In [1]:

```
import pandas as pd
```

In [ ]:

```

```

In [2]:

```
df = pd.read_csv('sample1.csv')
```

In [3]:

```
#PCAP Data File 1
df
```

Out[3]:

	No.	Time	Source	Destination	Protocol	Length	
0	1	0.000000	192.168.10.41	192.168.10.2	SIP	596	Request: R sip:192.168.10.2 (1
1	2	0.000692	192.168.10.2	192.168.10.41	SIP	610	Status: 401 Unau
2	3	0.005771	192.168.10.41	192.168.10.2	SIP	755	Request: R sip:192.168.10.2 (1
3	4	0.009246	192.168.10.2	192.168.10.41	SIP	625	Request: (sip:10009@192.168.10.4
4	5	0.010308	192.168.10.2	192.168.10.41	SIP	654	Status: 200 OK (1
...	...	...	...	...	...	...	
1037	1038	32.400035	192.168.10.41	192.168.10.2	RTP	214	PT=ITU-T G.7: SSRC=0xBEE0F2ED, Se
1038	1039	32.401915	192.168.10.41	192.168.10.2	SIP/SDP	942	Status:
1039	1040	32.402662	192.168.10.2	192.168.10.41	SIP	442	Requ sip:10009@192.168.10.4
1040	1041	32.402739	192.168.10.2	192.168.10.41	SIP	480	Req sip:10009@192.168.10.4
1041	1042	32.490028	192.168.10.41	192.168.10.2	SIP	421	Status:

1042 rows × 7 columns

In [4]:

```
#No of Packets file1
df.shape[0]
```

Out[4]:

```
1042
```

In [5]:

```
df1 = pd.read_csv('sample2.csv')
```

In [6]:

```
#PCAP Data File 2
df1
```

Out[6]:

	No.	Time	Source	Destination	Protocol	Length	
0	1	0.000000	200.57.7.195	200.57.7.204	SIP/SDP	740	Request: IN sip:francisco@bestel.com:5
1	2	0.007889	200.57.7.204	200.57.7.195	SIP	503	Status: 100 Try
2	3	0.047524	200.57.7.204	200.57.7.195	SIP	504	Status: 180 Ring
3	4	0.049780	200.57.7.206	200.57.7.197	TCP	54	1219 > 23 [ACK] Seq=1 A Win=17465 L
4	5	0.050802	200.57.7.197	200.57.7.206	TELNET	637	Telnet Da
...	...	...	...	...	...	...	
4264	4265	34.890149	200.57.7.204	200.57.7.194	HTTP	214	P /cems/applets/serviceR HTTP/1.1
4265	4266	34.890418	200.57.7.194	200.57.7.204	HTTP	79	HTTP/1.1 100 Con
4266	4267	34.893607	200.57.7.194	200.57.7.197	SNMP	211	get-rec 1.3.6.1.4.1.2858.100.40. 1
4267	4268	34.908251	200.57.7.199	200.57.7.196	UDP	214	4800 > 40378 Len
4268	4269	34.908735	200.57.7.196	200.57.7.204	RTP	214	PT=ITU-T G.711 PC SSRC=0x58F33I Seq=12

4269 rows × 7 columns

In [7]:

```
#No of Packets file2
df1.shape[0]
```

Out[7]:

```
4269
```

In [8]:

```
df2 = pd.read_csv('sample3.csv')
```

In [9]:

```
#PCAP Data File 3
df2
```

Out[9]:

	No.	Time	Source	Destination	Protocol	Length	In
0	1	0.000000	192.168.105.110	192.168.105.105	SIP	596	Request: REGISTE sip:192.168.105.1 (1 binc
1	2	0.000639	192.168.105.105	192.168.105.110	SIP	362	Status: 100 Tryin
2	3	0.032186	192.168.105.105	192.168.105.110	SIP	456	Status: 200 OK binding
3	4	10.000441	192.168.105.110	192.168.105.105	SIP	597	Request: REGISTE sip:192.168.105.1 (1 binc
4	5	10.001733	192.168.105.105	192.168.105.110	SIP	363	Status: 100 Tryin
...	...	...	...	...	...	...	
1355	1356	96.809551	192.168.105.110	192.168.105.172	RTP	294	PT=ITU-T G.7 PCM SSRC=0x9A7B53 Seq=533
1356	1357	96.829533	192.168.105.172	192.168.105.110	RTP	294	PT=ITU-T G.7 PCM SSRC=0x5711BF Seq=631
1357	1358	100.005644	192.168.105.110	192.168.105.105	SIP	597	Request: REGISTE sip:192.168.105.1 (1 binc
1358	1359	100.006096	192.168.105.105	192.168.105.110	SIP	363	Status: 100 Tryin
1359	1360	100.036779	192.168.105.105	192.168.105.110	SIP	457	Status: 200 OK binding

1360 rows × 7 columns

In [10]:

```
#No of Packets file3
df2.shape[0]
```

Out[10]:

```
1360
```

In [11]:

```
#List only SIP Packets in File 1
sip = df[df['Protocol'] == 'SIP']
sip
```

Out[11]:

	No.	Time	Source	Destination	Protocol	Length	
0	1	0.000000	192.168.10.41	192.168.10.2	SIP	596	Request: R sip:192.168.10.2 (1
1	2	0.000692	192.168.10.2	192.168.10.41	SIP	610	Status: 401 Unau
2	3	0.005771	192.168.10.41	192.168.10.2	SIP	755	Request: R sip:192.168.10.2 (1
3	4	0.009246	192.168.10.2	192.168.10.41	SIP	625	Request: (sip:10009@192.168.10.4
4	5	0.010308	192.168.10.2	192.168.10.41	SIP	654	Status: 200 OK (1
5	6	0.017462	192.168.10.41	192.168.10.2	SIP	593	Status:
6	7	0.024945	192.168.10.41	192.168.10.2	SIP	600	Request: SU sip:10009@192.
7	8	0.028999	192.168.10.2	192.168.10.41	SIP	611	Status: 401 Unau
8	9	0.032569	192.168.10.41	192.168.10.2	SIP	664	Request: SU sip:10008@192.
9	10	0.033144	192.168.10.2	192.168.10.41	SIP	599	Status: 401 Unau
10	11	0.043205	192.168.10.41	192.168.10.2	SIP	765	Request: SU sip:10009@192.
11	12	0.043782	192.168.10.2	192.168.10.41	SIP	528	Status: 404 N
12	13	0.047481	192.168.10.41	192.168.10.2	SIP	829	Request: SU sip:10008@192.
13	14	0.047988	192.168.10.2	192.168.10.41	SIP	516	Status: 404 N
15	16	8.778390	192.168.10.2	192.168.10.41	SIP	608	Status: 401 Unau
16	17	8.779575	192.168.10.41	192.168.10.2	SIP	394	Requ sip:10008@192.
18	19	8.784732	192.168.10.2	192.168.10.41	SIP	542	Status: 10
19	20	8.807730	192.168.10.2	192.168.10.41	SIP	558	Status: 180
26	27	16.477819	192.168.10.41	192.168.10.2	SIP	647	Requ sip:10008@192.
1039	1040	32.402662	192.168.10.2	192.168.10.41	SIP	442	Requ sip:10009@192.168.10.4
1040	1041	32.402739	192.168.10.2	192.168.10.41	SIP	480	Req sip:10009@192.168.10.4
1041	1042	32.490028	192.168.10.41	192.168.10.2	SIP	421	Status:

In [12]:

```
sip.shape
```

Out[12]:

```
(22, 7)
```

In [13]:

```
#List only SIP Packets in File 1
sip1 = df1[df1['Protocol'] == 'SIP']
sip1
```

Out[13]:

	No.	Time	Source	Destination	Protocol	Length	
1	2	0.007889	200.57.7.204	200.57.7.195	SIP	503	Status: 100 T
2	3	0.047524	200.57.7.204	200.57.7.195	SIP	504	Status: 180 Rin
151	152	4.056633	200.57.7.205	200.57.7.195	SIP	460	Request: REGI sip:Verso.com (1 bin
152	153	4.072335	200.57.7.195	200.57.7.205	SIP	514	Status: 200 OK (1 bin
516	517	8.524137	200.57.7.195	200.57.7.204	SIP	485	Request sip:francisco@200.57.7.204
1723	1724	17.457029	200.57.7.204	200.57.7.195	SIP	479	Request: REGI sip:bestel.com (1 bin
1726	1727	17.473413	200.57.7.195	200.57.7.204	SIP	532	Status: 200 OK (1 bin
2910	2911	24.309202	200.57.7.205	200.57.7.195	SIP	460	Request: REGI sip:Verso.com (1 bin
2911	2912	24.324792	200.57.7.195	200.57.7.205	SIP	514	Status: 200 OK (1 bin
2964	2965	24.674680	200.57.7.204	200.57.7.195	SIP	530	Status: 100 T
2966	2967	24.692752	200.57.7.204	200.57.7.195	SIP	531	Status: 180 Rin

In [14]:

```
sip1.shape
```

Out[14]:

```
(11, 7)
```

In [15]:

```
#List only SIP Packets in File 3
sip2 = df2[df2['Protocol'] == 'SIP']
sip2
```

Out[15]:

	No.	Time	Source	Destination	Protocol	Length	
0	1	0.000000	192.168.105.110	192.168.105.105	SIP	596	Reque sip:192.168.105
1	2	0.000639	192.168.105.105	192.168.105.110	SIP	362	Statu
2	3	0.032186	192.168.105.105	192.168.105.110	SIP	456	Status: 200 C
3	4	10.000441	192.168.105.110	192.168.105.105	SIP	597	Reque sip:192.168.105
4	5	10.001733	192.168.105.105	192.168.105.110	SIP	363	Statu
5	6	10.033344	192.168.105.105	192.168.105.110	SIP	457	Status: 200 C
6	7	36.002756	192.168.105.110	192.168.105.105	SIP	570	Re sip:2504@192
7	8	36.003190	192.168.105.105	192.168.105.110	SIP	355	Statu
8	9	36.019858	192.168.105.105	192.168.105.110	SIP	386	Status
9	10	36.024706	192.168.105.110	192.168.105.105	SIP	437	sip:2504@192
10	11	40.002985	192.168.105.110	192.168.105.105	SIP	596	Reque sip:192.168.105
11	12	40.003476	192.168.105.105	192.168.105.110	SIP	362	Statu
12	13	40.034723	192.168.105.105	192.168.105.110	SIP	454	Status: 200 C
13	14	52.003970	192.168.105.110	192.168.105.105	SIP	572	Re sip:2504@192
14	15	52.004399	192.168.105.105	192.168.105.110	SIP	357	Statu
15	16	52.033792	192.168.105.105	192.168.105.110	SIP	658	Re sip:2504@192.168
16	17	52.041339	192.168.105.110	192.168.105.105	SIP	513	Statu
17	18	53.102765	192.168.105.110	192.168.105.105	SIP	625	Status
18	19	53.110754	192.168.105.105	192.168.105.110	SIP	551	Status
23	24	70.003917	192.168.105.110	192.168.105.105	SIP	596	Reque sip:192.168.105
24	25	70.004412	192.168.105.105	192.168.105.110	SIP	362	Statu
25	26	70.035666	192.168.105.105	192.168.105.110	SIP	454	Status: 200 C
1357	1358	100.005644	192.168.105.110	192.168.105.105	SIP	597	Reque sip:192.168.105
1358	1359	100.006096	192.168.105.105	192.168.105.110	SIP	363	Statu
1359	1360	100.036779	192.168.105.105	192.168.105.110	SIP	457	Status: 200 C

In [16]:

```
sip2.shape
```

Out[16]:

```
(25, 7)
```

In [17]:

```
#List the SIP info fields wrt time for file 1
sip[['No.', 'Time', 'Info']]
```

Out[17]:

	No.	Time	Info
0	1	0.000000	Request: REGISTER sip:192.168.10.2 (1 binding...
1	2	0.000692	Status: 401 Unauthorized |
2	3	0.005771	Request: REGISTER sip:192.168.10.2 (1 binding...
3	4	0.009246	Request: OPTIONS sip:10009@192.168.10.41:13434...
4	5	0.010308	Status: 200 OK (1 binding) |
5	6	0.017462	Status: 200 OK |
6	7	0.024945	Request: SUBSCRIBE sip:10009@192.168.10.2 |
7	8	0.028999	Status: 401 Unauthorized |
8	9	0.032569	Request: SUBSCRIBE sip:10008@192.168.10.2 |
9	10	0.033144	Status: 401 Unauthorized |
10	11	0.043205	Request: SUBSCRIBE sip:10009@192.168.10.2 |
11	12	0.043782	Status: 404 Not Found |
12	13	0.047481	Request: SUBSCRIBE sip:10008@192.168.10.2 |
13	14	0.047988	Status: 404 Not Found |
15	16	8.778390	Status: 401 Unauthorized |
16	17	8.779575	Request: ACK sip:10008@192.168.10.2 |
18	19	8.784732	Status: 100 Trying |
19	20	8.807730	Status: 180 Ringing |
26	27	16.477819	Request: ACK sip:10008@192.168.10.2 |
1039	1040	32.402662	Request: ACK sip:10009@192.168.10.41:13434 |
1040	1041	32.402739	Request: BYE sip:10009@192.168.10.41:13434 |
1041	1042	32.490028	Status: 200 OK |

In [18]:

```
#List the SIP info fields wrt time for file 3
sip1[['No.', 'Time', 'Info']]
```

Out[18]:

	No.	Time	Info
1	2	0.007889	Status: 100 Trying |
2	3	0.047524	Status: 180 Ringing |
151	152	4.056633	Request: REGISTER sip:Verso.com (1 binding) |
152	153	4.072335	Status: 200 OK (1 binding) |
516	517	8.524137	Request: ACK sip:francisco@200.57.7.204:5061 |
1723	1724	17.457029	Request: REGISTER sip:bestel.com (1 binding) |
1726	1727	17.473413	Status: 200 OK (1 binding) |
2910	2911	24.309202	Request: REGISTER sip:Verso.com (1 binding) |
2911	2912	24.324792	Status: 200 OK (1 binding) |
2964	2965	24.674680	Status: 100 Trying |
2966	2967	24.692752	Status: 180 Ringing |

In [19]:

```
#List the SIP info fields wrt time for file 3
sip2[['No.', 'Time', 'Info']]
```

Out[19]:

	No.	Time	Info
0	1	0.000000	Request: REGISTER sip:192.168.105.105 (1 bind...
1	2	0.000639	Status: 100 Trying |
2	3	0.032186	Status: 200 OK (1 binding) |
3	4	10.000441	Request: REGISTER sip:192.168.105.105 (1 bind...
4	5	10.001733	Status: 100 Trying |
5	6	10.033344	Status: 200 OK (1 binding) |
6	7	36.002756	Request: INVITE sip:2504@192.168.105.105 |
7	8	36.003190	Status: 100 Trying |
8	9	36.019858	Status: 603 Decline |
9	10	36.024706	Request: ACK sip:2504@192.168.105.105 |
10	11	40.002985	Request: REGISTER sip:192.168.105.105 (1 bind...
11	12	40.003476	Status: 100 Trying |
12	13	40.034723	Status: 200 OK (1 binding) |
13	14	52.003970	Request: INVITE sip:2504@192.168.105.105 |
14	15	52.004399	Status: 100 Trying |
15	16	52.033792	Request: INVITE sip:2504@192.168.105.110:5060 |
16	17	52.041339	Status: 100 Trying |
17	18	53.102765	Status: 180 Ringing |
18	19	53.110754	Status: 180 Ringing |
23	24	70.003917	Request: REGISTER sip:192.168.105.105 (1 bind...
24	25	70.004412	Status: 100 Trying |
25	26	70.035666	Status: 200 OK (1 binding) |
1357	1358	100.005644	Request: REGISTER sip:192.168.105.105 (1 bind...
1358	1359	100.006096	Status: 100 Trying |
1359	1360	100.036779	Status: 200 OK (1 binding) |

In [20]:

```
#Analysis 1 File 1
infos = sip['Info'].to_list()
times = sip['Time'].to_list()
print('Type Fields\n')
flags = []
print('Time\t\t\tType\t\t\tCommand\n')
for info, time0 in zip(infos, times):
    flag = info.split(':')
    command = flag[1].split(' ')
    if(command[1].isdigit()):
        command1 = flag[1].strip().split(' ', 2)
        command = command1[1]
        print(time0, '\t\t', flag[0] ,'\t\t', command)
    else:
        command = flag[1].strip().split(' ', 1)
        print(time0, '\t\t', flag[0] ,'\t\t', command[0])
    flags.append(flag[0])
```

```
Type Fields

Time                    Type                    Command

0.0              Request                 REGISTER
0.000692                 Status                  Unauthorized
0.005771                 Request                 REGISTER
0.009246                 Request                 OPTIONS
0.010308                 Status                  OK
0.017462                 Status                  OK
0.024945                 Request                 SUBSCRIBE
0.028999                 Status                  Unauthorized
0.032569                 Request                 SUBSCRIBE
0.033144                 Status                  Unauthorized
0.043205                 Request                 SUBSCRIBE
0.043782                 Status                  Not
0.047481                 Request                 SUBSCRIBE
0.047988                 Status                  Not
8.77839                  Status                  Unauthorized
8.779575                 Request                 ACK
8.784732                 Status                  Trying
8.80773                  Status                  Ringing
16.477819                Request                 ACK
32.402662                Request                 ACK
32.402739                Request                 BYE
32.490028                Status                  OK
```

In [21]:

```
#Analysis 1 File 2
infos1 = sip1['Info'].to_list()
times1 = sip1['Time'].to_list()

print('Type Fields\n')
flags1 = []
print('Time\t\t\tType\t\t\t Command\n')
for info1, time1 in zip(infos1, times1):
    flag1 = info1.split(':')
    command1 = flag1[1].split(' ')
    if(command1[1].isdigit()):
        command2 = flag1[1].strip().split(' ', 2)
        command1 = command2[1]
        print(time1, '\t\t' ,flag1[0] ,'\t\t', command1)
    else:
        command1 = flag1[1].strip().split(' ', 1)
        print(time1, '\t\t' ,flag1[0] ,'\t\t', command1[0])
    flags1.append(flag1[0])
```

```
Type Fields

Time                    Type                     Command

0.007889                 Status                  Trying
0.047524                 Status                  Ringing
4.056633                 Request                 REGISTER
4.072335                 Status                  OK
8.524137                 Request                 ACK
17.457029                Request                 REGISTER
17.473413                Status                  OK
24.309202                Request                 REGISTER
24.324792                Status                  OK
24.67468                 Status                  Trying
24.692752                Status                  Ringing
```

In [22]:

```
#Analysis 1 File 1
infos2 = sip2['Info'].to_list()
times2 = sip2['Time'].to_list()

print('Type Fields\n')
flags2 = []
print('Time\t\t\tType\t\t\tCommand\n')
for info2, time2 in zip(infos2, times2):
    flag2 = info2.split(':')
    command2 = flag2[1].split(' ')
    if(command2[1].isdigit()):
        command3 = flag[1].strip().split(' ', 2)
        command2 = command3[1]
        print(time2, '\t\t', flag[0] ,'\t\t', command2)
    else:
        command2 = flag2[1].strip().split(' ', 1)
        print(time2, '\t\t', flag2[0] ,'\t\t', command2[0])
    flags2.append(flag2[0])
```

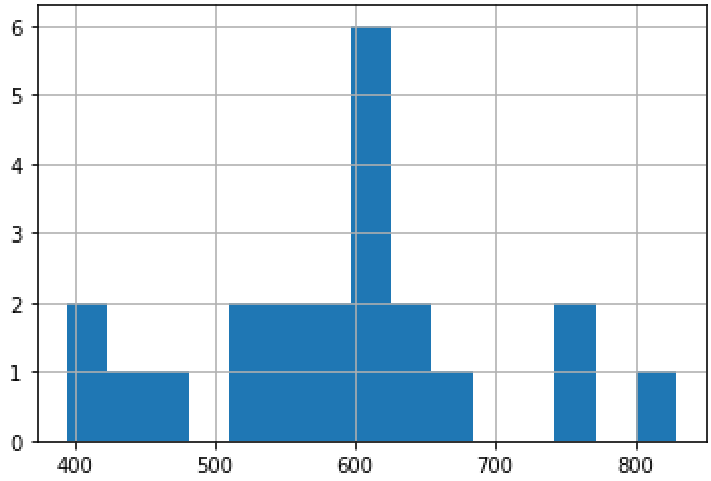
```
Type Fields

Time                    Type                    Command

0.0              Request                 REGISTER
0.000639                 Status                  OK
0.032186                 Status                  OK
10.000441                Request                 REGISTER
10.001733                Status                  OK
10.033344                Status                  OK
36.002756                Request                 INVITE
36.00319                 Status                  OK
36.019858                Status                  OK
36.024706                Request                 ACK
40.002985                Request                 REGISTER
40.003476                Status                  OK
40.034723                Status                  OK
52.00397                 Request                 INVITE
52.004399                Status                  OK
52.033792                Request                 INVITE
52.041339                Status                  OK
53.102765                Status                  OK
53.110754                Status                  OK
70.003917                Request                 REGISTER
70.004412                Status                  OK
70.035666                Status                  OK
100.005644               Request                 REGISTER
100.006096               Status                  OK
100.036779               Status                  OK
```

In [23]:

```
#Plot of Packets Length of SIP in File 1
%matplotlib inline
df[df['Protocol']=='SIP'].Length.hist(bins=15)
```

Out[23]:

```
<AxesSubplot:>
```

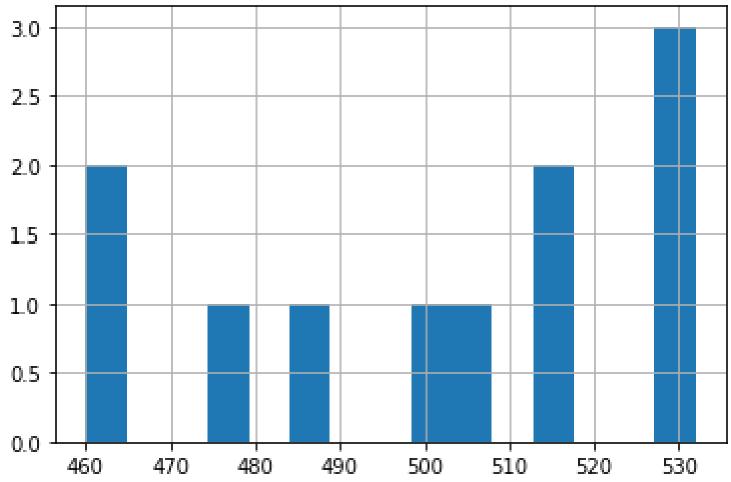


In [24]:

```
#Plot of Packets Length of SIP in File 2
%matplotlib inline
df1[df1['Protocol']=='SIP'].Length.hist(bins=15)
```

Out[24]:

```
<AxesSubplot:>
```

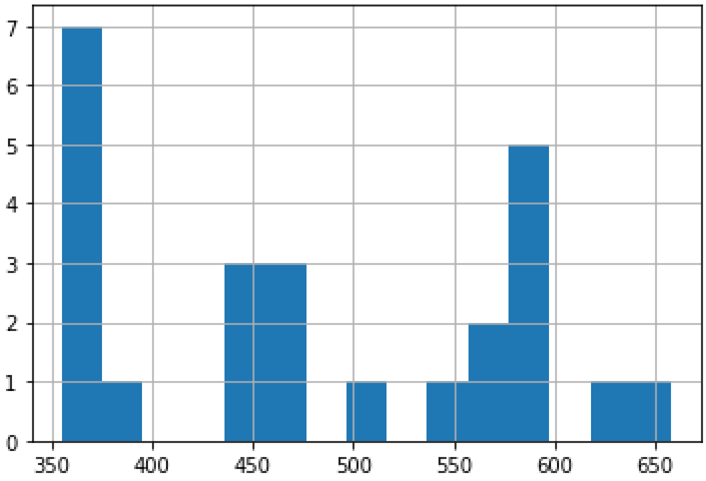


In [25]:

```
#Plot of Packets Length of SIP in File 3
%matplotlib inline
df2[df2['Protocol']=='SIP'].Length.hist(bins=15)
```

Out[25]:

```
<AxesSubplot:>
```

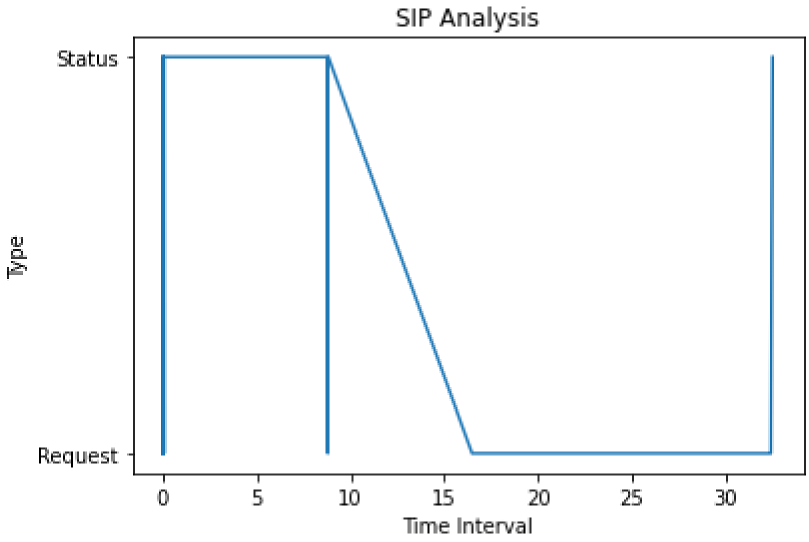


In [26]:

```
import matplotlib.pyplot as plt
```

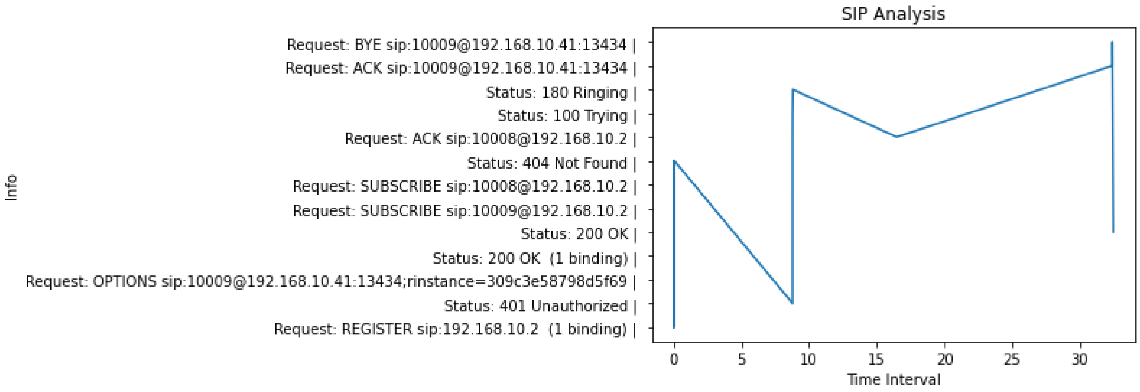
In [27]:

```
#Plot Type vs time interval for File1
plt.plot(times, flags)
plt.xlabel('Time Interval')
plt.ylabel('Type')
plt.title('SIP Analysis')
plt.show()
```



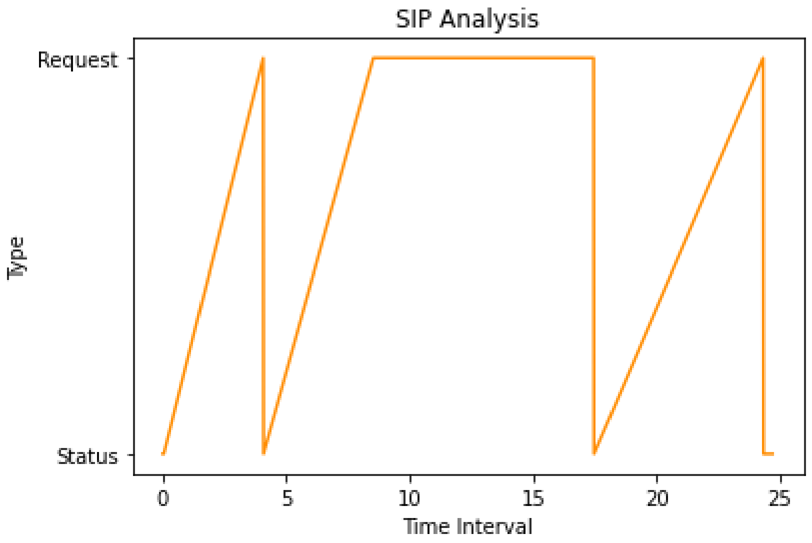
In [28]:

```
#Plot Information vs time interval for File1
plt.plot(times, infos)
plt.xlabel('Time Interval')
plt.ylabel('Info')
plt.title('SIP Analysis')
plt.show()
```



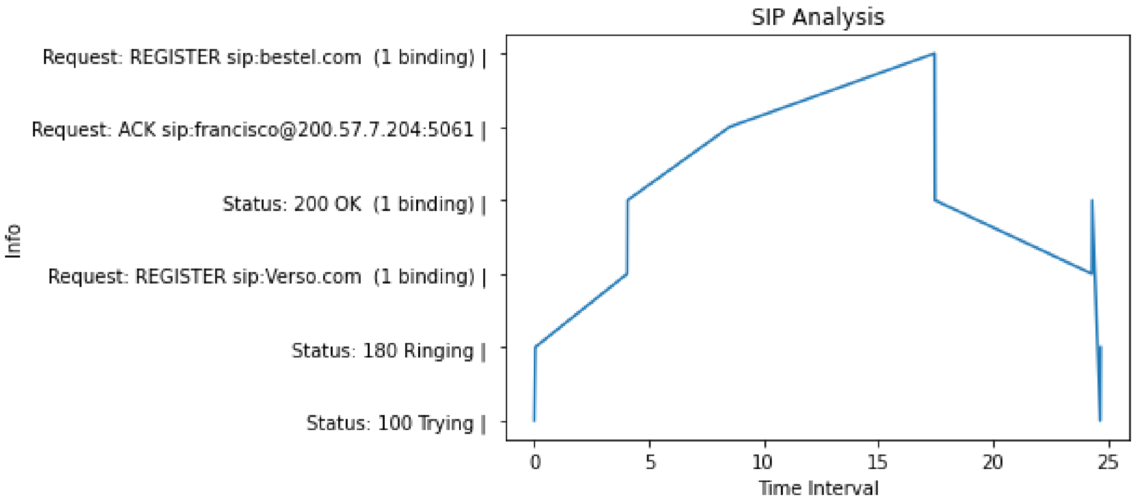
In [29]:

```
#Plot Type vs time interval for File2
plt.plot(times1, flags1, color='darkorange')
plt.xlabel('Time Interval')
plt.ylabel('Type')
plt.title('SIP Analysis')
plt.show()
```



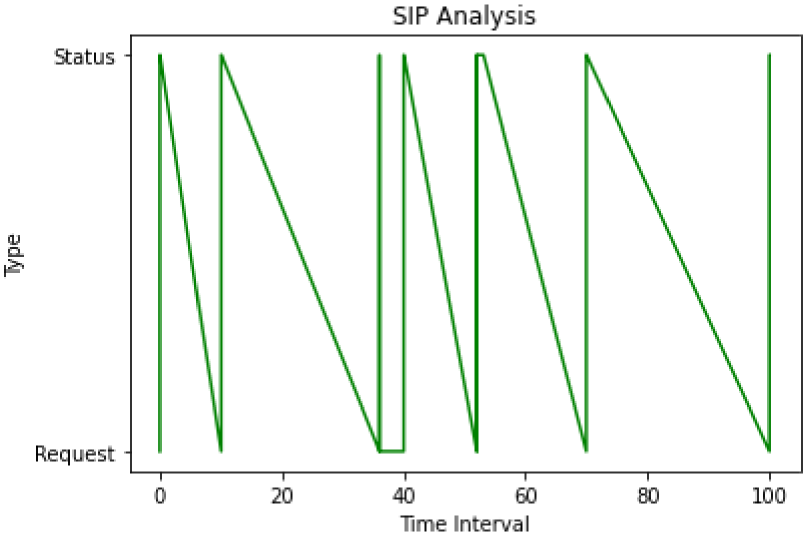
In [30]:

```
#Plot Information vs time interval for File2
plt.plot(times1, infos1)
plt.xlabel('Time Interval')
plt.ylabel('Info')
plt.title('SIP Analysis')
plt.show()
```



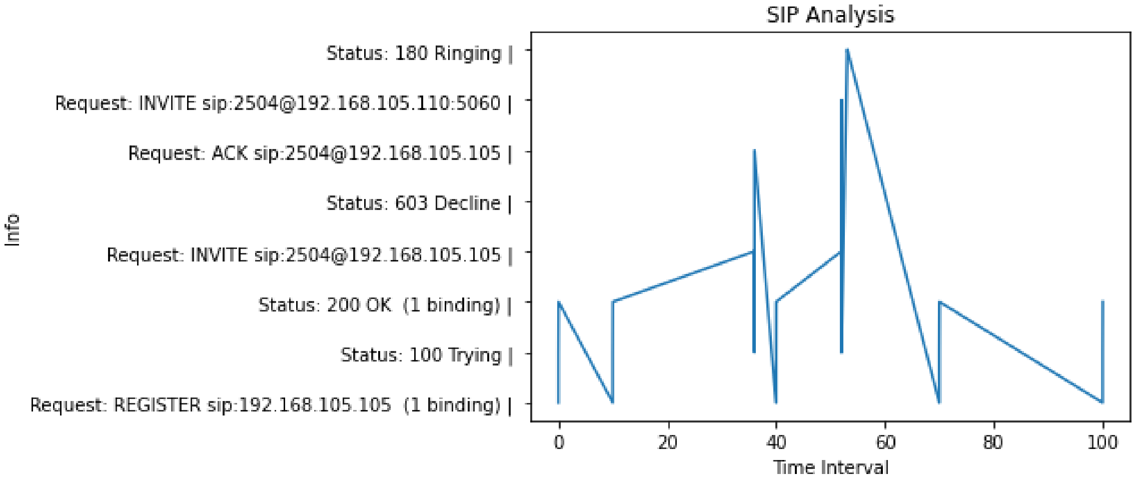
In [31]:

```
#Plot Type vs time interval for File3
plt.plot(times2, flags2, color='green')
plt.xlabel('Time Interval')
plt.ylabel('Type')
plt.title('SIP Analysis')
plt.show()
```



In [32]:

```
#Plot Information vs time interval for File3
plt.plot(times2, infos2)
plt.xlabel('Time Interval')
plt.ylabel('Info')
plt.title('SIP Analysis')
plt.show()
```

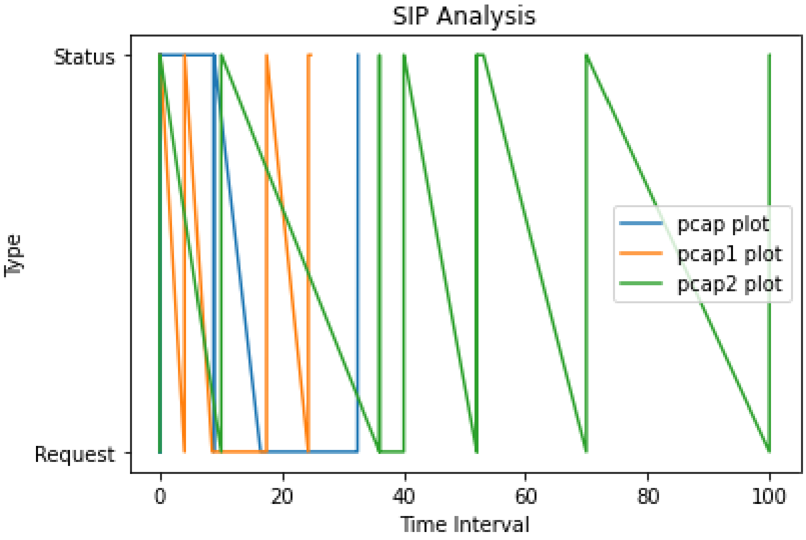


In [33]:

```
#Visualizing all the analysis in one plot
plt.plot(times, flags, label='pcap plot')
plt.plot(times1, flags1, label='pcap1 plot')
plt.plot(times2, flags2, label='pcap2 plot')
plt.xlabel('Time Interval')
plt.ylabel('Type')
plt.title('SIP Analysis')
plt.legend()
```

Out[33]:

```
<matplotlib.legend.Legend at 0x7fa04c450400>
```


SIP Analysis
Status
Request
Type
pcap plot
pcap1 plot
pcap2 plot
Time Interval