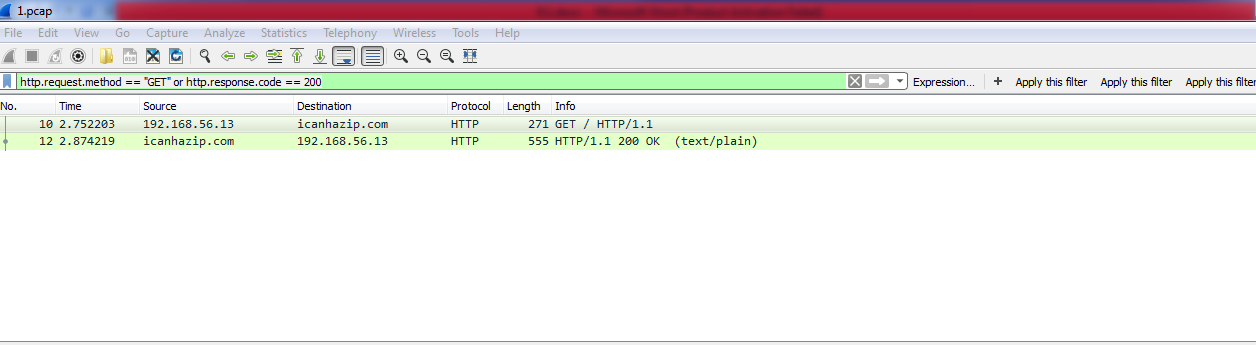
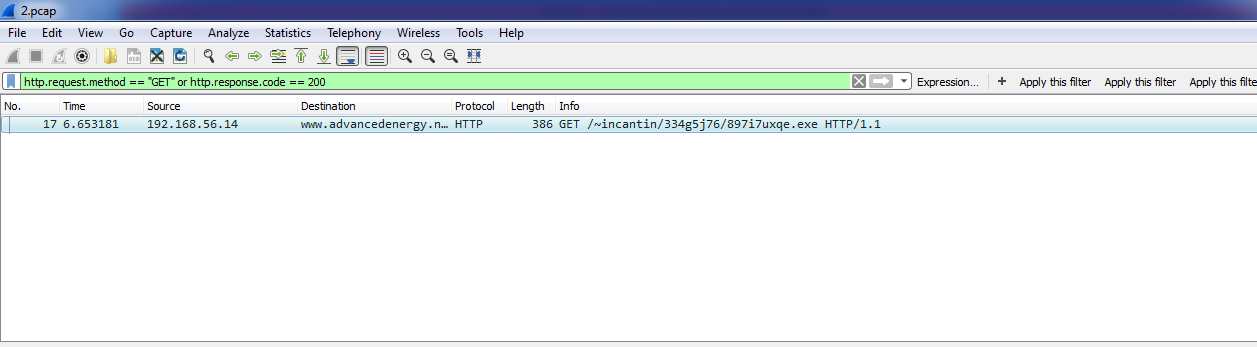
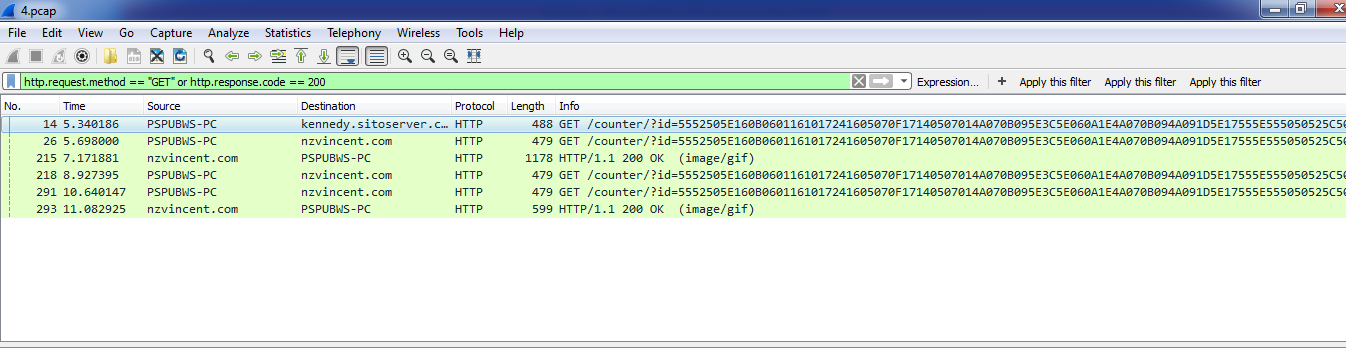
We are analyzing four email attachment using hybrid analysis. Hybrid analysis can not analyze 3 no email attachment.

After analyzing all email attachment from hybrid analysis ,then we download all pcap file.

To traffic analysis from all pcap file we filtering all pcap file “http.request.method == "GET" or http.response.code == 200”

Some snapshot of pcap file filtering.





We observe that there is a no http response in 4 no email of a http get request.That might be a possible attack.

When we analyzing all email attachment from VirusTotal, We found that there is a fhishing attack in 4 no mail.

By observing all these fact we said that infected email is 4 no email.

**9.1.1 Date and approximate time of the infection:**

Nov 7, 2015 04:22:38.688933000 Bangladesh Standard Time

**9.1.2 The infected computer's IP address:**

**10.3.66.103**

**9.1.3 The infected computer's MAC address:**

**00:24:e8:2d:90:81**

**9.1.4 The infected computer's host name:**

**174.121.246.162 kennedy.sitoserver.com**

**9.1.5 Which email the employee opened:**

**email number 4**