HTTP Packet Capture Objectives  
Answers with the Questions

* What seems to be the IP address of the main user? **145.254.160.237**
* What is the IP address of the DNS server? **145.253.2.203**
  + What is the domain name that is part of the DNS query? **pagead2.googlesyndication.com**
  + What is the packet number of the DNS response? **17**
  + What are the IP addresses of the domain name query?

**216.239.59.104**

**216.239.59.99**

* What are the two destination IP addresses when the main user is performing HTTP requests?

**65.208.228.223**

**216.239.59.99**

* + What are the host websites that these IP addresses translate to?

**65.208.228.223: www.ethereal.com**

**216.239.59.99: pagead2.googlesyndication.com**

* + What is the HTTP request method of both HTTP requests? **GET**
* What is the packet number which is the GET /download.html response? **38**
  + What packets are reassembled as part of this response? **6, 8, 10, 11, 14, 16, 20, 21, 23, 29, 31, 32, 34, 38**
  + What is the date and time that this response happened? **Thu, 13 May 2004 10:17:12 GMT**
  + What was the latency of this response? **4.846969000 – 0.911310000 = 3.935659**
* Which packets have “Bad TCP”? **36, 37**
  + What is the TCP SEQ/ACK analysis of packet number 37?

**SEQ=722**

**ACK=1591**

* + What is the relative acknowledgment number of packet 37? **1591**
  + What is the packet number that packet 37 is a duplicate of? **28**
  + What is the packet number that this duplicate acknowledgment is part of? **28**
  + What is the content type of the HTTP response? **text/html; charset=ISO-8859-1**