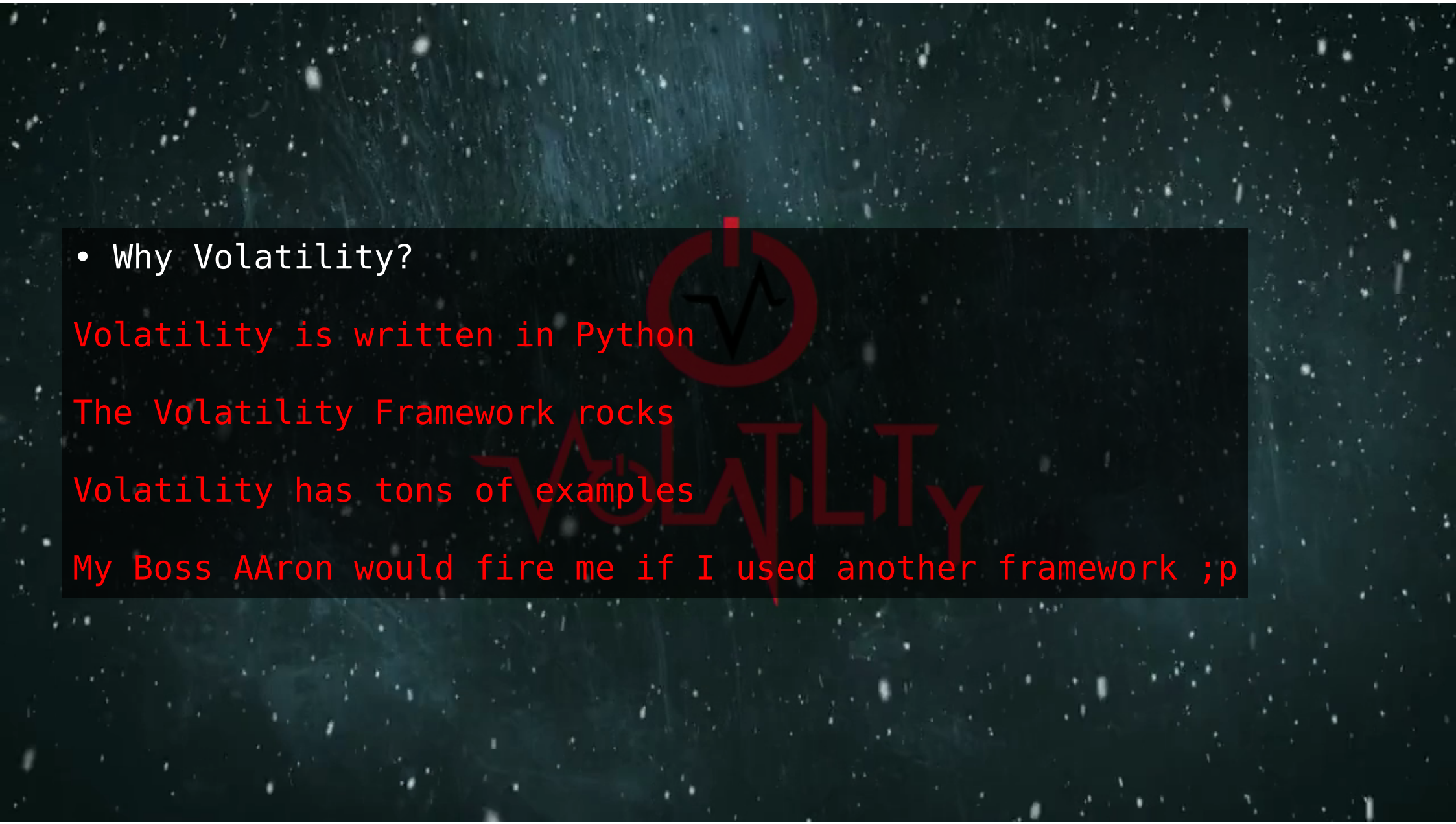
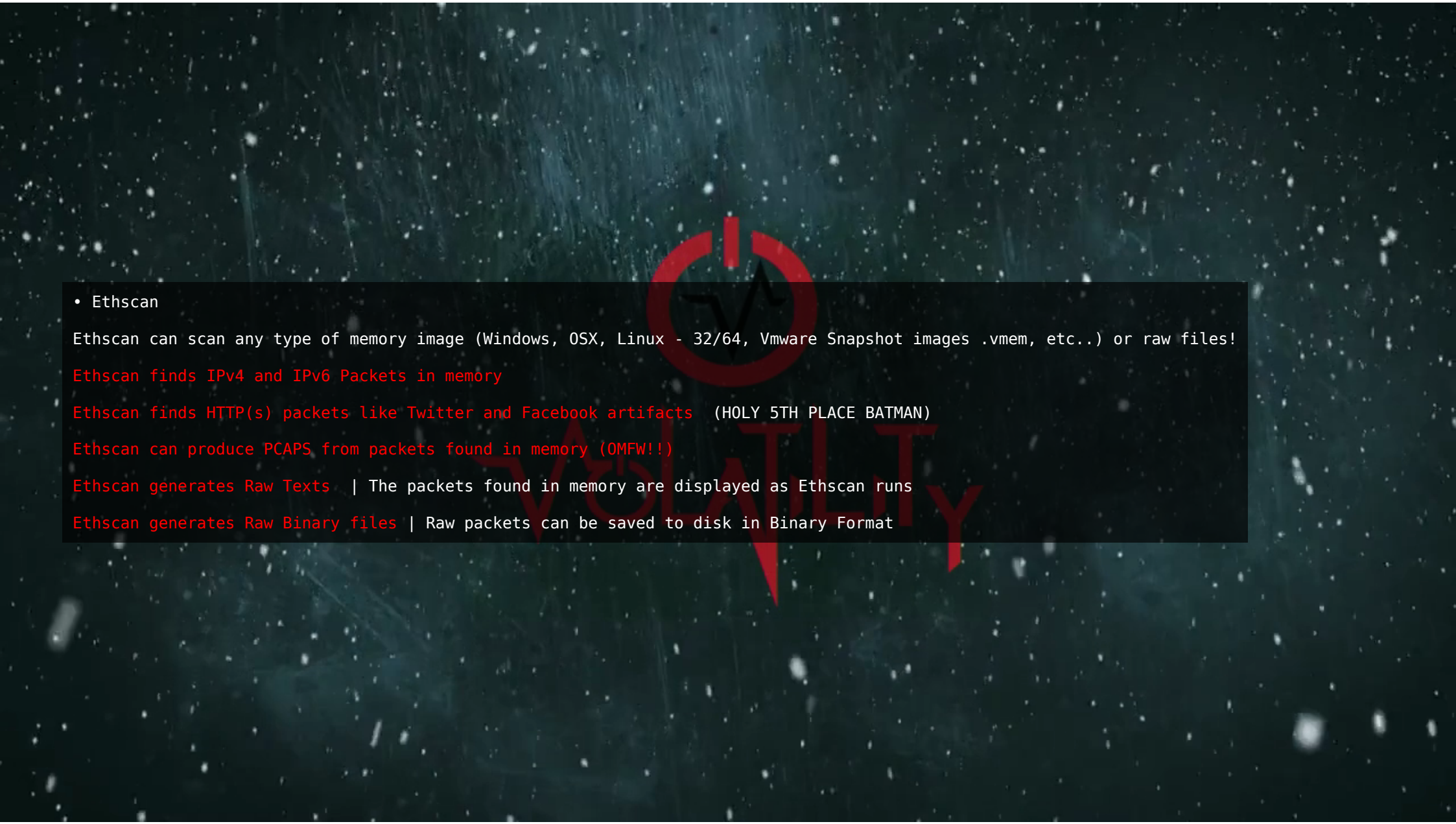
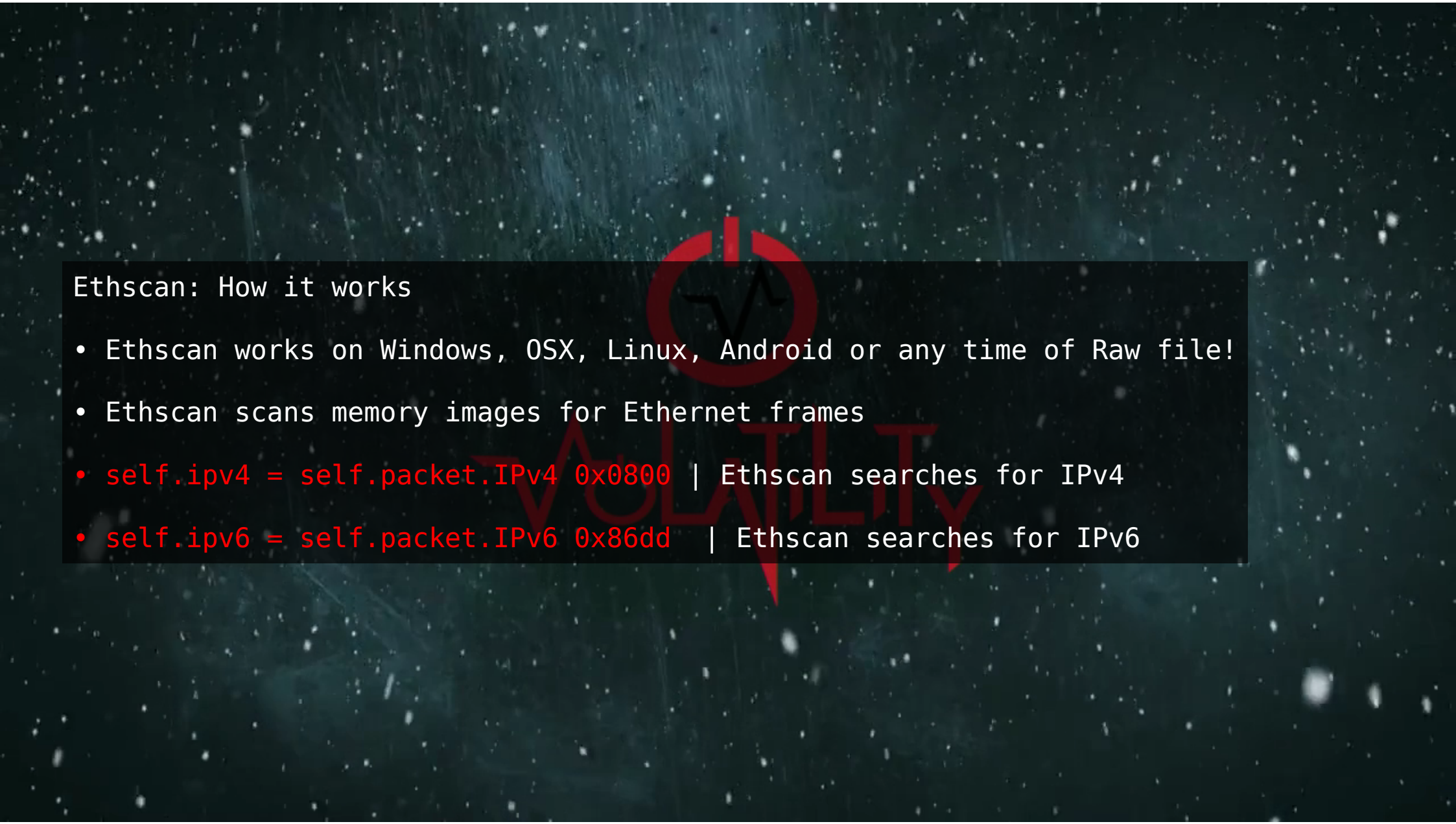


- Jamaal Speights | https://twitter.com/jamaalspeights | jspeights@terremark.com
- *Terremark*
- Background: Unix Admin | InfoSec | Reverse Engineering


• Why Volatility?
Volatility is written in Python
The Volatility Framework rocks
Volatility has tons of examples
My Boss AAron would fire me if I used another framework ;p


• Ethscan
Ethscan can scan any type of memory image (Windows, OSX, Linux - 32/64, Vmware Snapshot images .vmem, etc..) or raw files!
Ethscan finds IPv4 and IPv6 Packets in memory
Ethscan finds HTTP(s) packets like Twitter and Facebook artifacts (HOLY 5TH PLACE BATMAN)
Ethscan can produce PCAPS from packets found in memory (OMFW!!)
Ethscan generates Raw Texts | The packets found in memory are displayed as Ethscan runs
Ethscan generates Raw Binary files | Raw packets can be saved to disk in Binary Format


Ethscan: How it works
• Ethscan works on Windows, OSX, Linux, Android or any time of Raw file!
• Ethscan scans memory images for Ethernet frames
• self.ipv4 = self.packet.IPv4 0x0800 | Ethscan searches for IPv4
• self.ipv6 = self.packet.IPv6 0x86dd | Ethscan searches for IPv6

## Ethscan: How it works (cont..)

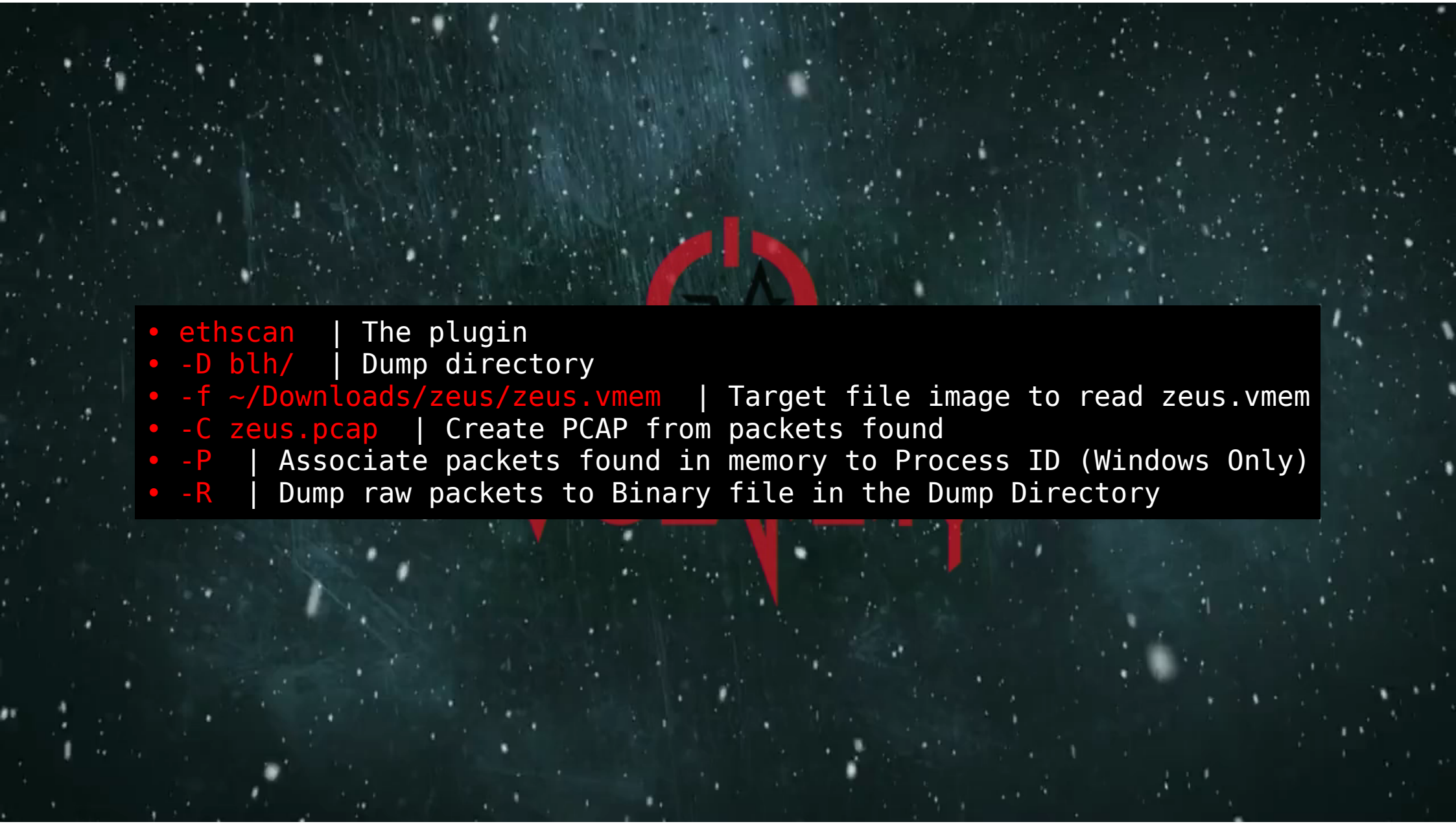
- Once an Ethernet Frame is found, the Protocol type is validated
- If the Protocal type is validied, Ethscan does IPv4 or IpV6 Checksum Validation
- Checksum Validation can be disabled (This option can produce more packets but lots of false positives
- MTU size is valided (This option can be changed from 1500)

- ETHSCAN plugin options help file

- Options:

```
  -D DUMP_DIR, --dump-dir=DUMP_DIR
                        Directory in which to dump executable files
  -C SAVE_PCAP, --save-pcap=SAVE_PCAP
                        Create a pcap file from recovered packets of given
                        name: "Example: -C out.pcap" (requires dpkt)
  -R, --save-raw        Create binary files of each packet found in memory
  -P, --enable-proc     Enable Packet to Process Association: Windows Only
                        (SLOW)
  -F FILTER_PACKET, --filter-packet=FILTER_PACKET
                        Filter packets based off of Protocol and Ethernet
                        types.  Example: " -F 0x0800,0x11 " - searches only
                        for TCP,UDP type packets.
  -M 1500, --set-mtu=1500
                        Set a new MTU size, default is 1500
  -S, --disable-checksum
                        Disable packet checksum validation, this option is
                        best used with -F (WARNING: LOTS OF FALSE POSITIVES)
```


Ethscan CLI example:
python ~/vol/vol.py ethscan -D blh/ -f ~/Downloads/zeus/zeus.vmem -C zeus.pcap -P -R rawdata.bin
VOLATILITY


• ethscan | The plugin
• -D blh/ | Dump directory
• -f ~/Downloads/zeus/zeus.vmem | Target file image to read zeus.vmem
• -C zeus.pcap | Create PCAP from packets found
• -P | Associate packets found in memory to Process ID (Windows Only)
• -R | Dump raw packets to Binary file in the Dump Directory

# Ethscan output

- Notice Packet 9 (of over 200!) is associaed with Process smss.exe because of the -P option (Windows Only)

```
Packets Found: 8
ProcName: smss.exe PID: 544 Base Address: 0x158000  End Address: 0x1000
Ethernet:    Src: (00:50:56:c0:00:08)       Dst: (ff:ff:ff:ff:ff:ff)
Type:        IPv4 (0x0800)
IPv4:        Src: 172.16.176.1:33262       Dst: 172.16.176.255:35072
Protocol:    UDP (17)
Packet Size: (92) Bytes
0x00000000  ff ff ff ff ff ff 00 50 56 c0 00 08 08 00 45 00   .......PV.....E.
0x00000010  00 4e cf e4 00 00 40 11 f1 98 ac 10 b0 01 ac 10   .N....@.........
0x00000020  b0 ff ee 81 00 89 00 3a 91 a0 1c 2e 01 10 00 01   .......:........
0x00000030  00 00 00 00 00 00 20 41 42 41 43 46 50 46 50 45   .......ABACFPFPE
0x00000040  4e 46 44 45 43 46 43 45 50 46 48 46 44 45 46 46   NFDECFCEPFHFDEFF
0x00000050  50 46 50 41 43 41 42 00 00 20 00 01               PFPACAB.....

Packets Found: 9
ProcName: smss.exe PID: 544 Base Address: 0x159000  End Address: 0x1000
Ethernet:    Src: (00:50:56:f1:2d:82)       Dst: (00:0c:29:a4:81:79)
Type:        IPv4 (0x0800)
IPv4:        Src: 131.107.115.254:47873       Dst: 172.16.176.143:3332
Protocol:    TCP (6)
Packet Size: (1422) Bytes
0x00000000  00 0c 29 a4 81 79 00 50 56 f1 2d 82 08 00 45 00   ..)..y.PV.-...E.
0x00000010  05 80 29 80 00 00 80 06 b7 ee 83 6b 73 fe ac 10   ..).........ks...
0x00000020  b0 8f 01 bb 04 0d 79 7e 38 9e d8 8d 3d 55 50 18   ......y~8...=UP.
0x00000030  fa f0 25 a5 00 00 06 03 55 04 07 13 07 52 65 64   ..%.....U....Red
0x00000040  6d 6f 6e 64 31 1e 30 1c 06 03 55 04 0a 13 15 4d   mond1.0...U....M
0x00000050  69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61   icrosoft.Corpora
0x00000060  74 69 6f 6e 31 34 30 32 06 03 55 04 03 13 2b 4d   tion1402..U...+M
0x00000070  69 63 72 6f 73 6f 66 74 20 50 72 6f 64 75 63 74   icrosoft.Product
0x00000080  20 53 65 63 75 72 65 20 43 6f 6d 6d 75 6e 69 63   .Secure.Communic
0x00000090  61 74 69 6f 6e 73 20 50 43 41 30 1e 17 0d 30 37   ations.PCA0...07
```

- Ethscan finds plenty of HTTP(S) packets and then some (FTW!)

```
Protocol:    TCP (6)
Packet Size: (431) Bytes
0x00000000  00 0c 29 a4 81 79 00 50 56 f1 2d 82 08 00 45 00   ..)..y.PV.-...E.
0x00000010  01 a1 29 59 00 00 80 06 bb f4 83 6b 73 fe ac 10   ..)Y.......ks...
0x00000020  b0 8f 00 50 04 0a b4 b2 20 ee 20 55 75 97 50 18   ...P.......Uu.P.
0x00000030  fa f0 b9 d8 00 00 48 54 54 50 2f 31 2e 31 20 34   ......HTTP/1.1.4
0x00000040  30 33 20 46 6f 72 62 69 64 64 65 6e 0d 0a 43 6f   03.Forbidden..Co
0x00000050  6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 32 31   ntent-Length:.21
0x00000060  38 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a   8..Content-Type:
0x00000070  20 74 65 78 74 2f 68 74 6d 6c 0d 0a 53 65 72 76   .text/html..Serv
0x00000080  65 72 3a 20 4d 69 63 72 6f 73 6f 66 74 2d 49 49   er:.Microsoft-II
0x00000090  53 2f 36 2e 30 0d 0a 58 2d 50 6f 77 65 72 65 64   S/6.0..X-Powered
0x000000a0  2d 42 79 3a 20 41 53 50 2e 4e 45 54 0d 0a 44 61   -By:.ASP.NET..Da
0x000000b0  74 65 3a 20 57 65 64 2c 20 31 31 20 41 75 67 20   te:.Wed,.11.Aug.
0x000000c0  32 30 31 30 20 30 36 3a 30 39 3a 30 36 20 47 4d   2010.06:09:06.GM
0x000000d0  54 0d 0a 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64   T....<html><head
0x000000e0  3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 3c 2f 74   ><title>Error</t
0x000000f0  69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64   itle></head><bod
0x00000100  79 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 44   y><head><title>D
0x00000110  69 72 65 63 74 6f 72 79 20 4c 69 73 74 69 6e 67   irectory.Listing
0x00000120  20 44 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 3c   .Denied</title><
0x00000130  2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 3c 68 31   /head>.<body><h1
0x00000140  3e 44 69 72 65 63 74 6f 72 79 20 4c 69 73 74 69   >Directory.Listi
0x00000150  6e 67 20 44 65 6e 69 65 64 3c 2f 68 31 3e 54 68   ng.Denied</h1>Th
0x00000160  69 73 20 56 69 72 74 75 61 6c 20 44 69 72 65 63   is.Virtual.Direc
0x00000170  74 6f 72 79 20 64 6f 65 73 20 6e 6f 74 20 61 6c   tory.does.not.al
0x00000180  6c 6f 77 20 63 6f 6e 74 65 6e 74 73 20 74 6f 20   low.contents.to.
0x00000190  62 65 20 6c 69 73 74 65 64 2e 3c 2f 62 6f 64 79   be.listed.</body
0x000001a0  3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e      ></body></html>

Packets Found: 38
Ethernet:    Src: (00:50:56:c0:00:08)      Dst: (ff:ff:ff:ff:ff:ff)
```

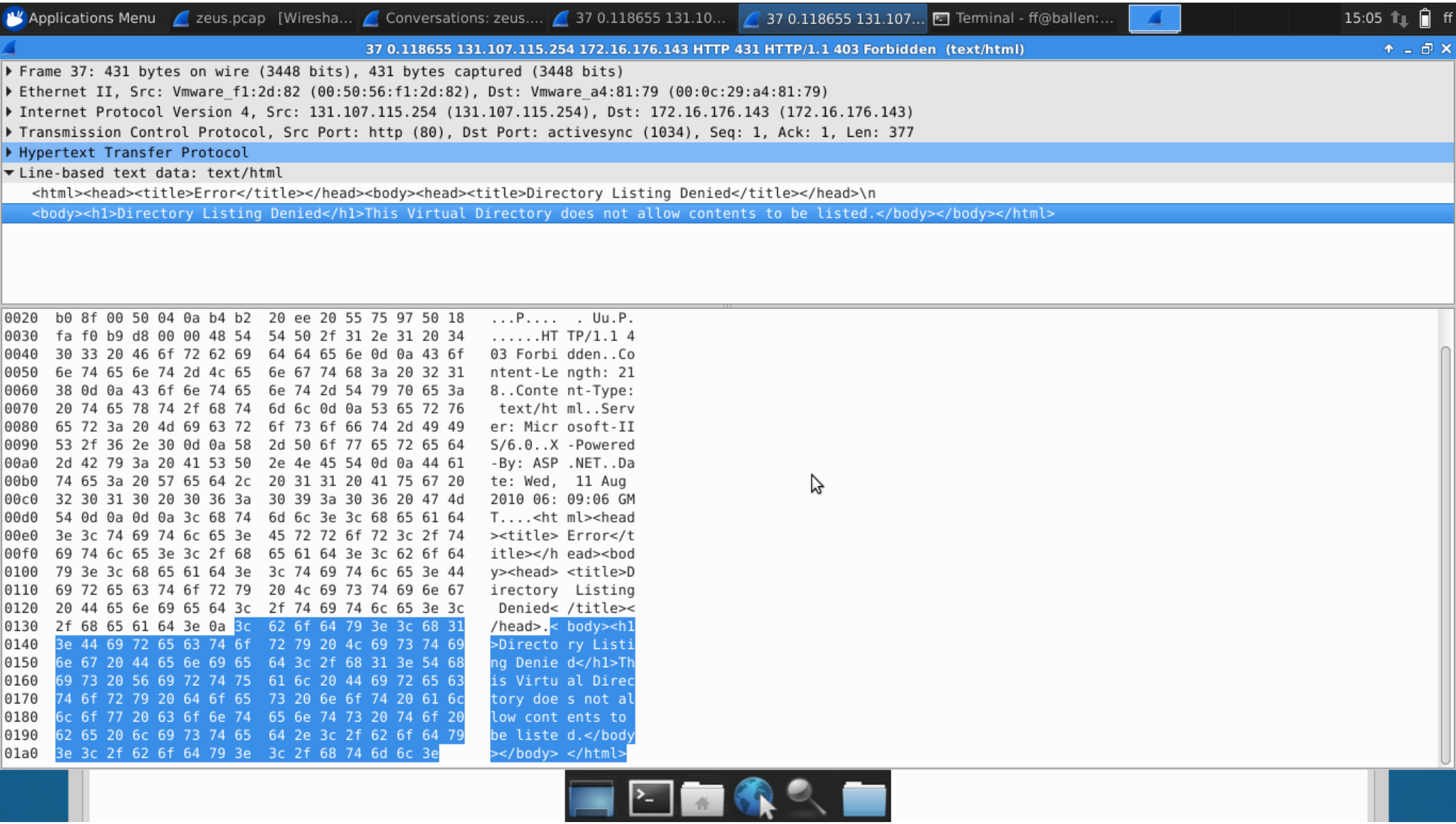
- A directly listing of the -D Dump directory "blh"

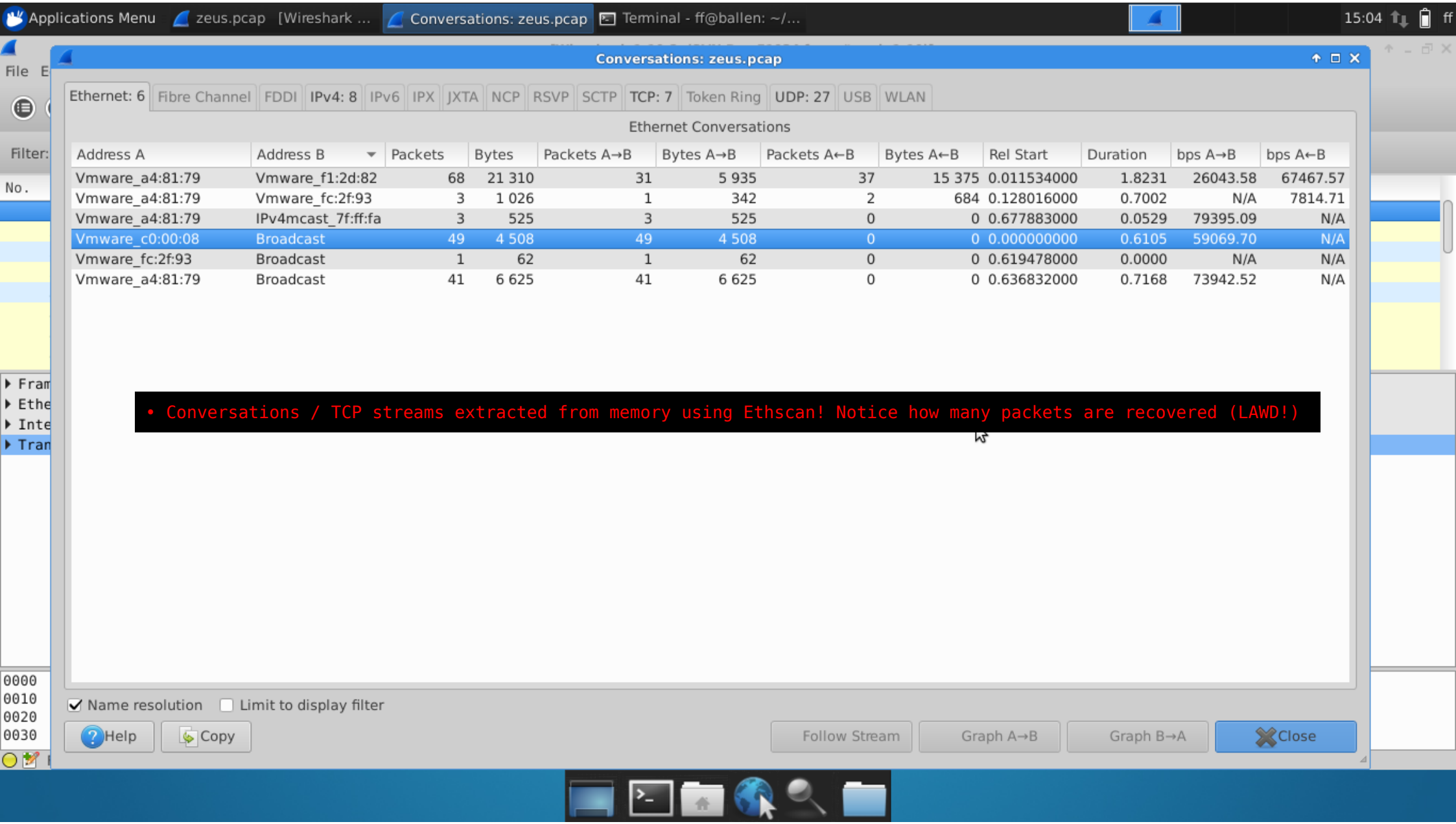
```
ff@ballen:~/omfw$ ls -l blh/
total 84
-rw-r--r-- 1 ff ff   92 Nov  4 15:28 10__172.16.176.1__33518__172.16.176.255__35072__UDP.bin
-rw-r--r-- 1 ff ff   92 Nov  4 15:28 11__172.16.176.1__34798__172.16.176.255__35072__UDP.bin
-rw-r--r-- 1 ff ff   92 Nov  4 15:28 1__172.16.176.1__35054__172.16.176.255__35072__UDP.bin
-rw-r--r-- 1 ff ff   92 Nov  4 15:28 12__172.16.176.1__33774__172.16.176.255__35072__UDP.bin
-rw-r--r-- 1 ff ff   92 Nov  4 15:28 13__172.16.176.1__28654__172.16.176.255__35072__UDP.bin
-rw-r--r-- 1 ff ff   92 Nov  4 15:28 14__172.16.176.1__34286__172.16.176.255__35072__UDP.bin
-rw-r--r-- 1 ff ff   92 Nov  4 15:28 15__172.16.176.1__28654__172.16.176.255__35072__UDP.bin
-rw-r--r-- 1 ff ff   92 Nov  4 15:28 16__172.16.176.1__34542__172.16.176.255__35072__UDP.bin
-rw-r--r-- 1 ff ff   92 Nov  4 15:28 17__172.16.176.1__34798__172.16.176.255__35072__UDP.bin
-rw-r--r-- 1 ff ff  121 Nov  4 15:28 18__131.107.115.254__47873__172.16.176.143__3332__TCP.bin
-rw-r--r-- 1 ff ff   92 Nov  4 15:28 19__172.16.176.1__35054__172.16.176.255__35072__UDP.bin
-rw-r--r-- 1 ff ff   92 Nov  4 15:28 2__172.16.176.1__34030__172.16.176.255__35072__UDP.bin
-rw-r--r-- 1 ff ff   92 Nov  4 15:28 3__172.16.176.1__35566__172.16.176.255__35072__UDP.bin
-rw-r--r-- 1 ff ff   58 Nov  4 15:28 4__131.107.115.254__47873__172.16.176.143__3332__TCP.bin
-rw-r--r-- 1 ff ff   54 Nov  4 15:28 5__131.107.115.254__47873__172.16.176.143__3332__TCP.bin
-rw-r--r-- 1 ff ff   92 Nov  4 15:28 6__172.16.176.1__35310__172.16.176.255__35072__UDP.bin
-rw-r--r-- 1 ff ff 1422 Nov  4 15:28 7__131.107.115.254__47873__172.16.176.143__3332__TCP.bin
-rw-r--r-- 1 ff ff   92 Nov  4 15:28 8__172.16.176.1__33262__172.16.176.255__35072__UDP.bin
-rw-r--r-- 1 ff ff 1422 Nov  4 15:28 9__131.107.115.254__47873__172.16.176.143__3332__TCP.bin
-rw-r--r-- 1 ff ff 4693 Nov  4 15:28 zeus.pcap
ff@ballen:~/omfw$
```

- Hexdump of raw packet found in memory in the Data directory

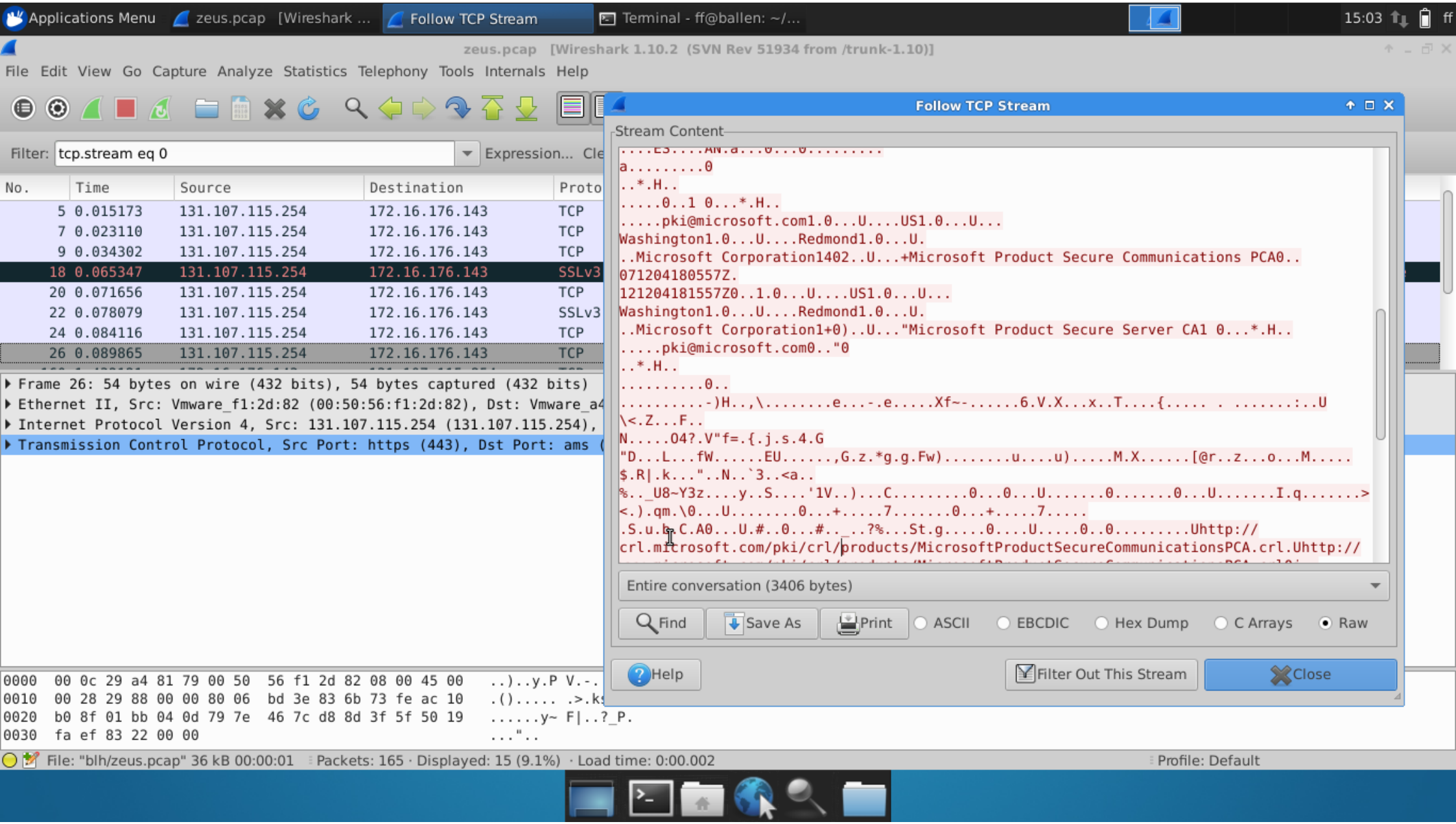
```
ff@ballen:~/omfw$ hexdump -C blh/7__131.107.115.254__47873__172.16.176.143__3332__TCP.bin | more
00000000  00 0c 29 a4 81 79 00 50  56 f1 2d 82 08 00 45 00  |..)..y.PV.-...E.|
00000010  05 80 29 7f 00 00 80 06  b7 ef 83 6b 73 fe ac 10  |..).........ks...|
00000020  b0 8f 01 bb 04 0d 79 7e  33 46 d8 8d 3d 55 50 18  |......y~3F..=UP.|
00000030  fa f0 83 08 00 00 16 03  00 11 e9 02 00 00 46 03  |..............F.|
00000040  00 4c 62 3e 86 1c 84 f1  cb cd fc be 83 d9 b3 31  |.Lb>...........1|
00000050  5b 1d ed e8 37 1b b6 38  31 37 bc 01 cd f0 99 d2  |[...7..817......|
00000060  15 20 30 0d 00 00 cc 24  42 11 1a 50 f3 dc cf 74  |. 0....$B..P...t|
00000070  c4 04 7a f5 da 1b 93 9c  51 f4 46 64 43 b2 55 17  |..z.....Q.FdC.U.|
00000080  48 f0 00 04 00 0b 00 11  97 00 11 94 00 04 89 30  |H..............0|
00000090  82 04 85 30 82 03 6d a0  03 02 01 02 02 0a 61 12  |...0..m.......a.|
000000a0  df 52 00 00 00 00 00 12  30 0d 06 09 2a 86 48 86  |.R......0...*.H.|
000000b0  f7 0d 01 01 05 05 00 30  81 a3 31 0b 30 09 06 03  |.......0..1.0...|
000000c0  55 04 06 13 02 55 53 31  13 30 11 06 03 55 04 08  |U....US1.0...U..|
000000d0  13 0a 57 61 73 68 69 6e  67 74 6f 6e 31 10 30 0e  |..Washington1.0.|
000000e0  06 03 55 04 07 13 07 52  65 64 6d 6f 6e 64 31 1e  |..U....Redmond1.|
000000f0  30 1c 06 03 55 04 0a 13  15 4d 69 63 72 6f 73 6f  |0...U....Microso|
00000100  66 74 20 43 6f 72 70 6f  72 61 74 69 6f 6e 31 2b  |ft Corporation1+|
00000110  30 29 06 03 55 04 03 13  22 4d 69 63 72 6f 73 6f  |0)..U..."Microso|
00000120  66 74 20 50 72 6f 64 75  63 74 20 53 65 63 75 72  |ft Product Secur|
00000130  65 20 53 65 72 76 65 72  20 43 41 31 20 30 1e 06  |e Server CA1 0..|
00000140  09 2a 86 48 86 f7 0d 01  09 01 16 11 70 6b 69 40  |.*.H........pki@|
00000150  6d 69 63 72 6f 73 6f 66  74 2e 63 6f 6d 30 1e 17  |microsoft.com0..|
00000160  0d 30 39 31 30 31 35 32  32 30 30 33 38 5a 17 0d  |.091015220038Z..|
00000170  31 32 30 31 31 35 32 32  30 30 33 38 5a 30 6f 31  |120115220038Z0o1|
00000180  0b 30 09 06 03 55 04 06  13 02 55 53 31 10 30 0e  |.0...U....US1.0.|
00000190  06 03 55 04 08 13 07 52  65 64 6d 6f 6e 64 31 0b  |..U....Redmond1.|
000001a0  30 09 06 03 55 04 07 13  02 57 41 31 12 30 10 06  |0...U....WA1.0..|
000001b0  03 55 04 0a 13 09 4d 69  63 72 6f 73 6f 66 74 31  |.U....Microsoft1|
```

- Using Wireshark to open the PCAP generated by EthScan




Applications Menu
zeus.pcap [Wireshark ...
Conversations: zeus.pcap
Terminal - ff@ballen: ~/...
15:04
Conversations: zeus.pcap
Ethernet: 6
Fibre Channel
FDDI
IPv4: 8
IPv6
IPX
JXTA
NCP
RSVP
SCTP
TCP: 7
Token Ring
UDP: 27
USB
WLAN
Ethernet Conversations
Address A
Address B
Packets
Bytes
Packets A→B
Bytes A→B
Packets A←B
Bytes A←B
Rel Start
Duration
bps A→B
bps A←B
Vmware_a4:81:79 Vmware_f1:2d:82 68 21 310 31 5 935 37 15 375 0.011534000 1.8231 26043.58 67467.57
Vmware_a4:81:79 Vmware_fc:2f:93 3 1 026 1 342 2 684 0.128016000 0.7002 N/A 7814.71
Vmware_a4:81:79 IPv4mcast_7f:ff:fa 3 525 3 525 0 0 0.677883000 0.0529 79395.09 N/A
Vmware_c0:00:08 Broadcast 49 4 508 49 4 508 0 0 0.000000000 0.6105 59069.70 N/A
Vmware_fc:2f:93 Broadcast 1 62 1 62 0 0 0.619478000 0.0000 N/A N/A
Vmware_a4:81:79 Broadcast 41 6 625 41 6 625 0 0 0.636832000 0.7168 73942.52 N/A
• Conversations / TCP streams extracted from memory using Ethscan! Notice how many packets are recovered (LAWD!)
Name resolution
Limit to display filter
Help
Copy
Follow Stream
Graph A→B
Graph B→A
Close

• Output of a complete TCP stream rebuilt from packets in memory with Ethscan




# Questions?


VOLATILITY