VŠB TECHNICKÁ UNIVERZITA OSTRAVA | FAKULTA ELEKTROTECHNIKY A INFORMATIKY | KATEDRA TELEKOMUNIKAČNÍ TECHNIKY

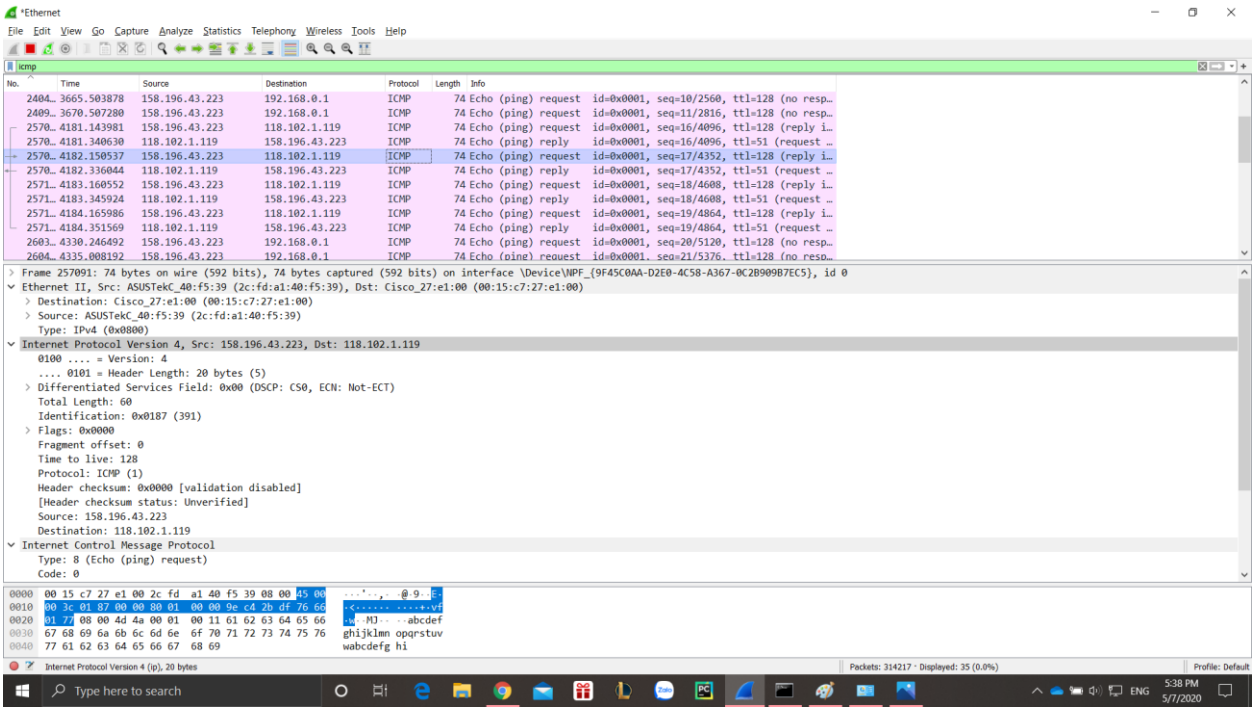
Telecommunication Networks Introduction to Computer Networks (homework)

Date: 22. 4. 2020
Name: Nguyen Thanh Tuan
Login: NGU0120
Subject: Telecommunication Networks

Tasks

1) Using the network analyzer Wireshark, capture and identify the ICMP (Internet Control Message Protocol) messages – echo request and echo reply (are generated by the command **`ping`**).

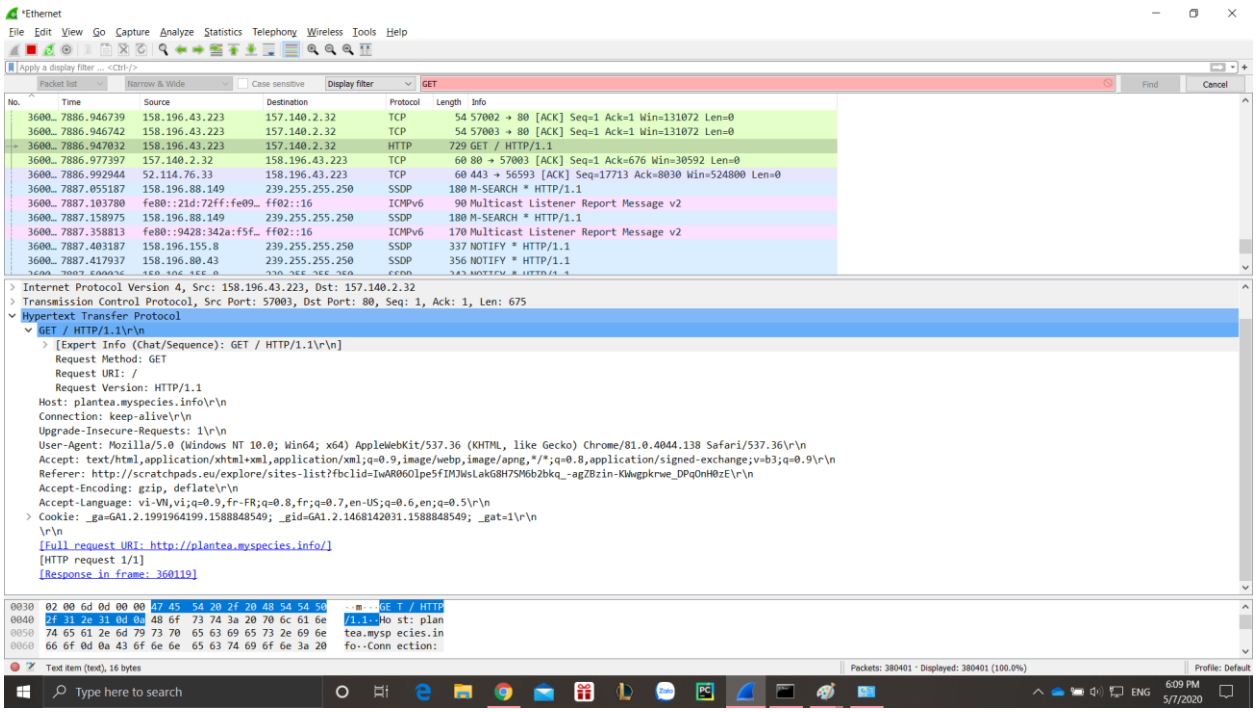
Answer:



Picture 1: ICMP messages captured by Wireshark

2) Using Wireshark, capture and identify communication when downloading a web page – HTTP (HyperText Transfer Protocol) at the application layer and TCP (Transmission Control Protocol) at the transport layer. To translate a web address into an IP address, the DNS (Domain Name System) protocol is used.

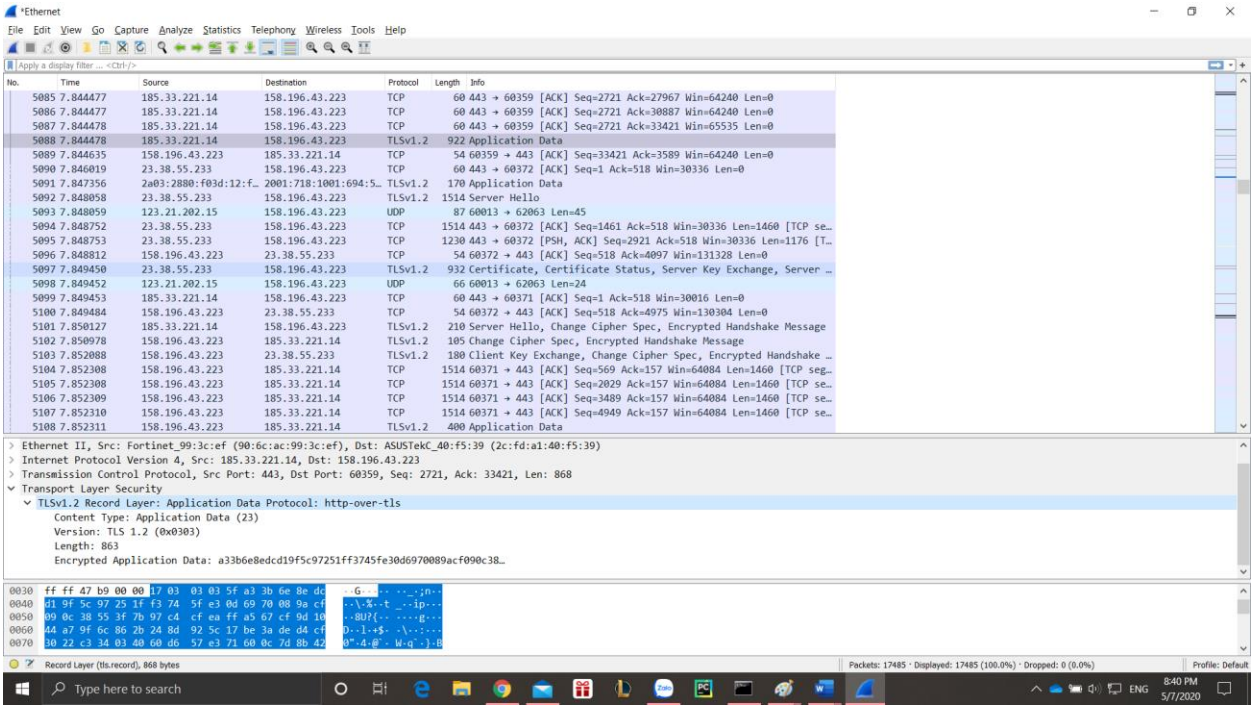
Answer:



Picture 2: The process of communication with a web server captured by Wireshark

3) Using Wireshark, capture and identify communication when sending an e-mail. When sending an e-mail via the web interface, HTTP is used. In general, SMTP (Simple Mail Transfer Protocol) is used for sending an e-mail and POP (Post Office Protocol) or IMAP (Internet Message Access Protocol) for downloading an e-mail from the e- mail box

Answer:



Picture 3: The process of secure communication when sending an e-mail by SMTP protocol captured by Wireshark

4) Create a report that contains images with an example of captured traffic according to tasks 1) - 3). Follow Fig. 1 - 3. IP addresses and web addresses may of course be different, but try to capture messages of the same protocols - ICMP, DNS, TCP, HTTP, TLS, etc. Briefly describe the captured communication. Submit the report in PDF format on the website lms.vsb.cz - Telecommunication Networks course.

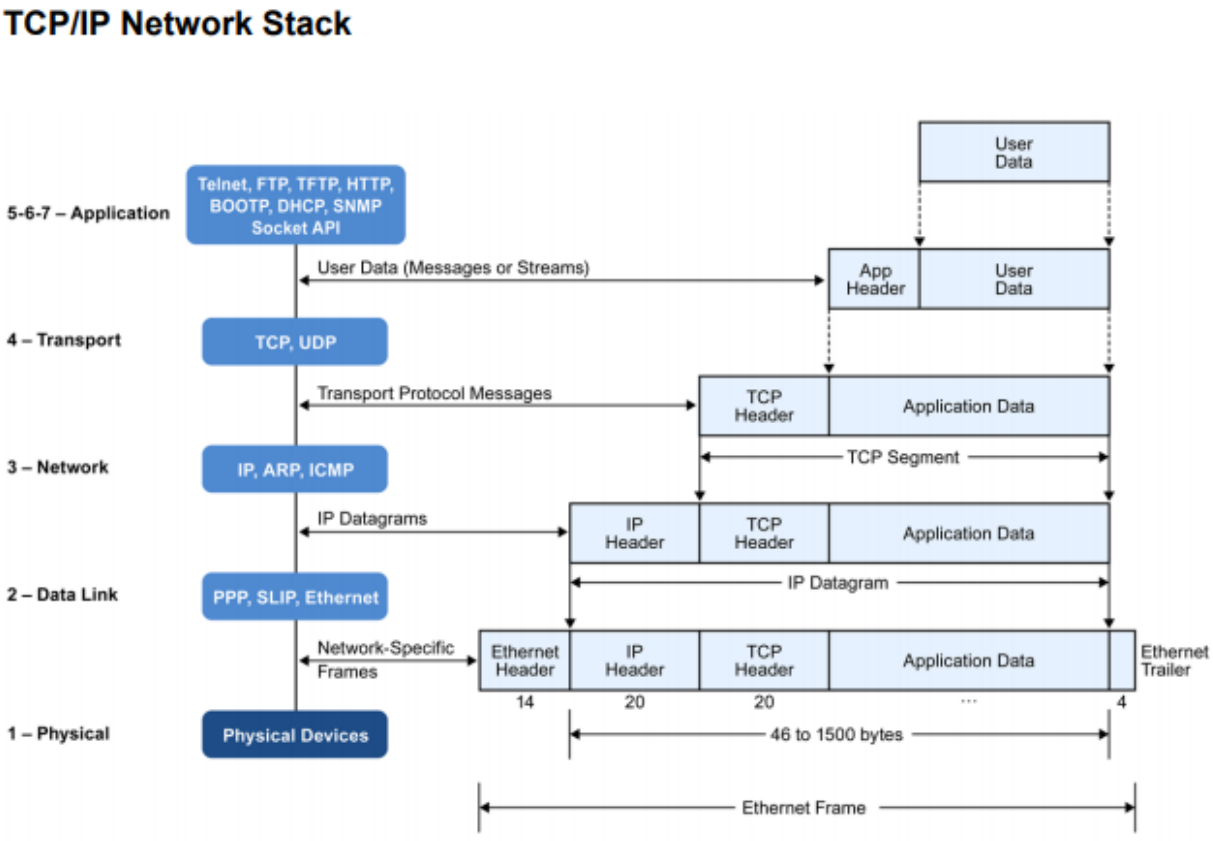
- The Internet Control Message Protocol (ICMP) is a supporting protocol in the Internet protocol suite. It is used by network devices, including routers, to send error messages and operational information indicating success or failure when communicating with another IP address, for example, an error is indicated when a requested service is not available or that a host or router could not be reached. ICMP differs from transport

protocols such as TCP and UDP in that it is not typically used to exchange data between systems, nor is it regularly employed by end-user network applications (with the exception of some diagnostic tools like ping and traceroute).

- ICMP is part of the Internet protocol suite as defined in RFC 792. ICMP messages are typically used for diagnostic or control purposes or generated in response to errors in IP operations (as specified in RFC 1122). ICMP errors are directed to the source IP address of the originating packet.

- For example, every device (such as an intermediate router) forwarding an IP datagram first decrements the time to live (TTL) field in the IP header by one. If the resulting TTL is 0, the packet is discarded and an ICMP time exceeded in transit message is sent to the datagram's source address.

- Many commonly used network utilities are based on ICMP messages. The traceroute command can be implemented by transmitting IP datagrams with specially set IP TTL header fields, and looking for ICMP time exceeded in transit and Destination unreachable messages generated in response. The related ping utility is implemented using the ICMP echo request and echo reply messages.



Picture 4: Encapsulation of Data in the TCP/IP Network Stack

- ICMP uses the basic support of IP as if it were a higher-level protocol, however, ICMP is actually an integral part of IP. Although ICMP messages are contained within

standard IP packets, ICMP messages are usually processed as a special case, distinguished from normal IP processing. In many cases, it is necessary to inspect the contents of the ICMP message and deliver the appropriate error message to the application responsible for transmitting the IP packet that prompted the ICMP message to be sent.

- ICMP is a network-layer protocol. There is no TCP or UDP port number associated with ICMP packets as these numbers are associated with the transport layer above.