Spying on my Network for a Day: Data Analysis for Networks.

PyData
Berlin 2017

Speaker: Aisha Bello
Cisco Systems
Virtual Systems Engineer (Data Center and Virtualization Practice)
Twitter: @AishaXBello

GitHub: https://github.com/shante66/pydata-berlin-2017

Frequently our home network inexplicably slows to a crawl. Sometimes it’s a phone backing up through the narrow upload bandwidth of our DSL line, but sometimes it’s not. A missed device? line problem? neighbor? The NSA? Who knows? - Quora

I have a lot of Questions

- How do I know what’s taking up all my network bandwidth?
- How do I capture my own data
- Where would I store it
- When Is the best time to collect my network data
- Now that I have my data How do I analyze it?

Experimentation setup

1. Operating System: Windows 8.1
2. Internet Speed

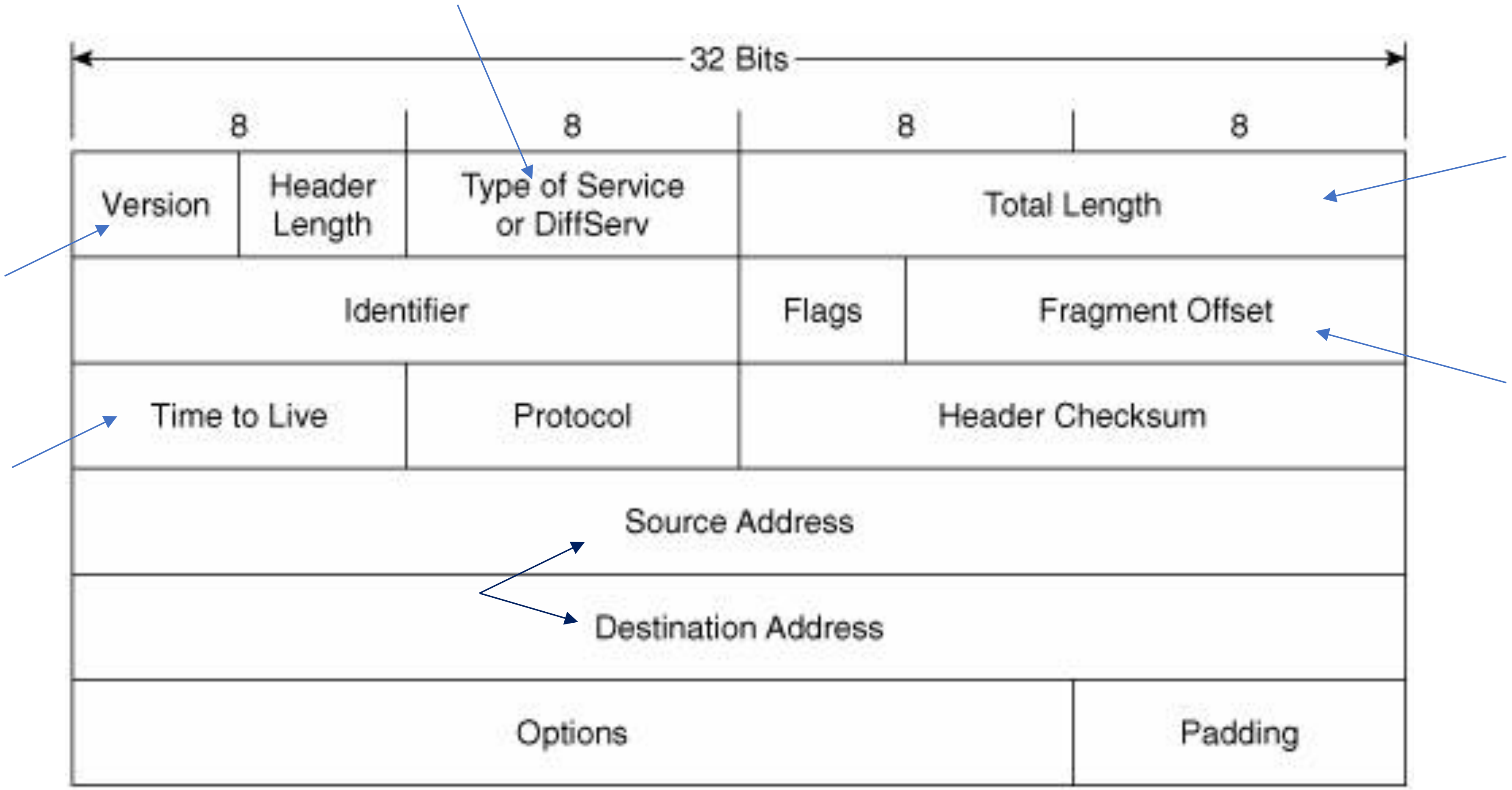
- Download : 100Mbps
- Upload : 10Mbps

3. Type of machine: Lenovo PC
4. Applications used: Wireshark, Bokeh, Jupyter

But Before… Network 101

Let’s Get some Domain knowledge

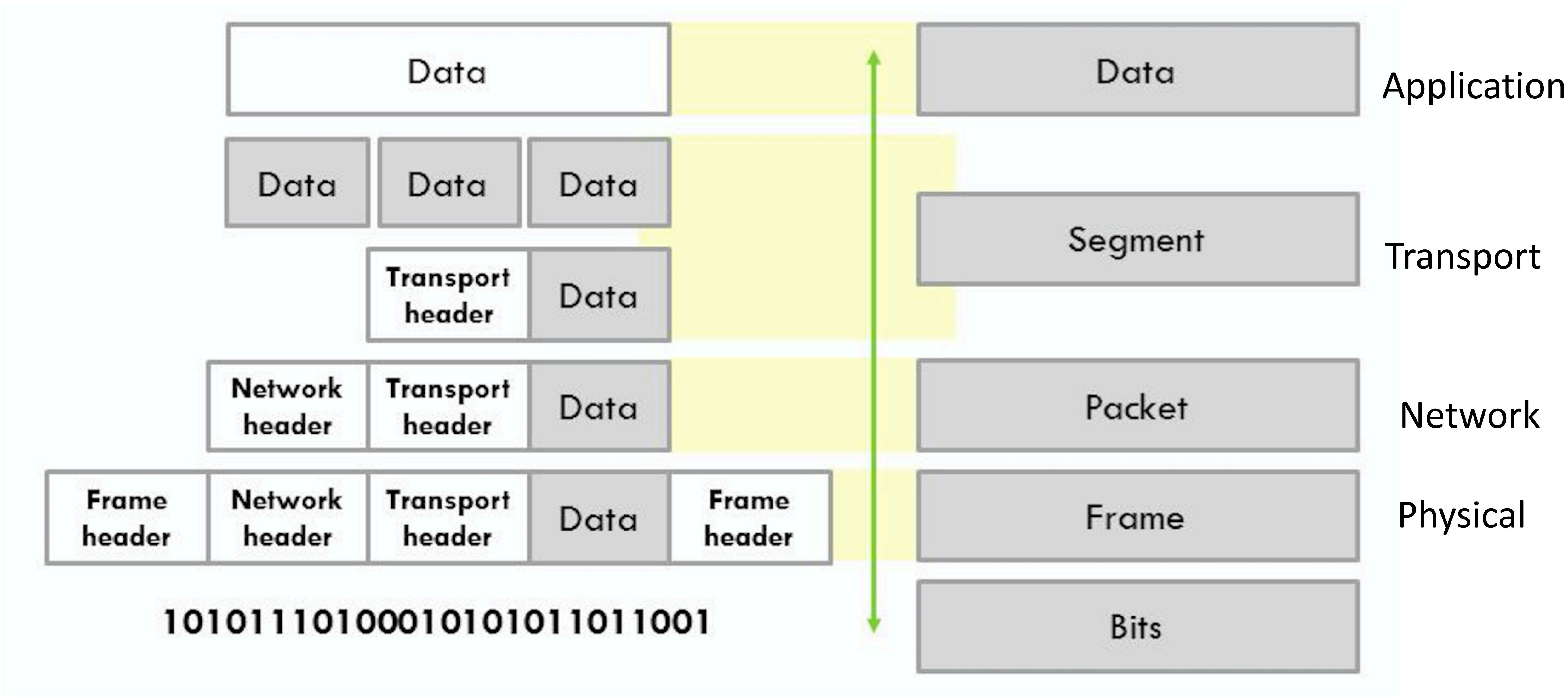
THE IP PACKET

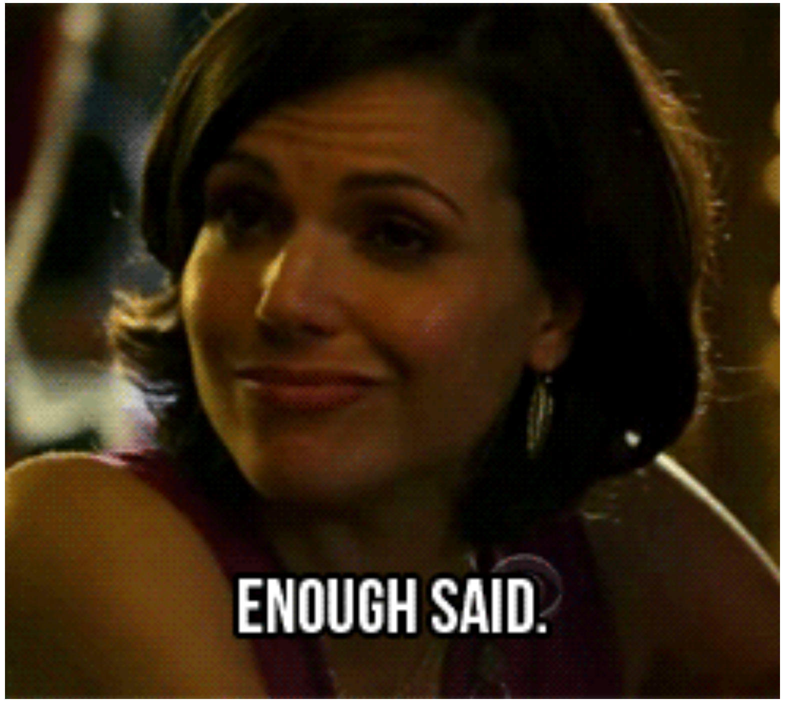


<table>
<tr><th colspan="8">32 Bits</th></tr>
<tr><th colspan="2">8</th><th colspan="2">8</th><th colspan="2">8</th><th colspan="2">8</th></tr>
<tr><td>Version</td><td>Header Length</td><td colspan="2">Type of Service or DiffServ</td><td colspan="4">Total Length</td></tr>
<tr><td colspan="4">Identifier</td><td>Flags</td><td colspan="3">Fragment Offset</td></tr>
<tr><td colspan="2">Time to Live</td><td colspan="2">Protocol</td><td colspan="4">Header Checksum</td></tr>
<tr><td colspan="8">Source Address</td></tr>
<tr><td colspan="8">Destination Address</td></tr>
<tr><td colspan="6">Options</td><td colspan="2">Padding</td></tr>
</table>

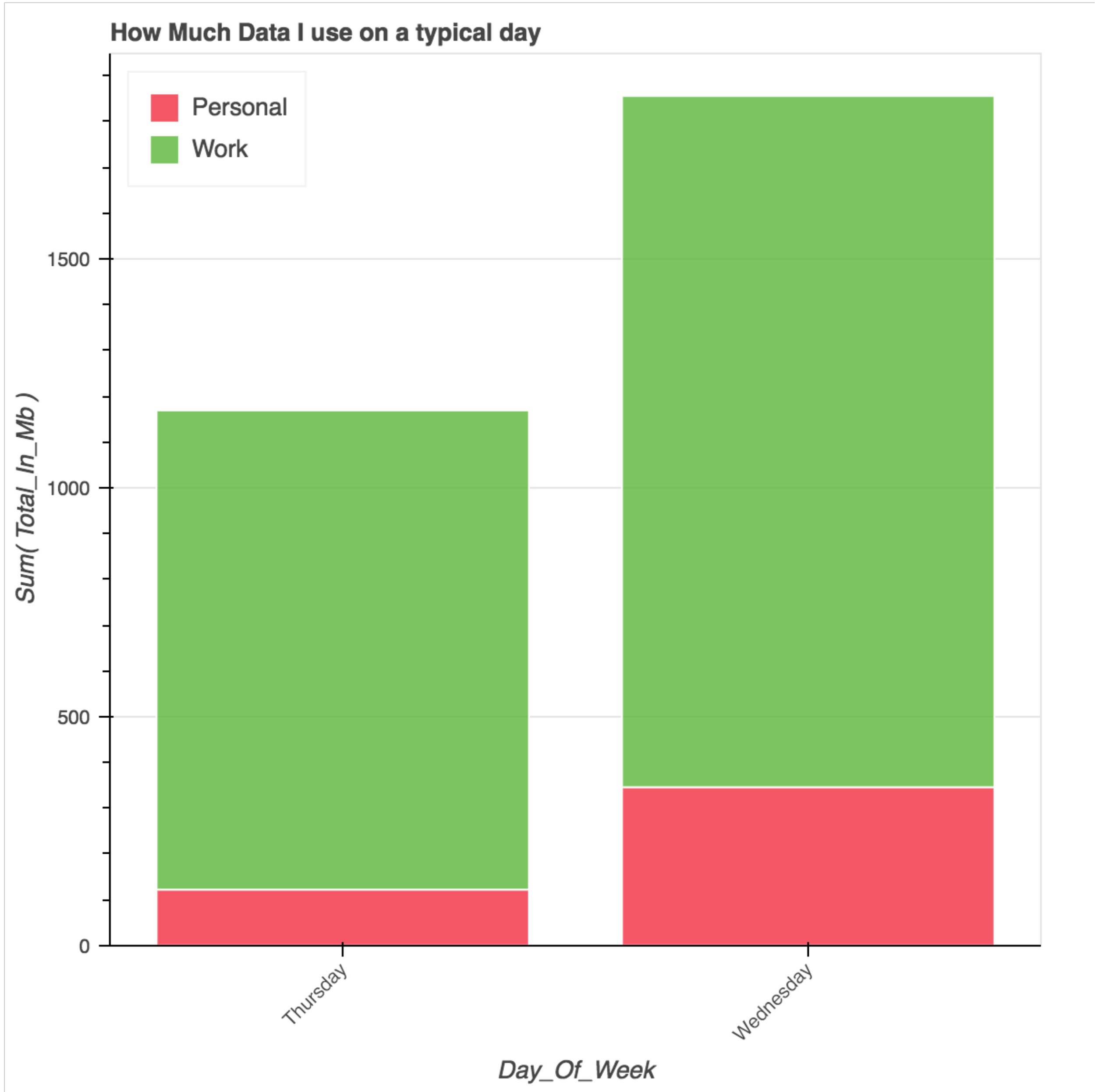
Payload

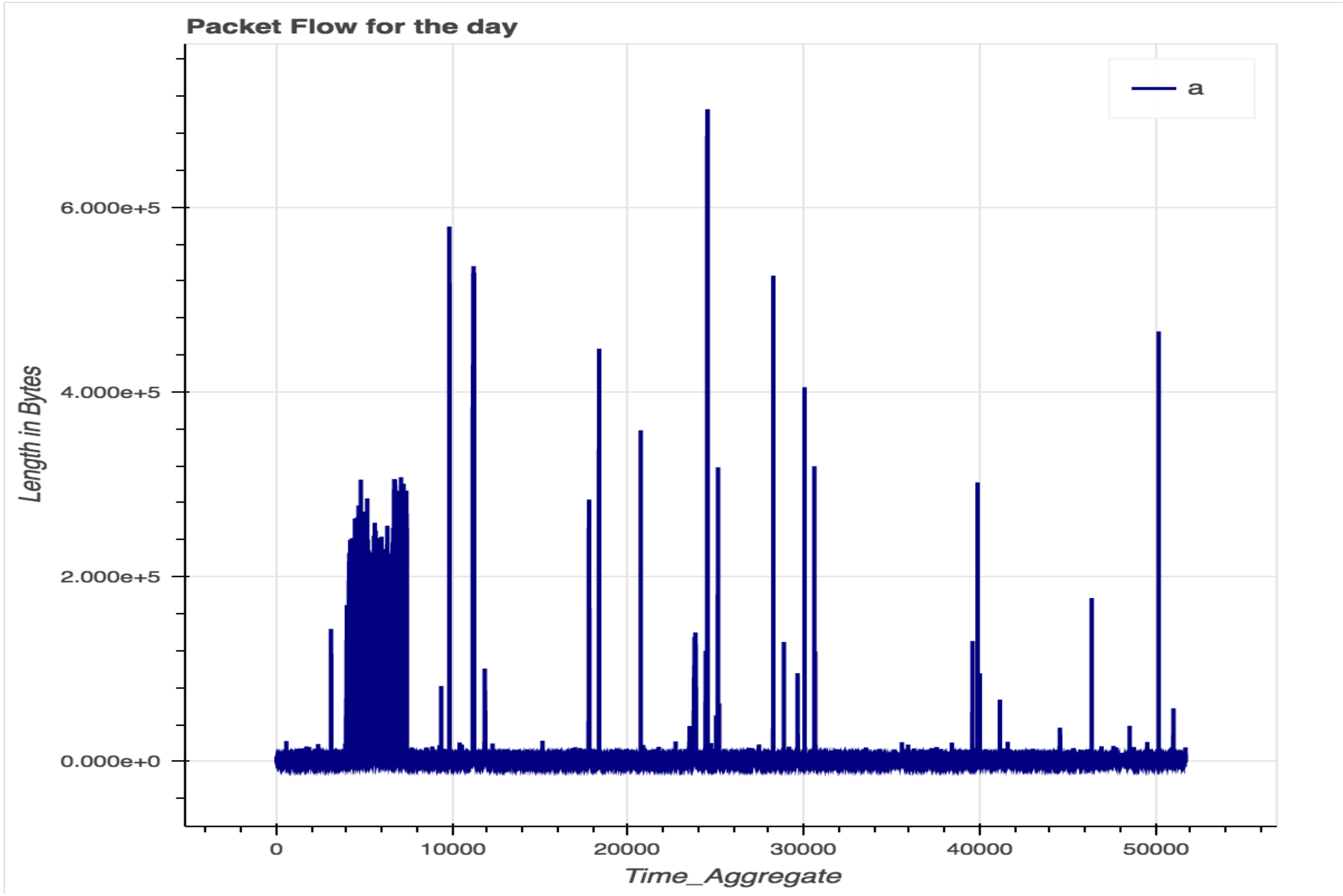
Encapsulation and De-capsulation in TCP/IP Model



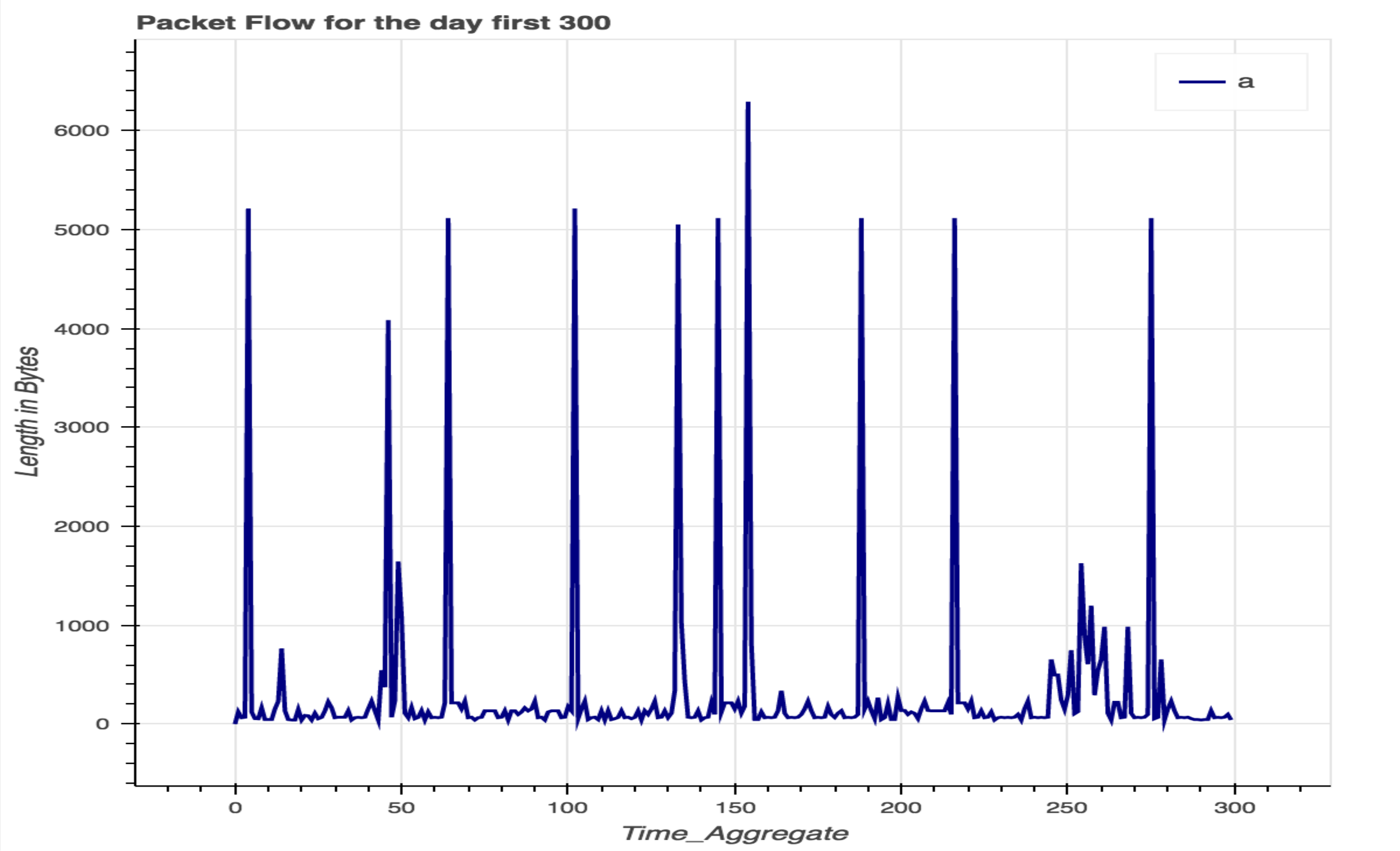


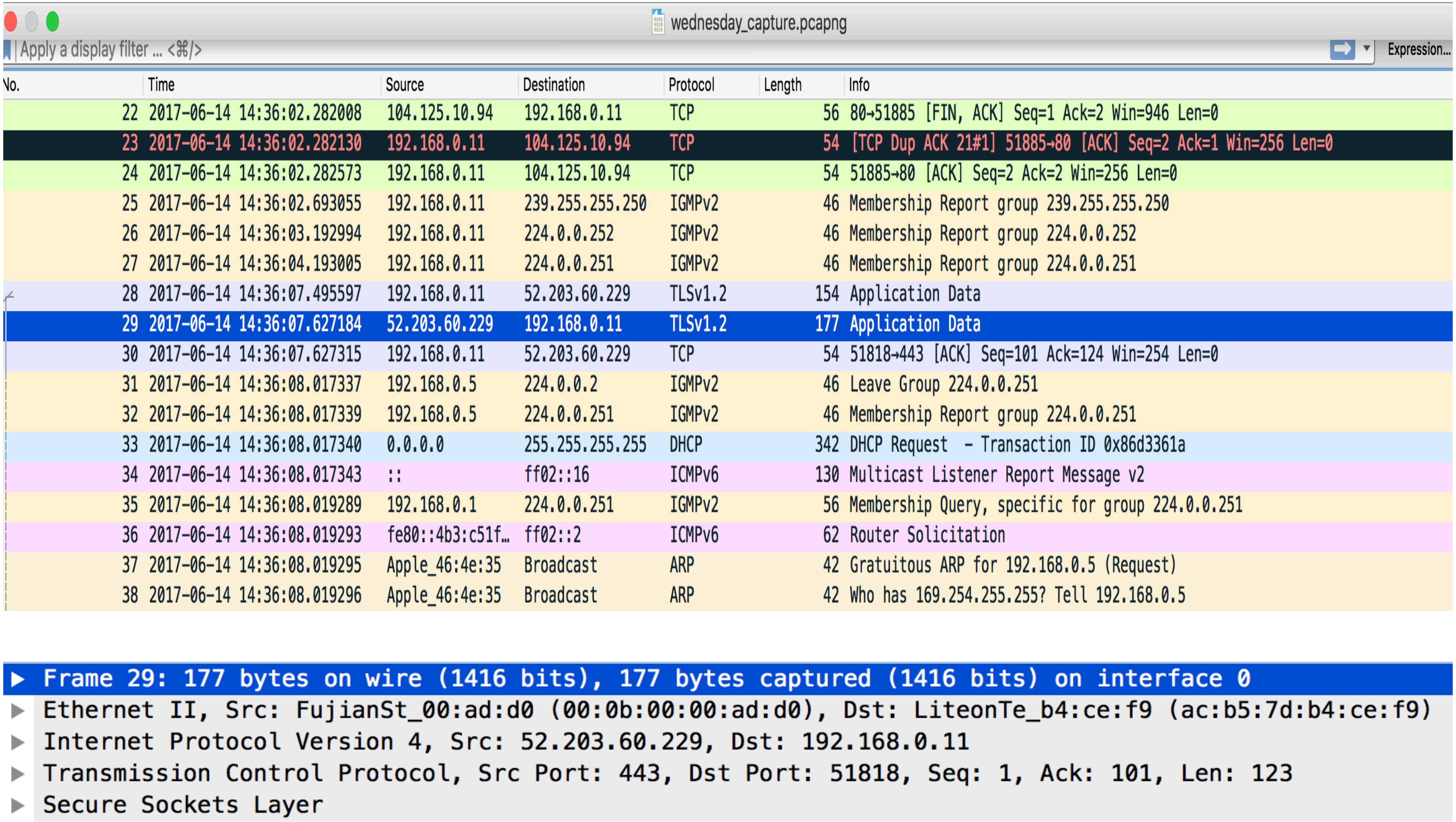
How much data on an average do I generate on a daily basis?


How Much Data I use on a typical day
🟥 Personal
🟩 Work
Sum(Total_In_Mb)
1500
1000
500
0
Thursday
Wednesday
Day_Of_Week


Packet Flow for the day
a
Length in Bytes
6.000e+5
4.000e+5
2.000e+5
0.000e+0
0
10000
20000
30000
40000
50000
Time_Aggregate

Zooming In ...

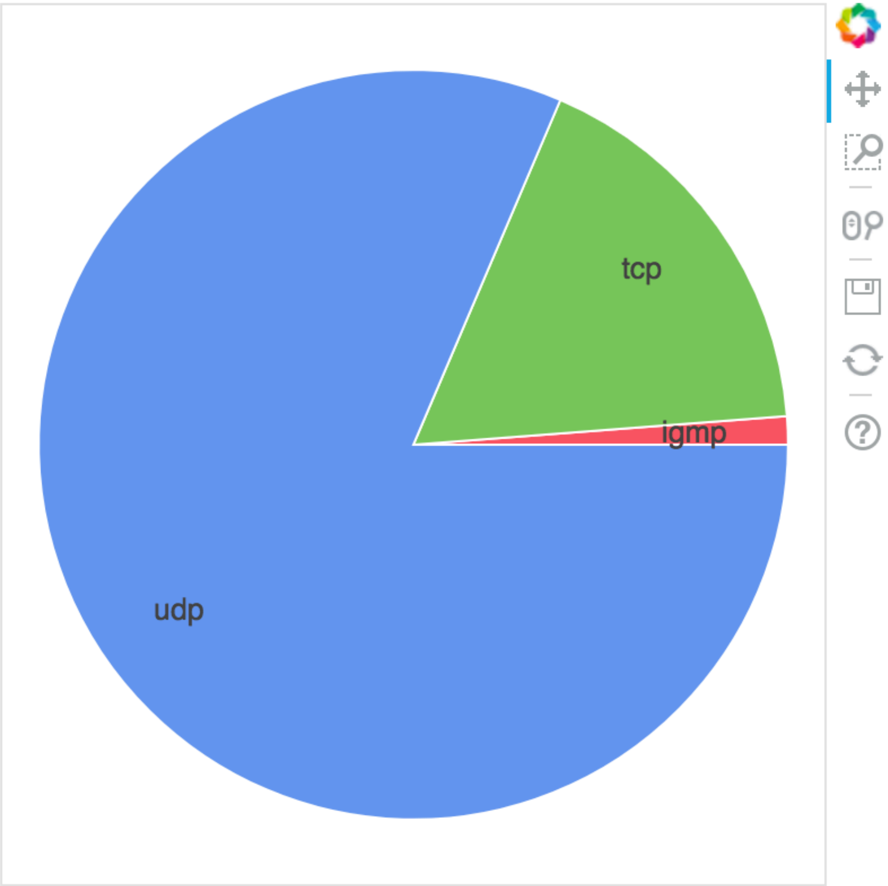

Packet Flow for the day first 300
a
Length in Bytes
6000
5000
4000
3000
2000
1000
0
0
50
100
150
200
250
300
Time_Aggregate

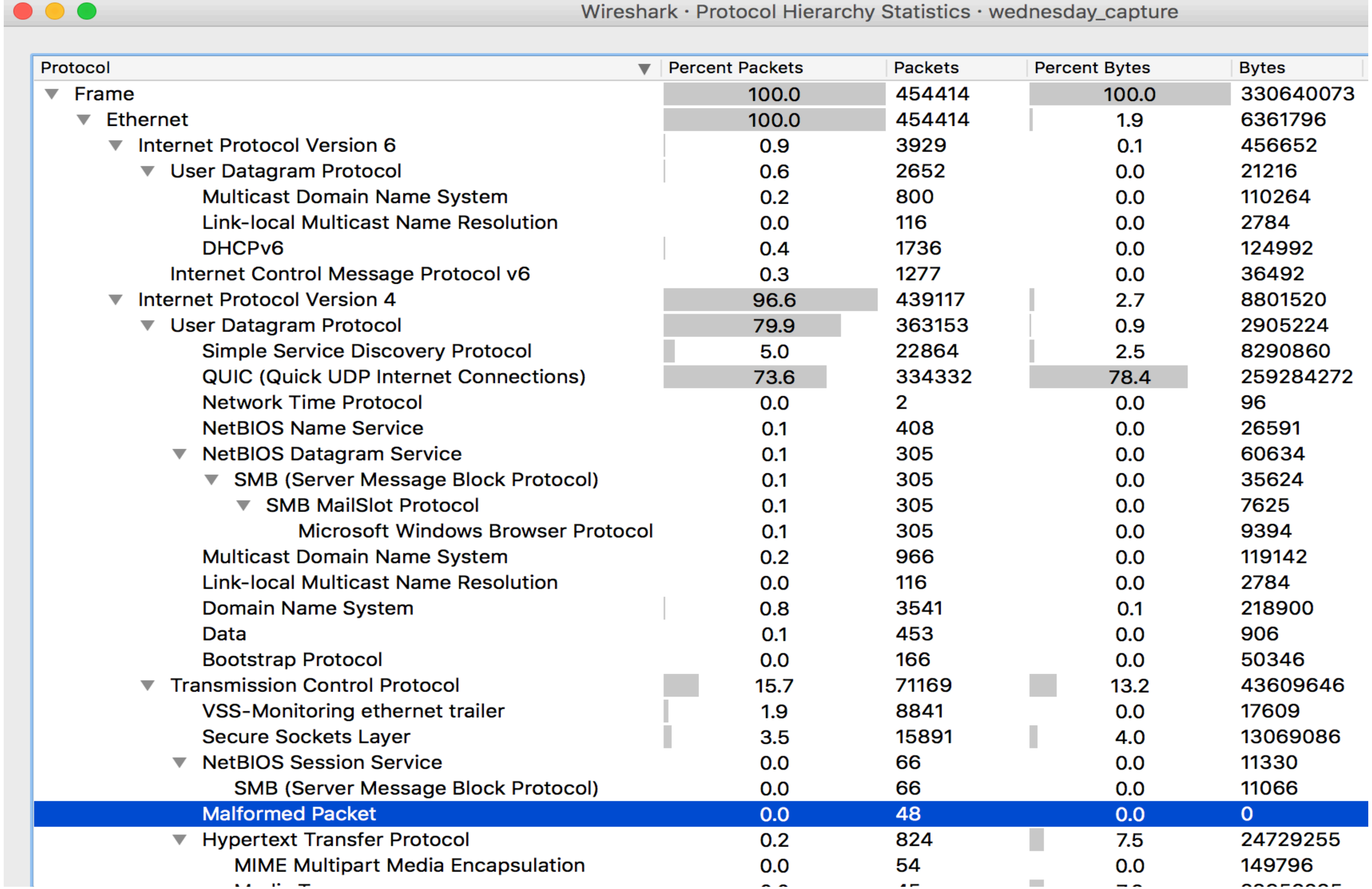


No.	Time	Source	Destination	Protocol	Length	Info
22	2017-06-14 14:36:02.282008	104.125.10.94	192.168.0.11	TCP	56	80→51885 [FIN, ACK] Seq=1 Ack=2 Win=946 Len=0
23	2017-06-14 14:36:02.282130	192.168.0.11	104.125.10.94	TCP	54	[TCP Dup ACK 21#1] 51885→80 [ACK] Seq=2 Ack=1 Win=256 Len=0
24	2017-06-14 14:36:02.282573	192.168.0.11	104.125.10.94	TCP	54	51885→80 [ACK] Seq=2 Ack=2 Win=256 Len=0
25	2017-06-14 14:36:02.693055	192.168.0.11	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
26	2017-06-14 14:36:03.192994	192.168.0.11	224.0.0.252	IGMPv2	46	Membership Report group 224.0.0.252
27	2017-06-14 14:36:04.193005	192.168.0.11	224.0.0.251	IGMPv2	46	Membership Report group 224.0.0.251
28	2017-06-14 14:36:07.495597	192.168.0.11	52.203.60.229	TLSv1.2	154	Application Data
29	2017-06-14 14:36:07.627184	52.203.60.229	192.168.0.11	TLSv1.2	177	Application Data
30	2017-06-14 14:36:07.627315	192.168.0.11	52.203.60.229	TCP	54	51818→443 [ACK] Seq=101 Ack=124 Win=254 Len=0
31	2017-06-14 14:36:08.017337	192.168.0.5	224.0.0.2	IGMPv2	46	Leave Group 224.0.0.251
32	2017-06-14 14:36:08.017339	192.168.0.5	224.0.0.251	IGMPv2	46	Membership Report group 224.0.0.251
33	2017-06-14 14:36:08.017340	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x86d3361a
34	2017-06-14 14:36:08.017343	::	ff02::16	ICMPv6	130	Multicast Listener Report Message v2
35	2017-06-14 14:36:08.019289	192.168.0.1	224.0.0.251	IGMPv2	56	Membership Query, specific for group 224.0.0.251
36	2017-06-14 14:36:08.019293	fe80::4b3:c51f…	ff02::2	ICMPv6	62	Router Solicitation
37	2017-06-14 14:36:08.019295	Apple_46:4e:35	Broadcast	ARP	42	Gratuitous ARP for 192.168.0.5 (Request)
38	2017-06-14 14:36:08.019296	Apple_46:4e:35	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.0.5

```
▶ Frame 29: 177 bytes on wire (1416 bits), 177 bytes captured (1416 bits) on interface 0
▶ Ethernet II, Src: FujianSt_00:ad:d0 (00:0b:00:00:ad:d0), Dst: LiteonTe_b4:ce:f9 (ac:b5:7d:b4:ce:f9)
▶ Internet Protocol Version 4, Src: 52.203.60.229, Dst: 192.168.0.11
▶ Transmission Control Protocol, Src Port: 443, Dst Port: 51818, Seq: 1, Ack: 101, Len: 123
▶ Secure Sockets Layer
```

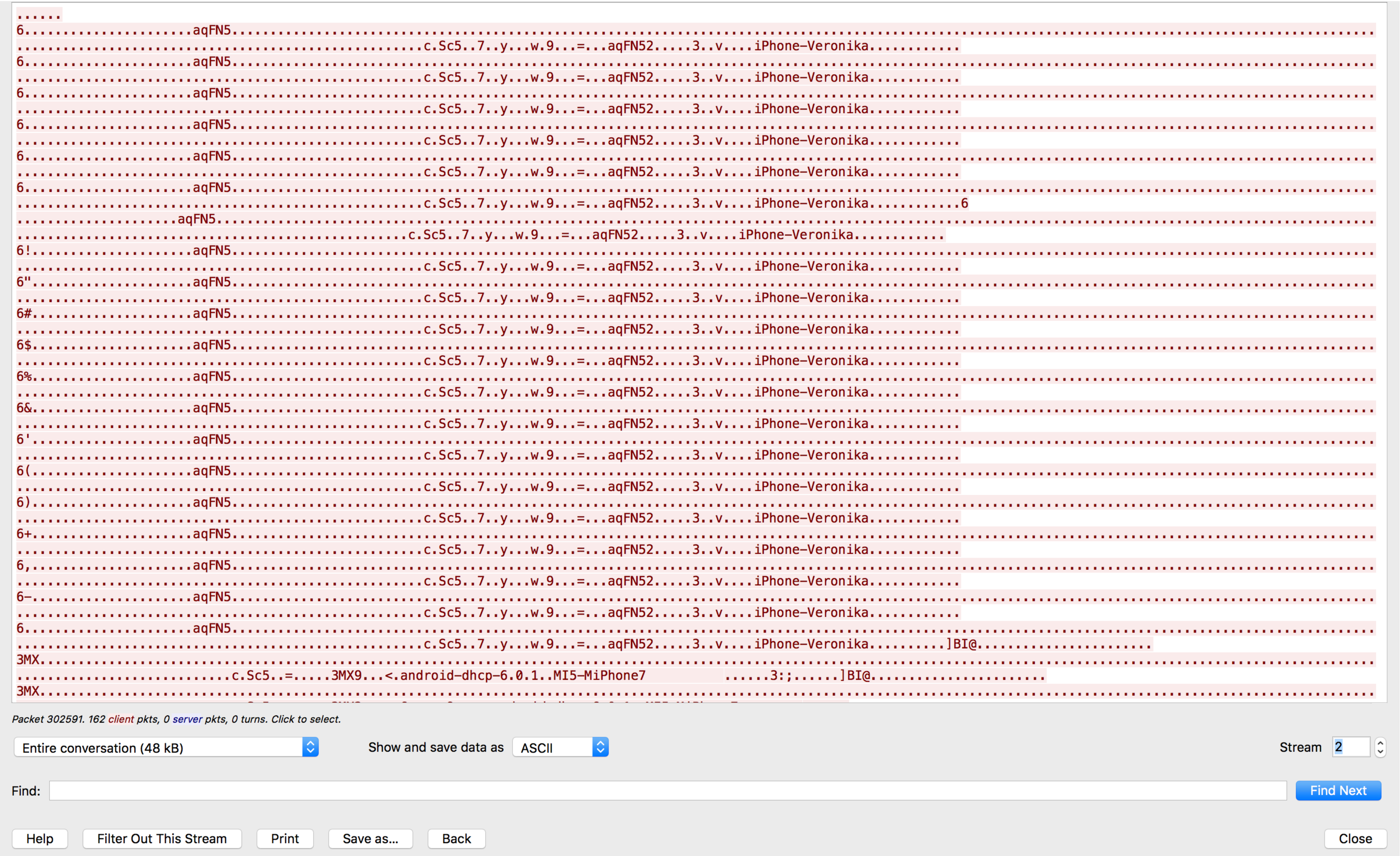
Where do I spend the most of my bandwidth on ?





Wireshark · Protocol Hierarchy Statistics · wednesday_capture

Protocol	Percent Packets	Packets	Percent Bytes	Bytes
▼ Frame	100.0	454414	100.0	330640073
▼ Ethernet	100.0	454414	1.9	6361796
▼ Internet Protocol Version 6	0.9	3929	0.1	456652
▼ User Datagram Protocol	0.6	2652	0.0	21216
Multicast Domain Name System	0.2	800	0.0	110264
Link-local Multicast Name Resolution	0.0	116	0.0	2784
DHCPv6	0.4	1736	0.0	124992
Internet Control Message Protocol v6	0.3	1277	0.0	36492
▼ Internet Protocol Version 4	96.6	439117	2.7	8801520
▼ User Datagram Protocol	79.9	363153	0.9	2905224
Simple Service Discovery Protocol	5.0	22864	2.5	8290860
QUIC (Quick UDP Internet Connections)	73.6	334332	78.4	259284272
Network Time Protocol	0.0	2	0.0	96
NetBIOS Name Service	0.1	408	0.0	26591
▼ NetBIOS Datagram Service	0.1	305	0.0	60634
▼ SMB (Server Message Block Protocol)	0.1	305	0.0	35624
▼ SMB MailSlot Protocol	0.1	305	0.0	7625
Microsoft Windows Browser Protocol	0.1	305	0.0	9394
Multicast Domain Name System	0.2	966	0.0	119142
Link-local Multicast Name Resolution	0.0	116	0.0	2784
Domain Name System	0.8	3541	0.1	218900
Data	0.1	453	0.0	906
Bootstrap Protocol	0.0	166	0.0	50346
▼ Transmission Control Protocol	15.7	71169	13.2	43609646
VSS-Monitoring ethernet trailer	1.9	8841	0.0	17609
Secure Sockets Layer	3.5	15891	4.0	13069086
▼ NetBIOS Session Service	0.0	66	0.0	11330
SMB (Server Message Block Protocol)	0.0	66	0.0	11066
Malformed Packet	0.0	48	0.0	0
▼ Hypertext Transfer Protocol	0.2	824	7.5	24729255
MIME Multipart Media Encapsulation	0.0	54	0.0	149796



```
......
6......................aqFN5......................................................................................................................................................
.....................................................c.Sc5..7..y...w.9...=...aqFN52.....3..v....iPhone-Veronika............
6......................aqFN5......................................................................................................................................................
.....................................................c.Sc5..7..y...w.9...=...aqFN52.....3..v....iPhone-Veronika............
6......................aqFN5......................................................................................................................................................
.....................................................c.Sc5..7..y...w.9...=...aqFN52.....3..v....iPhone-Veronika............
6......................aqFN5......................................................................................................................................................
.....................................................c.Sc5..7..y...w.9...=...aqFN52.....3..v....iPhone-Veronika............
6......................aqFN5......................................................................................................................................................
.....................................................c.Sc5..7..y...w.9...=...aqFN52.....3..v....iPhone-Veronika............
6......................aqFN5......................................................................................................................................................
.....................................................c.Sc5..7..y...w.9...=...aqFN52.....3..v....iPhone-Veronika............6
.....................aqFN5........................................................................................................................................................
...................................................c.Sc5..7..y...w.9...=...aqFN52.....3..v....iPhone-Veronika............
6!.....................aqFN5......................................................................................................................................................
.....................................................c.Sc5..7..y...w.9...=...aqFN52.....3..v....iPhone-Veronika............
6".....................aqFN5......................................................................................................................................................
.....................................................c.Sc5..7..y...w.9...=...aqFN52.....3..v....iPhone-Veronika............
6#.....................aqFN5......................................................................................................................................................
.....................................................c.Sc5..7..y...w.9...=...aqFN52.....3..v....iPhone-Veronika............
6$.....................aqFN5......................................................................................................................................................
.....................................................c.Sc5..7..y...w.9...=...aqFN52.....3..v....iPhone-Veronika............
6%.....................aqFN5......................................................................................................................................................
.....................................................c.Sc5..7..y...w.9...=...aqFN52.....3..v....iPhone-Veronika............
6&.....................aqFN5......................................................................................................................................................
.....................................................c.Sc5..7..y...w.9...=...aqFN52.....3..v....iPhone-Veronika............
6'.....................aqFN5......................................................................................................................................................
.....................................................c.Sc5..7..y...w.9...=...aqFN52.....3..v....iPhone-Veronika............
6(.....................aqFN5......................................................................................................................................................
.....................................................c.Sc5..7..y...w.9...=...aqFN52.....3..v....iPhone-Veronika............
6).....................aqFN5......................................................................................................................................................
.....................................................c.Sc5..7..y...w.9...=...aqFN52.....3..v....iPhone-Veronika............
6+.....................aqFN5......................................................................................................................................................
.....................................................c.Sc5..7..y...w.9...=...aqFN52.....3..v....iPhone-Veronika............
6,.....................aqFN5......................................................................................................................................................
.....................................................c.Sc5..7..y...w.9...=...aqFN52.....3..v....iPhone-Veronika............
6-.....................aqFN5......................................................................................................................................................
.....................................................c.Sc5..7..y...w.9...=...aqFN52.....3..v....iPhone-Veronika............
6......................aqFN5......................................................................................................................................................
.....................................................c.Sc5..7..y...w.9...=...aqFN52.....3..v....iPhone-Veronika..........]BI@......................
3MX...............................................................................................................................................................................
............................c.Sc5..=.....3MX9...<.android-dhcp-6.0.1..MI5-MiPhone7          ......3:;......]BI@......................
3MX...............................................................................................................................................................................
```

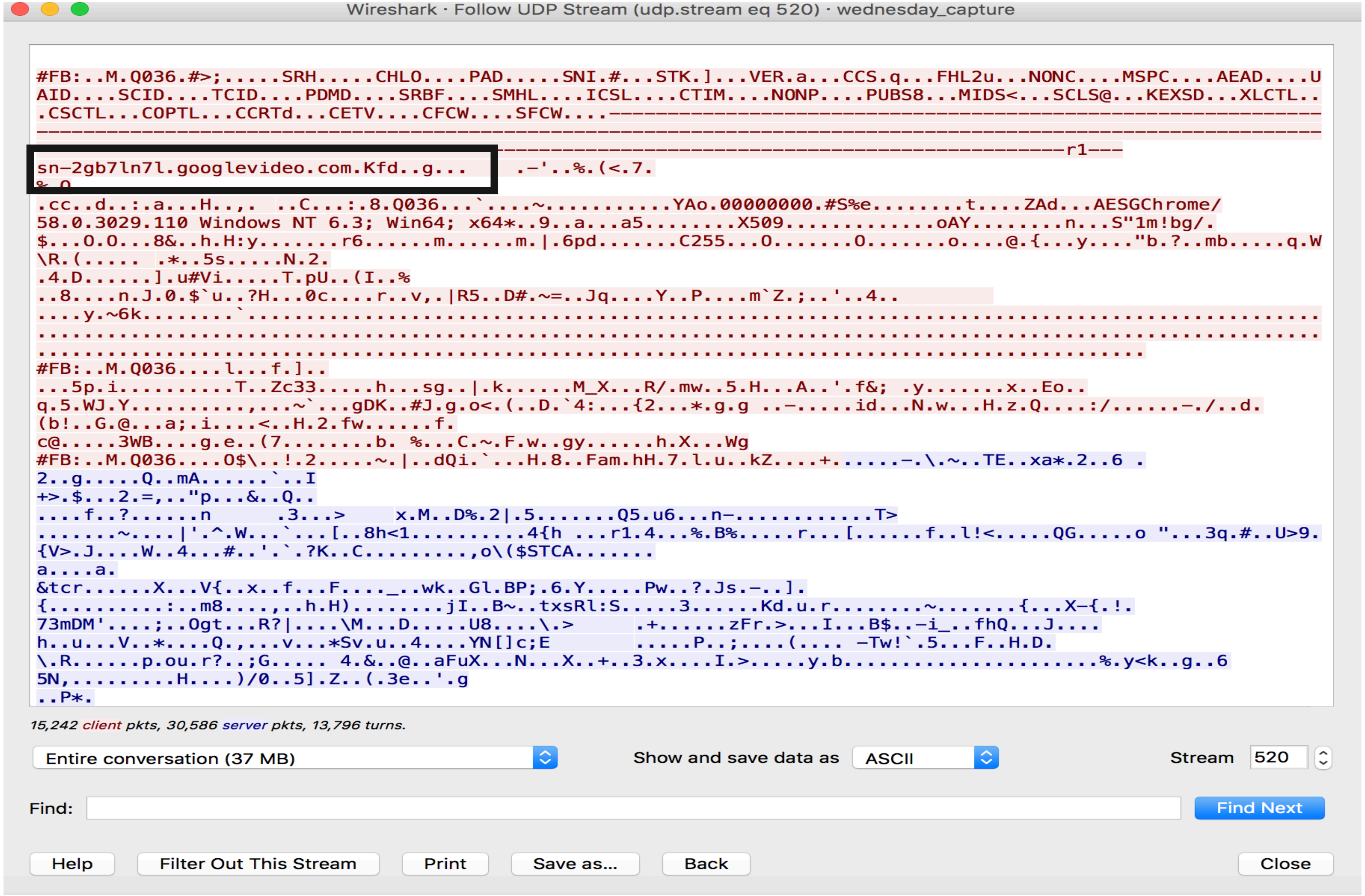
Packet 302591. 162 client pkts, 0 server pkts, 0 turns. Click to select.

Entire conversation (48 kB)

Show and save data as ASCII

Stream 2

Find:



Wireshark · Follow UDP Stream (udp.stream eq 520) · wednesday_capture

```
#FB:..M.Q036.#>;.....SRH.....CHLO....PAD.....SNI.#...STK.]...VER.a...CCS.q...FHL2u...NONC....MSPC....AEAD....U
AID....SCID....TCID....PDMD....SRBF....SMHL....ICSL....CTIM....NONP....PUBS8...MIDS<...SCLS@...KEXSD...XLCTL..
.CSCTL...COPTL...CCRTd...CETV....CFCW....SFCW....--------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------r1---
sn-2gb7ln7l.googlevideo.com.Kfd..g...   .-'..%.(<.7.
%.Q
.cc..d..:.a...H..,.  ..C...:.8.Q036...`....~...........YAo.00000000.#S%e........t....ZAd...AESGChrome/
58.0.3029.110 Windows NT 6.3; Win64; x64*..9..a...a5........X509.............oAY........n...S"1m!bg/.
$...O.O...8&..h.H:y.......r6......m......m.|.6pd.......C255...O.......O.......o....@.{...y...."b.?..mb.....q.W
\R.(.....  .*..5s.....N.2.
.4.D......].u#Vi.....T.pU..(I..%
..8....n.J.0.$`u..?H...0c....r..v,.|R5..D#.~=..Jq....Y..P....m`Z.;..'..4..
....y.~6k.......`...............................................................................................
.............................................................................................................
...............................................................................................
#FB:..M.Q036....l...f.]..
...5p.i..........T..Zc33.....h...sg..|.k......M_X...R/.mw..5.H...A..'.f&; .y.......x..Eo..
q.5.WJ.Y..........,...~`...gDK..#J.g.o<.(..D.`4:...{2...*.g.g ..-.....id...N.w...H.z.Q....:/......-./..d.
(b!..G.@...a;.i....<..H.2.fw......f.
c@.....3WB....g.e..(7........b. %...C.~.F.w..gy......h.X...Wg
#FB:..M.Q036....O$\..!.2.....~.|..dQi.`...H.8..Fam.hH.7.l.u..kZ....+......-.\.~..TE..xa*.2..6 .
2..g.....Q..mA......`..I
+>.$...2.=,.."p...&..Q..
....f..?......n      .3...>     x.M..D%.2|.5.......Q5.u6...n-............T>
.......~....|'.^.W...`...[..8h<1..........4{h ...r1.4...%.B%.....r...[......f..l!<.....QG.....o "...3q.#..U>9.
{V>.J....W..4...#..'.`.?K..C..........,o\($STCA.......
a....a.
&tcr......X...V{..x..f...F...._..wk..Gl.BP;.6.Y.....Pw..?.Js.-..].
{..........:..m8....,..h.H).........jI..B~..txsRl:S.....3......Kd.u.r.........~.......{...X-{.!.
73mDM'....;..Ogt...R?|....\M...D.....U8....\.>       .+......zFr.>...I...B$..-i_..fhQ...J....
h..u...V..*....Q.,...v...*Sv.u..4....YN[]c;E         .....P..;....(.... -Tw!`.5...F..H.D.
\.R......p.ou.r?..;G.....  4.&..@..aFuX...N...X..+..3.x....I.>.....y.b......................%.y<k..g..6
5N,..........H....)/0..5].Z..(.3e..'.g
..P*.
```

15,242 client pkts, 30,586 server pkts, 13,796 turns.

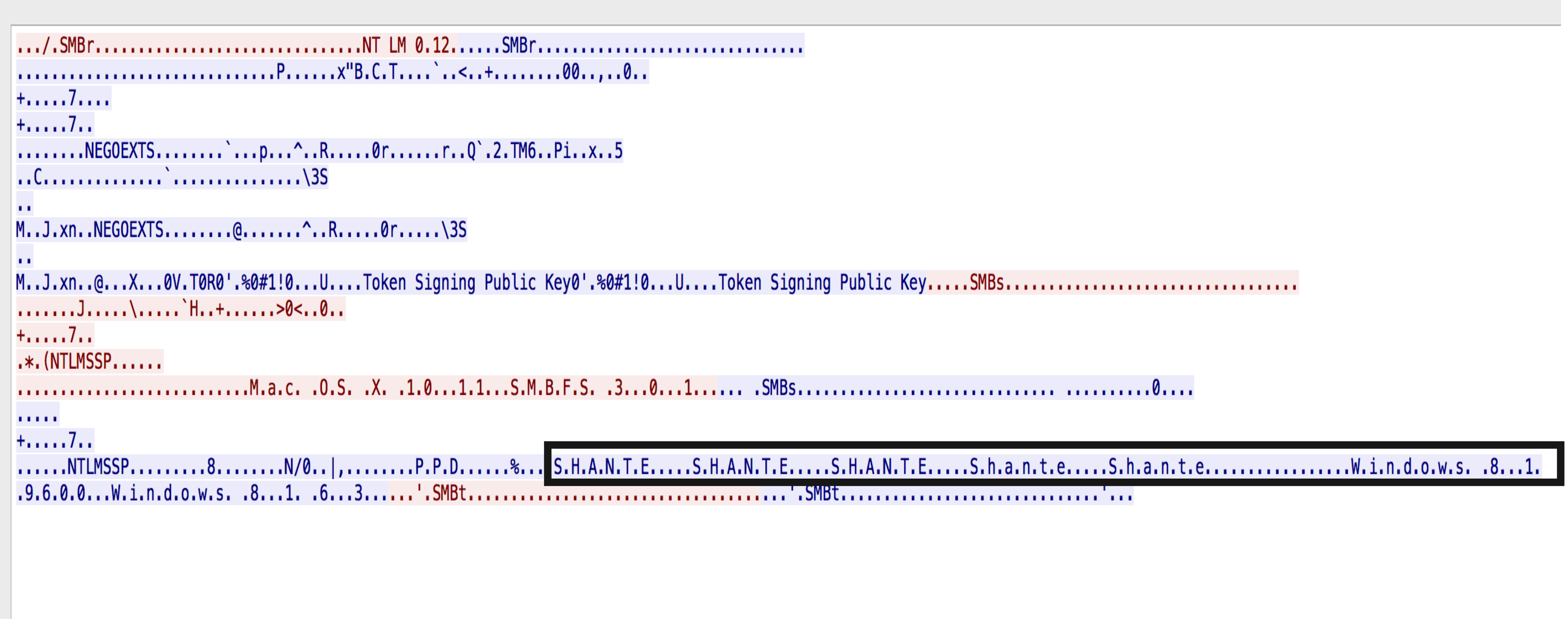
Entire conversation (37 MB)

Show and save data as ASCII

Stream 520

Find:

Guess Who?



```
.../.SMBr..............................NT LM 0.12......SMBr..............................
..............................P......x"B.C.T....`..<..+........00..,..0..
+.....7....
+.....7..
........NEGOEXTS........`...p...^..R.....0r......r..Q`.2.TM6..Pi..x..5
..C..............`...............\3S
..
M..J.xn..NEGOEXTS........@.......^..R.....0r.....\3S
..
M..J.xn..@...X...0V.T0R0'.%0#1!0...U....Token Signing Public Key0'.%0#1!0...U....Token Signing Public Key.....SMBs.................................
.......J.....\.....`H..+......>0<..0..
+.....7..
.*.(NTLMSSP......
...........................M.a.c. .O.S. .X. .1.0...1.1...S.M.B.F.S. .3...0...1...... .SMBs............................. ..........0....
.....
+.....7..
......NTLMSSP.........8........N/0..|,........P.P.D......%...S.H.A.N.T.E.....S.H.A.N.T.E.....S.H.A.N.T.E.....S.h.a.n.t.e.....S.h.a.n.t.e................W.i.n.d.o.w.s. .8...1.
.9.6.0.0...W.i.n.d.o.w.s. .8...1. .6...3......'.SMBt...................................'.SMBt.............................'...
```

Motivation for Analysing your Network

1. There is a lot of Data

2. SERIOUSLY There is even more data

3. Be Your own Police Use Machine Learning

Motivation for Automation

- Detect Intrusions
- Learn, Get Insights , Apply Rules, ReLearn.

You can do this differently…

- Think Layer 7 (Application Layer)

- Think Raspberry Pi or Man in The Middle

You can do this differently…

- Use other Open Source Tools like Snort, Scapy, Moloch ….e.t.c
- Or Hack your router Firmware with OpenWrt…

Notes to Self

- Disable Unnecessary Windows services like service.weather.microsoft.com

- Stella’s blog

- I can tell when someone is home. My mom, Visitors, or a Burgler ?

Questions ?