MuSecurity™

protocol fuzzing

past, present, future

luiz eduardo

senior systems & security engineer

leduardo (at) musecurity.com

gts x – são paulo

```
TCP     domain > 50237 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 TSV=2924684008 TSER=1994
TCP     domain > 50237 [ACK] Seq=1 Ack=1449 Win=8688 Len=0 TSV=2924684008 TSER=1994717l
TCP     domain > 50237 [ACK] [illegible]=2897 Win=11584 Len=0 TSV=2924684008 TSER=1994717l
TCP     domain > 50237 [ACK [illegible]q=1 Ack=4345 [illegible]4480 Len[illegible]
TCP     d[illegible]n > [illegible]37 [ACK] [illegible] Ack=579[illegible]
TCP     d[illegible]n > [illegible]37 [ACK] Seq[illegible]72[illegible]0 TSV=292[illegible]4008 [illegible]47171
TCP     d[illegible]n > [illegible]37 [ACK] Seq=1 [illegible]86[illegible]in=23168 [illegible]0 TSV=292[illegible]4008 [illegible]47171
TCP     d[illegible]37 [ACK [illegible]101[illegible]64 [illegible]94717
TCP     domain > 50237 [ACK] Seq=1 Ack=11585 Win=28960 Len=0 TSV=292[illegible] TSER=1994717l
TCP     domain > 50237 [ACK] Seq=1 Ack=13033 Win=31856 Len=0 TSV=2924684008 TSER=1994717l
TCP     domain > 50237 [ACK] Seq=1 Ack=14481 Win=34752 Len=0 TSV=2924684008 TSER=1994717l
TCP     domain > 50237 [ACK] Seq=1 Ack=15929 Win=37648 Len=0 TSV=2924684008 TSER=1994717l
TCP     domain > 50237 [ACK] Seq=1 Ack=17377 Win=40544 Len=0 TSV=2924684008 TSER=1994717l
TCP     domain > 50237 [ACK] Seq=1 Ack=18[illegible]25 Win=43440 Len=0 TSV=2924684008 TSER=1994717l
TCP     do[illegible]73 [illegible] TSER=1994717l
TCP     do[illegible] 50[illegible]21 [illegible]008 TSER=1994717l
TCP     do[illegible]in > 50237 [ACK] Seq=1 Ack=23169 Win=52[illegible] TSER=1994717l
TCP     domain > 50237 [ACK] Seq=1 Ack=24617 Win=55024 Len=0 TSV=2924684008 TSER=1994717l
TCP     domain > 50237 [ACK] Seq=1 Ack=26065 Win=57920 Len=0 TSV=2924684008 TSER=1994717l
TCP     domain > 50237 [ACK] Seq=1 Ack=27513 Win=60[illegible]16 Len=[illegible]TSV=292[illegible]684008 TSER=1994717l
TC[illegible] > 50237 [illegible] Len=[illegible]4717l
DN[illegible]known operation[illegible] response[illegible] implemented
TC[illegible] domain > 50237 [illegible] Seq=15 Ack=31857 Win=637[illegible] Len=0 TSV=2924684008 TSER=1994717l
TCP     domain > 50237 [ACK] Seq=15 Ack=34217 Win=63712 Len=0 TSV=2924684008 TSER=1994717l
TCP     domain > 50237 [ACK] Seq=15 Ack=37113 Win=63712 Len=0 TSV=2924684008 TSER=1994717l
TCP     domain > 50237 [ACK] Seq=15 Ack=40009 Win=63712 Len=0 TSV=2924684008 TSER=1994717l
TCP     domain > 50237 [ACK] [illegible]5 [illegible] 63712 Len=0 TSV=2924684008 TSER=1994717l
TCP     domain > 50237 [ACK] Seq=15 Ack=45801 Win=63712 Len=0 TSV=2924684008 TSER=1994717l
TCP     [illegible]684008 TSER=1994717l
TCP     domain > 50237 [ACK] Seq=15 Ack=50601 Win=63712 Len=0 TSV=2924684008 TSER=1994717l
TCP     domain > 50237 [ACK] Seq=15 Ack=53497 Win=63712 Len=0 TSV=2924684008 TSER=1994717l
TCP     domai[illegible] TSV=2924684008 TSER=1994717l
TCP     domain > 50237 [ACK] Seq=15 Ack=59289 Win=63712 Len=0 TSV=2924684008 TSER=1994717l
TCP     domain > 50237 [ACK] Seq=15 Ack=62185 Win=63712 Len=0 TSV=2924684008 TSER=1994717l
TCP     domain > 50237 [ACK] Seq=15 Ack=65081 Win=63712 Len=0 TSV=2924684008 TSER=1994717l
TCP     domain > 50237 [ACK] Seq=15 Ack=66985 Win=63712 Len=0 TSV=2924684008 TSER=1994717l
TCP     domain > 50237 [ACK] Seq=15 Ack=69881 Win=63712 Len=0 TSV=2924684008 TSER=1994717l
TCP     domain > 50237 [ACK] Seq=15 Ack=72[illegible] Win=63712 [illegible] TSV=2924684008 TSER=1994717l
```

agenda

- history of fuzzing
- protocol fuzzing
- fuzzable or not?
- non-sense fuzzing
- session-based fuzzing / stateful-based fuzzing
- tools | techniques
- challenges
- getting creative
- packet fun
- predictions
- resources

hi

- network security guy
- regular speaker at security conferences
- wlan at security conferences (defcon, blackhat, chaos computer congress, etc)
- networking goon @ defcon
- infosec certifications buff
- and. . .
- don't believe anything i say! (tm bruce potter)
- ok, at least question yourself (and others) about it. . .

abrindo parênteses

josé: eita, de novo!!! fuzzing?????? puxa luiz, traduza isso!

luiz: zé, não dá... nem em inglês tem um significado... mas vamos tentar:

- fuzzing é a técnica (ou arte) de enviar entradas não válidas para qualquer tipo de mecanismo de entrada.
- todo mecanismo de entrada deveria simplesmente descartar entradas inválidas, mas isso não acontece.

- então, "fuzzing" se tornou a técnica de exercitar os programas existentes* para entradas inválidas.

- "parecido" com uma técnica conhecida como:
  Análise do valor limite
  (ou boundary value analysis (BVA))

fuzzing history

- “created” @ university of madison in 1989 by professor barton miller and his crew
- why ?
- buzz word in the past fe
- not just a http thing
- file format fuzzing
- application fuzzing
- sorta “hope” to find 0 d
- and. . .

terms/ keywords/ etc

- malformed / semi-malformed/ invalid input
- random
- target
- exception-handling
- mutations
- instrumentation
- art / creativity
- agents
- negative-testing

changed the mentality of: "but.. . . . that packet doesn't follow the rfc spec"

or

"hmmmmm. . . but. . . people are not supposed to send these packets"

Visunrdansting ™

vulnerability scanners

protocol fuzzing

exploitation tools

wait! what's this 0 day thing?

(con)fuzzable or not?

“mainstreaming” fuzzing

- best “bang for the buck”
- numerous bugs found in the past few years
- some of them make the news
- others probably not . . .
- growth in the number of specific tools
- number of vulnerabilities increase, number o
  exploits not that much

corporate fuzzing

- again, nothing new. . .. but . . . if you don't fuzz, someone else will

- fuzzing became a "common practice" (regardless if it's done correctly or not)

- delivering products / services with "basic" testing is no longer acceptable

- Well. . ... Being reactive sux

so. . . protocol fuzzing, shall we?

- anything that has an input could be considered protocol fuzzing but. . .
- protocol abuse
- test robustness of the target
- from instability to crashes (or to remote code execution)
- if it's already hard for one to follow the rfc spec,
  how about the "anything but. . ." ?

ohhh, there is a difference. . .

fuzzers are not va scanners! fuzzers are not va scanners!

what to break in a protocol?

- structure
- state
- semantics

- Buffer Overflow
- Integer Overflow
- Invalid Message
- Format String
- Fragmented Field
- Invalid Header
- Null Character
- Wrong Encoding
- Invalid Index

- Invalid String
- Recursion
- Truncated
- Underflow
- Missing Field
- Mixed Case
- Out of Order
- Self-Reference
- Too Many Fields
- Invalid Offset

what protocols to fuzz?

- all of them, of course

- but... what's the buzz? what's new? what's not mature?

- sip
- scada
- ipv6
- wireless
- bluetooth
- videogames

non-sense fuzzing

session-based fuzzing

- first you establish a channel with the target and then start fuzzing at that level

- it could be the tony-montana-style fuzzing to certain tcp/udp port too
- but, somehow interacting w/ the target based on the protocol is more Corleone-style

stateful-based fuzzing

- one step above (simply) establishing a session (aka: better than Michael Corleone)
- “on-the-fly” fuzzing/ reading the target’s “mind”
- (possible) better fault isolation
- (possible) better code exercise ’

“attack” techniques

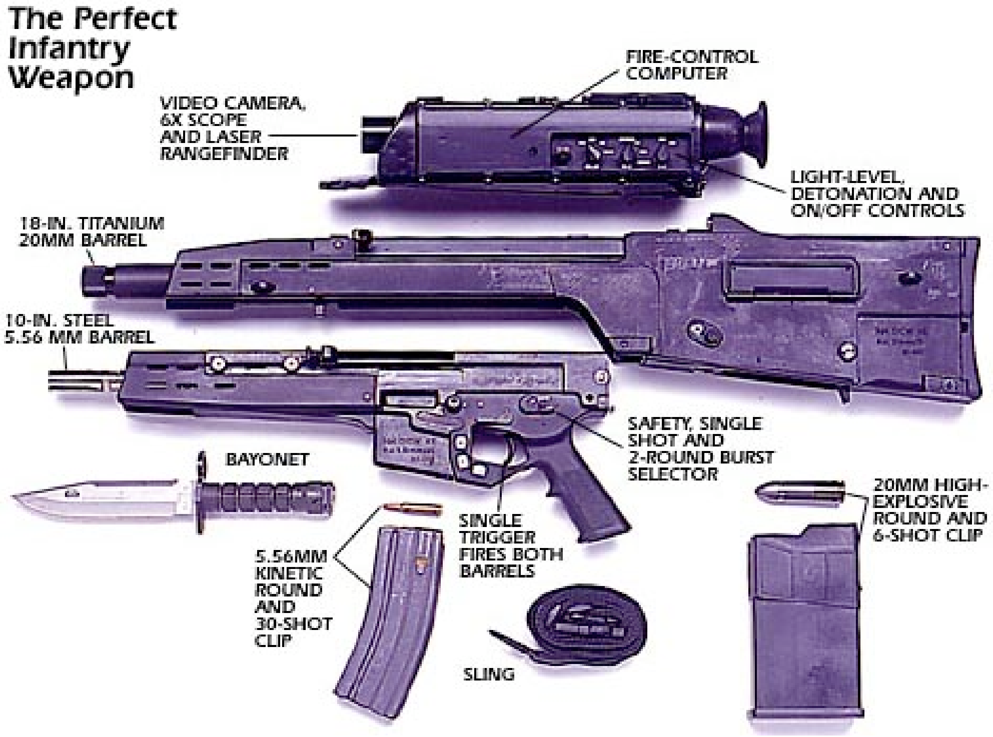
- random
- database
- (mix?)
- stateful

some of the usual challenges

- fault isolation
- the "bug behind the bug"
- "slow" protocol implementations
- monitor the target (memory leaks/ cpu spikes/ some type of redundancy)
- monitor processes/ child processes

tools

- manual testing
- spike / written in c/ block-based approach
- protos / java / different fuzzers
- peach / python / “written while drinking beer at ph-neutral”
- antiparser / python/ fuzzer and fault injection tool
- dfuz / c
- sulley/ parallel fuzzing capabilities /legos


The Perfect Infantry Weapon
FIRE-CONTROL COMPUTER
VIDEO CAMERA, 6X SCOPE AND LASER RANGEFINDER
LIGHT-LEVEL, DETONATION AND ON/OFF CONTROLS
18-IN. TITANIUM 20MM BARREL
10-IN. STEEL 5.56 MM BARREL
SAFETY, SINGLE SHOT AND 2-ROUND BURST SELECTOR
BAYONET
20MM HIGH-EXPLOSIVE ROUND AND 6-SHOT CLIP
SINGLE TRIGGER FIRES BOTH BARRELS
5.56MM KINETIC ROUND AND 30-SHOT CLIP
SLING

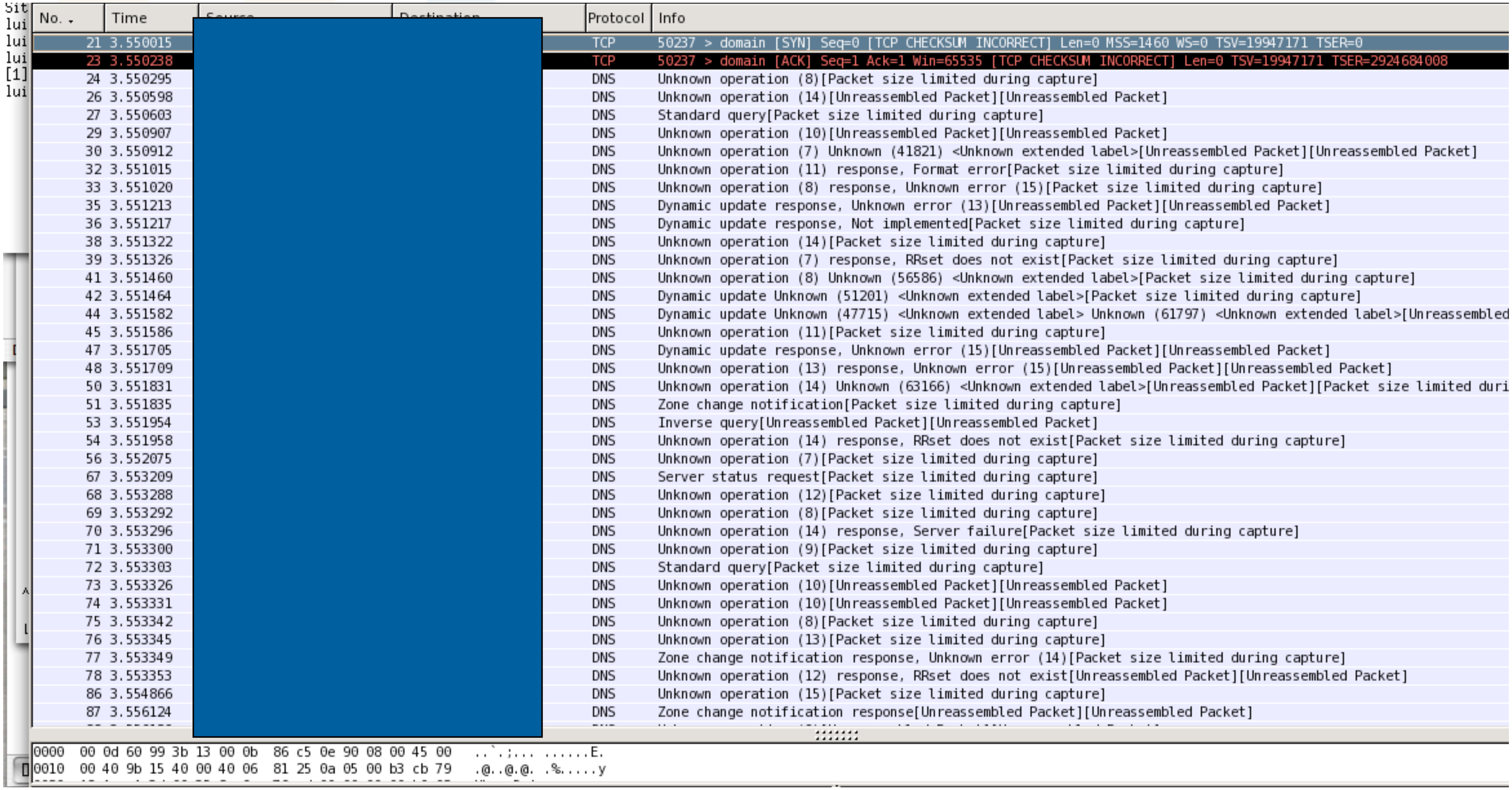
commercial

- bestorm
- codenomicom
- hydra
- mu security
- thread-x

getting creative / how to ~~break~~ test stuff

- use different fuzzing tools
- use the same fuzzing tool (parallel fuzzing)
- use a framework to integrate other stuff (traffic gen, nmap, exploitation tools, etc)
- use a framework to integrate agents for monitoring
- well. . . use any tools available

packets



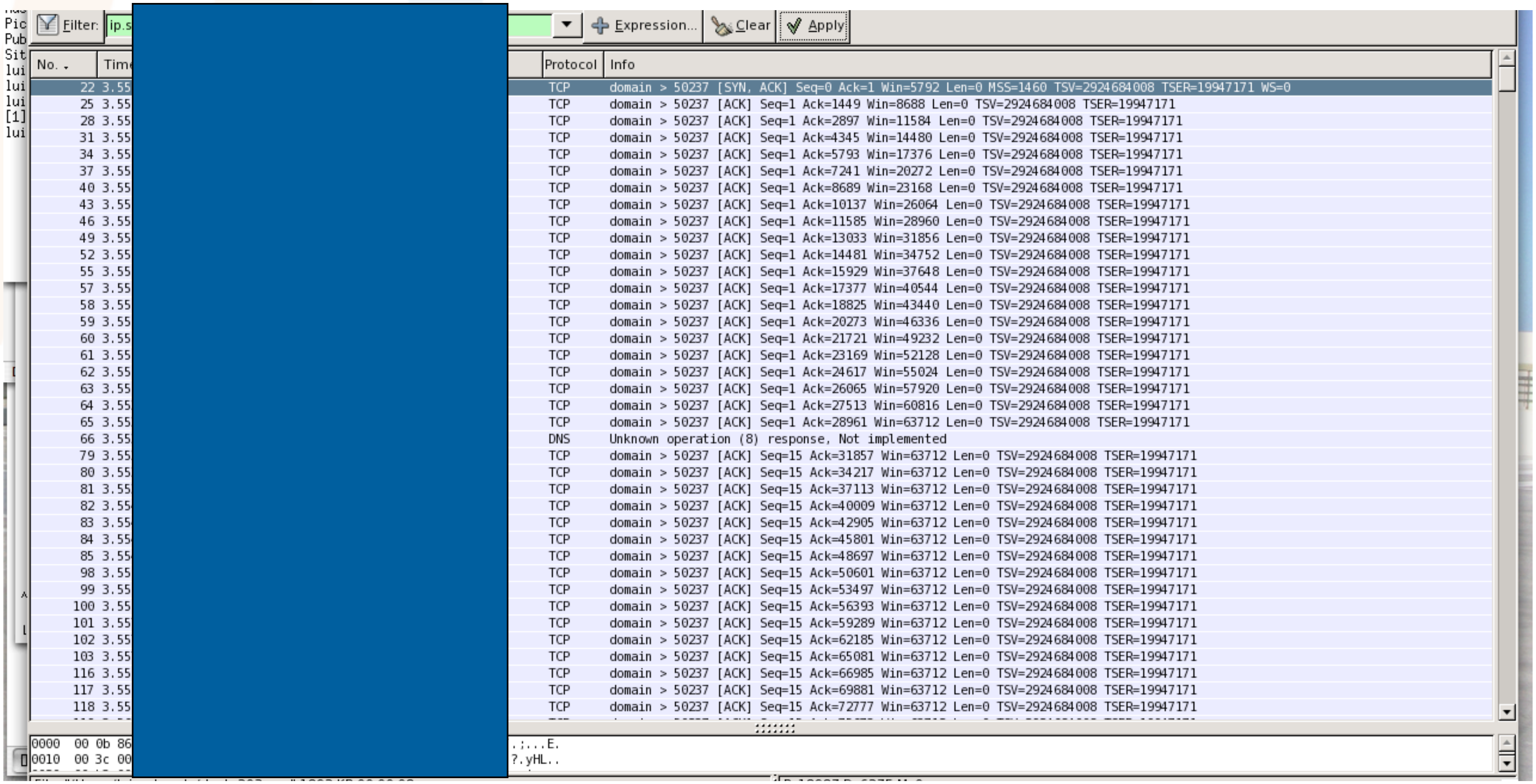
```
No. -  Time      Source/Destination  Protocol Info
21  3.550015  [redacted]  TCP  50237 > domain [SYN] Seq=0 [TCP CHECKSUM INCORRECT] Len=0 MSS=1460 WS=0 TSV=19947171 TSER=0
23  3.550238  [redacted]  TCP  50237 > domain [ACK] Seq=1 Ack=1 Win=65535 [TCP CHECKSUM INCORRECT] Len=0 TSV=19947171 TSER=2924684008
24  3.550295  [redacted]  DNS  Unknown operation (8)[Packet size limited during capture]
26  3.550598  [redacted]  DNS  Unknown operation (14)[Unreassembled Packet][Unreassembled Packet]
27  3.550603  [redacted]  DNS  Standard query[Packet size limited during capture]
29  3.550907  [redacted]  DNS  Unknown operation (10)[Unreassembled Packet][Unreassembled Packet]
30  3.550912  [redacted]  DNS  Unknown operation (7) Unknown (41821) <Unknown extended label>[Unreassembled Packet][Unreassembled Packet]
32  3.551015  [redacted]  DNS  Unknown operation (11) response, Format error[Packet size limited during capture]
33  3.551020  [redacted]  DNS  Unknown operation (8) response, Unknown error (15)[Packet size limited during capture]
35  3.551213  [redacted]  DNS  Dynamic update response, Unknown error (13)[Unreassembled Packet][Unreassembled Packet]
36  3.551217  [redacted]  DNS  Dynamic update response, Not implemented[Packet size limited during capture]
38  3.551322  [redacted]  DNS  Unknown operation (14)[Packet size limited during capture]
39  3.551326  [redacted]  DNS  Unknown operation (7) response, RRset does not exist[Packet size limited during capture]
41  3.551460  [redacted]  DNS  Unknown operation (8) Unknown (56586) <Unknown extended label>[Packet size limited during capture]
42  3.551464  [redacted]  DNS  Dynamic update Unknown (51201) <Unknown extended label>[Packet size limited during capture]
44  3.551582  [redacted]  DNS  Dynamic update Unknown (47715) <Unknown extended label> Unknown (61797) <Unknown extended label>[Unreassembled
45  3.551586  [redacted]  DNS  Unknown operation (11)[Packet size limited during capture]
47  3.551705  [redacted]  DNS  Dynamic update response, Unknown error (15)[Unreassembled Packet][Unreassembled Packet]
48  3.551709  [redacted]  DNS  Unknown operation (13) response, Unknown error (15)[Unreassembled Packet][Unreassembled Packet]
50  3.551831  [redacted]  DNS  Unknown operation (14) Unknown (63166) <Unknown extended label>[Unreassembled Packet][Packet size limited duri
51  3.551835  [redacted]  DNS  Zone change notification[Packet size limited during capture]
53  3.551954  [redacted]  DNS  Inverse query[Unreassembled Packet][Unreassembled Packet]
54  3.551958  [redacted]  DNS  Unknown operation (14) response, RRset does not exist[Packet size limited during capture]
56  3.552075  [redacted]  DNS  Unknown operation (7)[Packet size limited during capture]
67  3.553209  [redacted]  DNS  Server status request[Packet size limited during capture]
68  3.553288  [redacted]  DNS  Unknown operation (12)[Packet size limited during capture]
69  3.553292  [redacted]  DNS  Unknown operation (8)[Packet size limited during capture]
70  3.553296  [redacted]  DNS  Unknown operation (14) response, Server failure[Packet size limited during capture]
71  3.553300  [redacted]  DNS  Unknown operation (9)[Packet size limited during capture]
72  3.553303  [redacted]  DNS  Standard query[Packet size limited during capture]
73  3.553326  [redacted]  DNS  Unknown operation (10)[Unreassembled Packet][Unreassembled Packet]
74  3.553331  [redacted]  DNS  Unknown operation (10)[Unreassembled Packet][Unreassembled Packet]
75  3.553342  [redacted]  DNS  Unknown operation (8)[Packet size limited during capture]
76  3.553345  [redacted]  DNS  Unknown operation (13)[Packet size limited during capture]
77  3.553349  [redacted]  DNS  Zone change notification response, Unknown error (14)[Packet size limited during capture]
78  3.553353  [redacted]  DNS  Unknown operation (12) response, RRset does not exist[Unreassembled Packet][Unreassembled Packet]
86  3.554866  [redacted]  DNS  Unknown operation (15)[Packet size limited during capture]
87  3.556124  [redacted]  DNS  Zone change notification response[Unreassembled Packet][Unreassembled Packet]

0000  00 0d 60 99 3b 13 00 0b  86 c5 0e 90 08 00 45 00   ..`.;... ......E.
0010  00 40 9b 15 40 00 40 06  81 25 0a 05 00 b3 cb 79   .@..@.@. .%.....y
```

gts 10 - são paulo

Mu Security™

packets (cont)



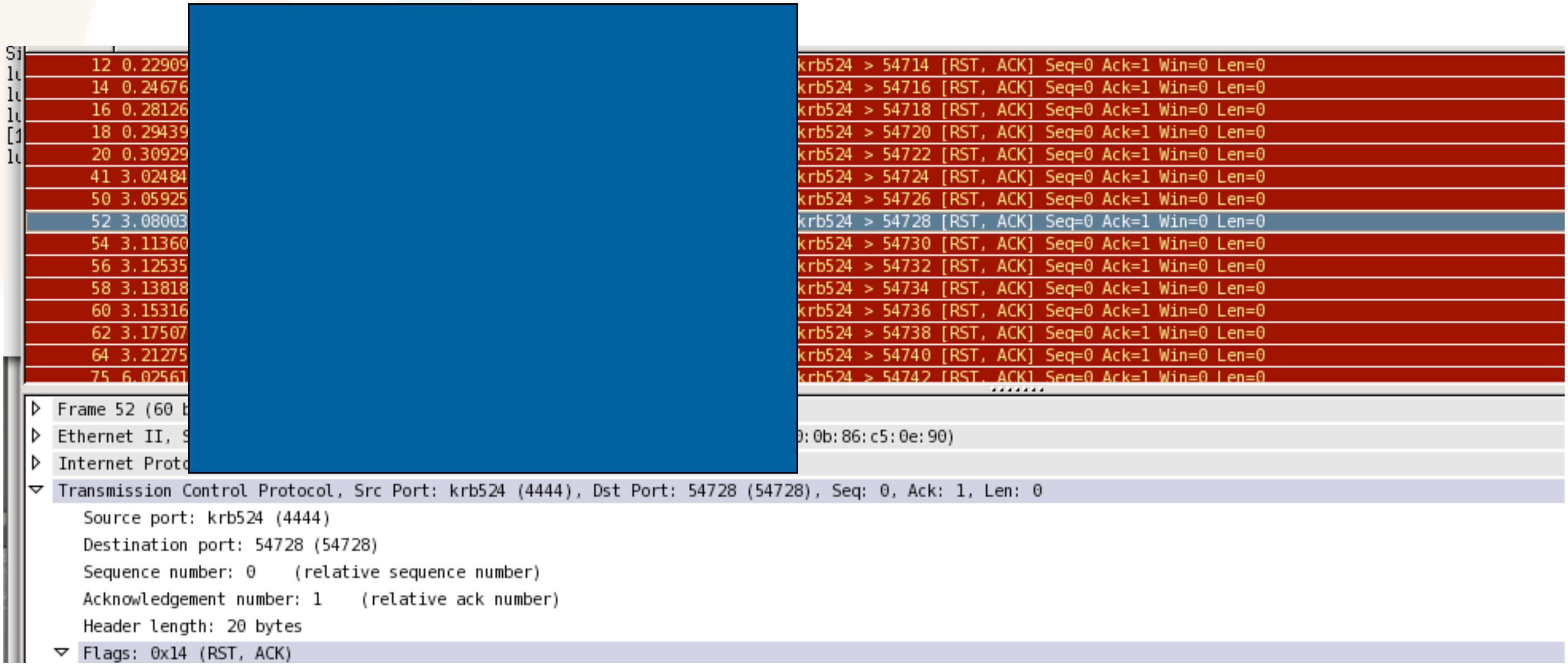
[redacted]

```
Filter: ip.s                                    ▼  Expression...  Clear  Apply

No. .   Time                   Protocol  Info
   22 3.55                     TCP       domain > 50237 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 TSV=2924684008 TSER=19947171 WS=0
   25 3.55                     TCP       domain > 50237 [ACK] Seq=1 Ack=1449 Win=8688 Len=0 TSV=2924684008 TSER=19947171
   28 3.55                     TCP       domain > 50237 [ACK] Seq=1 Ack=2897 Win=11584 Len=0 TSV=2924684008 TSER=19947171
   31 3.55                     TCP       domain > 50237 [ACK] Seq=1 Ack=4345 Win=14480 Len=0 TSV=2924684008 TSER=19947171
   34 3.55                     TCP       domain > 50237 [ACK] Seq=1 Ack=5793 Win=17376 Len=0 TSV=2924684008 TSER=19947171
   37 3.55                     TCP       domain > 50237 [ACK] Seq=1 Ack=7241 Win=20272 Len=0 TSV=2924684008 TSER=19947171
   40 3.55                     TCP       domain > 50237 [ACK] Seq=1 Ack=8689 Win=23168 Len=0 TSV=2924684008 TSER=19947171
   43 3.55                     TCP       domain > 50237 [ACK] Seq=1 Ack=10137 Win=26064 Len=0 TSV=2924684008 TSER=19947171
   46 3.55                     TCP       domain > 50237 [ACK] Seq=1 Ack=11585 Win=28960 Len=0 TSV=2924684008 TSER=19947171
   49 3.55                     TCP       domain > 50237 [ACK] Seq=1 Ack=13033 Win=31856 Len=0 TSV=2924684008 TSER=19947171
   52 3.55                     TCP       domain > 50237 [ACK] Seq=1 Ack=14481 Win=34752 Len=0 TSV=2924684008 TSER=19947171
   55 3.55                     TCP       domain > 50237 [ACK] Seq=1 Ack=15929 Win=37648 Len=0 TSV=2924684008 TSER=19947171
   57 3.55                     TCP       domain > 50237 [ACK] Seq=1 Ack=17377 Win=40544 Len=0 TSV=2924684008 TSER=19947171
   58 3.55                     TCP       domain > 50237 [ACK] Seq=1 Ack=18825 Win=43440 Len=0 TSV=2924684008 TSER=19947171
   59 3.55                     TCP       domain > 50237 [ACK] Seq=1 Ack=20273 Win=46336 Len=0 TSV=2924684008 TSER=19947171
   60 3.55                     TCP       domain > 50237 [ACK] Seq=1 Ack=21721 Win=49232 Len=0 TSV=2924684008 TSER=19947171
   61 3.55                     TCP       domain > 50237 [ACK] Seq=1 Ack=23169 Win=52128 Len=0 TSV=2924684008 TSER=19947171
   62 3.55                     TCP       domain > 50237 [ACK] Seq=1 Ack=24617 Win=55024 Len=0 TSV=2924684008 TSER=19947171
   63 3.55                     TCP       domain > 50237 [ACK] Seq=1 Ack=26065 Win=57920 Len=0 TSV=2924684008 TSER=19947171
   64 3.55                     TCP       domain > 50237 [ACK] Seq=1 Ack=27513 Win=60816 Len=0 TSV=2924684008 TSER=19947171
   65 3.55                     TCP       domain > 50237 [ACK] Seq=1 Ack=28961 Win=63712 Len=0 TSV=2924684008 TSER=19947171
   66 3.55                     DNS       Unknown operation (8) response, Not implemented
   79 3.55                     TCP       domain > 50237 [ACK] Seq=15 Ack=31857 Win=63712 Len=0 TSV=2924684008 TSER=19947171
   80 3.55                     TCP       domain > 50237 [ACK] Seq=15 Ack=34217 Win=63712 Len=0 TSV=2924684008 TSER=19947171
   81 3.55                     TCP       domain > 50237 [ACK] Seq=15 Ack=37113 Win=63712 Len=0 TSV=2924684008 TSER=19947171
   82 3.55                     TCP       domain > 50237 [ACK] Seq=15 Ack=40009 Win=63712 Len=0 TSV=2924684008 TSER=19947171
   83 3.55                     TCP       domain > 50237 [ACK] Seq=15 Ack=42905 Win=63712 Len=0 TSV=2924684008 TSER=19947171
   84 3.55                     TCP       domain > 50237 [ACK] Seq=15 Ack=45801 Win=63712 Len=0 TSV=2924684008 TSER=19947171
   85 3.55                     TCP       domain > 50237 [ACK] Seq=15 Ack=48697 Win=63712 Len=0 TSV=2924684008 TSER=19947171
   98 3.55                     TCP       domain > 50237 [ACK] Seq=15 Ack=50601 Win=63712 Len=0 TSV=2924684008 TSER=19947171
   99 3.55                     TCP       domain > 50237 [ACK] Seq=15 Ack=53497 Win=63712 Len=0 TSV=2924684008 TSER=19947171
  100 3.55                     TCP       domain > 50237 [ACK] Seq=15 Ack=56393 Win=63712 Len=0 TSV=2924684008 TSER=19947171
  101 3.55                     TCP       domain > 50237 [ACK] Seq=15 Ack=59289 Win=63712 Len=0 TSV=2924684008 TSER=19947171
  102 3.55                     TCP       domain > 50237 [ACK] Seq=15 Ack=62185 Win=63712 Len=0 TSV=2924684008 TSER=19947171
  103 3.55                     TCP       domain > 50237 [ACK] Seq=15 Ack=65081 Win=63712 Len=0 TSV=2924684008 TSER=19947171
  116 3.55                     TCP       domain > 50237 [ACK] Seq=15 Ack=66985 Win=63712 Len=0 TSV=2924684008 TSER=19947171
  117 3.55                     TCP       domain > 50237 [ACK] Seq=15 Ack=69881 Win=63712 Len=0 TSV=2924684008 TSER=19947171
  118 3.55                     TCP       domain > 50237 [ACK] Seq=15 Ack=72777 Win=63712 Len=0 TSV=2924684008 TSER=19947171

0000  00 0b 86                 .;...E.
0010  00 3c 00                 ?.yHL..
```

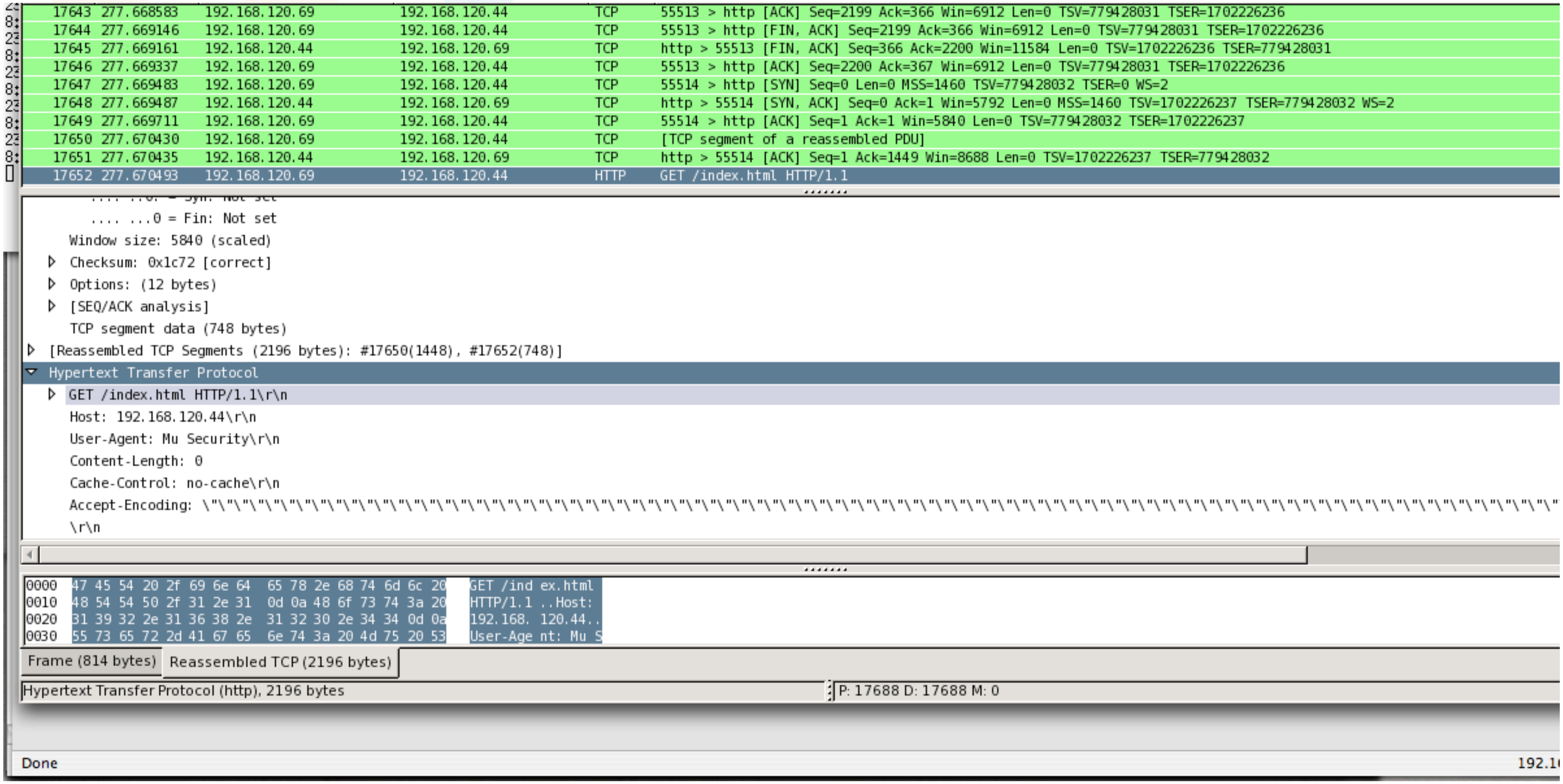
packets (again)



```
 12 0.22909 [redacted] krb524 > 54714 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
 14 0.24676            krb524 > 54716 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
 16 0.28126            krb524 > 54718 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
 18 0.29439            krb524 > 54720 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
 20 0.30929            krb524 > 54722 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
 41 3.02484            krb524 > 54724 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
 50 3.05925            krb524 > 54726 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
 52 3.08003            krb524 > 54728 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
 54 3.11360            krb524 > 54730 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
 56 3.12535            krb524 > 54732 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
 58 3.13818            krb524 > 54734 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
 60 3.15316            krb524 > 54736 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
 62 3.17507            krb524 > 54738 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
 64 3.21275            krb524 > 54740 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
 75 6.02561            krb524 > 54742 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0

▷ Frame 52 (60 b
▷ Ethernet II, S                                   0:0b:86:c5:0e:90)
▷ Internet Proto
▽ Transmission Control Protocol, Src Port: krb524 (4444), Dst Port: 54728 (54728), Seq: 0, Ack: 1, Len: 0
    Source port: krb524 (4444)
    Destination port: 54728 (54728)
    Sequence number: 0    (relative sequence number)
    Acknowledgement number: 1    (relative ack number)
    Header length: 20 bytes
  ▽ Flags: 0x14 (RST, ACK)
```

packets (again)



```
17643 277.668583  192.168.120.69    192.168.120.44    TCP   55513 > http [ACK] Seq=2199 Ack=366 Win=6912 Len=0 TSV=779428031 TSER=1702226236
17644 277.669146  192.168.120.69    192.168.120.44    TCP   55513 > http [FIN, ACK] Seq=2199 Ack=366 Win=6912 Len=0 TSV=779428031 TSER=1702226236
17645 277.669161  192.168.120.44    192.168.120.69    TCP   http > 55513 [FIN, ACK] Seq=366 Ack=2200 Win=11584 Len=0 TSV=1702226236 TSER=779428031
17646 277.669337  192.168.120.69    192.168.120.44    TCP   55513 > http [ACK] Seq=2200 Ack=367 Win=6912 Len=0 TSV=779428031 TSER=1702226236
17647 277.669483  192.168.120.69    192.168.120.44    TCP   55514 > http [SYN] Seq=0 Len=0 MSS=1460 TSV=779428032 TSER=0 WS=2
17648 277.669487  192.168.120.44    192.168.120.69    TCP   http > 55514 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 TSV=1702226237 TSER=779428032 WS=2
17649 277.669711  192.168.120.69    192.168.120.44    TCP   55514 > http [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSV=779428032 TSER=1702226237
17650 277.670430  192.168.120.69    192.168.120.44    TCP   [TCP segment of a reassembled PDU]
17651 277.670435  192.168.120.44    192.168.120.69    TCP   http > 55514 [ACK] Seq=1 Ack=1449 Win=8688 Len=0 TSV=1702226237 TSER=779428032
17652 277.670493  192.168.120.69    192.168.120.44    HTTP  GET /index.html HTTP/1.1
```

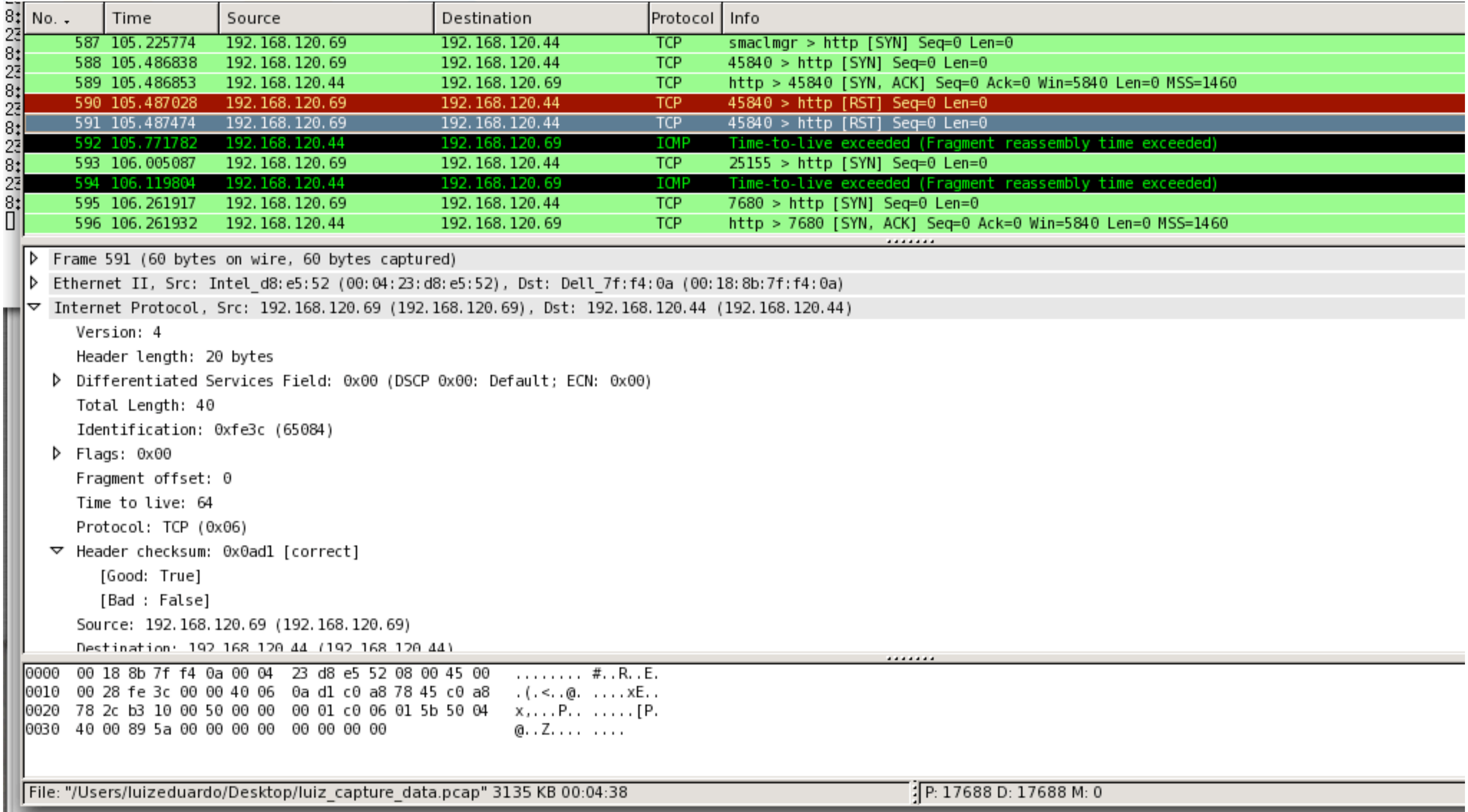
```
      .... ..0. = Syn: Not set
      .... ...0 = Fin: Not set
    Window size: 5840 (scaled)
  ▷ Checksum: 0x1c72 [correct]
  ▷ Options: (12 bytes)
  ▷ [SEQ/ACK analysis]
    TCP segment data (748 bytes)
▷ [Reassembled TCP Segments (2196 bytes): #17650(1448), #17652(748)]
▽ Hypertext Transfer Protocol
  ▷ GET /index.html HTTP/1.1\r\n
    Host: 192.168.120.44\r\n
    User-Agent: Mu Security\r\n
    Content-Length: 0
    Cache-Control: no-cache\r\n
    Accept-Encoding: \"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"
    \r\n
```

```
0000  47 45 54 20 2f 69 6e 64  65 78 2e 68 74 6d 6c 20   GET /ind ex.html
0010  48 54 54 50 2f 31 2e 31  0d 0a 48 6f 73 74 3a 20   HTTP/1.1 ..Host:
0020  31 39 32 2e 31 36 38 2e  31 32 30 2e 34 34 0d 0a   192.168. 120.44..
0030  55 73 65 72 2d 41 67 65  6e 74 3a 20 4d 75 20 53   User-Age nt: Mu S
```

Hypertext Transfer Protocol (http), 2196 bytes

P: 17688 D: 17688 M: 0

packets (yeah yeah)



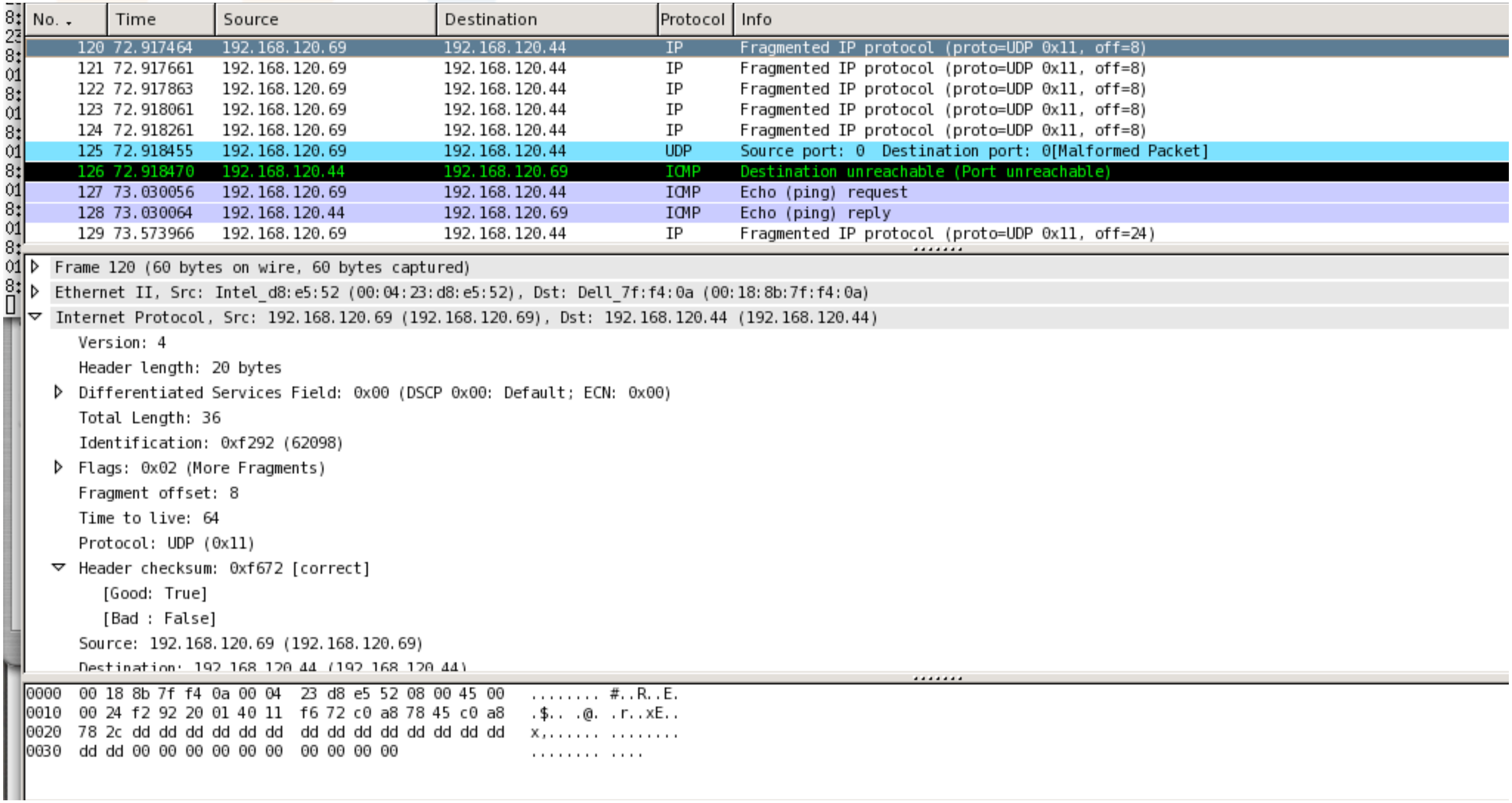
No.	Time	Source	Destination	Protocol	Info
587	105.225774	192.168.120.69	192.168.120.44	TCP	smaclmgr > http [SYN] Seq=0 Len=0
588	105.486838	192.168.120.69	192.168.120.44	TCP	45840 > http [SYN] Seq=0 Len=0
589	105.486853	192.168.120.44	192.168.120.69	TCP	http > 45840 [SYN, ACK] Seq=0 Ack=0 Win=5840 Len=0 MSS=1460
590	105.487028	192.168.120.69	192.168.120.44	TCP	45840 > http [RST] Seq=0 Len=0
591	105.487474	192.168.120.69	192.168.120.44	TCP	45840 > http [RST] Seq=0 Len=0
592	105.771782	192.168.120.44	192.168.120.69	ICMP	Time-to-live exceeded (Fragment reassembly time exceeded)
593	106.005087	192.168.120.69	192.168.120.44	TCP	25155 > http [SYN] Seq=0 Len=0
594	106.119804	192.168.120.44	192.168.120.69	ICMP	Time-to-live exceeded (Fragment reassembly time exceeded)
595	106.261917	192.168.120.69	192.168.120.44	TCP	7680 > http [SYN] Seq=0 Len=0
596	106.261932	192.168.120.44	192.168.120.69	TCP	http > 7680 [SYN, ACK] Seq=0 Ack=0 Win=5840 Len=0 MSS=1460

```
▷ Frame 591 (60 bytes on wire, 60 bytes captured)
▷ Ethernet II, Src: Intel_d8:e5:52 (00:04:23:d8:e5:52), Dst: Dell_7f:f4:0a (00:18:8b:7f:f4:0a)
▽ Internet Protocol, Src: 192.168.120.69 (192.168.120.69), Dst: 192.168.120.44 (192.168.120.44)
    Version: 4
    Header length: 20 bytes
  ▷ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 40
    Identification: 0xfe3c (65084)
  ▷ Flags: 0x00
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
  ▽ Header checksum: 0x0ad1 [correct]
      [Good: True]
      [Bad : False]
    Source: 192.168.120.69 (192.168.120.69)
    Destination: 192.168.120.44 (192.168.120.44)
```

```
0000  00 18 8b 7f f4 0a 00 04  23 d8 e5 52 08 00 45 00   ........ #..R..E.
0010  00 28 fe 3c 00 00 40 06  0a d1 c0 a8 78 45 c0 a8   .(.<..@. ....xE..
0020  78 2c b3 10 00 50 00 00  00 01 c0 06 01 5b 50 04   x,...P.. .....[P.
0030  40 00 89 5a 00 00 00 00  00 00 00 00               @..Z.... ....
```

File: "/Users/luizeduardo/Desktop/luiz_capture_data.pcap" 3135 KB 00:04:38 | P: 17688 D: 17688 M: 0

packets (one more?)

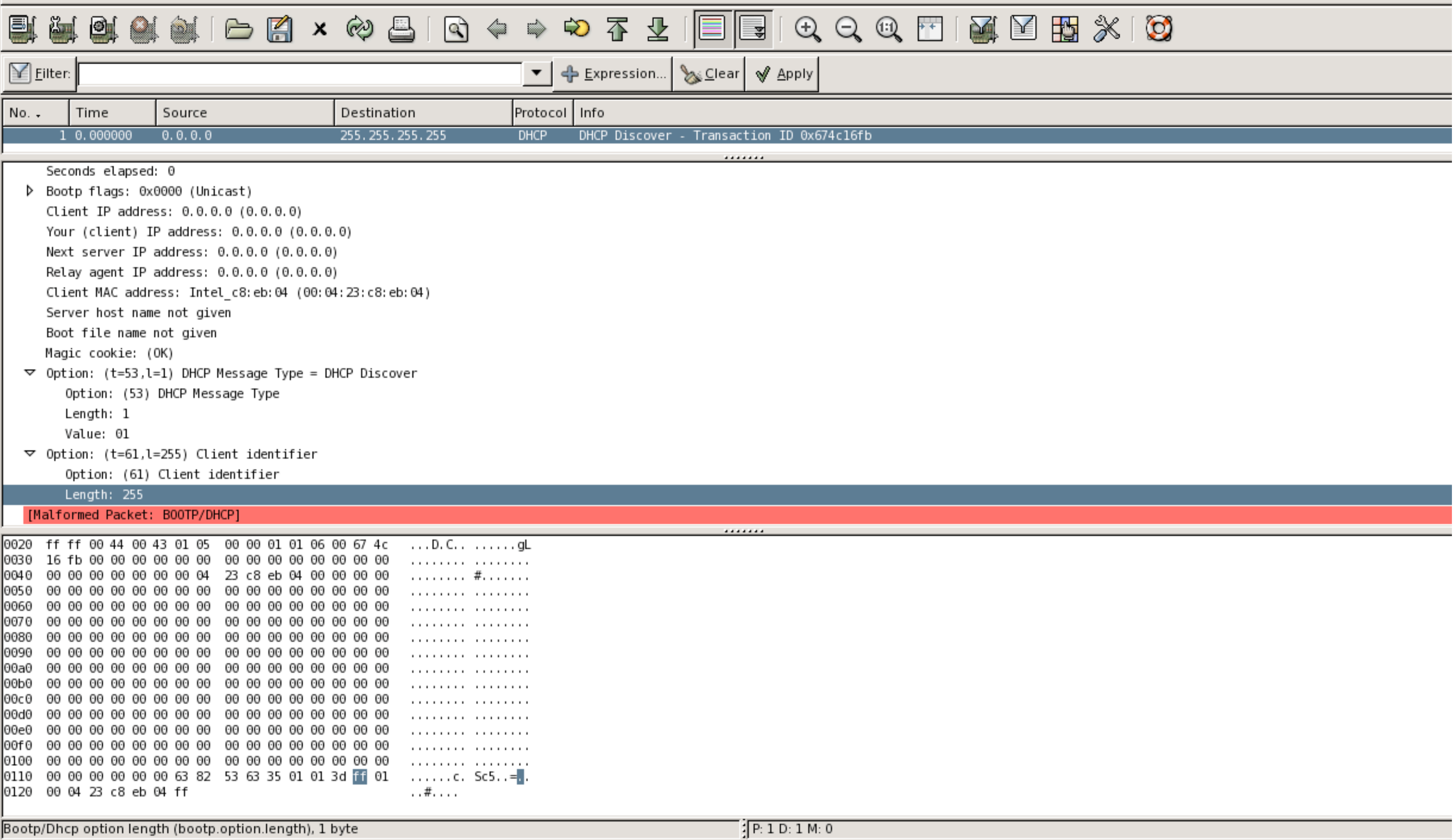


```
No. .  Time        Source            Destination       Protocol  Info
  120  72.917464   192.168.120.69    192.168.120.44    IP        Fragmented IP protocol (proto=UDP 0x11, off=8)
  121  72.917661   192.168.120.69    192.168.120.44    IP        Fragmented IP protocol (proto=UDP 0x11, off=8)
  122  72.917863   192.168.120.69    192.168.120.44    IP        Fragmented IP protocol (proto=UDP 0x11, off=8)
  123  72.918061   192.168.120.69    192.168.120.44    IP        Fragmented IP protocol (proto=UDP 0x11, off=8)
  124  72.918261   192.168.120.69    192.168.120.44    IP        Fragmented IP protocol (proto=UDP 0x11, off=8)
  125  72.918455   192.168.120.69    192.168.120.44    UDP       Source port: 0  Destination port: 0[Malformed Packet]
  126  72.918470   192.168.120.44    192.168.120.69    ICMP      Destination unreachable (Port unreachable)
  127  73.030056   192.168.120.69    192.168.120.44    ICMP      Echo (ping) request
  128  73.030064   192.168.120.44    192.168.120.69    ICMP      Echo (ping) reply
  129  73.573966   192.168.120.69    192.168.120.44    IP        Fragmented IP protocol (proto=UDP 0x11, off=24)
```

```
▷ Frame 120 (60 bytes on wire, 60 bytes captured)
▷ Ethernet II, Src: Intel_d8:e5:52 (00:04:23:d8:e5:52), Dst: Dell_7f:f4:0a (00:18:8b:7f:f4:0a)
▽ Internet Protocol, Src: 192.168.120.69 (192.168.120.69), Dst: 192.168.120.44 (192.168.120.44)
     Version: 4
     Header length: 20 bytes
   ▷ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
     Total Length: 36
     Identification: 0xf292 (62098)
   ▷ Flags: 0x02 (More Fragments)
     Fragment offset: 8
     Time to live: 64
     Protocol: UDP (0x11)
   ▽ Header checksum: 0xf672 [correct]
        [Good: True]
        [Bad : False]
     Source: 192.168.120.69 (192.168.120.69)
     Destination: 192.168.120.44 (192.168.120.44)
```

```
0000  00 18 8b 7f f4 0a 00 04  23 d8 e5 52 08 00 45 00   ........ #..R..E.
0010  00 24 f2 92 20 01 40 11  f6 72 c0 a8 78 45 c0 a8   .$.. .@. .r..xE..
0020  78 2c dd dd dd dd dd dd  dd dd dd dd dd dd dd dd   x,...... ........
0030  dd dd 00 00 00 00 00 00  00 00 00 00               ........ ....
```

packets (cont)



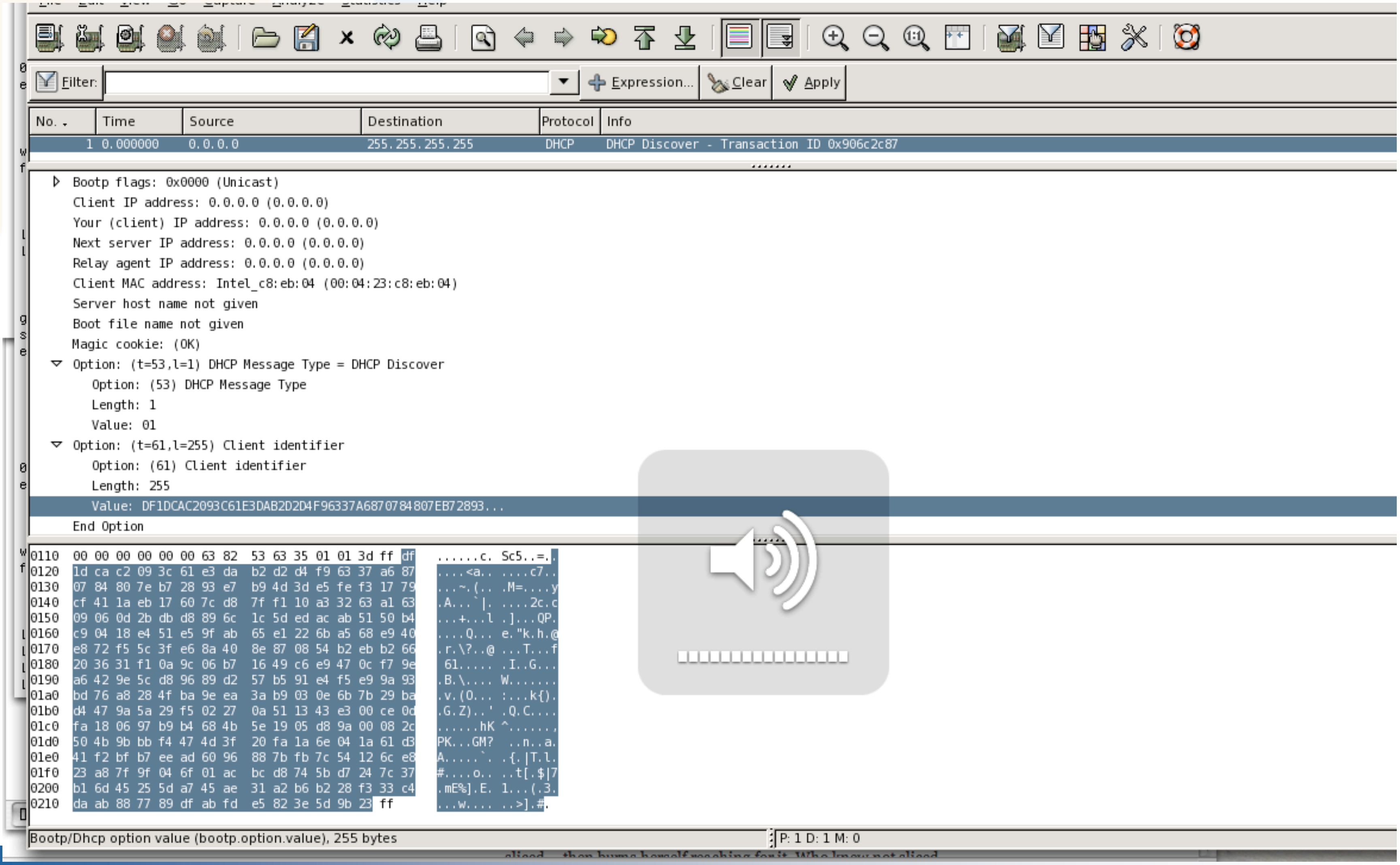
```
No. .   Time       Source         Destination        Protocol  Info
     1  0.000000   0.0.0.0        255.255.255.255    DHCP      DHCP Discover - Transaction ID 0x674c16fb
```

```
    Seconds elapsed: 0
  ▷ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: Intel_c8:eb:04 (00:04:23:c8:eb:04)
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
  ▽ Option: (t=53,l=1) DHCP Message Type = DHCP Discover
      Option: (53) DHCP Message Type
      Length: 1
      Value: 01
  ▽ Option: (t=61,l=255) Client identifier
      Option: (61) Client identifier
      Length: 255
  [Malformed Packet: BOOTP/DHCP]
```

```
0020  ff ff 00 44 00 43 01 05  00 00 01 01 06 00 67 4c   ...D.C.. ......gL
0030  16 fb 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0040  00 00 00 00 00 00 00 04  23 c8 eb 04 00 00 00 00   ........ #.......
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0110  00 00 00 00 00 00 63 82  53 63 35 01 01 3d ff 01   ......c. Sc5..=..
0120  00 04 23 c8 eb 04 ff                               ..#....
```

```
Bootp/Dhcp option length (bootp.option.length), 1 byte          P: 1 D: 1 M: 0
```

packets (last one)



```
No. -   Time       Source      Destination       Protocol  Info
      1 0.000000   0.0.0.0     255.255.255.255   DHCP      DHCP Discover - Transaction ID 0x906c2c87
```

```
▷ Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0 (0.0.0.0)
  Your (client) IP address: 0.0.0.0 (0.0.0.0)
  Next server IP address: 0.0.0.0 (0.0.0.0)
  Relay agent IP address: 0.0.0.0 (0.0.0.0)
  Client MAC address: Intel_c8:eb:04 (00:04:23:c8:eb:04)
  Server host name not given
  Boot file name not given
  Magic cookie: (OK)
▽ Option: (t=53,l=1) DHCP Message Type = DHCP Discover
    Option: (53) DHCP Message Type
    Length: 1
    Value: 01
▽ Option: (t=61,l=255) Client identifier
    Option: (61) Client identifier
    Length: 255
    Value: DF1DCAC2093C61E3DAB2D2D4F96337A68707848O7EB72893...
  End Option
```

```
0110  00 00 00 00 00 00 63 82  53 63 35 01 01 3d ff df   ......c. Sc5..=..
0120  1d ca c2 09 3c 61 e3 da  b2 d2 d4 f9 63 37 a6 87   ....<a.. ....c7..
0130  07 84 80 7e b7 28 93 e7  b9 4d 3d e5 fe f3 17 79   ...~.(.. .M=....y
0140  cf 41 1a eb 17 60 7c d8  7f f1 10 a3 32 63 a1 63   .A...`|. ....2c.c
0150  09 06 0d 2b db d8 89 6c  1c 5d ed ac ab 51 50 b4   ...+...l .]...QP.
0160  c9 04 18 e4 51 e5 9f ab  65 e1 22 6b a5 68 e9 40   ....Q... e."k.h.@
0170  e8 72 f5 5c 3f e6 8a 40  8e 87 08 54 b2 eb b2 66   .r.\?..@ ...T...f
0180  20 36 31 f1 0a 9c 06 b7  16 49 c6 e9 47 0c f7 9e    61..... .I..G...
0190  a6 42 9e 5c d8 96 89 d2  57 b5 91 e4 f5 e9 9a 93   .B.\.... W.......
01a0  bd 76 a8 28 4f ba 9e ea  3a b9 03 0e 6b 7b 29 ba   .v.(O... :...k{).
01b0  d4 47 9a 5a 29 f5 02 27  0a 51 13 43 e3 00 ce 0d   .G.Z)..' .Q.C....
01c0  fa 18 06 97 b9 b4 68 4b  5e 19 05 d8 9a 00 08 2c   ......hK ^......,
01d0  50 4b 9b bb f4 47 4d 3f  20 fa 1a 6e 04 1a 61 d3   PK...GM?  ..n..a.
01e0  41 f2 bf b7 ee ad 60 96  88 7b fb 7c 54 12 6c e8   A.....`. .{.|T.l.
01f0  23 a8 7f 9f 04 6f 01 ac  bc d8 74 5b d7 24 7c 37   #....o.. ..t[.$|7
0200  b1 6d 45 25 5d a7 45 ae  31 a2 b6 b2 28 f3 33 c4   .mE%].E. 1...(.3.
0210  da ab 88 77 89 df ab fd  e5 82 3e 5d 9b 23 ff      ...w.... ..>].#.
```

Bootp/Dhcp option value (bootp.option.value), 255 bytes

P: 1 D: 1 M: 0

(con)fuzzing state of the security community

- "bad" defense in depth implementations (and possibly concepts)
- again. . .. lots of security is ONLY based on known attacks
- critical infrastructure (?)
- fuzzing is not the red pill, but certainly has helped changing the way people think

The future

- most people already got fuzzing
- more intelligence has to be incoporated to protocol fuzzing
  - protocol/ application "adaptation"
  - offline protocol fuzzing/ protocol correlation (and playback?)
  - redundant system testing
  - fuzzing through tunnels
  - proxy-fuzzing (not a-la spike proxy)
  - fuzz through/ on/ with non-standard media types (traffic shapers, etc)

- creativity is key : use the brain, for anything
- better integration with other tools

- anything is fuzzable

resources

- http://labs.musecurity.com
- book: fuzzing: brute force vulnerability discovery: pedram et al
  http://fuzzing.org
- http://www.hacksafe.com.au/blog/2006/08/21/fuzz-testing-tools-and-techniques/
- http://www.immunitysec.com/downloads/advantages_of_block_based_analysis.pdf
- fuzzing mailing list by gadi evron
  http://www.whitestar.linuxbox.org/mailman/listinfo/fuzzing

muito obrigado

leduardo (at) musecurity.com