1. Intro (file http.cap)

- Observe protocol architecture
- Observe source/destination addresses at various protocol layers

2. http (file http.cap)

- Apply http filter
    - Specify the hosts (IP addresses) involved in the data exchange. (see source/destination IP addresses of packets no. 4-18-27-38; client is always 145.254.160.237; 2 servers are involved)
- Observe packet no. 4
    - Which TCP ports are used? (client= irrelevant, server=80)
    - Which http method is used? (get)
    - Which http version is used? (1.1)
    - What does line "Connection: keep-alive" indicate? (TCP connection is persistent)
    - Which http resource is requested and on which host? (download.html on host www.ethereal.com)
    - Which packet transports the reply to this request message? (no. 38)
- Observe the reply to the request message in packet no. 4
    - Which status code and phrase are sent? What do they indicate? (200 OK. Resource is present and is sent with this packet)

3. SMTP (file smtp.cap)

- Which TCP ports are used? (client= irrelevant, server=25)
- Observe the message exchange between SMTP client and server (use the visualization filter).

4. DNS (file Question & Answer.pcapng.cap)

- Which transport protocol is used? Which ports are used? (UDP; Client: irrelevant, Server: 53)
- Which address resolution mode is used? (recursive, see corresponding flag)
- Which name is being resolved? (google.com)
- Which address is provided as response to the DNS query? (several IP addresses)

5. TCP (file tcp.cap=http.cap)

- Observe flags in the first packet
    - Which are the active flags? Why? Where is the "response" to these flags? (SYN, to start the TCP connection; the acknowledgement to start the TCP connection is sent with packet no. 2, where also the TCP connection in the opposite direction is initiated (SYN/ACK flags are set); 3-ways handshake is completed at packet no. 3)
    - Which TCP ports are used? (client= irrelevant, server=80)
- Consider packet no. 6.

    - What is the packet total length? (1434 bytes)
    - What is the header length at the various layers? (H2=14 bytes, H3=20 bytes, H4=20 bytes)
    - What is the payload size? (TCP payload = 1434-54= 1380 bytes)
    - Which bytes are transported? How can we understand this? (bytes no. 1 to 1380; observing the value of SN field and considering the payload length calculated above)
    - Which segment transports the corresponding ACK? How can we state this? (no. 7, since the value of AN is 1381)
- Observe packet no. 36, it represents a retransmitted packet. Which packet is being retransmitted? How can we state this? (packet no. 26, it is exchanged between the same S/D pair and it has the same values of SN=1 and Len=1430)
- Which packets transport acks corresponding to these two packets (the original one and the retransmitted packet)? (packet no. 26 is acknowledged by no. 28, which is a CUMULATIVE ACK also for packet no. 27, as it has AN=1591; packet no. 36 is acknowledged by packet no. 37, which is a repeated ACK, as it transports again AN=1591)
- Which host starts the tear down of TCP connection? In which packet? How can we state this? (server 65.208.228.223 in packet 40, client in packet 42; SYN flag is set)
- Is the TCP connection closed with 3-way handshake? No, it's closed with a 2-way handshake in each direction (packets 40-41 and 42-43)

6. ICMP (file ICMP.cap)

- Observe packets from 7 to 16
    - How many ICMP requests are present? (4)
    - How many ICMP replies are present? (4)
    - Which "type" is used in the various requests and replies? (8 in requests, 0 in replies)
    - Do ICMP message contain also some payload? (yes, it is repeated in each request/reply pair)

7. Traceroute (file traceroute_MPLS.cap)

- Which protocol is used to perform traceroute? (UDP)
- Which IP address starts traceroute? What is the destination of traceroute? (10.0.1.2; 172.16.0.2)
- How many packets are sent at each iteration? How can we state this? (3; TTL is increased by 1 every 3 packets; consequently, each router in the path provides three replies of type *time exceeded*)
- Observe used S/D ports. What can we observe from them? (they are never fixed, but increased by 1 at each packet sent by the source host)
- Which type of message is used by the routers to reply? (ICMP *time exceeded*; at the last ICMP request, the reply is of type destination unreachable (type=3) + port unreachable (code=3))
- Write the entire path obtained with traceroute at the end of the whole operation. (10.0.1.2; 10.0.1.1; 10.0.9.5; 10.0.9.2; 10.0.2.1; 10.0.2.2.; 172.16.0.2)

8. DHCP (file dhcp.pcap)

- Which transport protocol is used? Which ports are used? (UDP; Server: 67, Client: 68)

- What is the sequence of DHCP messages between client and server? (Discover, Offer, Request, ACK)
- Which IP addresses are used in the first message? Why? (S: empty; D: local broadcast. Because the IP address of the DHCP server is not known and because the source host is requesting the assignment of an IP address)
- Which addresses are used at layer 2? (S: given MAC, D: broadcast)
- Repeat previous points for the remaining packets. (N.B. in the 2nd and 4th packets, destination IP address is indeed a local broadcast, as the host hasn't received the assignment of an IP address; however, anyway Wireshark interprets the destination IP address as if it is inserted in the destination address of the IP header)

9. RIP v1 (file RIPv1.cap)

- Which transport protocol is used? Which ports are used? (UDP, 520)
- Which address (IP-MAC) is the destination of RIP messages? Why? (broadcast; RIP sends distance vector to its neighbors; inserting broadcast MAC/IP addresses does not represent a problem because each router receiving such packets – i.e., with IP destination = limited broadcast – does not propagate the packet on its other interfaces)
- Which network(s) becomes unreachable? How can we state this? (192.168.2.0; in some messages there are networks with cost = 16)

10. RIP v2 (file RIPv2.cap)

- Which transport protocol is used? Which ports are used? (UDP, 520)
- Which information is added compared to RIPv1? (netmask and next-hop, among others)

11. RARP (file rarp_req_reply.pcap)

- Which IU incapsulates RARP message? (directly in an Ethernet frame)
- What is the destination address for RARP request? And what is the destination for RARP reply? Why?
- Which are the empty fields in RARP request? Why? (N.B., in RARP request also "target hardware address" field is non-empty, but in general it may be left empty)

Useful links

http://packetlife.net/

https://wiki.wireshark.org/SampleCaptures