Carving Malware From PCAPs

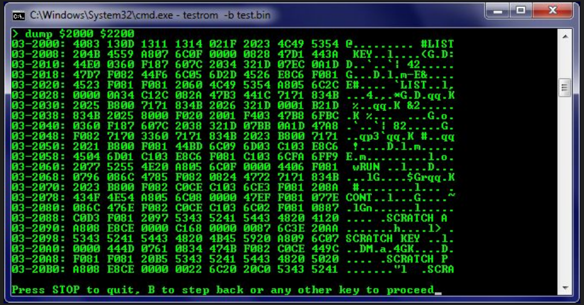
Mike Moss

What is file carving?

What is file carving?

+ =

What is file carving?

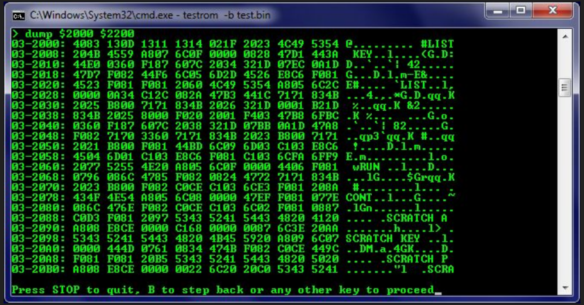


```
> dump $2000 $2200
03-2000: 4083 130D 1311 1314 021F 2023 4C49 5354 @......... #LIST
03-2008: 204B 4559 A807 6C0F 0000 0828 47D1 443A  KEY..l....(G.D:
03-2010: 44E0 0360 F187 607C 2034 321D 07EC 0A1D D..`..`| 42.....
03-2018: 47D7 F082 44F6 6C05 6D2D 4526 E8C6 F081 G...D.l.m-E&....
03-2020: 4523 F081 F081 2060 4C49 5354 A805 6C2C E#.... `LIST..l,
03-2028: 0000 0A34 C12C 082A 47B3 441C 7171 834B ...4.,.*G.D.qq.K
03-2030: 2025 B800 7171 834B 2026 321D 0001 B21D  %..qq.K &2.....
03-2038: 834B 2025 8000 F020 2001 F403 47B8 6FBC .K %....  ...G.o.
03-2040: 0360 F187 607C 2038 321D 07BB 0A1D 47A8 .`..`| 82.....G.
03-2048: F082 7170 3360 7171 834B 2023 B800 7171 ..qp3`qq.K #..qq
03-2050: 2021 B800 F081 44BD 6C09 6D03 C103 E8C6  !....D.l.m.....
03-2058: 4504 6D01 C103 E8C6 F081 C103 6CFA 6FF9 E.m.........l.o.
03-2060: 2077 5255 4E20 A805 6C0F 0000 4406 F081  wRUN ..l...D...
03-2068: 0796 086C 4785 F082 0824 4772 7171 834B ...lG....$Grqq.K
03-2070: 2023 B800 F082 C0CE C103 6CE3 F081 208A  #........l... .
03-2078: 434F 4E54 A805 6C08 0000 47EF F081 077E CONT..l...G....~
03-2080: 086C 476E F082 C0CE C103 6C02 F081 0887 .lGn......l.....
03-2088: C0D3 F081 2097 5343 5241 5443 4820 4120 .... .SCRATCH A
03-2090: A808 E8CE 0000 C168 0000 0087 6C3E 20AA ........h....l> .
03-2098: 5343 5241 5443 4820 4B45 5920 A809 6C07 SCRATCH KEY ..l.
03-20A0: 0000 444D 0761 0834 474B F082 C0CE 449C ..DM.a.4GK....D.
03-20A8: F081 F081 20B5 5343 5241 5443 4820 5020 .... .SCRATCH P
03-20B0: A808 E8CE 0000 0022 6C20 20C0 5343 5241 ......."l  .SCRA

Press STOP to quit, B to step back or any other key to proceed_
```

+

=

What is file carving?

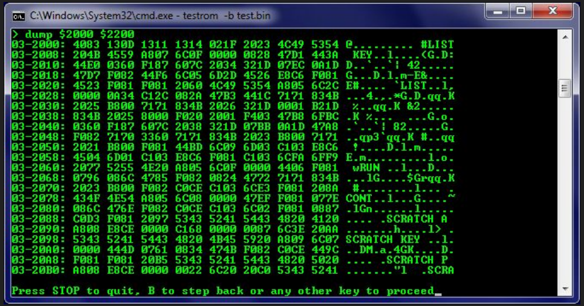


```
> dump $2000 $2200
03-2000: 4083 130D 1311 1314 021F 2023 4C49 5354 @.......... #LIST
03-2008: 204B 4559 A807 6C0F 0000 0828 47D1 443A  KEY..l....(G.D:
03-2010: 44E0 0360 F187 607C 2034 321D 07EC 0A1D D..`..`¦ 42.....
03-2018: 47D7 F082 44F6 6C05 6D2D 4526 E8C6 F081 G...D.l.m-E&....
03-2020: 4523 F081 F081 2060 4C49 5354 A805 6C2C E#.... `LIST..l,
03-2028: 0000 0A34 C12C 082A 47B3 441C 7171 834B ...4.,.*G.D.qq.K
03-2030: 2025 B800 7171 834B 2026 321D 0001 B21D  %..qq.K &2.....
03-2038: 834B 2025 8000 F020 2001 F403 47B8 6FBC .K %...  ...G.o.
03-2040: 0360 F187 607C 2038 321D 07BB 0A1D 47A8 .`..`¦ 82.....G.
03-2048: F082 7170 3360 7171 834B 2023 B800 7171 ..qp3`qq.K #..qq
03-2050: 2021 B800 F081 44BD 6C09 6D03 C103 E8C6  !....D.l.m.....
03-2058: 4504 6D01 C103 E8C6 F081 C103 6CFA 6FF9 E.m.........l.o.
03-2060: 2077 5255 4E20 A805 6C0F 0000 4406 F081  wRUN ..l...D...
03-2068: 0796 086C 4785 F082 0824 4772 7171 834B ...lG....$Grqq.K
03-2070: 2023 B800 F082 C0CE C103 6CE3 F081 208A  #.........l... .
03-2078: 434F 4E54 A805 6C08 0000 47EF F081 077E CONT..l...G....~
03-2080: 086C 476E F082 C0CE C103 6C02 F081 0887 .lGn......l.....
03-2088: C0D3 F081 2097 5343 5241 5443 4820 4120 .... .SCRATCH A
03-2090: A808 E8CE 0000 C168 0000 0087 6C3E 20AA .......h....l> .
03-2098: 5343 5241 5443 4820 4B45 5920 A809 6C07 SCRATCH KEY ..l.
03-20A0: 0000 444D 0761 0834 474B F082 C0CE 449C ..DM.a.4GK....D.
03-20A8: F081 F081 20B5 5343 5241 5443 4820 5020 .... .SCRATCH P
03-20B0: A808 E8CE 0000 0022 6C20 20C0 5343 5241 ......."l  .SCRA

Press STOP to quit, B to step back or any other key to proceed_
```

+

=

What is file carving?

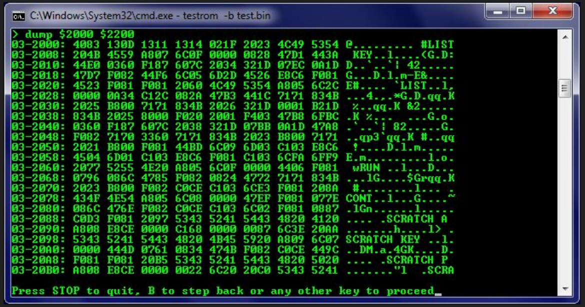


```
> dump $2000 $2200
03-2000: 4083 130D 1311 1314 021F 2023 4C49 5354 @......... #LIST
03-2008: 204B 4559 A807 6C0F 0000 0828 47D1 443A  KEY..l....(G.D:
03-2010: 44E0 0360 F187 607C 2034 321D 07EC 0A1D D..`..`| 42.....
03-2018: 47D7 F082 44F6 6C05 6D2D 4526 E8C6 F081 G...D.l.m-E&....
03-2020: 4523 F081 F081 2060 4C49 5354 A805 6C2C E#.... `LIST..l,
03-2028: 0000 0A34 C12C 082A 47B3 441C 7171 834B ...4.,.*G.D.qq.K
03-2030: 2025 B800 7171 834B 2026 321D 0001 B21D  %..qq.K &2.....
03-2038: 834B 2025 8000 F020 2001 F403 47B8 6FBC .K %....  ...G.o.
03-2040: 0360 F187 607C 2038 321D 07BB 0A1D 47A8 .`..`| 82.....G.
03-2048: F082 7170 3360 7171 834B 2023 B800 7171 ..qp3`qq.K #..qq
03-2050: 2021 B800 F081 44BD 6C09 6D03 C103 E8C6  !....D.l.m.....
03-2058: 4504 6D01 C103 E8C6 F081 C103 6CFA 6FF9 E.m.........l.o.
03-2060: 2077 5255 4E20 A805 6C0F 0000 4406 F081  wRUN ..l...D...
03-2068: 0796 086C 4785 F082 0824 4772 7171 834B ...lG....$Grqq.K
03-2070: 2023 B800 F082 C0CE C103 6CE3 F081 208A  #.........l... .
03-2078: 434F 4E54 A805 6C08 0000 47EF F081 077E CONT..l...G....~
03-2080: 086C 476E F082 C0CE C103 6C02 F081 0887 .lGn......l.....
03-2088: C0D3 F081 2097 5343 5241 5443 4820 4120 .... .SCRATCH A
03-2090: A808 E8CE 0000 C168 0000 0087 6C3E 20AA ........h....l> .
03-2098: 5343 5241 5443 4820 4B45 5920 A809 6C07 SCRATCH KEY ..l.
03-20A0: 0000 444D 0761 0834 474B F082 C0CE 449C ..DM.a.4GK....D.
03-20A8: F081 F081 20B5 5343 5241 5443 4820 5020 .... .SCRATCH P
03-20B0: A808 E8CE 0000 0022 6C20 20C0 5343 5241 ......."l  .SCRA

Press STOP to quit, B to step back or any other key to proceed_
```

+

=

What is file carving?



```
> dump $2000 $2200
03-2000: 4083 130D 1311 1314 021F 2023 4C49 5354 @......... #LIST
03-2008: 204B 4559 A807 6C0F 0000 0828 47D1 443A  KEY..l....(G.D:
03-2010: 44E0 0360 F187 607C 2034 321D 07EC 0A1D D..`..`| 42.....
03-2018: 47D7 F082 44F6 6C05 6D2D 4526 E8C6 F081 G...D.l.m-E&....
03-2020: 4523 F081 F081 2060 4C49 5354 A805 6C2C E#.... `LIST..l,
03-2028: 0000 0A34 C12C 082A 47B3 441C 7171 834B ...4.,.*G.D.qq.K
03-2030: 2025 B800 7171 834B 2026 321D 0001 B21D  %..qq.K &2.....
03-2038: 834B 2025 8000 F020 2001 F403 47B8 6FBC .K %...  ...G.o.
03-2040: 0360 F187 607C 2038 321D 07BB 0A1D 47A8 .`..`| 82.....G.
03-2048: F082 7170 3360 7171 834B 2023 B800 7171 ..qp3`qq.K #..qq
03-2050: 2021 B800 F081 44BD 6C09 6D03 C103 E8C6  !....D.l.m.....
03-2058: 4504 6D01 C103 E8C6 F081 C103 6CFA 6FF9 E.m.........l.o.
03-2060: 2077 5255 4E20 A805 6C0F 0000 4406 F081  wRUN ..l...D...
03-2068: 0796 086C 4785 F082 0824 4772 7171 834B ...lG....$Grqq.K
03-2070: 2023 B800 F082 C0CE C103 6CE3 F081 208A  #........l... .
03-2078: 434F 4E54 A805 6C08 0000 47EF F081 077E CONT..l...G....~
03-2080: 086C 476E F082 C0CE C103 6C02 F081 0887 .lGn......l.....
03-2088: C0D3 F081 2097 5343 5241 5443 4820 4120 .... .SCRATCH A
03-2090: A808 E8CE 0000 C168 0000 0087 6C3E 20AA .......h....l> .
03-2098: 5343 5241 5443 4820 4B45 5920 A809 6C07 SCRATCH KEY ..l.
03-20A0: 0000 444D 0761 0834 474B F082 C0CE 449C ..DM.a.4GK....D.
03-20A8: F081 F081 20B5 5343 5241 5443 4820 5020 .... .SCRATCH P
03-20B0: A808 E8CE 0000 0022 6C20 20C0 5343 5241 ......."l  .SCRA

Press STOP to quit, B to step back or any other key to proceed_
```

+

=

meoware?

=>

this is hard =>

this is hard => abstract

Carving PE File Malware From PCAPs

Mike Moss

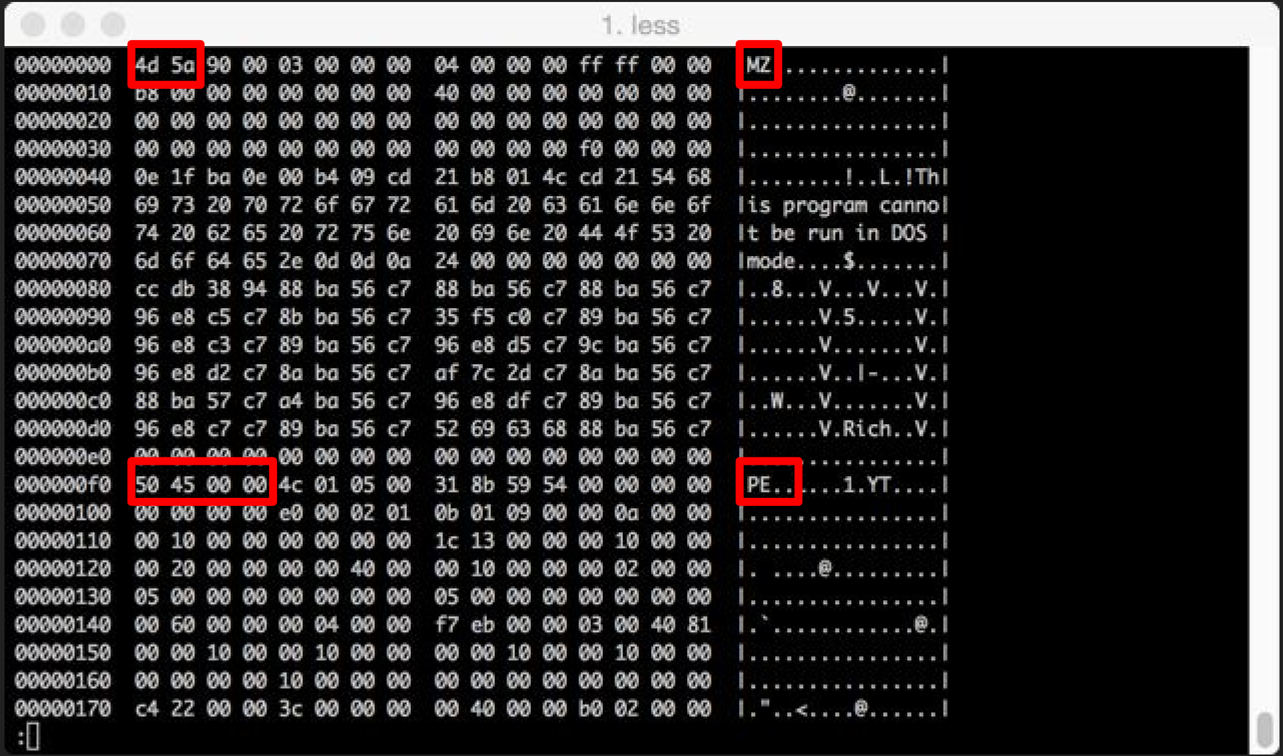
=>

find PE files =>

find PE files => determine if malware

find PE files ==

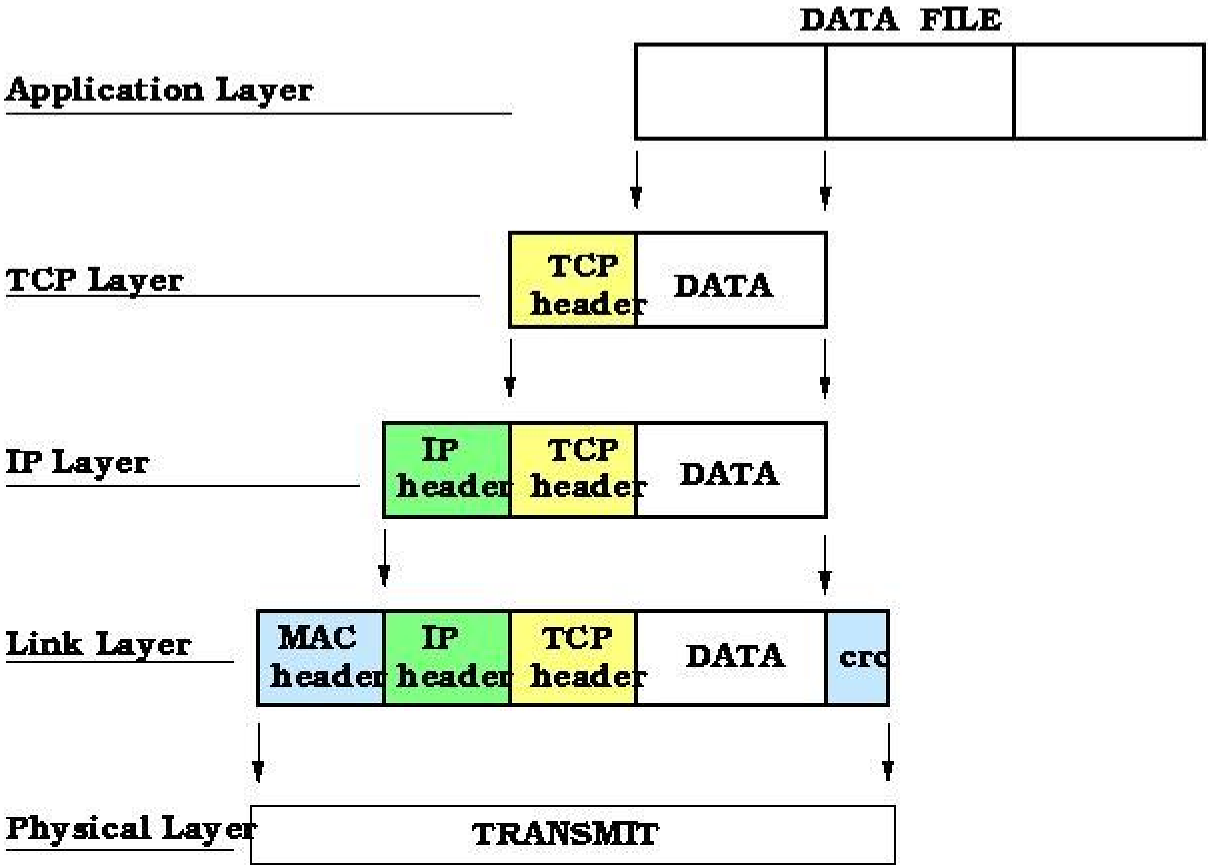
find PE files == hard



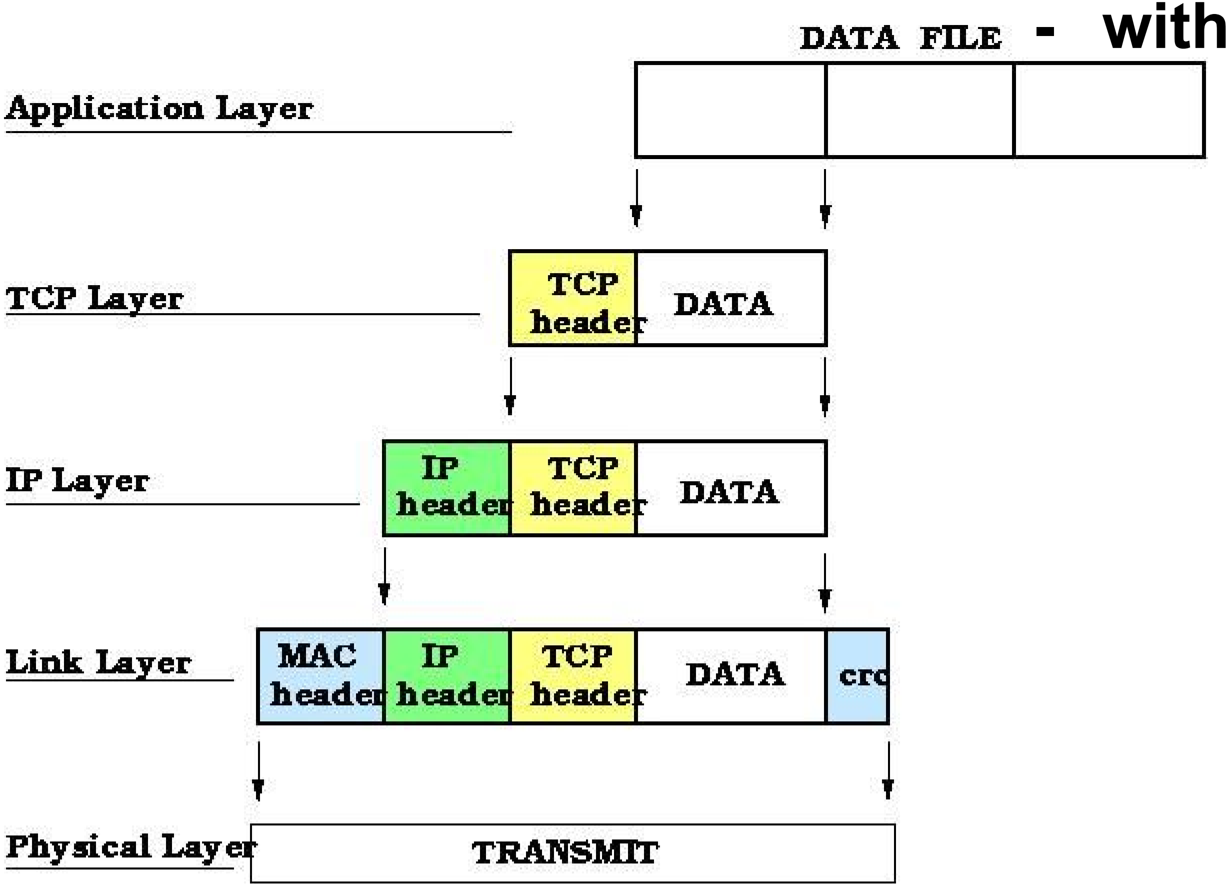
```
00000000  4d 5a 90 00 03 00 00 00  04 00 00 00 ff ff 00 00  |MZ..............|
00000010  b8 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00  |........@.......|
00000020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000030  00 00 00 00 00 00 00 00  00 00 00 00 f0 00 00 00  |................|
00000040  0e 1f ba 0e 00 b4 09 cd  21 b8 01 4c cd 21 54 68  |........!..L.!Th|
00000050  69 73 20 70 72 6f 67 72  61 6d 20 63 61 6e 6e 6f  |is program canno|
00000060  74 20 62 65 20 72 75 6e  20 69 6e 20 44 4f 53 20  |t be run in DOS |
00000070  6d 6f 64 65 2e 0d 0d 0a  24 00 00 00 00 00 00 00  |mode....$.......|
00000080  cc db 38 94 88 ba 56 c7  88 ba 56 c7 88 ba 56 c7  |..8...V...V...V.|
00000090  96 e8 c5 c7 8b ba 56 c7  35 f5 c0 c7 89 ba 56 c7  |......V.5.....V.|
000000a0  96 e8 c3 c7 89 ba 56 c7  96 e8 d5 c7 9c ba 56 c7  |......V.......V.|
000000b0  96 e8 d2 c7 8a ba 56 c7  af 7c 2d c7 8a ba 56 c7  |......V..|-...V.|
000000c0  88 ba 57 c7 a4 ba 56 c7  96 e8 df c7 89 ba 56 c7  |..W...V.......V.|
000000d0  96 e8 c7 c7 89 ba 56 c7  52 69 63 68 88 ba 56 c7  |......V.Rich..V.|
000000e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
000000f0  50 45 00 00 4c 01 05 00  31 8b 59 54 00 00 00 00  |PE......1.YT....|
00000100  00 00 00 00 e0 00 02 01  0b 01 09 00 00 0a 00 00  |................|
00000110  00 10 00 00 00 00 00 00  1c 13 00 00 00 10 00 00  |................|
00000120  00 20 00 00 00 00 40 00  00 10 00 00 00 02 00 00  |. ....@.........|
00000130  05 00 00 00 00 00 00 00  05 00 00 00 00 00 00 00  |................|
00000140  00 60 00 00 00 04 00 00  f7 eb 00 00 03 00 40 81  |.`............@.|
00000150  00 00 10 00 00 10 00 00  00 00 10 00 00 10 00 00  |................|
00000160  00 00 00 00 10 00 00 00  00 00 00 00 00 00 00 00  |................|
00000170  c4 22 00 00 3c 00 00 00  00 40 00 00 b0 02 00 00  |."..<....@......|
:
```

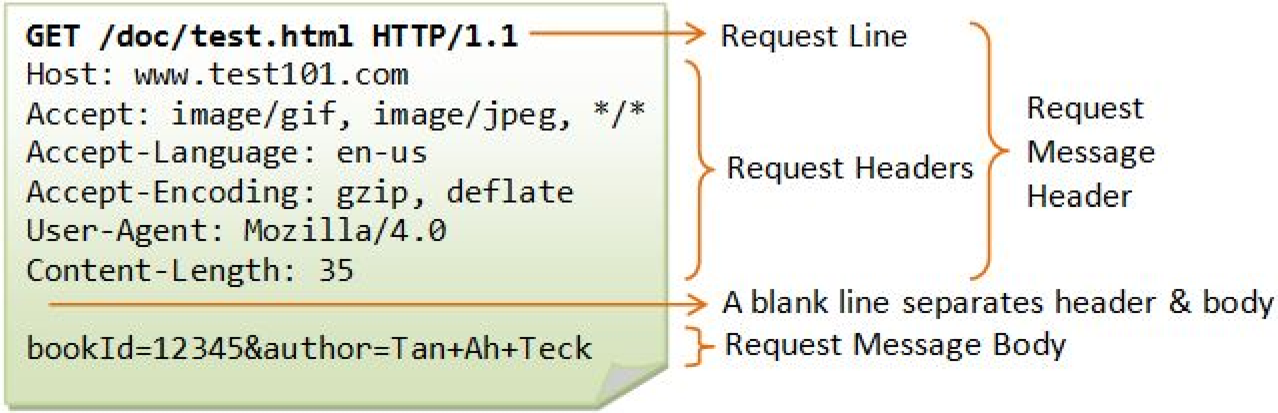
but why is this hard?

application layer


DATA FILE
Application Layer
TCP Layer
TCP header
DATA
IP Layer
IP header
TCP header
DATA
Link Layer
MAC header
IP header
TCP header
DATA
crc
Physical Layer
TRANSMIT

- with extra crap





```
GET /doc/test.html HTTP/1.1
Host: www.test101.com
Accept: image/gif, image/jpeg, */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0
Content-Length: 35

bookId=12345&author=Tan+Ah+Teck
```

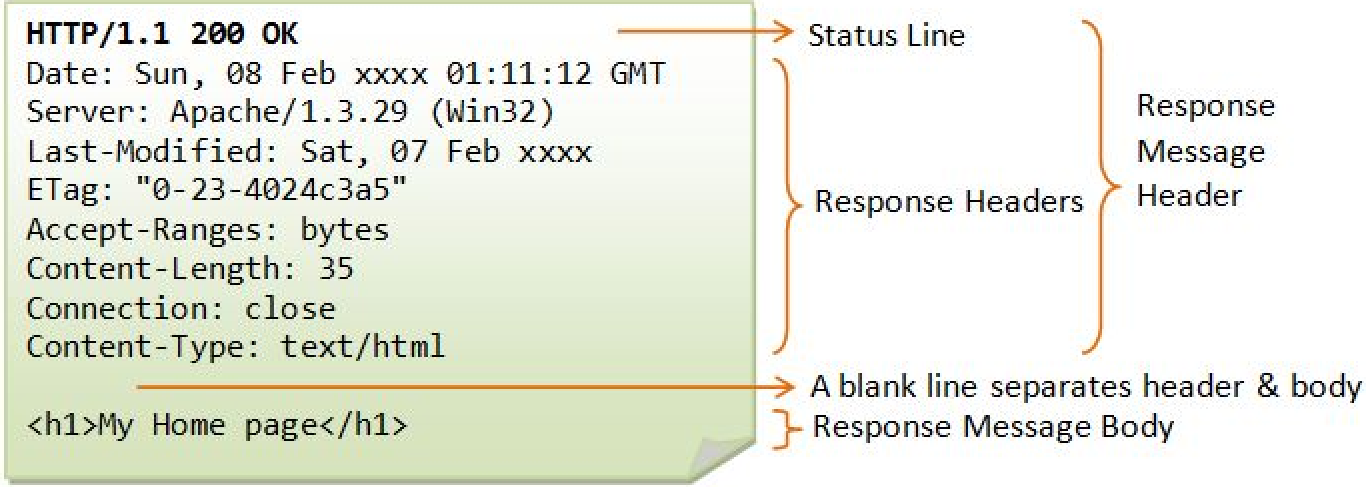
Request Line

Request Headers

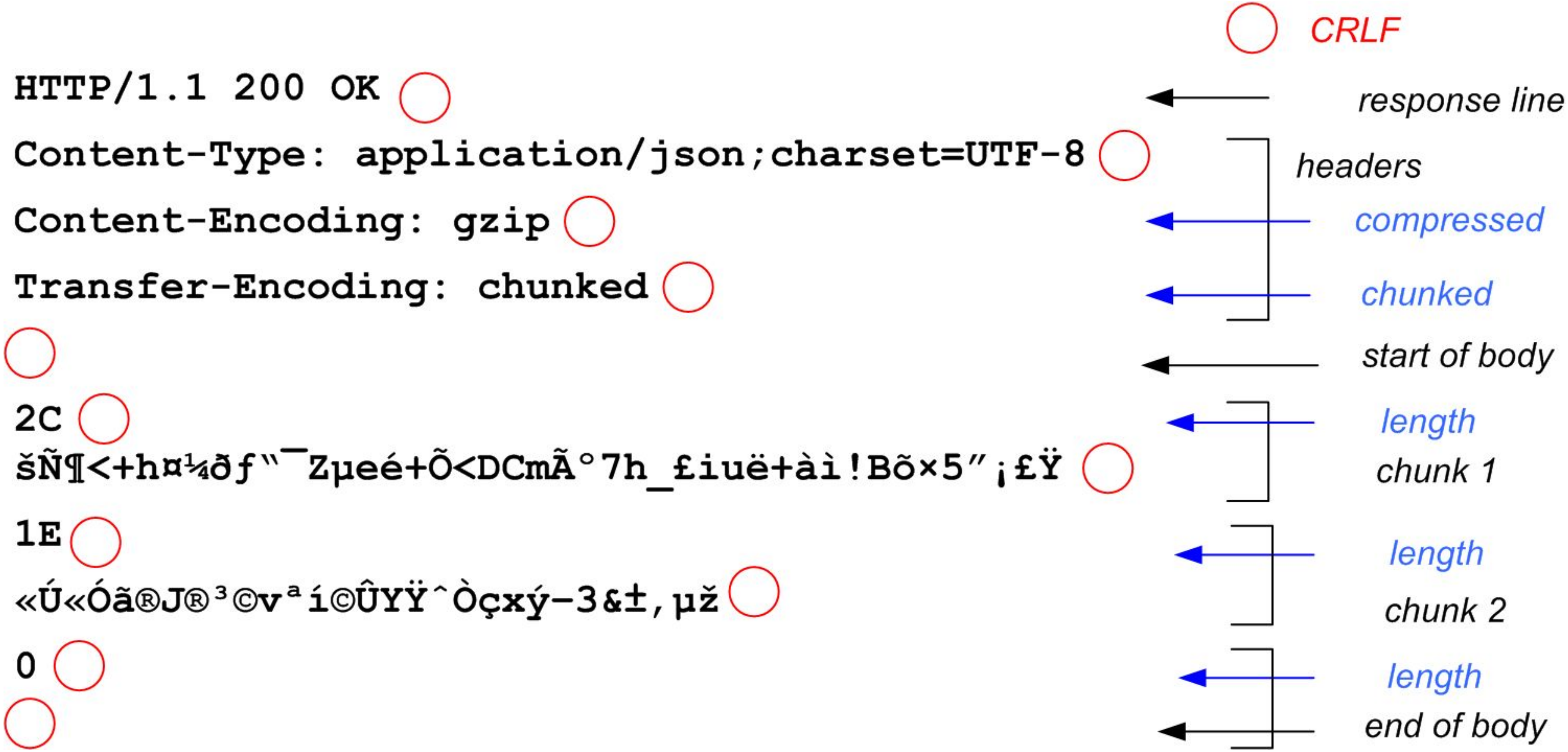
Request Message Header

A blank line separates header & body

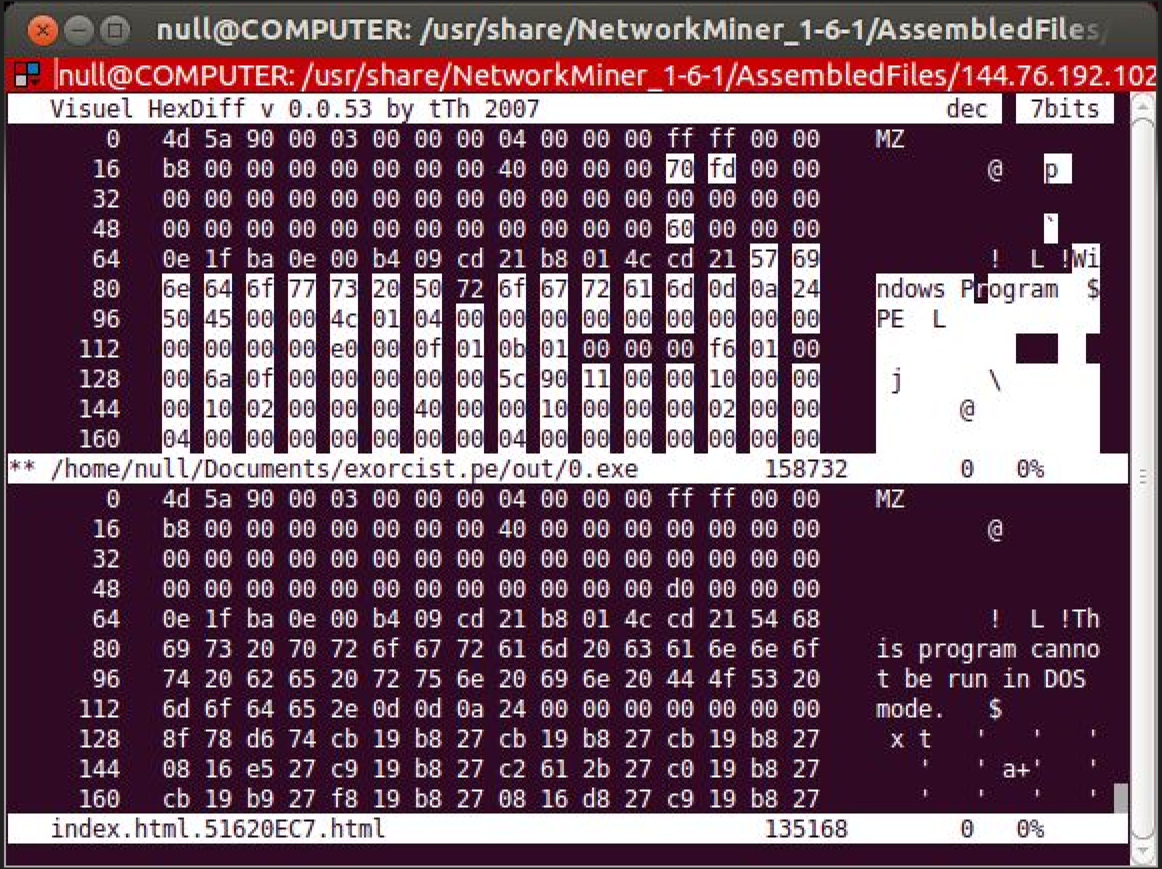
Request Message Body



```
HTTP/1.1 200 OK
Date: Sun, 08 Feb xxxx 01:11:12 GMT
Server: Apache/1.3.29 (Win32)
Last-Modified: Sat, 07 Feb xxxx
ETag: "0-23-4024c3a5"
Accept-Ranges: bytes
Content-Length: 35
Connection: close
Content-Type: text/html

<h1>My Home page</h1>
```

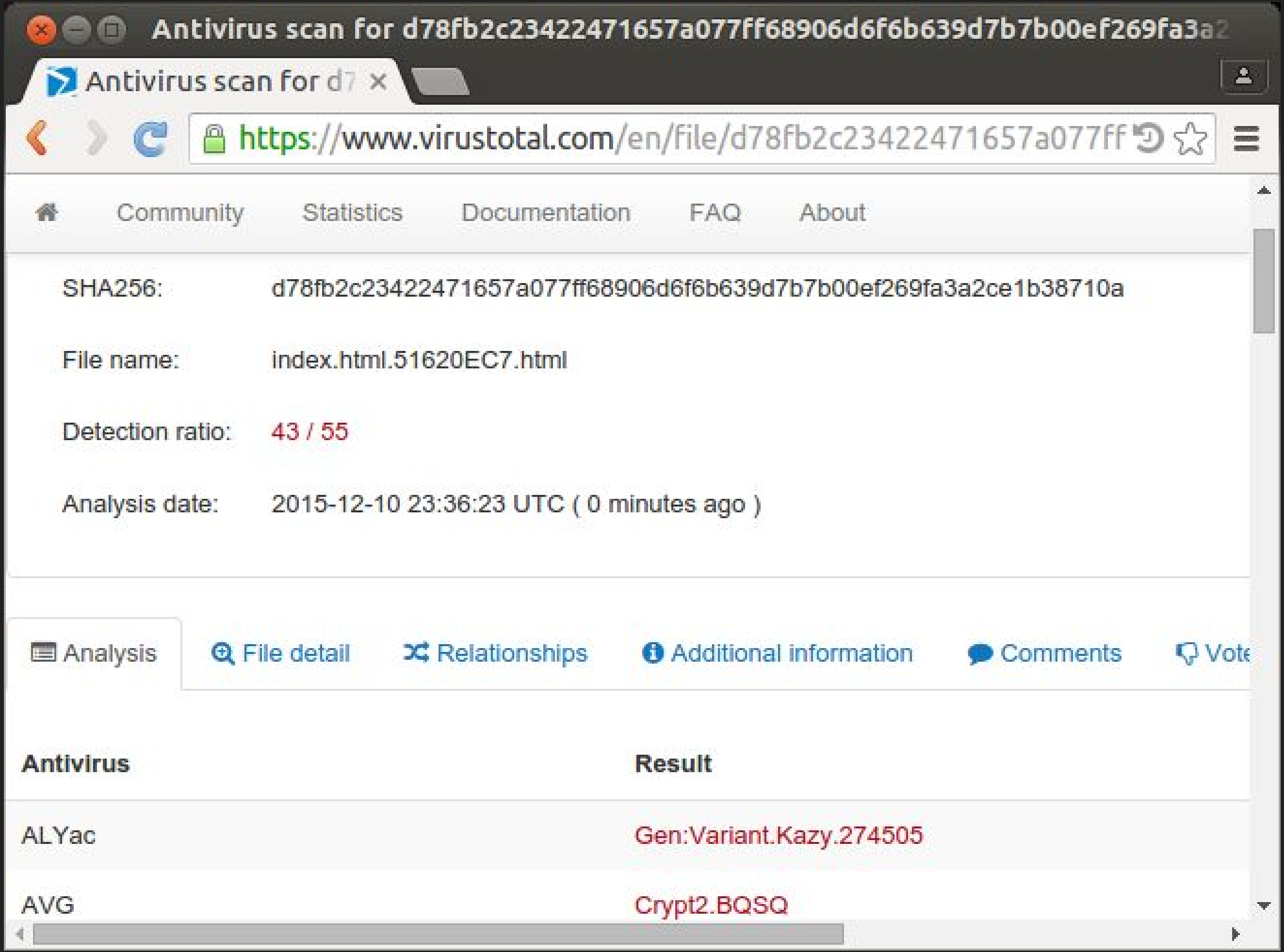


```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Content-Encoding: gzip
Transfer-Encoding: chunked

2C
šÑ¶<+h¤¼ðƒ“¯Zµeé+Õ<DCmÃ°7h_£iuë+àì!Bõ×5”¡£Ÿ
1E
«Ú«Óã®J®³©vªí©ÛYŸˆÒçxý–3&±,µž
0

```



```
null@COMPUTER: /usr/share/NetworkMiner_1-6-1/AssembledFiles
null@COMPUTER: /usr/share/NetworkMiner_1-6-1/AssembledFiles/144.76.192.102
  Visuel HexDiff v 0.0.53 by tTh 2007                                dec   7bits
       0    4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00    MZ
      16    b8 00 00 00 00 00 00 00 40 00 00 00 70 fd 00 00            @   p
      32    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      48    00 00 00 00 00 00 00 00 00 00 00 00 60 00 00 00                `
      64    0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 57 69            !  L !Wi
      80    6e 64 6f 77 73 20 50 72 6f 67 72 61 6d 0d 0a 24    ndows Program  $
      96    50 45 00 00 4c 01 04 00 00 00 00 00 00 00 00 00    PE  L
     112    00 00 00 00 e0 00 0f 01 0b 01 00 00 00 f6 01 00
     128    00 6a 0f 00 00 00 00 00 5c 90 11 00 00 10 00 00     j      \
     144    00 10 02 00 00 00 40 00 00 10 00 00 00 02 00 00          @
     160    04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00
** /home/null/Documents/exorcist.pe/out/0.exe          158732        0   0%
       0    4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00    MZ
      16    b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00            @
      32    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      48    00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 00
      64    0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68            !  L !Th
      80    69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f    is program canno
      96    74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20    t be run in DOS
     112    6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00    mode.   $
     128    8f 78 d6 74 cb 19 b8 27 cb 19 b8 27 cb 19 b8 27     x t    '   '   '
     144    08 16 e5 27 c9 19 b8 27 c2 61 2b 27 c0 19 b8 27       '   ' a+'   '
     160    cb 19 b9 27 f8 19 b8 27 08 16 d8 27 c9 19 b8 27       '   '   '   '
  index.html.51620EC7.html                             135168        0   0%
```

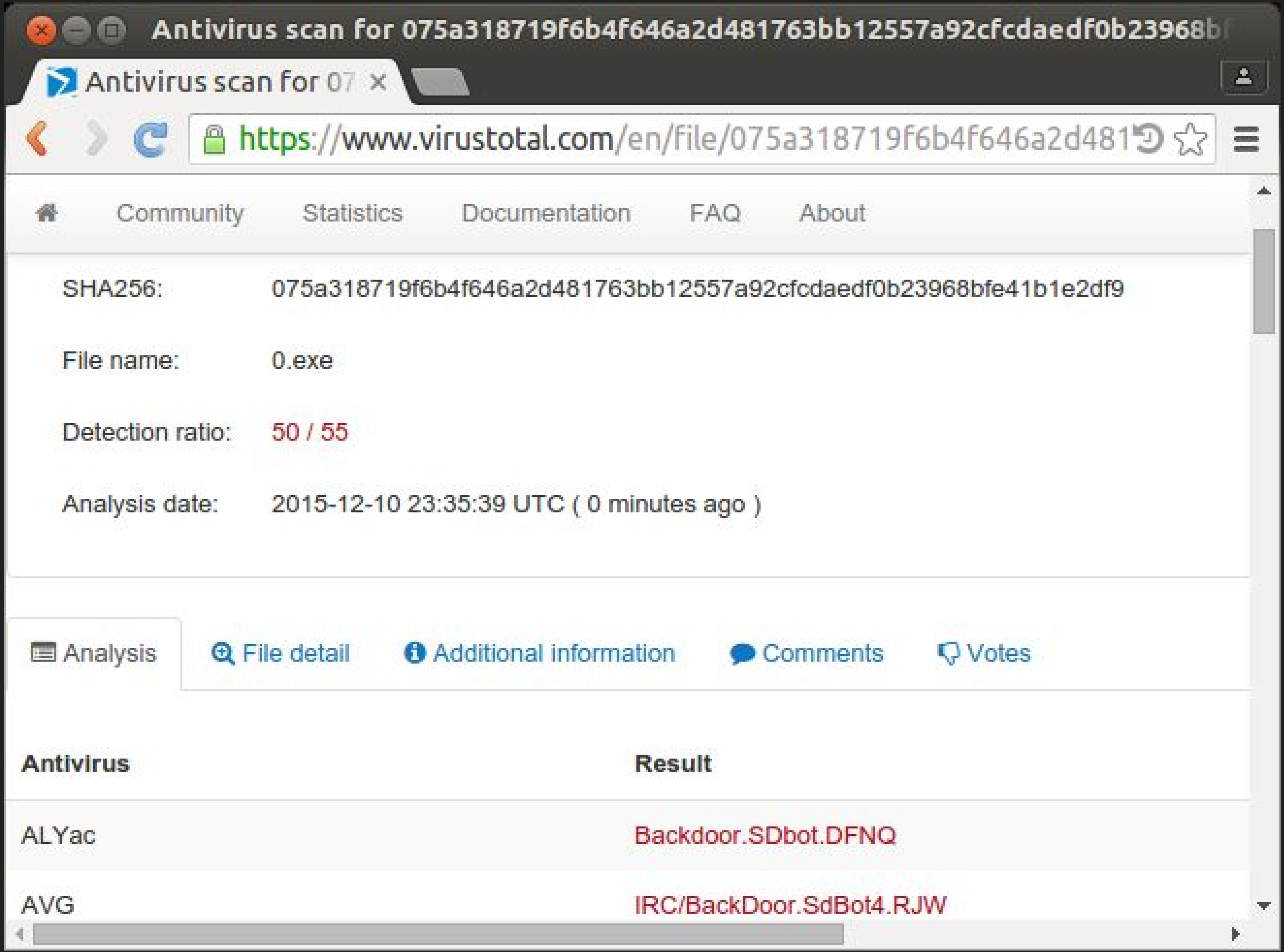
how much does this affect malware detection?



https://www.virustotal.com/en/file/d78fb2c23422471657a077ff

SHA256:	d78fb2c23422471657a077ff68906d6f6b639d7b7b00ef269fa3a2ce1b38710a
File name:	index.html.51620EC7.html
Detection ratio:	43 / 55
Analysis date:	2015-12-10 23:36:23 UTC (0 minutes ago)

Antivirus	Result
ALYac	Gen:Variant.Kazy.274505
AVG	Crypt2.BQSQ



Antivirus scan for 075a318719f6b4f646a2d481763bb12557a92cfcdaedf0b23968b
Antivirus scan for 07
https://www.virustotal.com/en/file/075a318719f6b4f646a2d481
Community
Statistics
Documentation
FAQ
About
Analysis
File detail
Additional information
Comments
Votes

SHA256: 075a318719f6b4f646a2d481763bb12557a92cfcdaedf0b23968bfe41b1e2df9

File name: 0.exe

Detection ratio: 50 / 55

Analysis date: 2015-12-10 23:35:39 UTC (0 minutes ago)

Antivirus	Result
ALYac	Backdoor.SDbot.DFNQ
AVG	IRC/BackDoor.SdBot4.RJW

Making Malware Look More Like Malware

Mike Moss

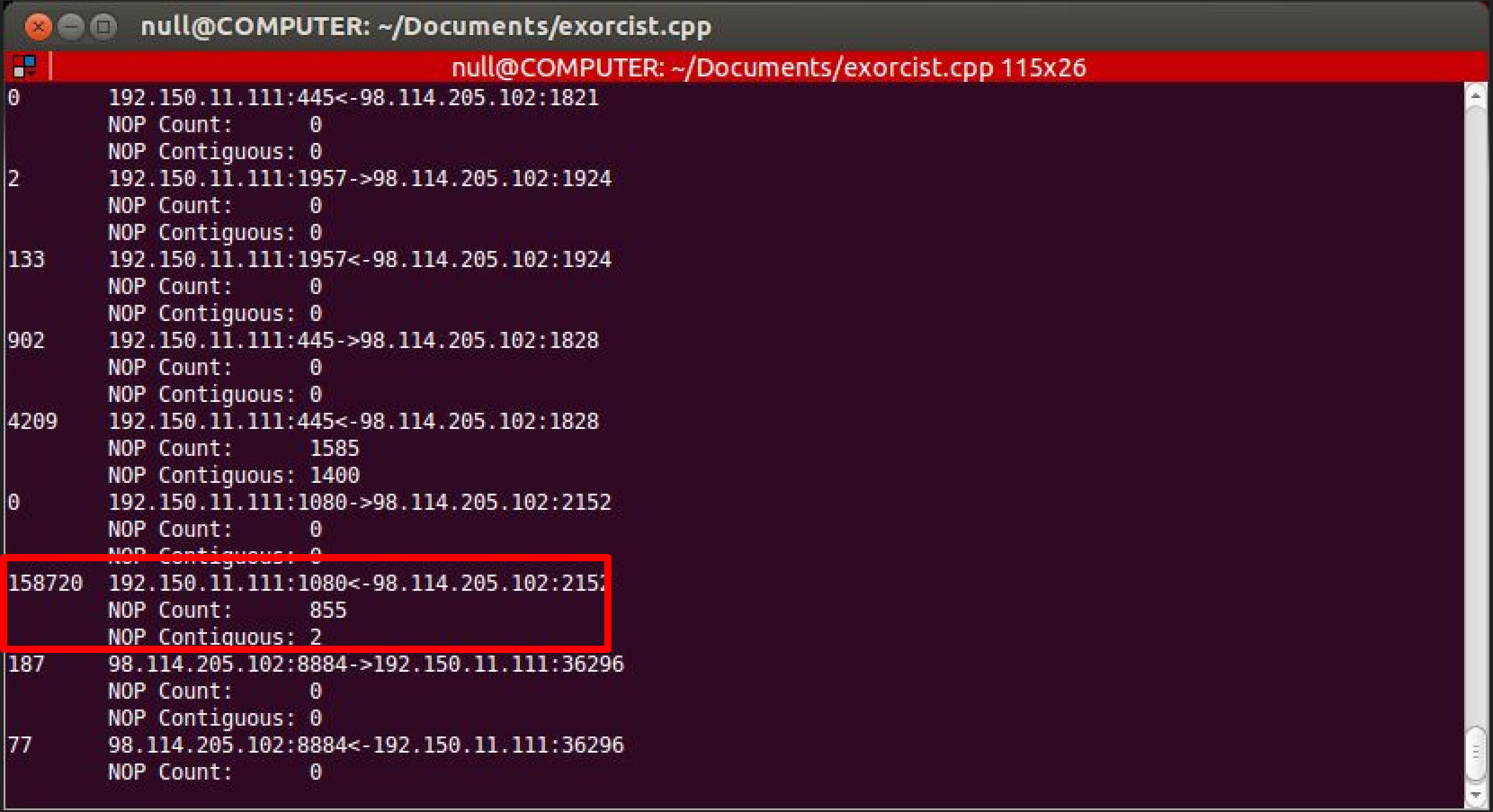
MMLMLM

Mike Moss

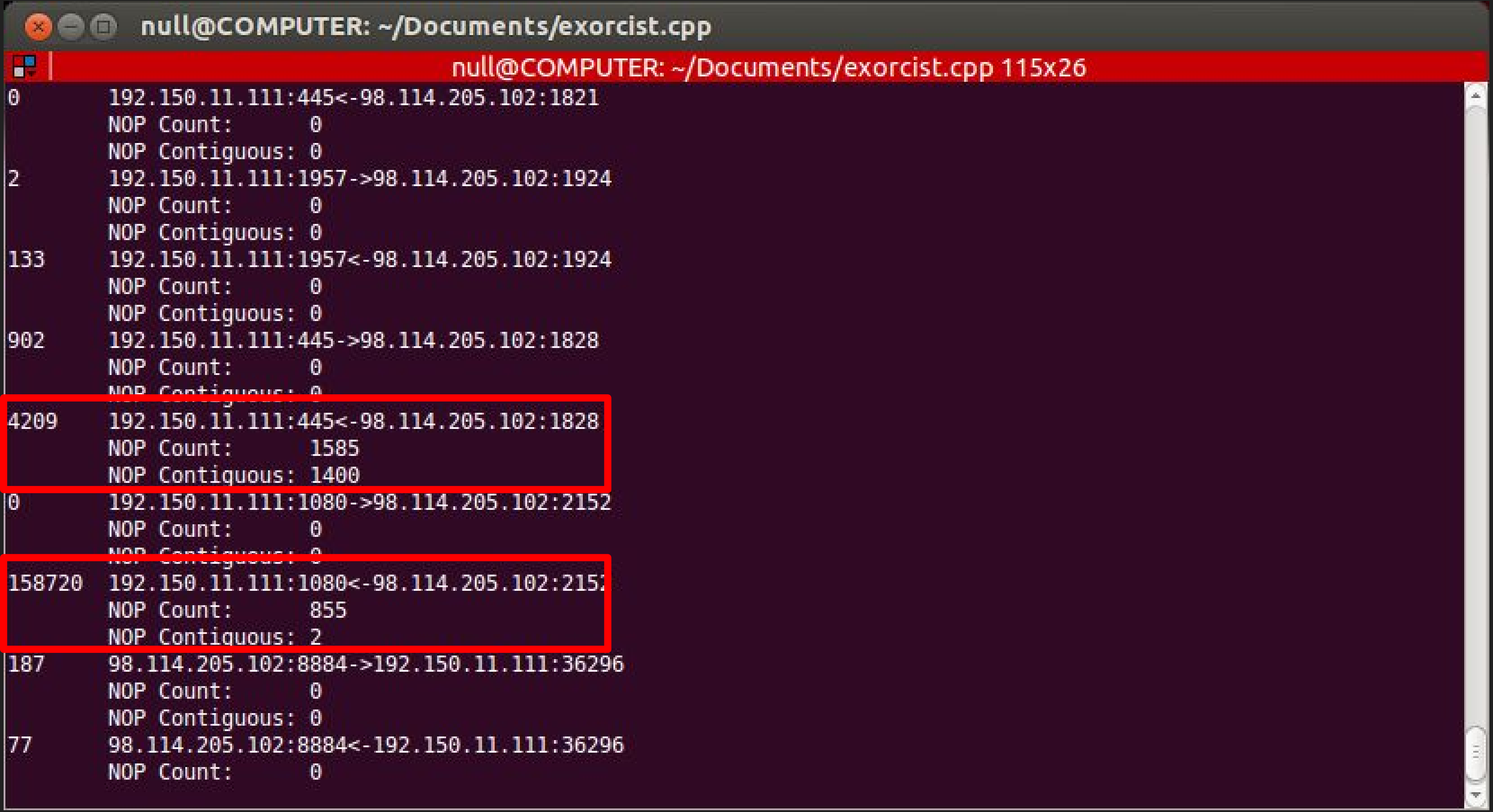
determine if malware

determine if malware == hard

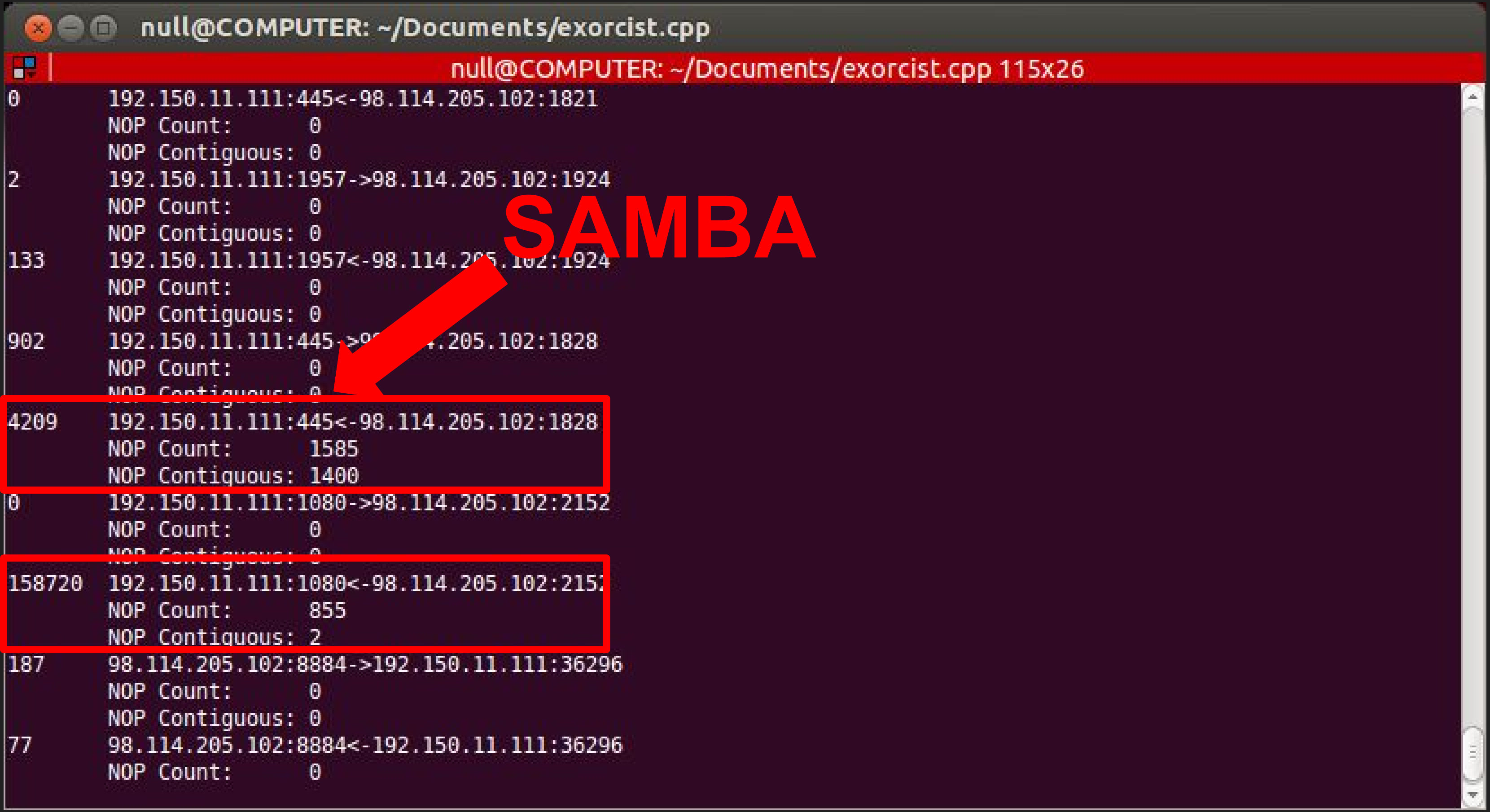
count contiguous NOPs
(look for NOP sleds)


null@COMPUTER: ~/Documents/exorcist.cpp
null@COMPUTER: ~/Documents/exorcist.cpp 115x26

```
0       192.150.11.111:445<-98.114.205.102:1821
        NOP Count:      0
        NOP Contiguous: 0
2       192.150.11.111:1957->98.114.205.102:1924
        NOP Count:      0
        NOP Contiguous: 0
133     192.150.11.111:1957<-98.114.205.102:1924
        NOP Count:      0
        NOP Contiguous: 0
902     192.150.11.111:445->98.114.205.102:1828
        NOP Count:      0
        NOP Contiguous: 0
4209    192.150.11.111:445<-98.114.205.102:1828
        NOP Count:      1585
        NOP Contiguous: 1400
0       192.150.11.111:1080->98.114.205.102:2152
        NOP Count:      0
        NOP Contiguous: 0
158720  192.150.11.111:1080<-98.114.205.102:2152
        NOP Count:      855
        NOP Contiguous: 2
187     98.114.205.102:8884->192.150.11.111:36296
        NOP Count:      0
        NOP Contiguous: 0
77      98.114.205.102:8884<-192.150.11.111:36296
        NOP Count:      0
```


null@COMPUTER: ~/Documents/exorcist.cpp
null@COMPUTER: ~/Documents/exorcist.cpp 115x26

```
0       192.150.11.111:445<-98.114.205.102:1821
        NOP Count:      0
        NOP Contiguous: 0
2       192.150.11.111:1957->98.114.205.102:1924
        NOP Count:      0
        NOP Contiguous: 0
133     192.150.11.111:1957<-98.114.205.102:1924
        NOP Count:      0
        NOP Contiguous: 0
902     192.150.11.111:445->98.114.205.102:1828
        NOP Count:      0
        NOP Contiguous: 0
4209    192.150.11.111:445<-98.114.205.102:1828
        NOP Count:      1585
        NOP Contiguous: 1400
0       192.150.11.111:1080->98.114.205.102:2152
        NOP Count:      0
        NOP Contiguous: 0
158720  192.150.11.111:1080<-98.114.205.102:2152
        NOP Count:      855
        NOP Contiguous: 2
187     98.114.205.102:8884->192.150.11.111:36296
        NOP Count:      0
        NOP Contiguous: 0
77      98.114.205.102:8884<-192.150.11.111:36296
        NOP Count:      0
```

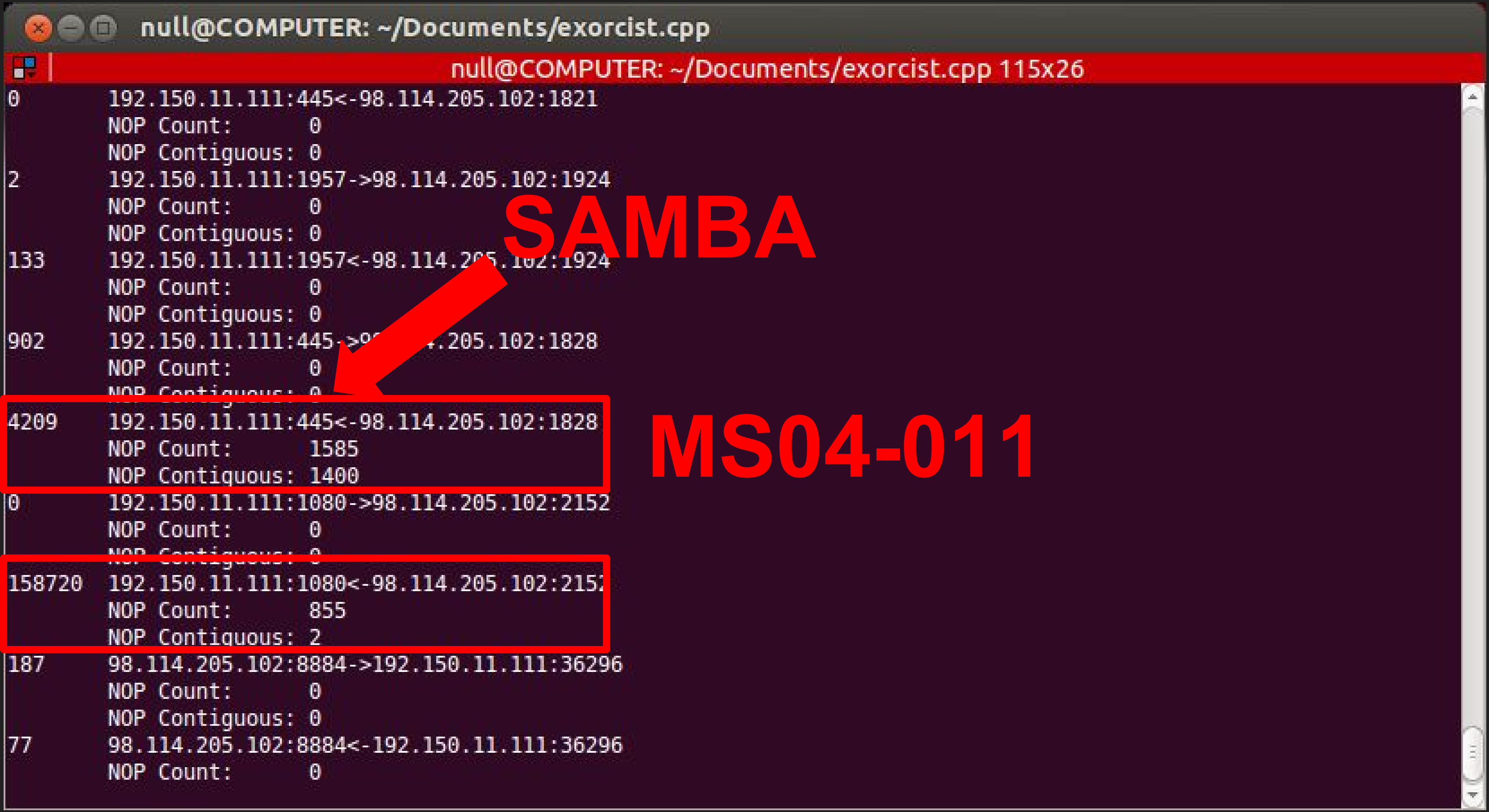


null@COMPUTER: ~/Documents/exorcist.cpp

null@COMPUTER: ~/Documents/exorcist.cpp 115x26

```
0       192.150.11.111:445<-98.114.205.102:1821
        NOP Count:      0
        NOP Contiguous: 0
2       192.150.11.111:1957->98.114.205.102:1924
        NOP Count:      0
        NOP Contiguous: 0
133     192.150.11.111:1957<-98.114.205.102:1924
        NOP Count:      0
        NOP Contiguous: 0
902     192.150.11.111:445->98.114.205.102:1828
        NOP Count:      0
        NOP Contiguous: 0
4209    192.150.11.111:445<-98.114.205.102:1828
        NOP Count:      1585
        NOP Contiguous: 1400
0       192.150.11.111:1080->98.114.205.102:2152
        NOP Count:      0
        NOP Contiguous: 0
158720  192.150.11.111:1080<-98.114.205.102:2152
        NOP Count:      855
        NOP Contiguous: 2
187     98.114.205.102:8884->192.150.11.111:36296
        NOP Count:      0
        NOP Contiguous: 0
77      98.114.205.102:8884<-192.150.11.111:36296
        NOP Count:      0
```

SAMBA


null@COMPUTER: ~/Documents/exorcist.cpp
null@COMPUTER: ~/Documents/exorcist.cpp 115x26

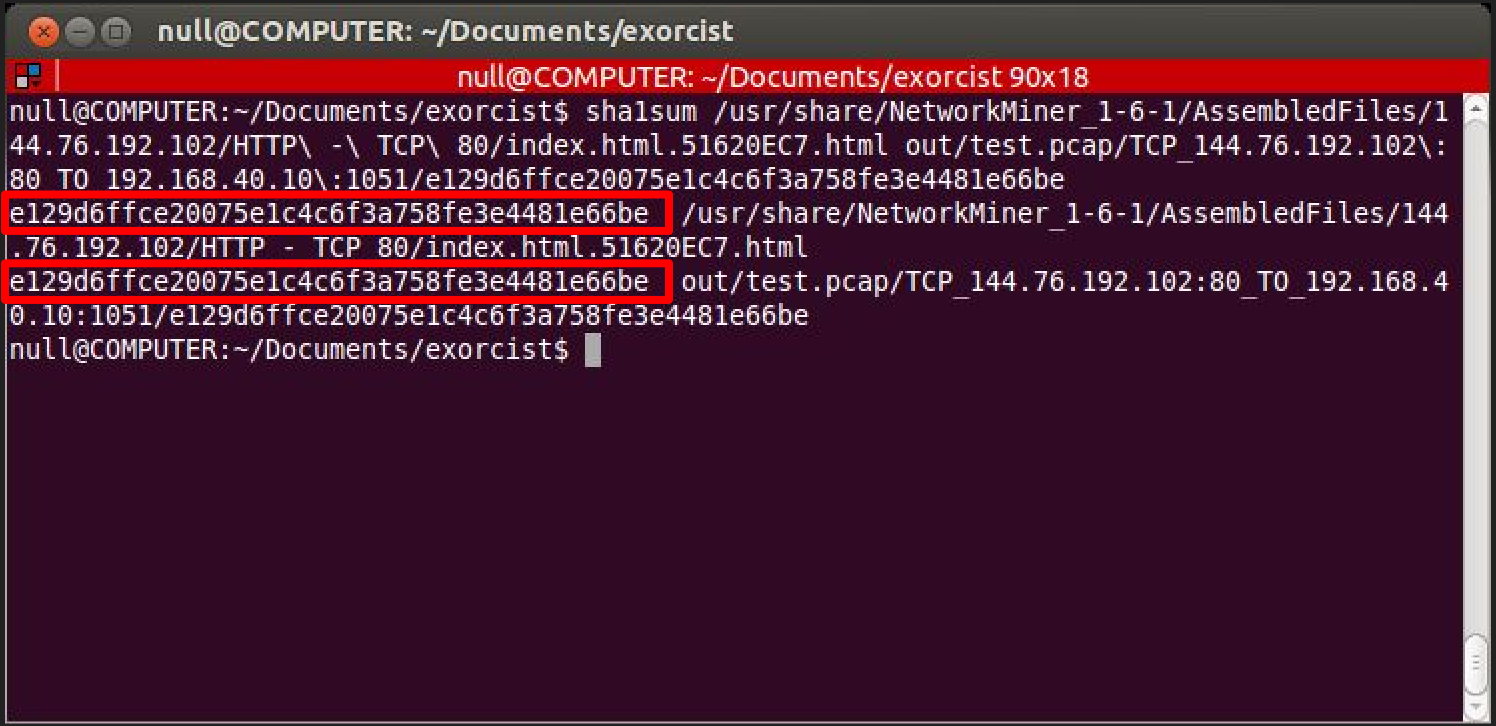
```
0       192.150.11.111:445<-98.114.205.102:1821
        NOP Count:      0
        NOP Contiguous: 0
2       192.150.11.111:1957->98.114.205.102:1924
        NOP Count:      0
        NOP Contiguous: 0
133     192.150.11.111:1957<-98.114.205.102:1924
        NOP Count:      0
        NOP Contiguous: 0
902     192.150.11.111:445->98.114.205.102:1828
        NOP Count:      0
        NOP Contiguous: 0
4209    192.150.11.111:445<-98.114.205.102:1828
        NOP Count:      1585
        NOP Contiguous: 1400
0       192.150.11.111:1080->98.114.205.102:2152
        NOP Count:      0
        NOP Contiguous: 0
158720  192.150.11.111:1080<-98.114.205.102:2152
        NOP Count:      855
        NOP Contiguous: 2
187     98.114.205.102:8884->192.150.11.111:36296
        NOP Count:      0
        NOP Contiguous: 0
77      98.114.205.102:8884<-192.150.11.111:36296
        NOP Count:      0
```

SAMBA

MS04-011

Carving HTTP Files From PCAPs

Mike Moss

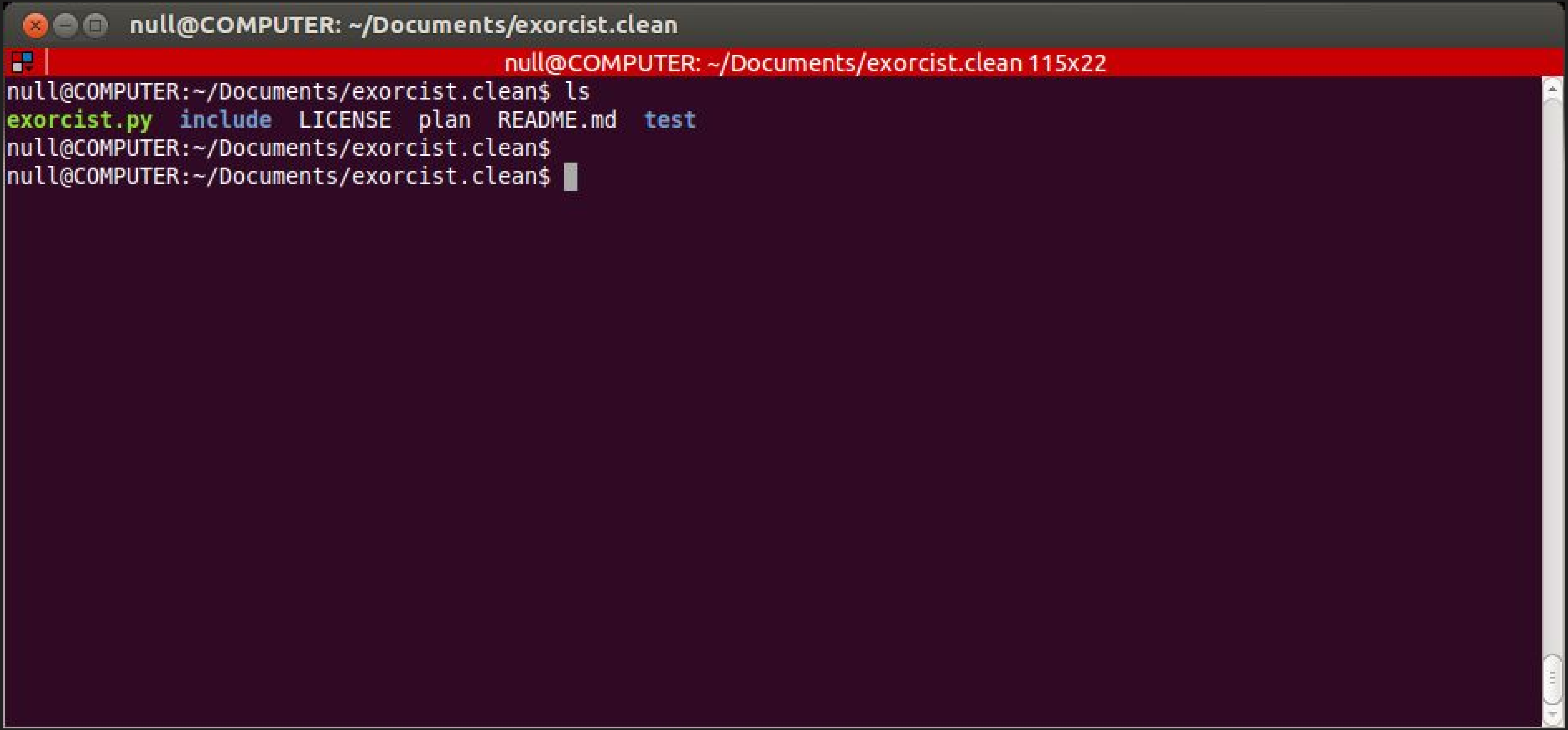

null@COMPUTER: ~/Documents/exorcist
null@COMPUTER: ~/Documents/exorcist 90x18

```
null@COMPUTER:~/Documents/exorcist$ sha1sum /usr/share/NetworkMiner_1-6-1/AssembledFiles/1
44.76.192.102/HTTP\ -\ TCP\ 80/index.html.51620EC7.html out/test.pcap/TCP_144.76.192.102\:
80_TO_192.168.40.10\:1051/e129d6ffce20075e1c4c6f3a758fe3e4481e66be
e129d6ffce20075e1c4c6f3a758fe3e4481e66be  /usr/share/NetworkMiner_1-6-1/AssembledFiles/144
.76.192.102/HTTP - TCP 80/index.html.51620EC7.html
e129d6ffce20075e1c4c6f3a758fe3e4481e66be  out/test.pcap/TCP_144.76.192.102:80_TO_192.168.4
0.10:1051/e129d6ffce20075e1c4c6f3a758fe3e4481e66be
null@COMPUTER:~/Documents/exorcist$ 
```

exorcist

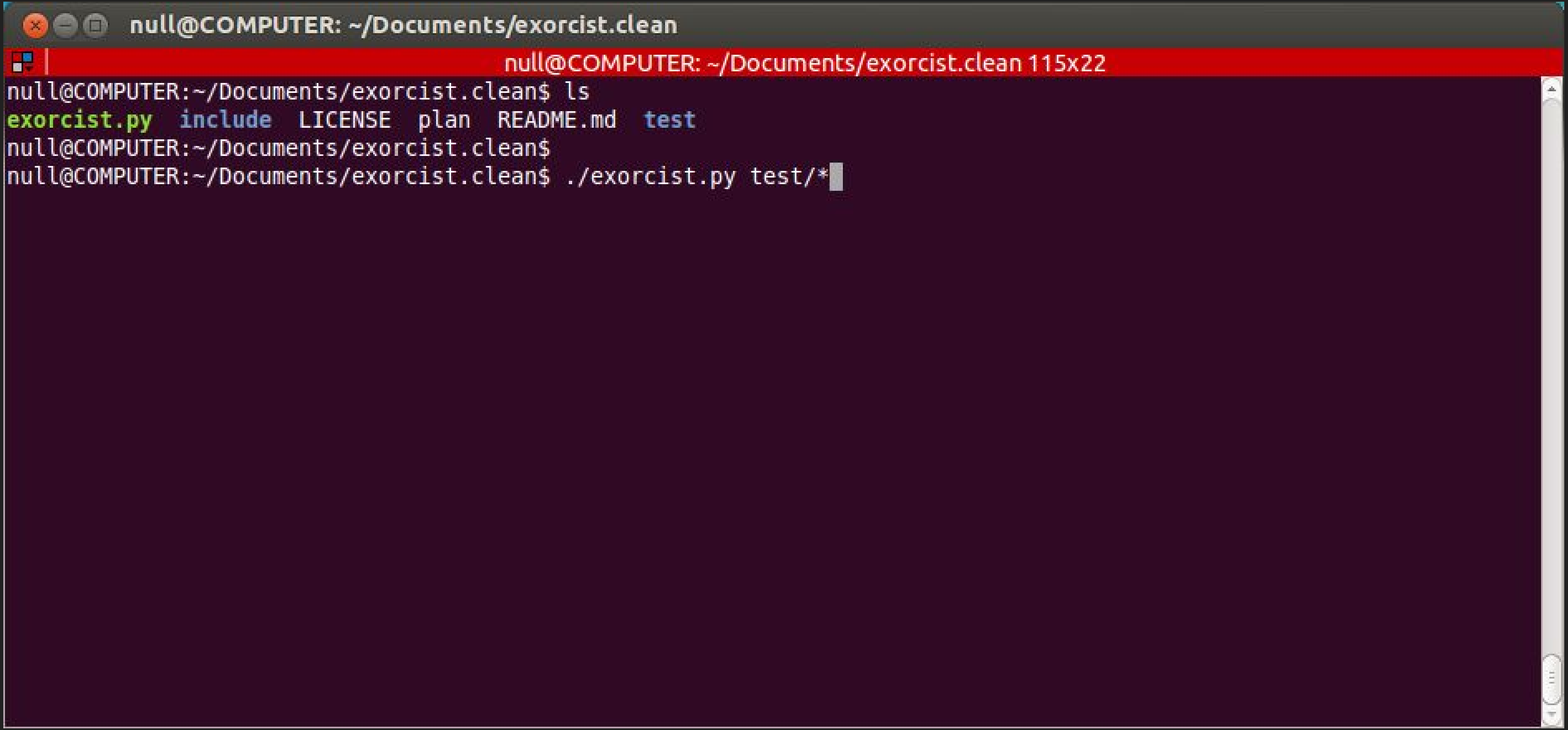
https://github.com/mrmoss/exorcist.git

```
./exorcist.py pcaps...
```



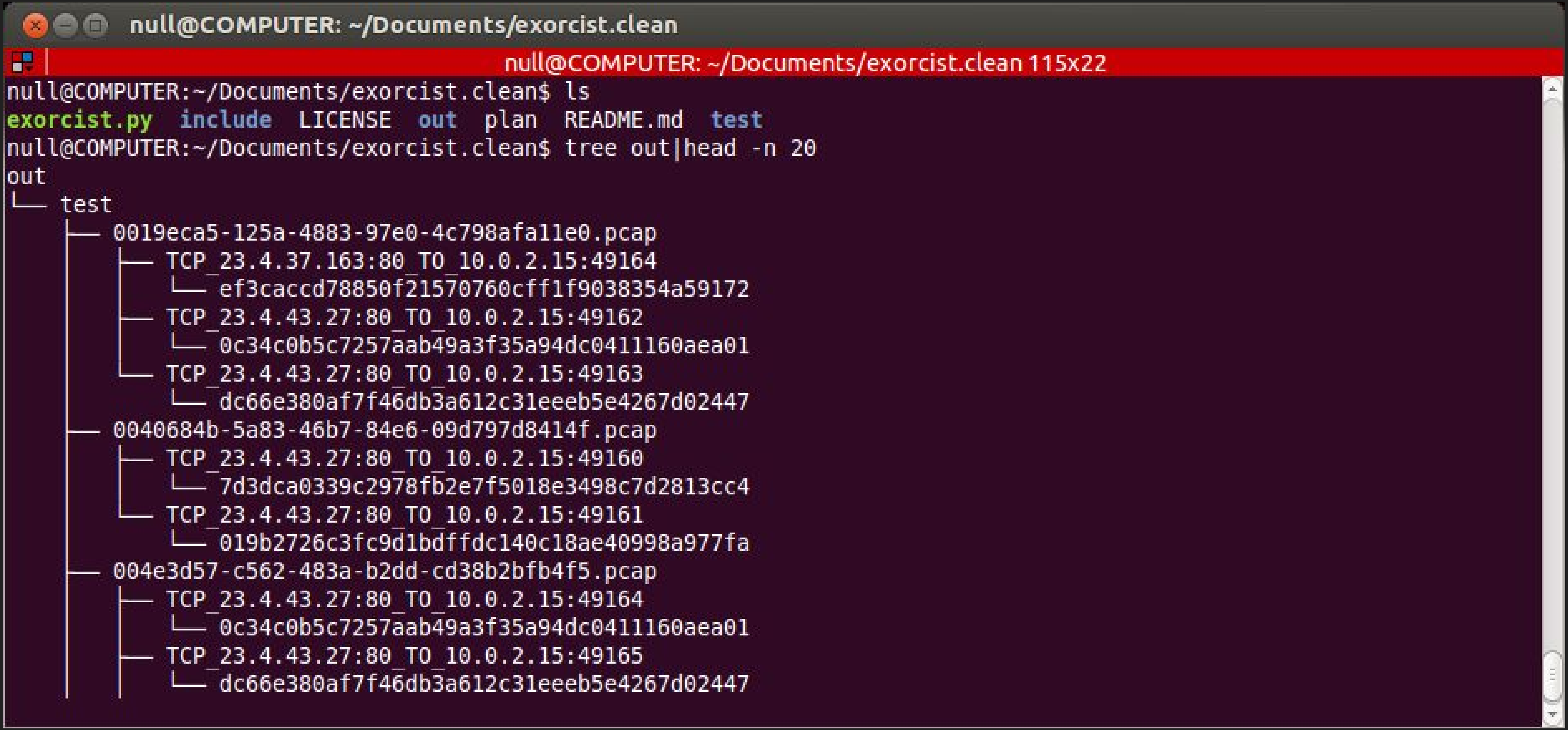
null@COMPUTER: ~/Documents/exorcist.clean
null@COMPUTER: ~/Documents/exorcist.clean 115x22

```
null@COMPUTER:~/Documents/exorcist.clean$ ls
exorcist.py  include  LICENSE  plan  README.md  test
null@COMPUTER:~/Documents/exorcist.clean$
null@COMPUTER:~/Documents/exorcist.clean$ 
```



null@COMPUTER: ~/Documents/exorcist.clean
null@COMPUTER: ~/Documents/exorcist.clean 115x22

```
null@COMPUTER:~/Documents/exorcist.clean$ ls
exorcist.py  include  LICENSE  plan  README.md  test
null@COMPUTER:~/Documents/exorcist.clean$
null@COMPUTER:~/Documents/exorcist.clean$ ./exorcist.py test/*
```


null@COMPUTER: ~/Documents/exorcist.clean
null@COMPUTER: ~/Documents/exorcist.clean 115x22

```
null@COMPUTER:~/Documents/exorcist.clean$ ls
exorcist.py  include  LICENSE  out  plan  README.md  test
null@COMPUTER:~/Documents/exorcist.clean$ tree out|head -n 20
out
└── test
    ├── 0019eca5-125a-4883-97e0-4c798afa11e0.pcap
    │   ├── TCP_23.4.37.163:80_TO_10.0.2.15:49164
    │   │   └── ef3caccd78850f21570760cff1f9038354a59172
    │   ├── TCP_23.4.43.27:80_TO_10.0.2.15:49162
    │   │   └── 0c34c0b5c7257aab49a3f35a94dc0411160aea01
    │   └── TCP_23.4.43.27:80_TO_10.0.2.15:49163
    │       └── dc66e380af7f46db3a612c31eeeb5e4267d02447
    ├── 0040684b-5a83-46b7-84e6-09d797d8414f.pcap
    │   ├── TCP_23.4.43.27:80_TO_10.0.2.15:49160
    │   │   └── 7d3dca0339c2978fb2e7f5018e3498c7d2813cc4
    │   └── TCP_23.4.43.27:80_TO_10.0.2.15:49161
    │       └── 019b2726c3fc9d1bdffdc140c18ae40998a977fa
    ├── 004e3d57-c562-483a-b2dd-cd38b2bfb4f5.pcap
    │   ├── TCP_23.4.43.27:80_TO_10.0.2.15:49164
    │   │   └── 0c34c0b5c7257aab49a3f35a94dc0411160aea01
    │   ├── TCP_23.4.43.27:80_TO_10.0.2.15:49165
    │   │   └── dc66e380af7f46db3a612c31eeeb5e4267d02447
```

future development:

- send files through virustotal?
- add more application layer protocols?

questions?