Listening to Your Internet Traffic

Michael Cooley
@irishjack

What is Packet Capturing?

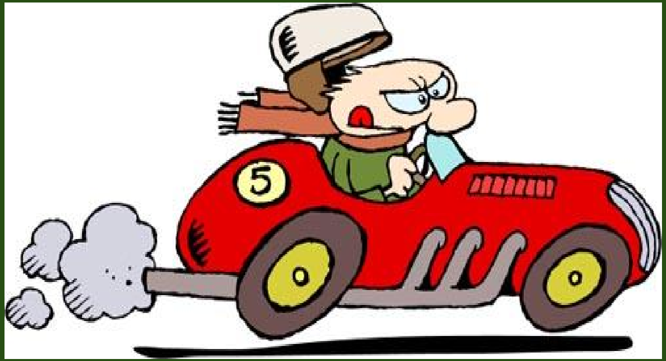
Why do it?

- Troubleshoot problems
- See what is going on

What is Packet Capturing?

What is a packet?

- How data moves across the network
- Has a defined structure
    - Like sending a letter



What is Packet Capturing?

How does it work?

- How to get access to the datastream
- What is promiscuous mode
- Like listening in on a conversation

What is Packet Capturing?

What can you learn from it?

- What is talking to what
- What is being said
- Is traffic flowing properly

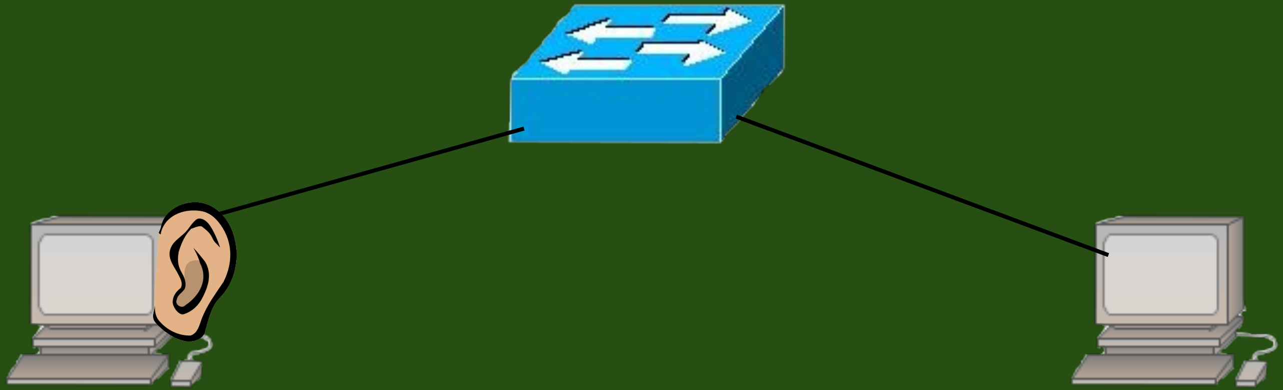
Getting Started

What tools are out there?

- Software:
  - tcpdump
  - wireshark
- Hardware:
  - Throwing star LAN tap
  - Hubs
  - Port Mirroring

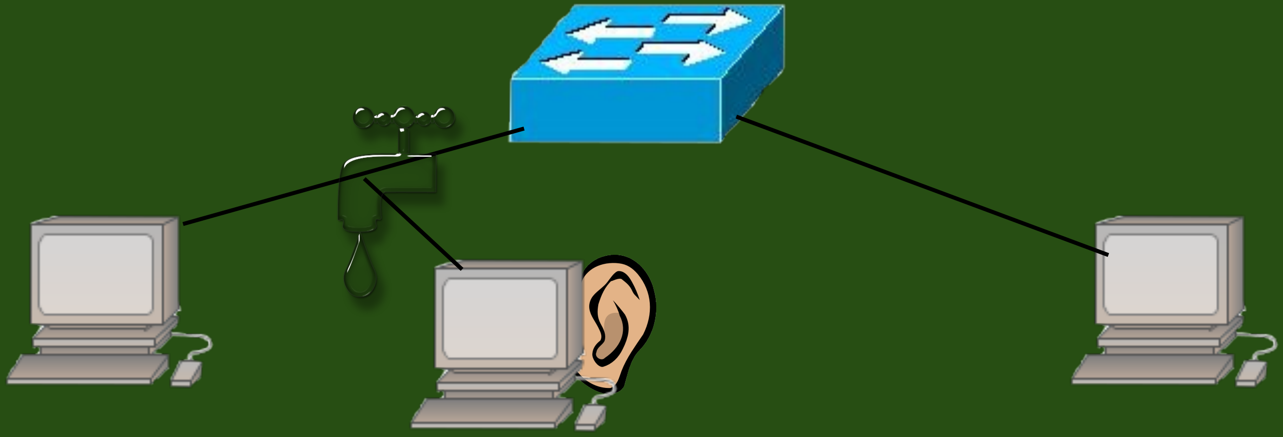
Getting Started

Putting yourself into the conversation



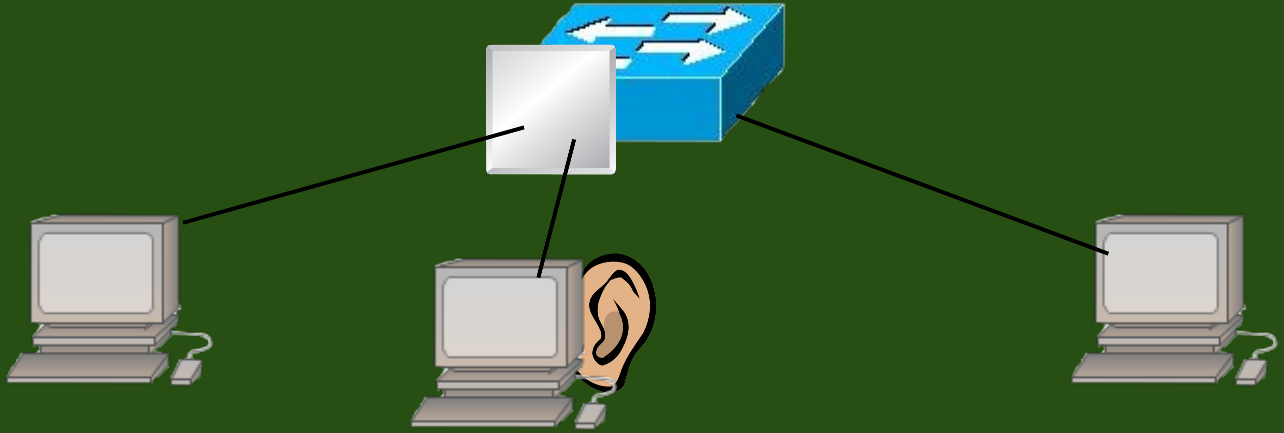
Getting Started

Putting yourself into the conversation



Getting Started

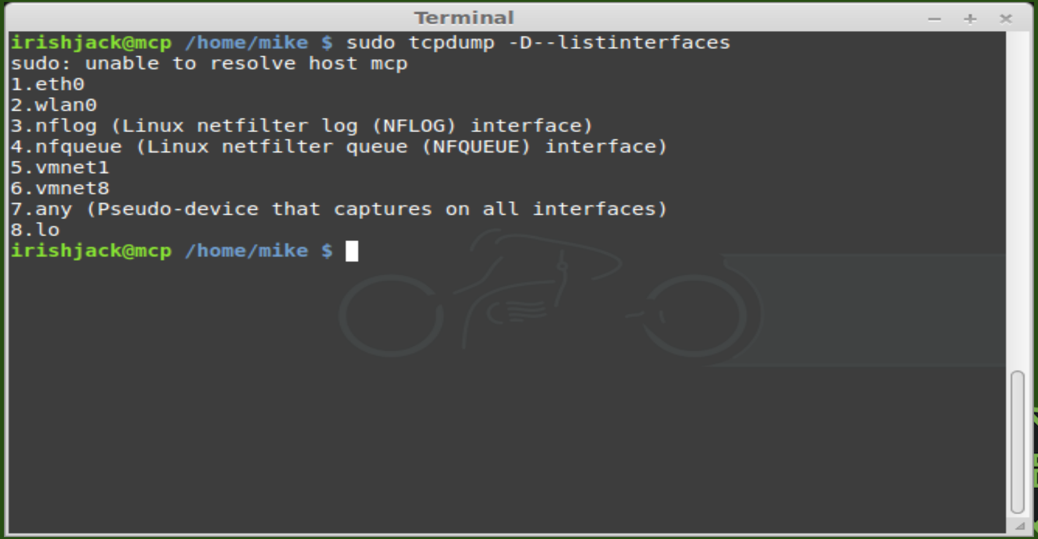
Putting yourself into the conversation



Getting Started

Using tcpdump to capture the data

- http://www.tcpdump.org/manpages/tcpdump.1.html
- *tcpdump -D--listinterfaces*

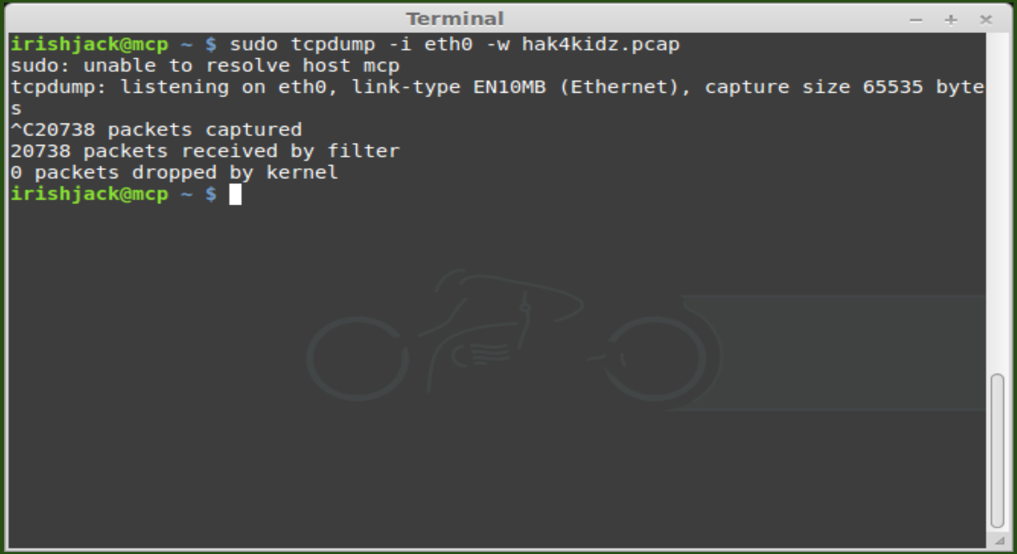


```
irishjack@mcp /home/mike $ sudo tcpdump -D--listinterfaces
sudo: unable to resolve host mcp
1.eth0
2.wlan0
3.nflog (Linux netfilter log (NFLOG) interface)
4.nfqueue (Linux netfilter queue (NFQUEUE) interface)
5.vmnet1
6.vmnet8
7.any (Pseudo-device that captures on all interfaces)
8.lo
irishjack@mcp /home/mike $
```

Getting Started

Using tcpdump to capture the data

- *tcpdump -i <interface> -w <outputfile>*
- *tcpdump -i eth0 -w hak4kidz.pcap*

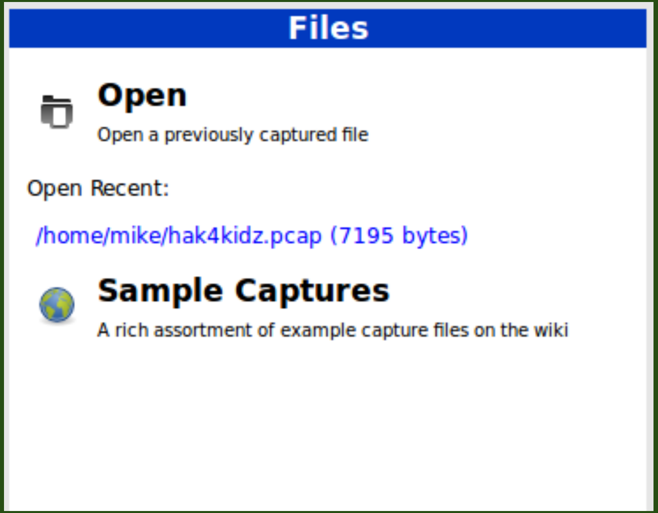


```
irishjack@mcp ~ $ sudo tcpdump -i eth0 -w hak4kidz.pcap
sudo: unable to resolve host mcp
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 byte
s
^C20738 packets captured
20738 packets received by filter
0 packets dropped by kernel
irishjack@mcp ~ $ 
```

Getting Started

Using Wireshark to view the capture

- https://www.wireshark.org/
- Opening a capture file



Files

Open

Open a previously captured file

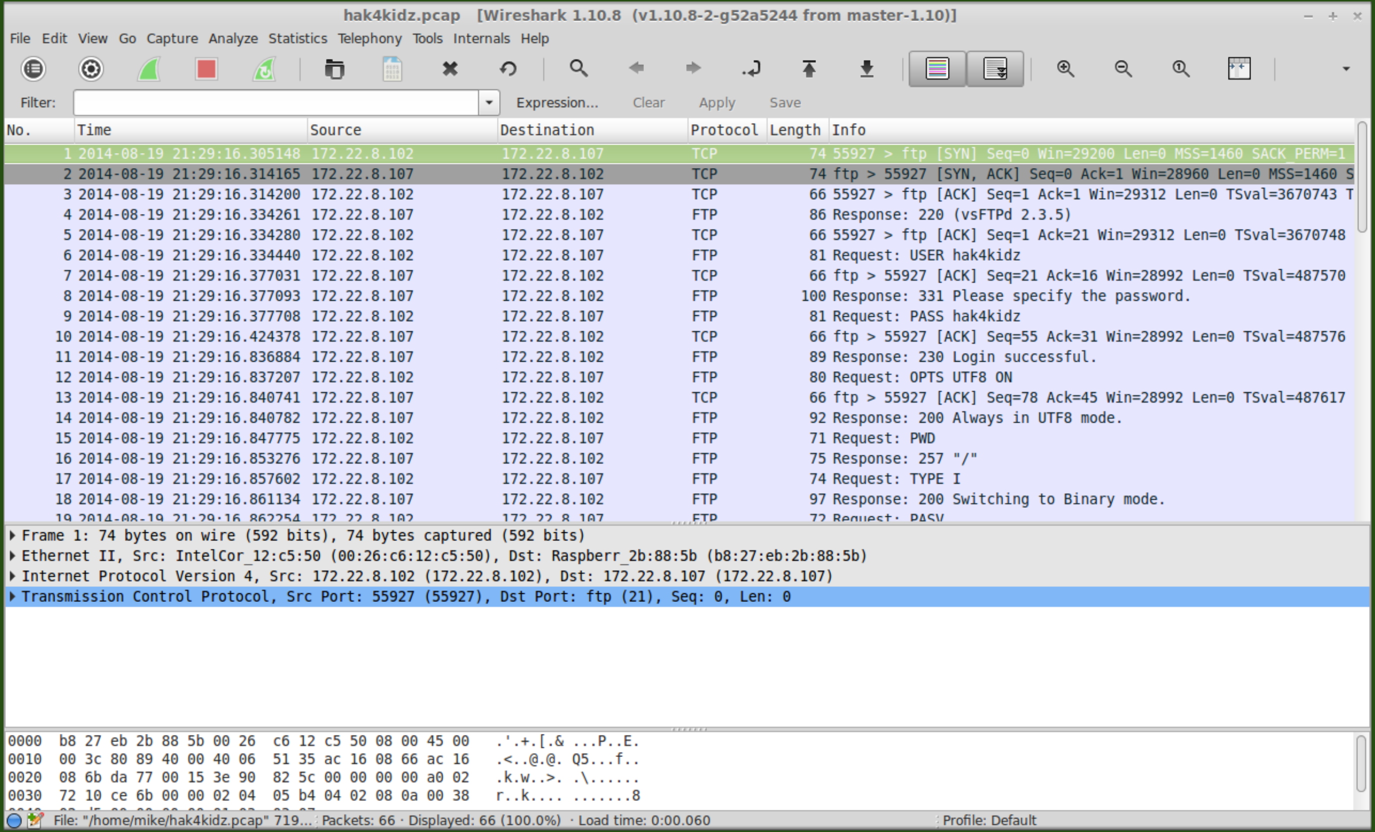
Open Recent:

/home/mike/hak4kidz.pcap (7195 bytes)

Sample Captures

A rich assortment of example capture files on the wiki

Looking at the Capture



hak4kidz.pcap [Wireshark 1.10.8 (v1.10.8-2-g52a5244 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression...
Clear
Apply
Save

```
No.  Time                        Source         Destination    Protocol Length Info
   1 2014-08-19 21:29:16.305148 172.22.8.102   172.22.8.107   TCP        74 55927 > ftp [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1
   2 2014-08-19 21:29:16.314165 172.22.8.107   172.22.8.102   TCP        74 ftp > 55927 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 S
   3 2014-08-19 21:29:16.314200 172.22.8.102   172.22.8.107   TCP        66 55927 > ftp [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3670743 T
   4 2014-08-19 21:29:16.334261 172.22.8.107   172.22.8.102   FTP        86 Response: 220 (vsFTPd 2.3.5)
   5 2014-08-19 21:29:16.334280 172.22.8.102   172.22.8.107   TCP        66 55927 > ftp [ACK] Seq=1 Ack=21 Win=29312 Len=0 TSval=3670748
   6 2014-08-19 21:29:16.334440 172.22.8.102   172.22.8.107   FTP        81 Request: USER hak4kidz
   7 2014-08-19 21:29:16.377031 172.22.8.107   172.22.8.102   TCP        66 ftp > 55927 [ACK] Seq=21 Ack=16 Win=28992 Len=0 TSval=487570
   8 2014-08-19 21:29:16.377093 172.22.8.107   172.22.8.102   FTP       100 Response: 331 Please specify the password.
   9 2014-08-19 21:29:16.377708 172.22.8.102   172.22.8.107   FTP        81 Request: PASS hak4kidz
  10 2014-08-19 21:29:16.424378 172.22.8.107   172.22.8.102   TCP        66 ftp > 55927 [ACK] Seq=55 Ack=31 Win=28992 Len=0 TSval=487576
  11 2014-08-19 21:29:16.836884 172.22.8.107   172.22.8.102   FTP        89 Response: 230 Login successful.
  12 2014-08-19 21:29:16.837207 172.22.8.102   172.22.8.107   FTP        80 Request: OPTS UTF8 ON
  13 2014-08-19 21:29:16.840741 172.22.8.107   172.22.8.102   TCP        66 ftp > 55927 [ACK] Seq=78 Ack=45 Win=28992 Len=0 TSval=487617
  14 2014-08-19 21:29:16.840782 172.22.8.107   172.22.8.102   FTP        92 Response: 200 Always in UTF8 mode.
  15 2014-08-19 21:29:16.847775 172.22.8.102   172.22.8.107   FTP        71 Request: PWD
  16 2014-08-19 21:29:16.853276 172.22.8.107   172.22.8.102   FTP        75 Response: 257 "/"
  17 2014-08-19 21:29:16.857602 172.22.8.102   172.22.8.107   FTP        74 Request: TYPE I
  18 2014-08-19 21:29:16.861134 172.22.8.107   172.22.8.102   FTP        97 Response: 200 Switching to Binary mode.
  19 2014-08-19 21:29:16.862254 172.22.8.102   172.22.8.107   FTP        72 Request: PASV
```

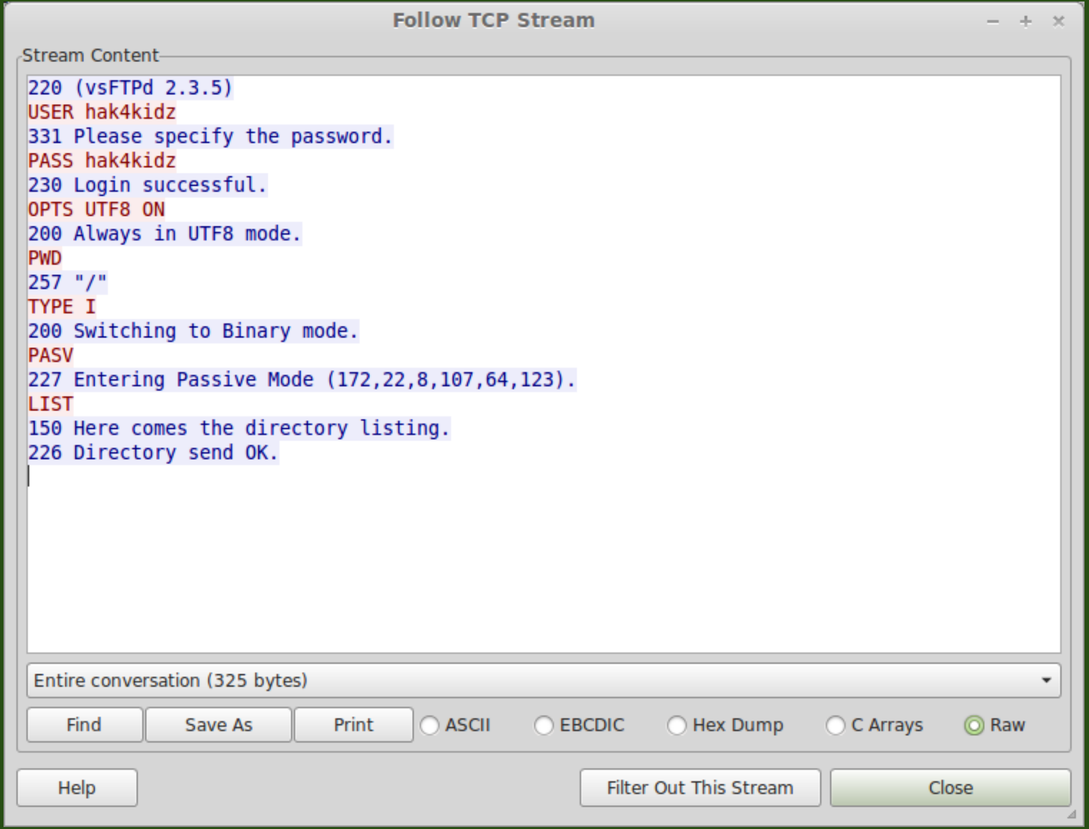
```
▸ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
▸ Ethernet II, Src: IntelCor_12:c5:50 (00:26:c6:12:c5:50), Dst: Raspberr_2b:88:5b (b8:27:eb:2b:88:5b)
▸ Internet Protocol Version 4, Src: 172.22.8.102 (172.22.8.102), Dst: 172.22.8.107 (172.22.8.107)
▸ Transmission Control Protocol, Src Port: 55927 (55927), Dst Port: ftp (21), Seq: 0, Len: 0
```

```
0000  b8 27 eb 2b 88 5b 00 26  c6 12 c5 50 08 00 45 00   .'.+.[.& ...P..E.
0010  00 3c 80 89 40 00 40 06  51 35 ac 16 08 66 ac 16   .<..@.@. Q5...f..
0020  08 6b da 77 00 15 3e 90  82 5c 00 00 00 00 a0 02   .k.w..>. .\......
0030  72 10 ce 6b 00 00 02 04  05 b4 04 02 08 0a 00 38   r..k.... .......8
```

File: "/home/mike/hak4kidz.pcap" 719... Packets: 66 · Displayed: 66 (100.0%) · Load time: 0:00.060 Profile: Default

Looking at the Capture

OMG I totes have the user and password!!



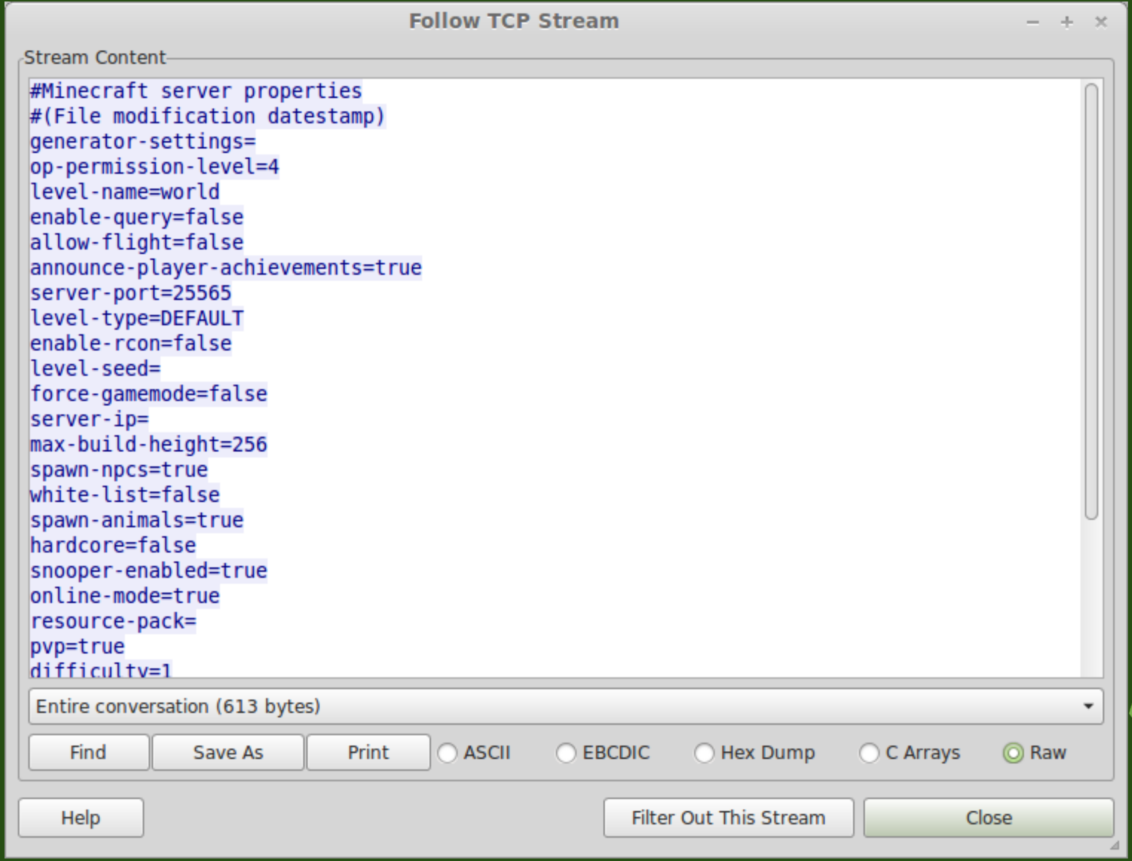
```
220 (vsFTPd 2.3.5)
USER hak4kidz
331 Please specify the password.
PASS hak4kidz
230 Login successful.
OPTS UTF8 ON
200 Always in UTF8 mode.
PWD
257 "/"
TYPE I
200 Switching to Binary mode.
PASV
227 Entering Passive Mode (172,22,8,107,64,123).
LIST
150 Here comes the directory listing.
226 Directory send OK.
```

Entire conversation (325 bytes)

○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

Looking at the Capture

hmm there's the file I wanted. I guess I don't need to pull it off the server.



```
#Minecraft server properties
#(File modification datestamp)
generator-settings=
op-permission-level=4
level-name=world
enable-query=false
allow-flight=false
announce-player-achievements=true
server-port=25565
level-type=DEFAULT
enable-rcon=false
level-seed=
force-gamemode=false
server-ip=
max-build-height=256
spawn-npcs=true
white-list=false
spawn-animals=true
hardcore=false
snooper-enabled=true
online-mode=true
resource-pack=
pvp=true
difficulty=1
```

Entire conversation (613 bytes)

Demonstration!

Don’t mess this up ol’ Gill really needs this!

The End?

- What more can you do?
- Questions?

Contact

@irishjack twitter

irishjack@methodicallyaimless.net

Special Thanks

- Grape Ape @grap3_ap3
- Heal Wit’ Hans @DSchwartzberg
- Sherman Chong
- La Dosa Nostra @ladosanostra #LDN