e 31 20 33
30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65
6e 74 6c 79 0d 0a 53 65 72 76 65 72 3a 20 41 70
61 63 68 65 0d 0a 58 2d 43 6f 6e 74 65 6e 74 2d
54 79 70 65 2d 4f 70 74 69 6f 6e 73 3a 20 6e 6f
73 6e 69 66 66 0d 0a 56 61 72 79 3a 20 41 63 63
65 70 74 2d 45 6e 63 6f 64 69 6e 67 2c 43 6f 6f
6b 69 65 0d 0a 45 78 70 69 72 65 73 3a 20 54 68
75 2c 20 30 31 20 4a 61 6e 20 31 39 37 30 20 30
30 3a 30 30 3a 30 30 20 47 4d 54 0d 0a 43 61 63
68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 70 72 69 76
61 74 65 2c 20 6d 75 73 74 2d 72 65 76 61 6c 69
64 61 74 65 2c 20 6d 61 78 2d 61 67 65 3d 30 0d
0a 4c 61 73 74 2d 4d 6f 64 69 66 69 65 64 3a 20
53 61 74 2c 20 30 37 20 53 65 70 20 32 30 31 33
20 31 31 3a 32 32 3a 34 36 20 47 4d 54 0d 0a 4c
6f 63 61 74 69 6f 6e 3a 20 68 74 74 70 3a 2f 2f
32 30 31 33 2e 62 72 75 63 6f 6e 2e 6f 72 67 2f
69 6e 64 65 78 2e 70 68 70 2f 4d 61 69 6e 5f 50
61 67 65 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70
4 3d 75 74 66 2d 38 0d 0a 54 72 61
2 2d 45 6e 63 6f 64 69 6e 67 3a 20
b 65 64 0d 0a 44 61 74 65 3a 20 53
0 37 20 53 65 70 20 32 30 31 33 20
2 3a 34 36 20 47 4d 54 0d 0a 58 2d
9 73 68 3a 20 31 34 35 37 39 30 37
a 41 67 65 3a 20 30 0d 0a 56 69 6
1 20 76 61 72 6e 69 73 68 0d 0a 4
3 74 69 6f 6e 3a 20 6b 65 65 70 2
5 0d 0a 0d 0a

HTTP Solution

IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

```
    i = IP(dst="www.brucon.org")
t = TCP(sport=2203, dport=80, flags='S')
syn_packet =  i/t

syn_ack = sr1(syn_packet)

i = IP(dst="www.brucon.org")
t = TCP(dport=80, sport=syn_ack[TCP].dport, \ seq=syn_ack[TCP].ack,
ack=syn_ack[TCP].seq + 1, flags='A')
request =  i/t/"GET / HTTP/1.1\r\nHost: www.brucon.org\r\n\r\n"
reply = sr1(request)

reply.display()
```

IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

In Summary...

Ether / ARP who has 172.16.206.2 says 172.16.206.138

Ether / ARP is at 00:50:56:f7:0a:ec says 172.16.206.2 / Padding

Ether / IP / UDP / BOOTP(chaddr='2b:42:31:5c:2a:73', xid=31337)/

DHCP(options=[("message-type","request"),IPField("requested_addr","192.168.0.12"),"end"])

Ether / IP / UDP / BOOTP(chaddr= ='2b:42:31:5c:2a:73',xid=31337)/

Ether / IP / UDP 172.16.206.2:bootps > 172.16.206.138:bootpc / BOOTP / DHCP

DHCP(options=[("message-type","request"),IPField("requested_addr","172.16.206.138"),"end"])

Ether / IP / UDP 172.16.206.2:bootps > 172.16.206.138:bootpc / BOOTP / DHCP

Ether / IP / UDP / DNS Qry "www.brucon.org."

Ether / IP / UDP / DNS Ans "88.190.16.219"

Ether / IP / TCP 172.16.206.138:666 > 88.190.16.219:http S

Ether / IP / TCP 88.190.16.219:http > 172.16.206.138:666 SA / Padding

Ether / IP / TCP 172.16.206.138:666 > 88.190.16.219:http A / Raw

Ether / IP / TCP 88.190.16.219:http > 172.16.206.138:666 A / Padding

Ether / IP / TCP 88.190.16.219:http > 172.16.206.138:666 PA / Raw

Ether / IP / TCP 88.190.16.219:http > 172.16.206.138:666 PA / Raw / Padding

Ether / IP / TCP 88.190.16.219:http > 172.16.206.138:666 PA / Raw

IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

Thank you !
Questions ?
BEER !!!