Hunting hidden MiddleBox

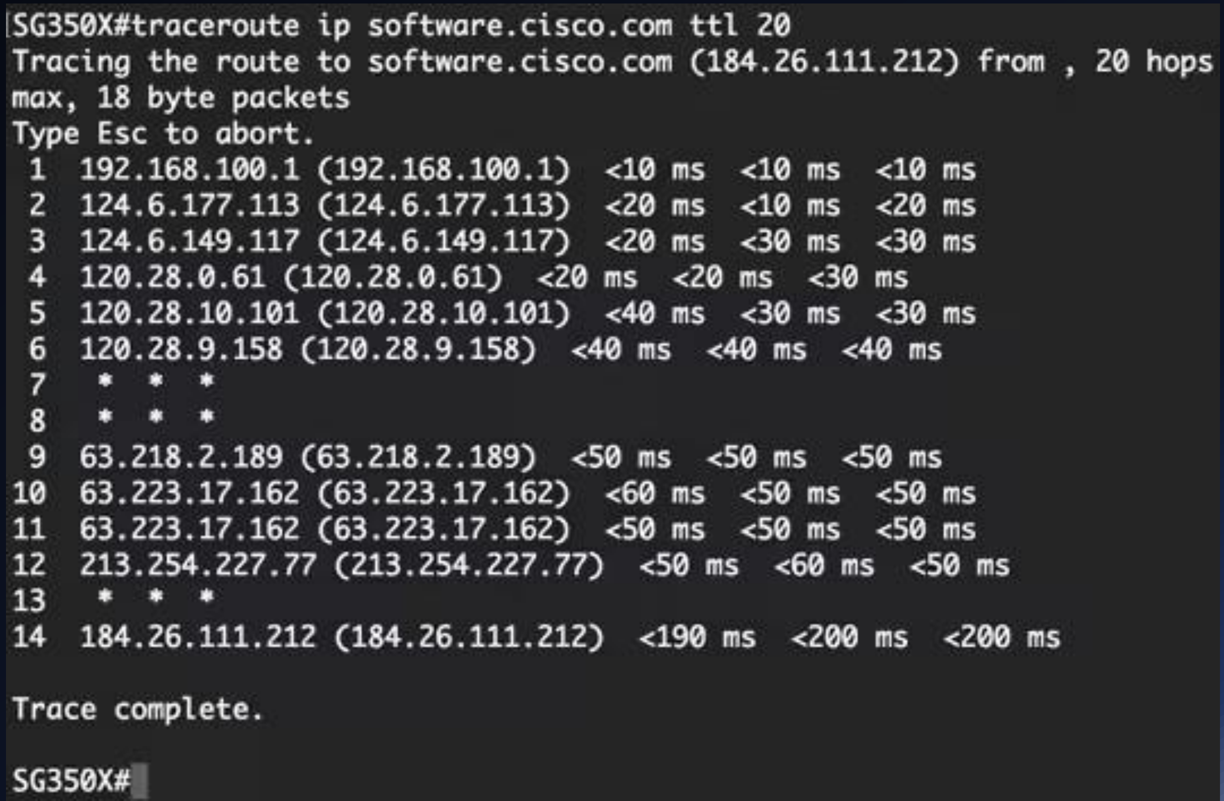
In Fiber, no one can hear your scream

```
nous@le_carlie:~# nmap -O -v darcosion.local
```

- **Darcosion**, darcommuniste, dargrosion, « darco » for my friends
- Work at SERMA SAFETY & SECURITY
- Do a lot of OSINT in OSINT-FR (the frens)
- Love networks ☺
- Do know how to do network ☹ ↓
- LOVE TRACEROUTES

The famous traceroute

- ➢ Work with TTL (*Time To Live*)
  - ➢ TTL decrementing at every « IP hop »
  - ➢ When it’s 0, packet dropped and packet ICMP TIME_EXCEEDED returned
- ➢ For traceroute, we start with TTL at 0, increment and it end like that :

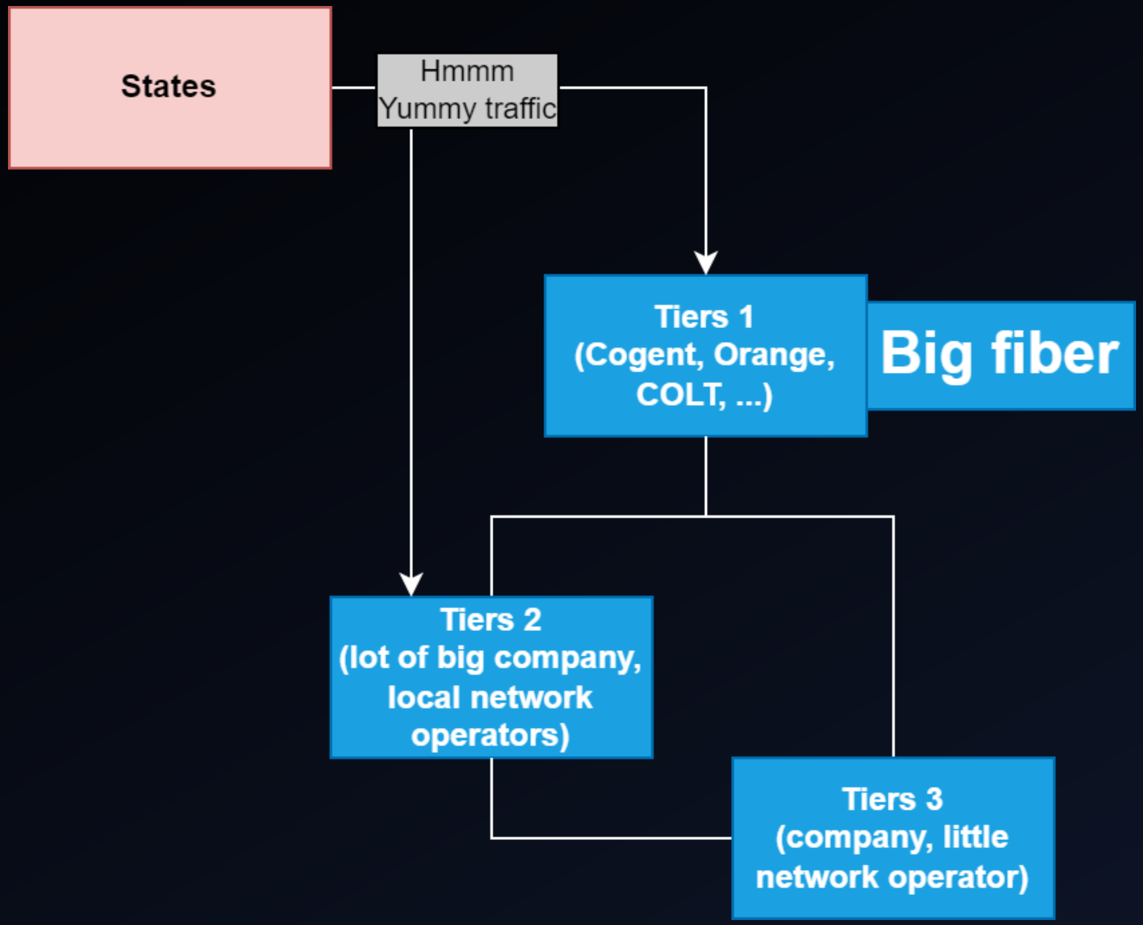


```
SG350X#traceroute ip software.cisco.com ttl 20
Tracing the route to software.cisco.com (184.26.111.212) from , 20 hops
max, 18 byte packets
Type Esc to abort.
 1  192.168.100.1 (192.168.100.1)  <10 ms  <10 ms  <10 ms
 2  124.6.177.113 (124.6.177.113)  <20 ms  <10 ms  <20 ms
 3  124.6.149.117 (124.6.149.117)  <20 ms  <30 ms  <30 ms
 4  120.28.0.61 (120.28.0.61)  <20 ms  <20 ms  <30 ms
 5  120.28.10.101 (120.28.10.101)  <40 ms  <30 ms  <30 ms
 6  120.28.9.158 (120.28.9.158)  <40 ms  <40 ms  <40 ms
 7   *  *  *
 8   *  *  *
 9  63.218.2.189 (63.218.2.189)  <50 ms  <50 ms  <50 ms
10  63.223.17.162 (63.223.17.162)  <60 ms  <50 ms  <50 ms
11  63.223.17.162 (63.223.17.162)  <50 ms  <50 ms  <50 ms
12  213.254.227.77 (213.254.227.77)  <50 ms  <60 ms  <50 ms
13   *  *  *
14  184.26.111.212 (184.26.111.212)  <190 ms  <200 ms  <200 ms

Trace complete.

SG350X#
```

The network


States
Hmmm
Yummy traffic
Tiers 1
(Cogent, Orange, COLT, ...)
Big fiber
Tiers 2
(lot of big company, local network operators)
Tiers 3
(company, little network operator)

- Many actor
- ISP, private provider, fiber company...

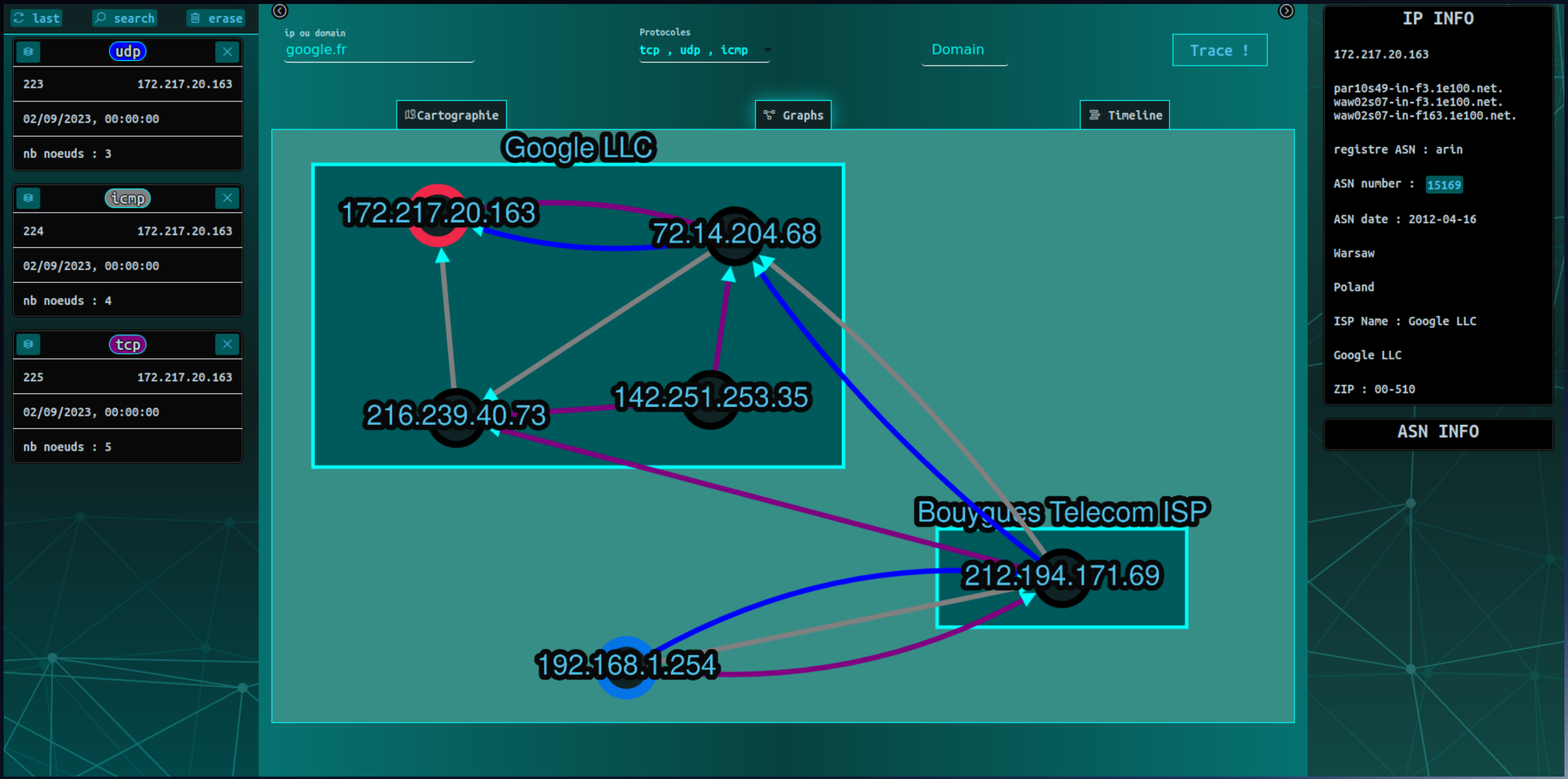
But what is a middlebox ?

- Technologie of packet manipulation/interception
- Could be load balancers, firewalls, NAT, WAN optimizator, TLG/ALG, NAT-PT, socks/proxies, WAF, gatekeepers, CDN, …
- Often visible on network

- Famous example of middlebox problem : TLS 1.3 protocol forced to change specification because of traffic dropped by middlebox

Seeing classical middlebox

- A simple example : Google Load Balancing



udp
223 172.217.20.163
02/09/2023, 00:00:00
nb noeuds : 3

icmp
224 172.217.20.163
02/09/2023, 00:00:00
nb noeuds : 4

tcp
225 172.217.20.163
02/09/2023, 00:00:00
nb noeuds : 5

ip ou domain: google.fr

Protocoles: tcp , udp , icmp

IP INFO

172.217.20.163

par10s49-in-f3.1e100.net.
waw02s07-in-f3.1e100.net.
waw02s07-in-f163.1e100.net.

registre ASN : arin

ASN number : 15169

ASN date : 2012-04-16

Warsaw

Poland

ISP Name : Google LLC

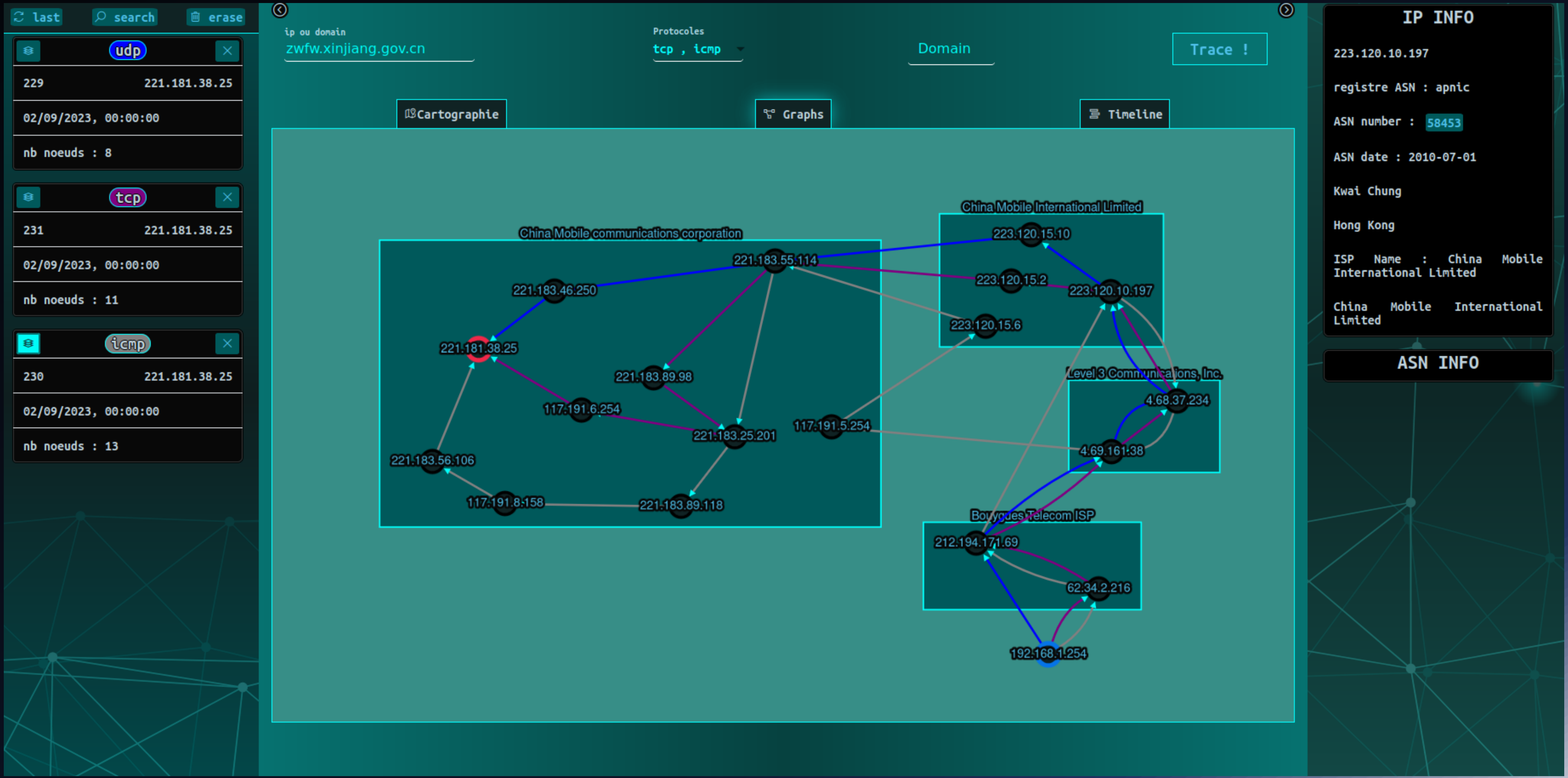
Google LLC

ZIP : 00-510

ASN INFO

Seeing classical middlebox

- A big example : the great firewall



udp
229 221.181.38.25
02/09/2023, 00:00:00
nb noeuds : 8

tcp
231 221.181.38.25
02/09/2023, 00:00:00
nb noeuds : 11

icmp
230 221.181.38.25
02/09/2023, 00:00:00
nb noeuds : 13

ip ou domain: zwfw.xinjiang.gov.cn

Protocoles: tcp , icmp

IP INFO

223.120.10.197

registre ASN : apnic

ASN number : 58453

ASN date : 2010-07-01

Kwai Chung

Hong Kong

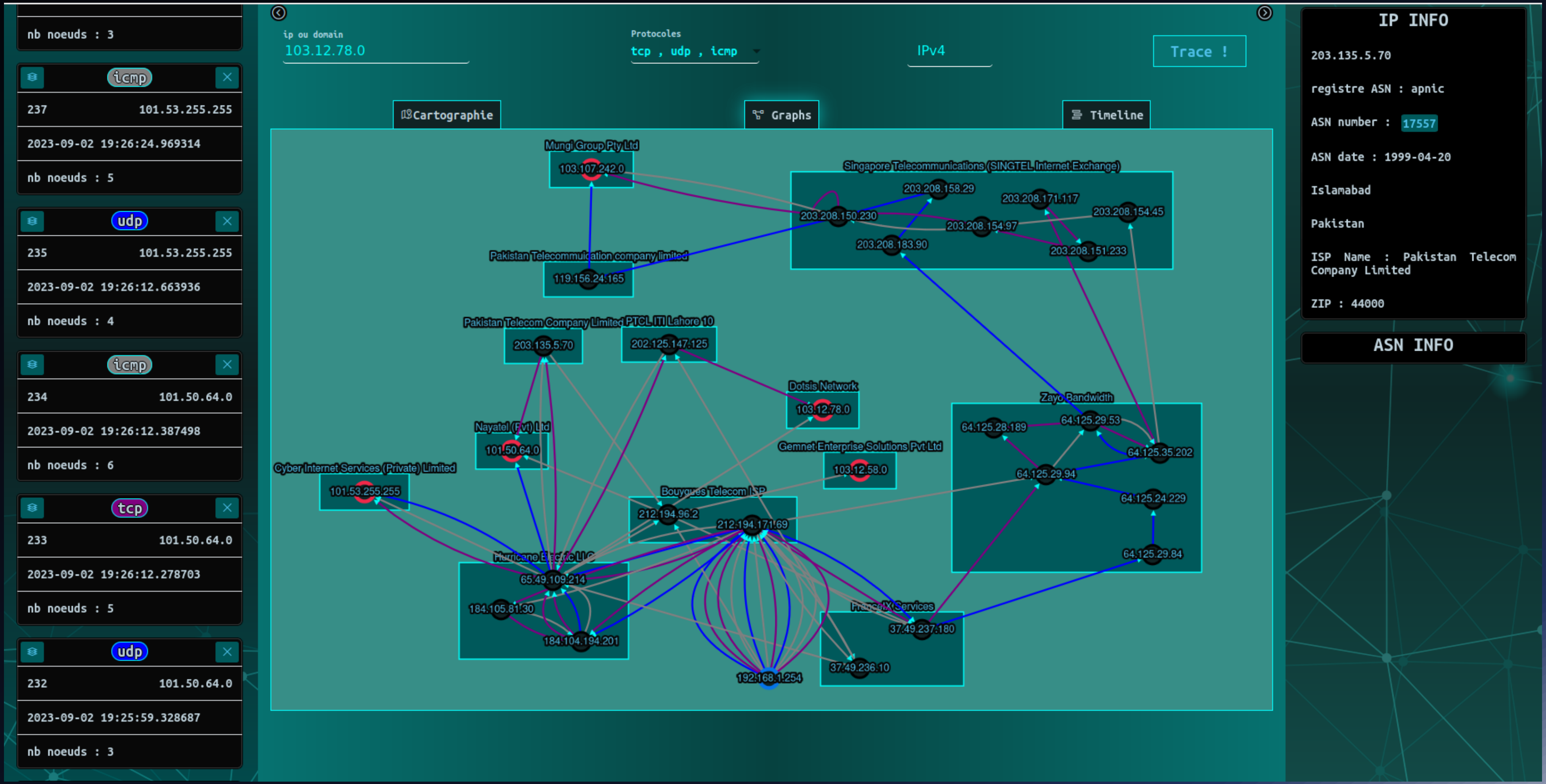
ISP Name : China Mobile International Limited

China Mobile International Limited

ASN INFO

Seeing classical middlebox

- A weird example : Pakistan Telecom DPI ?



```
nb noeuds : 3

icmp
237                101.53.255.255
2023-09-02 19:26:24.969314
nb noeuds : 5

udp
235                101.53.255.255
2023-09-02 19:26:12.663936
nb noeuds : 4

icmp
234                   101.50.64.0
2023-09-02 19:26:12.387498
nb noeuds : 6

tcp
233                   101.50.64.0
2023-09-02 19:26:12.278703
nb noeuds : 5

udp
232                   101.50.64.0
2023-09-02 19:25:59.328687
nb noeuds : 3
```

ip ou domain: 103.12.78.0

Protocoles: tcp , udp , icmp

IPv4

Trace !

```
IP INFO
203.135.5.70
registre ASN : apnic
ASN number : 17557
ASN date : 1999-04-20
Islamabad
Pakistan
ISP Name : Pakistan Telecom Company Limited
ZIP : 44000

ASN INFO
```

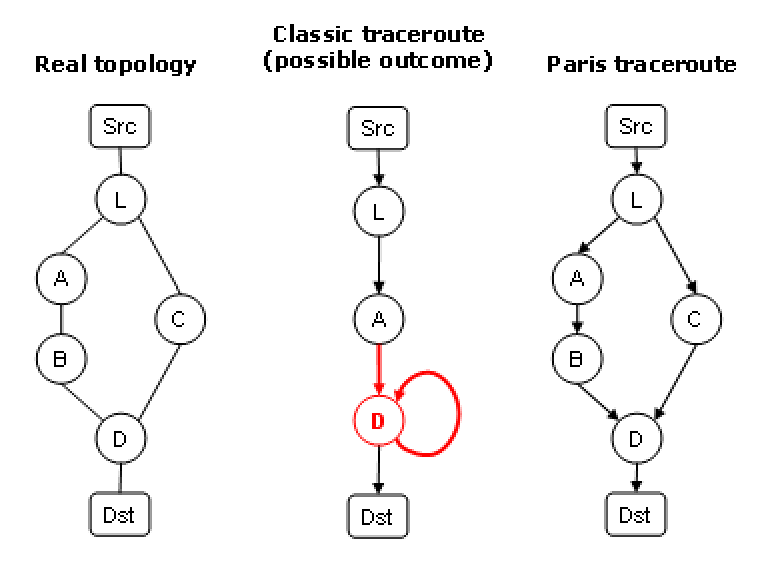
Seeing classical middlebox

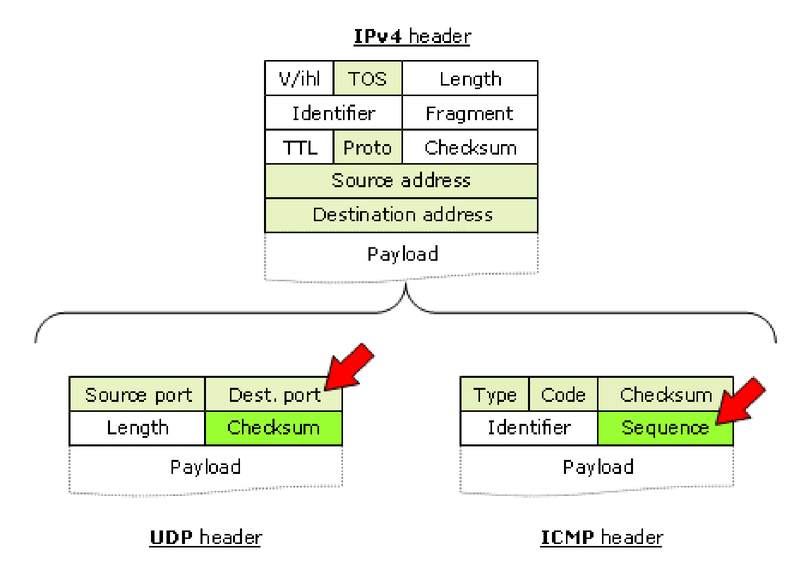
- Detection by « fuzzing » traceroute

Just an example :

Paris Traceroute model

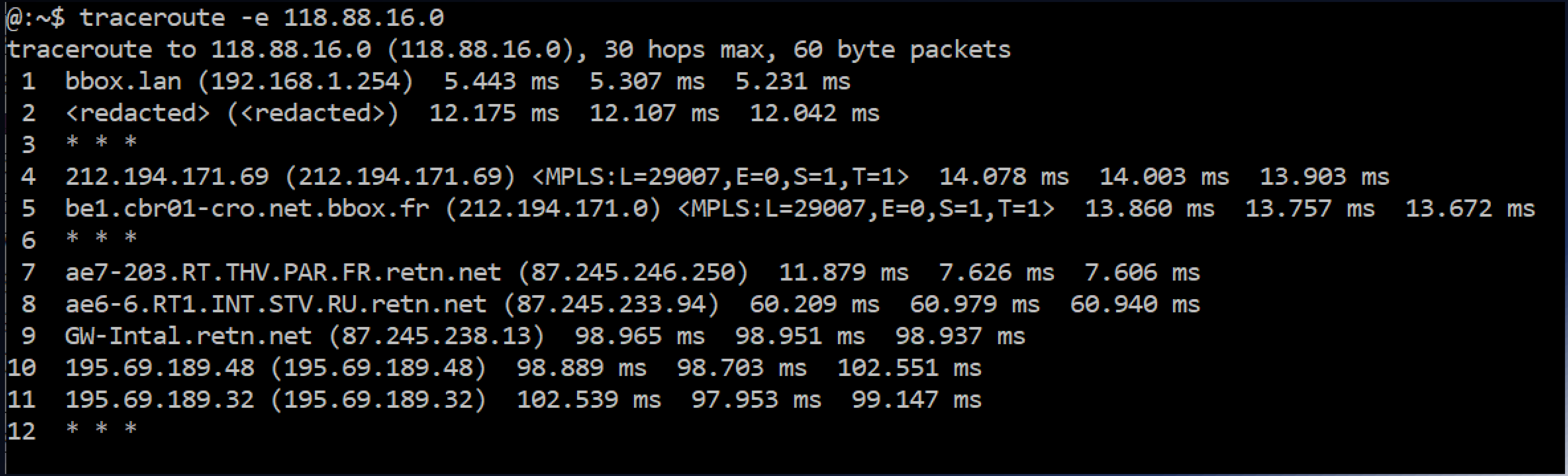
Header variation





Seeing classical middlebox

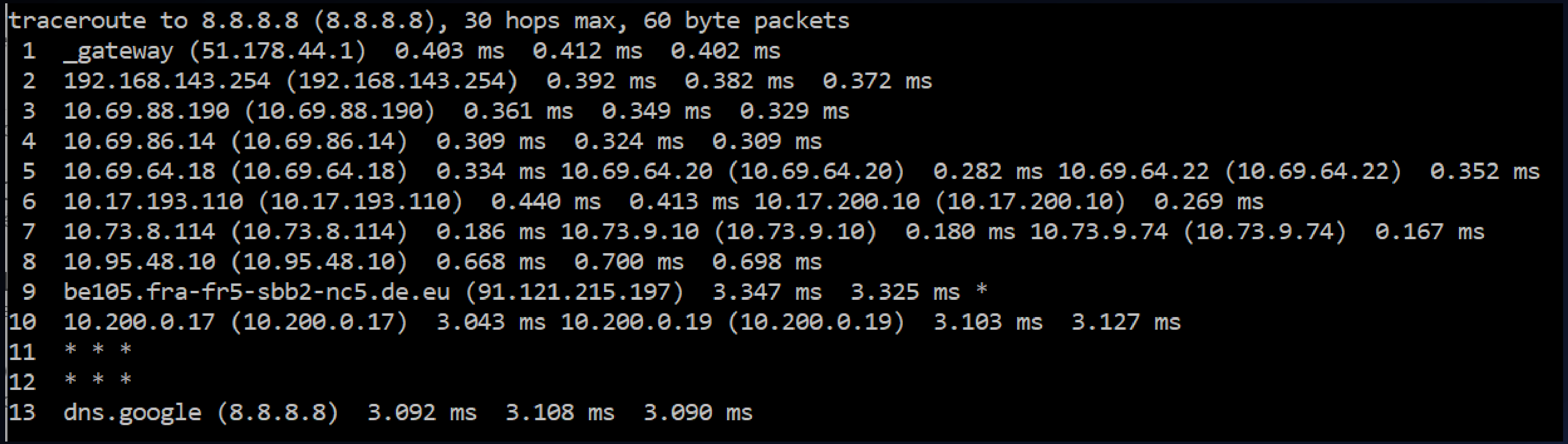
- Using ICMP tricks for seeing MPLS
  - Featuring RFC4950 (just traceroute with « -e » !)
  - Enable the view of MPLS material/configuration
  - Usefull on company pentest/red team



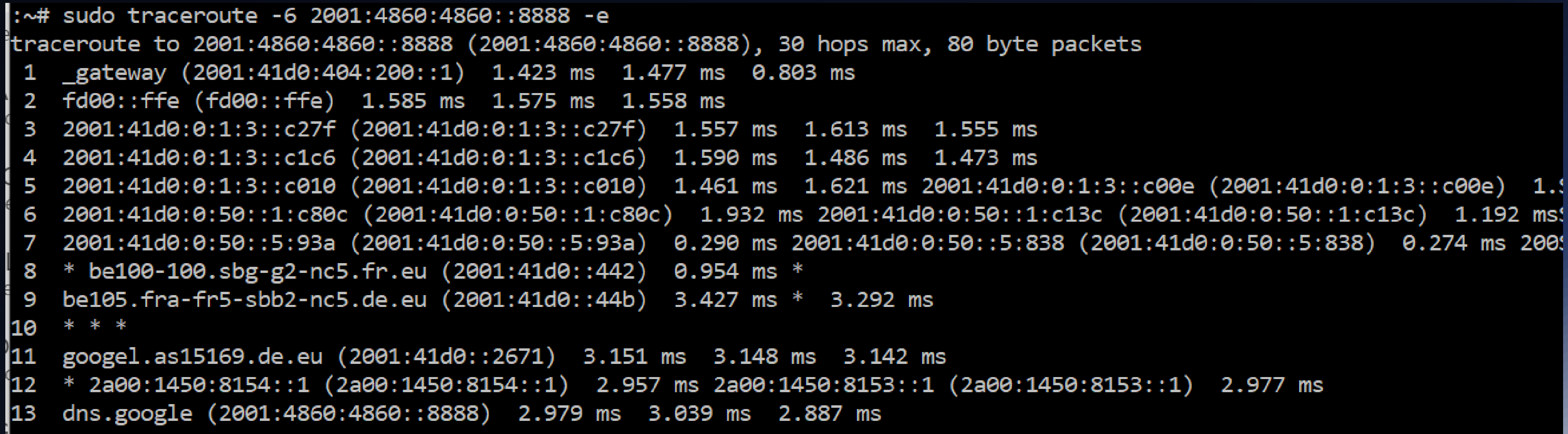
```
@:~$ traceroute -e 118.88.16.0
traceroute to 118.88.16.0 (118.88.16.0), 30 hops max, 60 byte packets
 1  bbox.lan (192.168.1.254)  5.443 ms  5.307 ms  5.231 ms
 2  <redacted> (<redacted>)  12.175 ms  12.107 ms  12.042 ms
 3  * * *
 4  212.194.171.69 (212.194.171.69) <MPLS:L=29007,E=0,S=1,T=1>  14.078 ms  14.003 ms  13.903 ms
 5  be1.cbr01-cro.net.bbox.fr (212.194.171.0) <MPLS:L=29007,E=0,S=1,T=1>  13.860 ms  13.757 ms  13.672 ms
 6  * * *
 7  ae7-203.RT.THV.PAR.FR.retn.net (87.245.246.250)  11.879 ms  7.626 ms  7.606 ms
 8  ae6-6.RT1.INT.STV.RU.retn.net (87.245.233.94)  60.209 ms  60.979 ms  60.940 ms
 9  GW-Intal.retn.net (87.245.238.13)  98.965 ms  98.951 ms  98.937 ms
10  195.69.189.48 (195.69.189.48)  98.889 ms  98.703 ms  102.551 ms
11  195.69.189.32 (195.69.189.32)  102.539 ms  97.953 ms  99.147 ms
12  * * *
```

Seeing classical middlebox

- Comparing IPv4 and IPv6



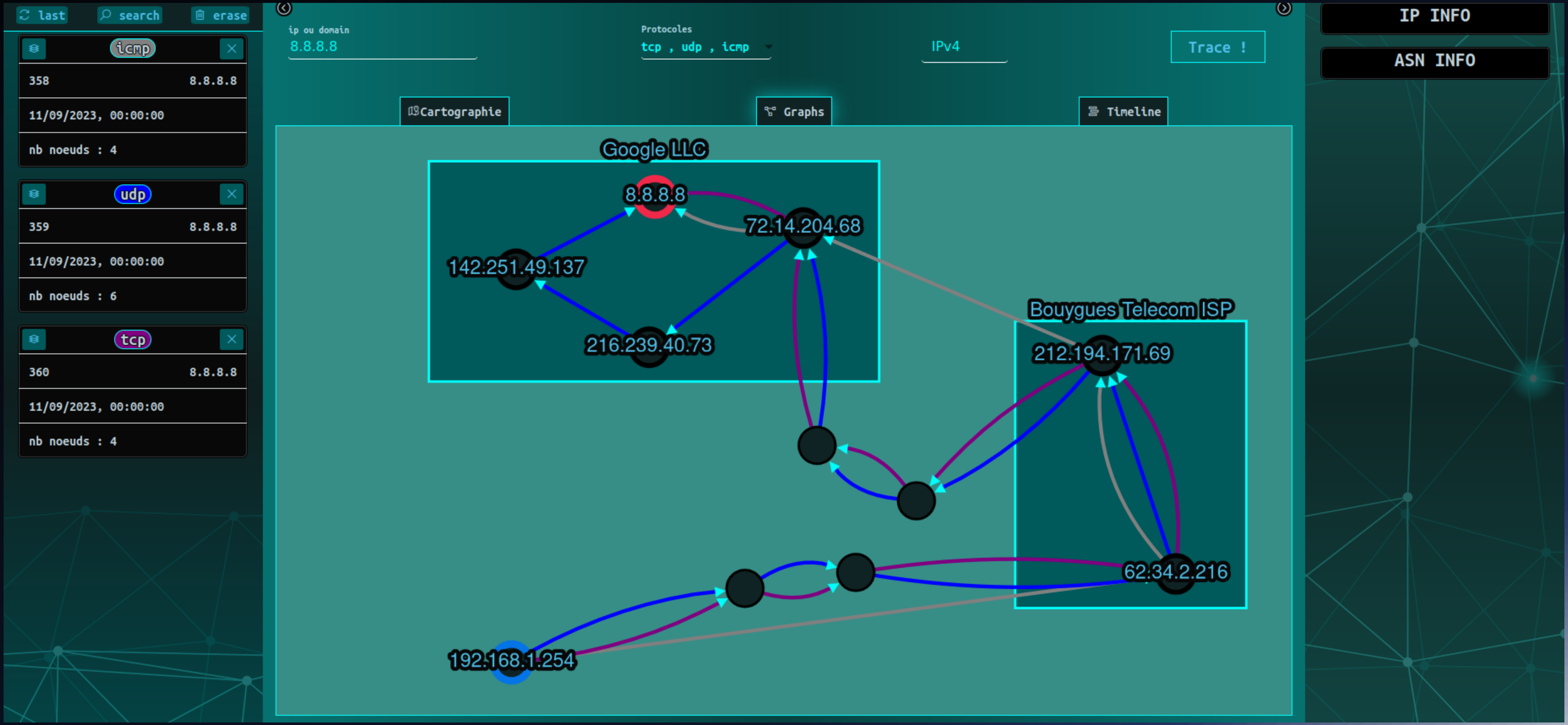
```
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  _gateway (51.178.44.1)  0.403 ms  0.412 ms  0.402 ms
 2  192.168.143.254 (192.168.143.254)  0.392 ms  0.382 ms  0.372 ms
 3  10.69.88.190 (10.69.88.190)  0.361 ms  0.349 ms  0.329 ms
 4  10.69.86.14 (10.69.86.14)  0.309 ms  0.324 ms  0.309 ms
 5  10.69.64.18 (10.69.64.18)  0.334 ms 10.69.64.20 (10.69.64.20)  0.282 ms 10.69.64.22 (10.69.64.22)  0.352 ms
 6  10.17.193.110 (10.17.193.110)  0.440 ms  0.413 ms 10.17.200.10 (10.17.200.10)  0.269 ms
 7  10.73.8.114 (10.73.8.114)  0.186 ms 10.73.9.10 (10.73.9.10)  0.180 ms 10.73.9.74 (10.73.9.74)  0.167 ms
 8  10.95.48.10 (10.95.48.10)  0.668 ms  0.700 ms  0.698 ms
 9  be105.fra-fr5-sbb2-nc5.de.eu (91.121.215.197)  3.347 ms  3.325 ms *
10  10.200.0.17 (10.200.0.17)  3.043 ms 10.200.0.19 (10.200.0.19)  3.103 ms  3.127 ms
11  * * *
12  * * *
13  dns.google (8.8.8.8)  3.092 ms  3.108 ms  3.090 ms
```



```
:~# sudo traceroute -6 2001:4860:4860::8888 -e
traceroute to 2001:4860:4860::8888 (2001:4860:4860::8888), 30 hops max, 80 byte packets
 1  _gateway (2001:41d0:404:200::1)  1.423 ms  1.477 ms  0.803 ms
 2  fd00::ffe (fd00::ffe)  1.585 ms  1.575 ms  1.558 ms
 3  2001:41d0:0:1:3::c27f (2001:41d0:0:1:3::c27f)  1.557 ms  1.613 ms  1.555 ms
 4  2001:41d0:0:1:3::c1c6 (2001:41d0:0:1:3::c1c6)  1.590 ms  1.486 ms  1.473 ms
 5  2001:41d0:0:1:3::c010 (2001:41d0:0:1:3::c010)  1.461 ms  1.621 ms 2001:41d0:0:1:3::c00e (2001:41d0:0:1:3::c00e)  1.
 6  2001:41d0:0:50::1:c80c (2001:41d0:0:50::1:c80c)  1.932 ms 2001:41d0:0:50::1:c13c (2001:41d0:0:50::1:c13c)  1.192 ms
 7  2001:41d0:0:50::5:93a (2001:41d0:0:50::5:93a)  0.290 ms 2001:41d0:0:50::5:838 (2001:41d0:0:50::5:838)  0.274 ms 200
 8  * be100-100.sbg-g2-nc5.fr.eu (2001:41d0::442)  0.954 ms *
 9  be105.fra-fr5-sbb2-nc5.de.eu (2001:41d0::44b)  3.427 ms *  3.292 ms
10  * * *
11  googel.as15169.de.eu (2001:41d0::2671)  3.151 ms  3.148 ms  3.142 ms
12  * 2a00:1450:8154::1 (2a00:1450:8154::1)  2.957 ms 2a00:1450:8153::1 (2a00:1450:8153::1)  2.977 ms
13  dns.google (2001:4860:4860::8888)  2.979 ms  3.039 ms  2.887 ms
```

Seeing classical middlebox

- Never forget : the TTL is your best friend



icmp

358 8.8.8.8

11/09/2023, 00:00:00

nb noeuds : 4

udp

359 8.8.8.8

11/09/2023, 00:00:00

nb noeuds : 6

tcp

360 8.8.8.8

11/09/2023, 00:00:00

nb noeuds : 4

ip ou domain: 8.8.8.8

Protocoles: tcp , udp , icmp

IPv4

Less classical middlebox

- Visible DPI (« Deep Packet Inspection »)
- Active Censorship Firewall (Great Firewall, maybe Eagle, …)
- Firewall used as censorship equipment (SonicWall, Fortiweb, …)
- BGP « optimizator » (used as anti-DDOS and BGP protection)
- Many other ! :D

Tips to find less classical middlebox

- Fuzzing everywhere ! Hoping to see abnormal trafic management
  - Fuzzing with IP packet fragmentation
  - Cryptography ! (playing with tls/ssh/kerberos sessions)
  - You can do that easily with « fuzz() » function on scapy !
- Play with censorship rules
  - Try domains list as SNI on TLS packet, HTTP packet, DNS query…
- Search for abnormal process time
  - maybe your packets aren’t just routed ? (¬‿¬)
  - Inconsistency of TCP stream, or on UDP encrypted stream
- Try weird protocols
  - Torrents, darknets, old protocols… Endless possibility !

Why searching middlebox ?

- For fun ~~and profit~~ !

- Discovering new equipment, understand *how network actually work*, understand *policy* on network (censorship, « *QoS* », security policies, …)

Why searching middlebox ?

- For profit ?

- Hiding on pentest, try to discovery hidden equipement on pentest session, understand security policy or investigate shadow network equipments

Questions ?

Don’t be shy ~~like middleboxes~~ ☺

References

- https://www.bortzmeyer.org/search?pattern=middleboxe
- « ICMP Extensions for Multiprotocol Label Switching » https://www.rfc-editor.org/rfc/rfc4950.html
- « traceroute(8) - Linux man page » https://linux.die.net/man/8/traceroute
- «IAB Workshop on Stack Evolution in a Middlebox Internet (SEMI) Report » https://www.rfc-editor.org/rfc/rfc7663.html
- « Middleboxes: Taxonomy and Issues » https://datatracker.ietf.org/doc/html/rfc3234
- « Weaponizing Middleboxes for TCP Reflected amplification » https://geneva.cs.umd.edu/papers/usenix-weaponizing-ddos.pdf