WELCOME TO CLASS 6!

BLACK HAT PYTHON3

RALEIGH ISSA

GITHUB REPO

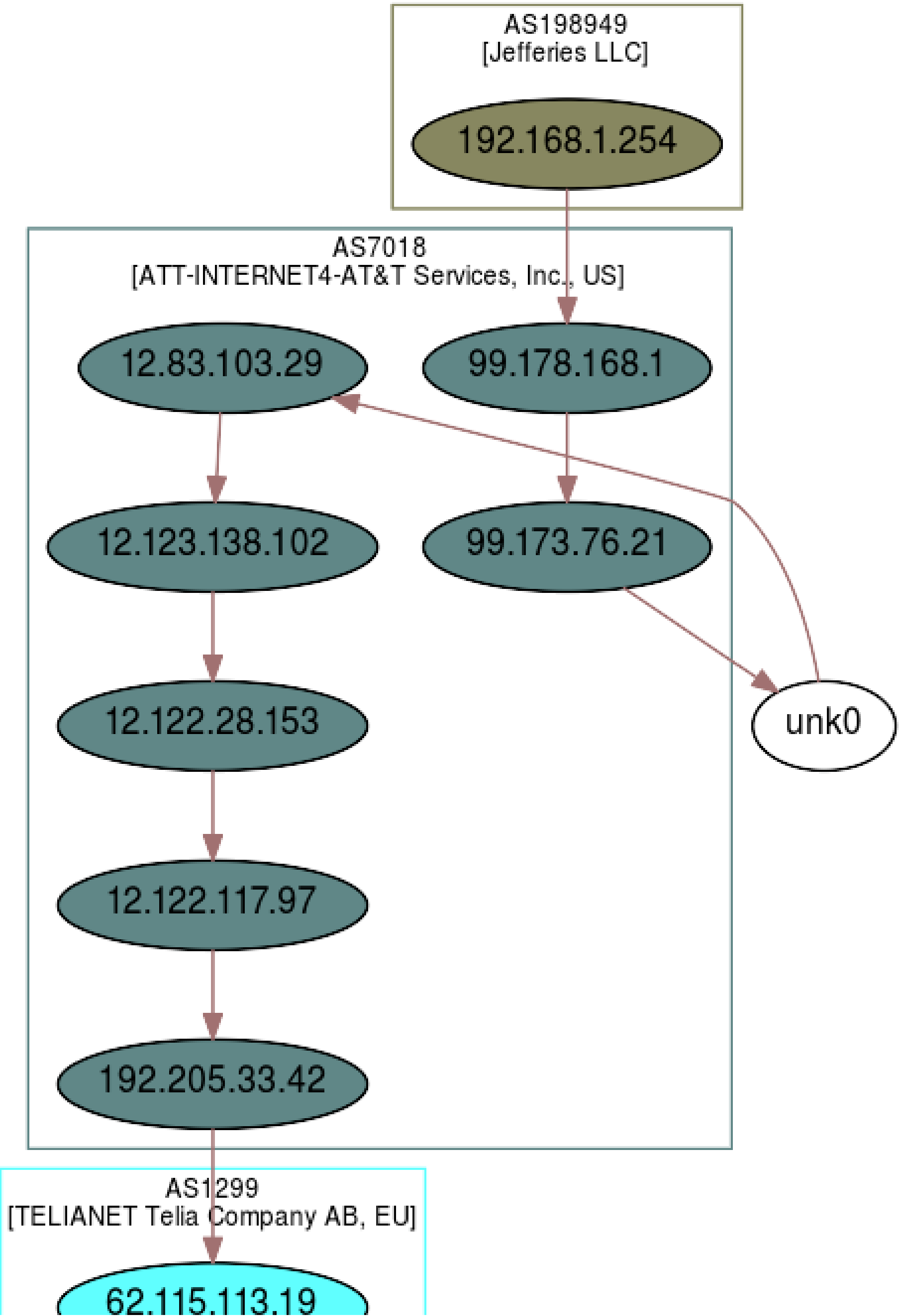
https://github.com/tiarno/bhp3_class

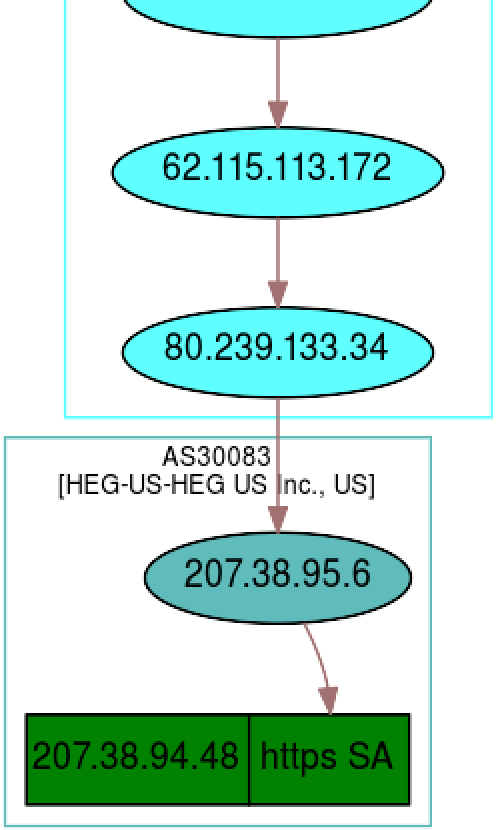
SUMMARY FROM LAST CLASS

- scapy w/graphics
- bpf
- arp watch/poison
- three-way handshake
- named tuples

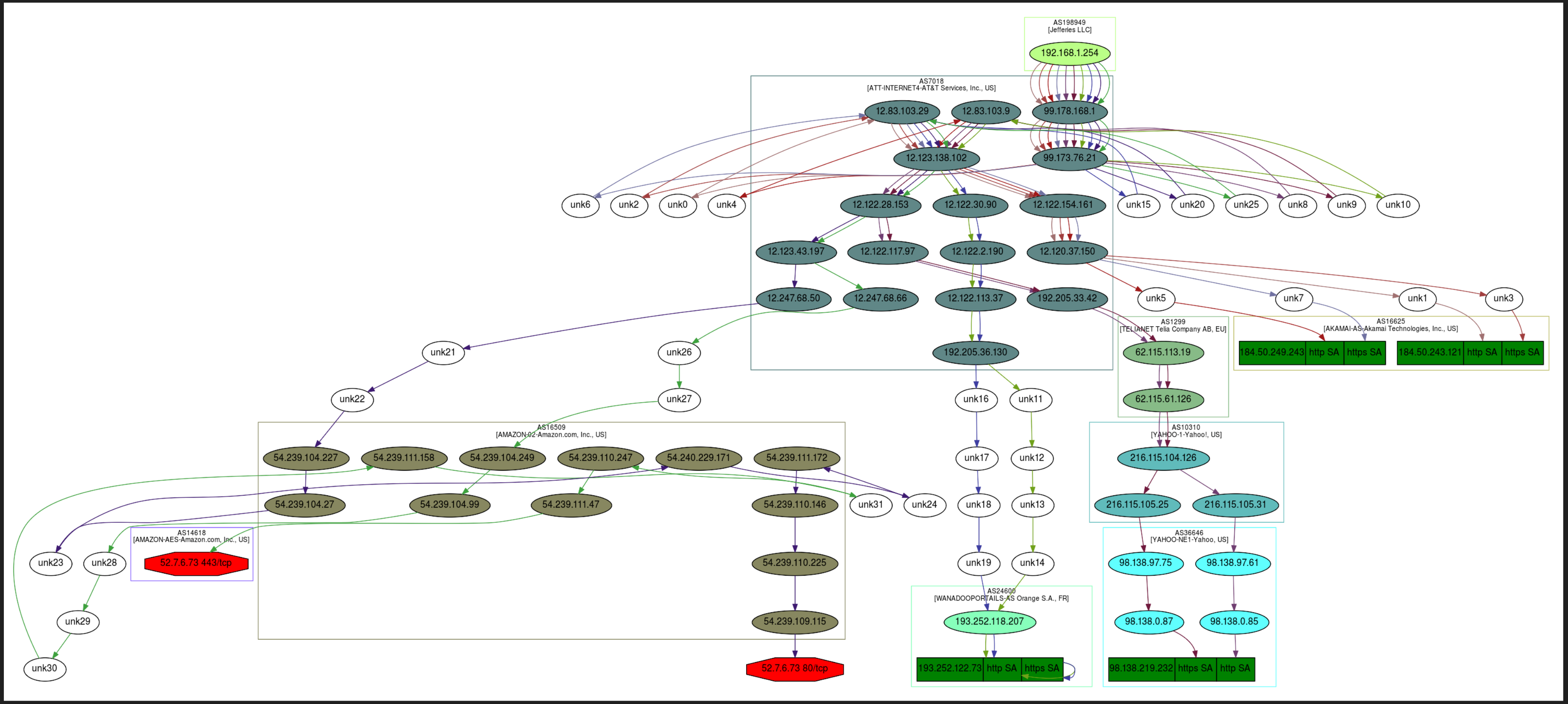
GRAPHICS

```
res, unans = traceroute(['reachtim.com'], dport=[443], maxttl=

res.graph()
```

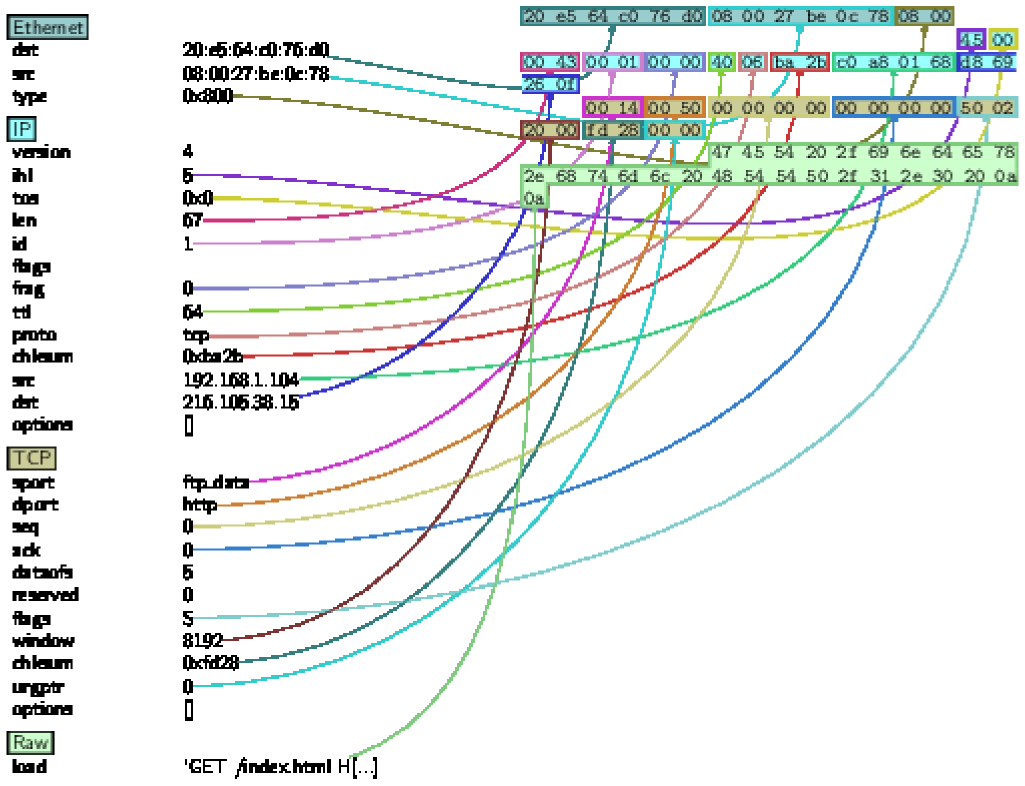

AS198949
[Jefferies LLC]
192.168.1.254
AS7018
[ATT-INTERNET4-AT&T Services, Inc., US]
12.83.103.29
99.178.168.1
12.123.138.102
99.173.76.21
unk0
12.122.28.153
12.122.117.97
192.205.33.42
AS1299
[TELIANET Telia Company AB, EU]
62.115.113.19


62.115.113.172
80.239.133.34
AS30083
[HEG-US-HEG US Inc., US]
207.38.95.6
207.38.94.48
https SA

```
hosts = [
    'www.microsoft.com', 'www.cisco.com',
    'www.yahoo.com', 'www.wanadoo.fr',
    'www.pacsec.com']

res, unans = traceroute(hosts, dport=[80,443], maxttl=20, retr
res.graph()
```


AS198949
[Jefferies LLC]
192.168.1.254
AS7018
[ATT-INTERNET4-AT&T Services, Inc., US]
12.83.103.29
12.83.103.9
99.178.168.1
12.123.138.102
99.173.76.21
unk6
unk2
unk0
unk4
12.122.28.153
12.122.30.90
12.122.154.161
unk15
unk20
unk25
unk8
unk9
unk10
12.123.43.197
12.122.117.97
12.122.2.190
12.120.37.150
12.247.68.50
12.247.68.66
12.122.113.37
192.205.33.42
unk5
unk7
unk1
unk3
192.205.36.130
AS1299
[TELIANET Telia Company AB, EU]
62.115.113.19
62.115.61.126
AS16625
[AKAMAI-AS-Akamai Technologies, Inc., US]
184.50.249.243
http SA
https SA
184.50.243.121
http SA
https SA
unk21
unk26
unk22
unk27
unk16
unk11
AS16509
[AMAZON-02-Amazon.com, Inc., US]
54.239.104.227
54.239.111.158
54.239.104.249
54.239.110.247
54.240.229.171
54.239.111.172
54.239.104.27
54.239.104.99
54.239.111.47
54.239.110.146
unk31
unk24
54.239.110.225
54.239.109.115
52.7.6.73 80/tcp
AS14618
[AMAZON-AES-Amazon.com, Inc., US]
52.7.6.73 443/tcp
unk23
unk28
unk29
unk30
unk17
unk12
unk18
unk13
unk19
unk14
AS24600
[WANADOOPORTAILS-AS Orange S.A., FR]
193.252.118.207
193.252.122.73
http SA
https SA
AS10310
[YAHOO-1-Yahoo!, US]
216.115.104.126
216.115.105.25
216.115.105.31
AS36646
[YAHOO-NE1-Yahoo, US]
98.138.97.75
98.138.97.61
98.138.0.87
98.138.0.85
98.138.219.232
https SA
http SA

```
a = Ether()/IP(dst="www.slashdot.org")/TCP()/"GET /index.html
a[0].pdfdump(layer_shift=1)
```



```
Ethernet
dst         20:e5:64:c0:76:d0
src         08:00:27:be:0c:78
type        0x800
IP
version     4
ihl         5
tos         0x0
len         67
id          1
flags
frag        0
ttl         64
proto       tcp
chksum      0xba2b
src         192.168.1.104
dst         216.105.38.15
options     []
TCP
sport       ftp_data
dport       http
seq         0
ack         0
dataofs     5
reserved    0
flags       S
window      8192
chksum      0xfd28
urgptr      0
options     []
Raw
load        'GET /index.html H[...]
```

```
20 e5 64 c0 76 d0 08 00 27 be 0c 78 08 00
                                           45 00
00 43 00 01 00 00 40 06 ba 2b c0 a8 01 68 d8 69
26 0f
      00 14 00 50 00 00 00 00 00 00 00 00 50 02
20 00 fd 28 00 00
                  47 45 54 20 2f 69 6e 64 65 78
2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 30 20 0a
0a
```

CARTOPY WORLD MAP

```
mapfile = '/root/GeoLite2-City/GeoLite2-City.mmdb'
conf.geoip_city = mapfile
traceroute_map('www.gsxt.gov.cn', 'reachtim.com')
```

MAPPING LINKS

- https://dev.maxmind.com/geoip/geoip2/geolite2/
- https://scitools.org.uk/cartopy/docs/latest/index.htm
- https://scitools.org.uk/cartopy/docs/latest/matplotlib

THREE-WAY HANDSHAKE

- on client (Kali):
  - `iptables -t filter -I OUTPUT -p tcp --sport 10000 --tcp-flags RST RST -j DROP`
  - `tcpdump -ni any port 8000 -S`
- on server:
  - `python2 -m SimpleHTTPServer` or
  - `python3 -m http.server`

```
me, sport = '192.168.1.104', 10000 # client
them, dport = '192.168.1.69', 8000 # server
#
ip = IP(src=me, dst=them)
syn = TCP(sport=sport, dport=dport, flags='S', seq=1000)
synack = sr1(ip/syn)
ack = TCP(sport=sport, dport=dport, flags='A', seq=synack.ack,
send(ip/ack)
```

ARP POISON PROGRAM

`arper.py`

DNS SPOOFING:

https://thepacketgeek.com/scapy-p-09-scapy-and-dns/

`dns_spoof.py`

EXTRACT CONTENT FROM PCAP FILE

`recapper.py`

- https://developer.mozilla.org/en-US/docs/Glossary/MIME_type

DEMO: IDENTIFY FACES

- `detector.py`

SCAPY QUICK TAKES

- ping of death

```
send( fragment(IP(dst="192.168.1.104")
             /ICMP()/("X"*60000)) )
```

- ack scan

```
ans, unans = sr(IP(dst="www.issa.org")
              /TCP(dport=[80,666],flags="
```

- Xmas packet

```
ans, unans = sr(IP(dst="192.168.1.104")
              /TCP(dport=666,flags="FPU")
```

- ARP ping

```
ans, unans = srp(Ether(dst="ff:ff:ff:ff:ff:ff")
               /ARP(pdst="192.168.1.0/24"),timeo
```

- ICMP ping

```
ans, unans = sr(IP(dst="192.168.1.1-254")
              /ICMP())
```

- TCP ping

```
ans, unans = sr( IP(dst="192.168.1.*")
               /TCP(dport=80,flags="S") )
```

- UDP ping

```
ans, unans = sr( IP(dst="192.168.*.1-10")
               /UDP(dport=0) )
```

- TCP SYN traceroute

```
ans, unans = sr(IP(dst="8.8.8.8",ttl=(1,10))
             /TCP(dport=53, flags="S"))
```

- UDP traceroute

```
res, unans = sr(IP(dst="8.8.8.8", ttl=(1,20))
             /UDP()/DNS(qd=DNSQR(qname="test.c
```

YOUR JOB

- write your own arp poison tool
- experiment with graphics and scapy
- write your own pcap extraction tool (recapper)
- examine code for scapy.arpcachepoison

READING

- Slides: http://www.secdev.org/conf/scapy_hack.lu.pdf
- Refer: https://scapy.readthedocs.io/en/latest/index.html
- Explore: https://github.com/DanMcInerney
- Explore: https://github.com/0x90/uberscapy

FEEDBACK PLEASE!

- tim@reachtim.com
- discord: https://discord.gg/WR23qUj