In [43]:
```
url="https://github.com/rufinachettiar/git/blob/master/shootlog.pcap"
```

In [44]:
```
!curl -o /home/rufina/Documents/github-dropbox/rename/new/git/shootlog.pcap $url
```

```
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 24504    0 24504    0     0   151k      0 --:--:-- --:--:-- --:--:--  152k
```

In [45]:
```
ls -l /home/rufina/Documents/github-dropbox/rename/new/git/shootlog.pcap
```

```
-rw-r--r-- 1 rufina rufina 24504 Mar 24 10:12 /home/rufina/Documents/github-dropbox/rename/new/git/shootlog.pcap
```

In [47]:
```
!tshark -v
```

```
TShark 1.10.6 (v1.10.6 from master-1.10)

Copyright 1998-2014 Gerald Combs <gerald@wireshark.org> and contributors.
This is free software; see the source for copying conditions. There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

Compiled (64-bit) with GLib 2.39.91, with libpcap, with libz 1.2.8, with POSIX
capabilities (Linux), without libnl, with SMI 0.4.8, with c-ares 1.10.0, with
Lua 5.2, without Python, with GnuTLS 2.12.23, with Gcrypt 1.5.3, with MIT
Kerberos, with GeoIP.

Running on Linux 3.13.0-46-generic, with locale en_US.UTF-8, with libpcap
version 1.5.3, with libz 1.2.8.
Intel(R) Xeon(R) CPU E5-1607 v3 @ 3.10GHz

Built using gcc 4.8.2.
```

In [48]:
```
!tshark -n -r /home/rufina/Documents/github-dropbox/rename/new/git/shoot.log -T fields -Eheader=y -e frame.number -e frame
```

In [49]:
```
!head -10 frame.len
```

```
frame.number    frame.len
1       74
2       74
3       66
4       385
5       66
6       623
7       66
8       1514
9       66
```

In [50]:
```
import pandas as pd
```

In [51]:
```
df=pd.read_table("frame.len")
```

In [52]:
```
df
```

Out[52]:

	frame.number	frame.len
0	1	74
1	2	74
2	3	66
3	4	385
4	5	66
5	6	623
6	7	66
7	8	1514
8	9	66
9	10	490
10	11	66
11	12	74
12	13	74
13	14	74
14	15	66
15	16	505

In [53]:
```
df["frame.len"].describe()
```

Out[53]:
```
count     129.000000
mean      164.124031
std       248.922397
min        66.000000
25%        66.000000
50%        66.000000
75%        74.000000
max      1514.000000
Name: frame.len, dtype: float64
```

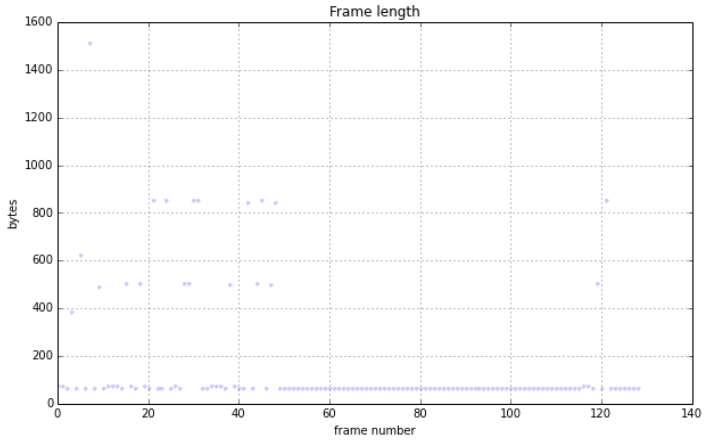
In [54]:
```
%pylab inline
```

```
Populating the interactive namespace from numpy and matplotlib
```

In [55]:
```
figsize(10,6)
```

In [56]:
```
df["frame.len"].plot(style=".", alpha=0.2)
title("Frame length")
ylabel("bytes")
xlabel("frame number")
```

Out[56]:
```
<matplotlib.text.Text at 0x7f40803143d0>
```



In [57]:
```
import subprocess
import datetime
import pandas as pd

def read_pcap(filename, fields=[], display_filter="",
              timeseries=False, strict=False):
    if timeseries:
        fields = ["frame.time_epoch"] + fields
    fieldspec = " ".join("-e %s" % f for f in fields)

    display_filters = fields if strict else []
    if display_filter:
        display_filters.append(display_filter)
    filterspec = "-R '%s'" % " and ".join(f for f in display_filters)

    options = "-r %s -n -T fields -Eheader=y" % filename
    cmd = "tshark %s %s %s" % (options, filterspec, fieldspec)
    proc = subprocess.Popen(cmd, shell = True,
                                 stdout=subprocess.PIPE)
    if timeseries:
        df = pd.read_table(proc.stdout,
                           index_col = "frame.time_epoch",
                           parse_dates=True,
                           date_parser=datetime.datetime.fromtimestamp)
    else:
        df = pd.read_table(proc.stdout)
    return df
```

In [58]:
```
framelen=read_pcap("/home/rufina/Documents/github-dropbox/rename/new/git/shoot.log", ["frame.len"], timeseries=True)
framelen
```

Out[58]:

	frame.len
frame.time_epoch	
2015-03-22 01:57:15.612750	74
2015-03-22 01:57:15.686926	74
2015-03-22 01:57:15.686991	66
2015-03-22 01:57:15.695736	385
2015-03-22 01:57:15.769928	66
2015-03-22 01:57:15.776000	623
2015-03-22 01:57:15.776036	66
2015-03-22 01:57:15.776116	1514

In [59]:
```
bytes_per_second=framelen.resample("S", how="sum")
```

In [60]:
```
bytes_per_second.head()
```

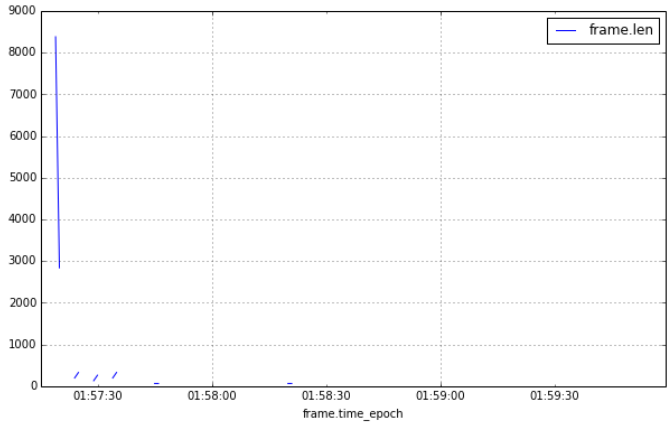
Out[60]:

	frame.len
frame.time_epoch	
2015-03-22 01:57:15	3490
2015-03-22 01:57:16	NaN
2015-03-22 01:57:17	NaN
2015-03-22 01:57:18	NaN
2015-03-22 01:57:19	8384

5 rows × 1 columns

In [61]:
```
bytes_per_second.plot()
```

Out[61]:
```
<matplotlib.axes.AxesSubplot at 0x7f40801dc350>
```



In [62]:
```
fields=["tcp.stream", "ip.src", "ip.dst", "tcp.seq", "tcp.ack", "tcp.window_size", "tcp.len"]
ts=read_pcap("/home/rufina/Documents/github-dropbox/rename/new/git/shoot.log", fields, timeseries=True, strict=True)
ts
```

Out[62]:

	tcp.stream	ip.src	ip.dst	tcp.seq	tcp.ack	tcp.window_size	tcp.len
frame.time_epoch							
2015-03-22 01:57:15.686926	0	91.189.90.41	128.119.247.197	0	1	5792	0
2015-03-22 01:57:15.686991	0	128.119.247.197	91.189.90.41	1	1	29312	0
2015-03-22 01:57:15.695736	0	128.119.247.197	91.189.90.41	1	1	29312	319
2015-03-22 01:57:15.769928	0	91.189.90.41	128.119.247.197	1	320	6912	0
2015-03-22 01:57:15.776000	0	91.189.90.41	128.119.247.197	1	320	6912	557
2015-03-22 01:57:15.776036	0	128.119.247.197	91.189.90.41	320	558	30336	0
2015-03-22 01:57:15.776116	0	91.189.90.41	128.119.247.197	558	320	6912	1448
2015-03-22 01:57:15.776129	0	128.119.247.197	91.189.90.41	320	2006	33280	0
2015-03-22 01:57:15.776176	0	91.189.90.41	128.119.247.197	2006	320	6912	424
2015-03-22 01:57:15.776187	0	128.119.247.197	91.189.90.41	320	2430	36224	0
2015-03-22 01:57:19.174729	1	72.21.91.29	128.119.247.197	0	1	14480	0
2015-03-22 01:57:19.174771	1	128.119.247.197	72.21.91.29	1	1	29312	0
2015-03-22 01:57:19.174913	1	128.119.247.197	72.21.91.29	1	1	29312	439
2015-03-22 01:57:19.175741	2	72.21.91.29	128.119.247.197	0	1	14480	0
2015-03-22 01:57:19.175778	2	128.119.247.197	72.21.91.29	1	1	29312	0
2015-03-22 01:57:19.175890	2	128.119.247.197	72.21.91.29	1	1	29312	439
2015-03-22 01:57:19.182698	1	72.21.91.29	128.119.247.197	1	440	15872	0
2015-03-22 01:57:19.183224	1	72.21.91.29	128.119.247.197	1	440	15872	788
2015-03-22 01:57:19.183244	1	128.119.247.197	72.21.91.29	440	789	30848	0
2015-03-22 01:57:19.183473	2	72.21.91.29	128.119.247.197	1	440	15872	0
2015-03-22 01:57:19.184041	2	72.21.91.29	128.119.247.197	1	440	15872	788
2015-03-22 01:57:19.184063	2	128.119.247.197	72.21.91.29	440	789	30848	0
2015-03-22 01:57:19.184117	3	72.21.91.29	128.119.247.197	0	1	14480	0

In [65]:
```
stream=ts[ts["tcp.stream"] == 10]
```

In [69]:
```
per_stream=ts.groupby("tcp.stream")
per_stream.head()
```

Out[69]:

0	**2015-03-22 01:57:15.695736**	0	128.119.247.197	91.189.90.41	1	1	29312	319
	2015-03-22 01:57:15.769928	0	91.189.90.41	128.119.247.197	1	320	6912	0
	2015-03-22 01:57:15.776000	0	91.189.90.41	128.119.247.197	1	320	6912	557
1	**2015-03-22 01:57:19.174729**	1	72.21.91.29	128.119.247.197	0	1	14480	0
	2015-03-22 01:57:19.174771	1	128.119.247.197	72.21.91.29	1	1	29312	0
	2015-03-22 01:57:19.174913	1	128.119.247.197	72.21.91.29	1	1	29312	439
2	**2015-03-22 01:57:19.175741**	2	72.21.91.29	128.119.247.197	0	1	14480	0
	2015-03-22 01:57:19.175778	2	128.119.247.197	72.21.91.29	1	1	29312	0
	2015-03-22 01:57:19.175890	2	128.119.247.197	72.21.91.29	1	1	29312	439
1	**2015-03-22 01:57:19.182698**	1	72.21.91.29	128.119.247.197	1	440	15872	0
	2015-03-22 01:57:19.183224	1	72.21.91.29	128.119.247.197	1	440	15872	788
2	**2015-03-22 01:57:19.183473**	2	72.21.91.29	128.119.247.197	1	440	15872	0
	2015-03-22 01:57:19.184041	2	72.21.91.29	128.119.247.197	1	440	15872	788
3	**2015-03-22 01:57:19.184117**	3	72.21.91.29	128.119.247.197	0	1	14480	0
	2015-03-22 01:57:19.184142	3	128.119.247.197	72.21.91.29	1	1	29312	0
4	**2015-03-22 01:57:19.961868**	4	216.58.219.206	128.119.247.197	0	1	42540	0
	2015-03-22 01:57:19.961896	4	128.119.247.197	216.58.219.206	1	1	29312	0
	2015-03-22 01:57:19.961997	4	128.119.247.197	216.58.219.206	1	1	29312	437
5	**2015-03-22 01:57:19.968281**	5	216.58.219.206	128.119.247.197	0	1	42540	0
	2015-03-22 01:57:19.968323	5	128.119.247.197	216.58.219.206	1	1	29312	0
4	**2015-03-22 01:57:19.969457**	4	216.58.219.206	128.119.247.197	1	438	43648	0
	2015-03-22 01:57:19.990941	4	216.58.219.206	128.119.247.197	1	438	43648	781
3	**2015-03-22 01:57:24.194701**	3	128.119.247.197	72.21.91.29	1	1	29312	0
	2015-03-22 01:57:24.202402	3	72.21.91.29	128.119.247.197	1	2	14848	0
	2015-03-22 01:57:24.202437	3	128.119.247.197	72.21.91.29	2	2	29312	0

In [65]:
```
stream=ts[ts["tcp.stream"] == 10]
```

In [69]:
```
per_stream=ts.groupby("tcp.stream")
per_stream.head()
```

Out[69]:

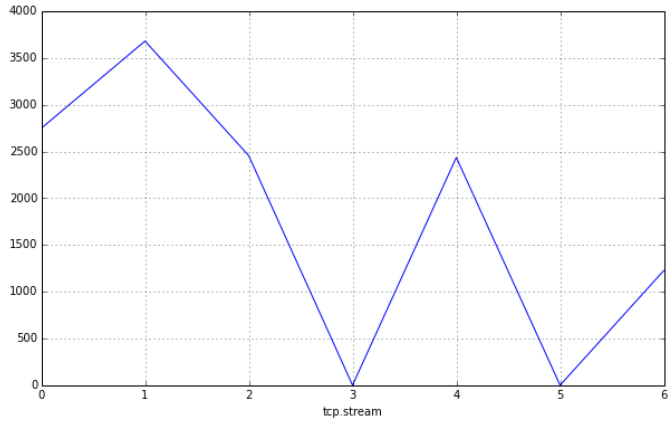
0	**2015-03-22 01:57:15.695736**	0	128.119.247.197	91.189.90.41	1	1	29312	319
	2015-03-22 01:57:15.769928	0	91.189.90.41	128.119.247.197	1	320	6912	0
	2015-03-22 01:57:15.776000	0	91.189.90.41	128.119.247.197	1	320	6912	557
1	**2015-03-22 01:57:19.174729**	1	72.21.91.29	128.119.247.197	0	1	14480	0
	2015-03-22 01:57:19.174771	1	128.119.247.197	72.21.91.29	1	1	29312	0
	2015-03-22 01:57:19.174913	1	128.119.247.197	72.21.91.29	1	1	29312	439
2	**2015-03-22 01:57:19.175741**	2	72.21.91.29	128.119.247.197	0	1	14480	0
	2015-03-22 01:57:19.175778	2	128.119.247.197	72.21.91.29	1	1	29312	0
	2015-03-22 01:57:19.175890	2	128.119.247.197	72.21.91.29	1	1	29312	439
1	**2015-03-22 01:57:19.182698**	1	72.21.91.29	128.119.247.197	1	440	15872	0
	2015-03-22 01:57:19.183224	1	72.21.91.29	128.119.247.197	1	440	15872	788
2	**2015-03-22 01:57:19.183473**	2	72.21.91.29	128.119.247.197	1	440	15872	0
	2015-03-22 01:57:19.184041	2	72.21.91.29	128.119.247.197	1	440	15872	788
3	**2015-03-22 01:57:19.184117**	3	72.21.91.29	128.119.247.197	0	1	14480	0
	2015-03-22 01:57:19.184142	3	128.119.247.197	72.21.91.29	1	1	29312	0
4	**2015-03-22 01:57:19.961868**	4	216.58.219.206	128.119.247.197	0	1	42540	0
	2015-03-22 01:57:19.961896	4	128.119.247.197	216.58.219.206	1	1	29312	0
	2015-03-22 01:57:19.961997	4	128.119.247.197	216.58.219.206	1	1	29312	437
5	**2015-03-22 01:57:19.968281**	5	216.58.219.206	128.119.247.197	0	1	42540	0
	2015-03-22 01:57:19.968323	5	128.119.247.197	216.58.219.206	1	1	29312	0
4	**2015-03-22 01:57:19.969457**	4	216.58.219.206	128.119.247.197	1	438	43648	0
	2015-03-22 01:57:19.990941	4	216.58.219.206	128.119.247.197	1	438	43648	781
3	**2015-03-22 01:57:24.194701**	3	128.119.247.197	72.21.91.29	1	1	29312	0
	2015-03-22 01:57:24.202402	3	72.21.91.29	128.119.247.197	1	2	14848	0
	2015-03-22 01:57:24.202437	3	128.119.247.197	72.21.91.29	2	2	29312	0

In [70]:
```
bytes_per_stream = per_stream["tcp.len"].sum()
bytes_per_stream.head()
```

Out[70]:
```
tcp.stream
0            2748
1            3681
2            2454
3               0
4            2436
Name: tcp.len, dtype: int64
```

In [71]:
```
bytes_per_stream.plot()
```

Out[71]:
```
<matplotlib.axes.AxesSubplot at 0x7f4080146410>
```



In [39]:
```
bytes_per_stream.max()
```

Out[39]:
```
3681
```

In [72]:
```
!tshark -r /home/rufina/Documents/github-dropbox/rename/new/git/shoot.log -q -z conv,eth -z conv,ip -z conv,tcp
```

```
================================================================================
TCP Conversations
Filter:<No Filter>
                                               |       <-      | |       ->      | |     Total     |    Relative    |   D
uration   |
                                               | Frames  Bytes | | Frames  Bytes | | Frames  Bytes |      Start     |
          |
128.119.247.197:43454 <-> 91.189.90.41:http         17      3559      19      1581      36      5140     0.000000000
  115.5583
128.119.247.197:38489 <-> 216.58.219.206:http       16      2626      19      2136      35      4762     4.341708000
  116.1504
128.119.247.197:33209 <-> 72.21.91.29:http           8      2900      10      1985      18      4885     3.554377000
   16.6040
128.119.247.197:33210 <-> 72.21.91.29:http           7      2046       8      1414      15      3460     3.554417000
   15.6295
128.119.247.197:33252 <-> 72.21.91.29:http           6      1192       7       909      13      2101   148.742120000
   15.5300
128.119.247.197:38490 <-> 216.58.219.206:http        2       140       4       272       6       412     4.348184000
    5.2412
128.119.247.197:33211 <-> 72.21.91.29:http           2       140       4       272       6       412     3.563802000
    5.0259
================================================================================
================================================================================
IPv4 Conversations
Filter:<No Filter>
                                               |       <-      | |       ->      | |     Total     |    Relative    |   D
uration   |
                                               | Frames  Bytes | | Frames  Bytes | | Frames  Bytes |      Start     |
          |
128.119.247.197      <-> 72.21.91.29              23      6278      29      4580      52     10858     3.554377000
 160.7177
216.58.219.206       <-> 128.119.247.197          23      2408      18      2766      41      5174     4.341708000
 116.1504
128.119.247.197      <-> 91.189.90.41             17      3559      19      1581      36      5140     0.000000000
 115.5583
================================================================================
================================================================================
Ethernet Conversations
Filter:<No Filter>
                                               |       <-      | |       ->      | |     Total     |    Relative    |   D
uration   |
                                               | Frames  Bytes | | Frames  Bytes | | Frames  Bytes |      Start     |
          |
98:90:96:a7:10:36    <-> 5c:5e:ab:dd:de:81       58     12603      71      8569     129     21172     0.000000000
 164.2721
================================================================================
```