Wireshark:

1. **Uvod:**

Da lakše uočite što uopće gledate na Wiresharku (a gledati ćete između ostalog headere i trailere za pojedine pakete), pogledajte koje sve podatke sadrže pojedina zaglavlja (UDP i TCP header, IP header i Data Link Header i trailer):

UDP i TCP header: https://skminhaj.wordpress.com/2016/02/15/tcp-segment-vs-udp-datagram-header-format/

IP header: https://skminhaj.wordpress.com/2014/12/22/ip-protocol-header-fundamentals-explained-with-diagrams/

Data Link Header i trailer: https://en.wikipedia.org/wiki/Ethernet_frame

2. **Instalacija Wireshark programa**

Trebate na računalo instalirati program Wireshark: https://www.wireshark.org/

3. **Upute za ra s Wireshark programom**

Wireshark Tutorial For Beginners (2020) From Absolute Basics To intermediate Level

https://www.youtube.com/watch?v=DCqbOhWSFus

https://www.youtube.com/watch?v=z25YNudxayA

Dodatni filmovi s uputama za rad s mladim gospodinom i/ili mladom damom:
https://www.youtube.com/watch?v=TkCSr30UojM
https://www.youtube.com/watch?v=6X5TwvGXHP0
https://www.youtube.com/watch?v=f4zqMDzXt6k
https://www.youtube.com/watch?v=dN8PcdOdcHs

4. **Proučiti**
   a. **Što su portovi u računalu i čemu služe?**
      https://helpdeskgeek.com/networking/hdg-explains-what-is-a-computer-port-what-are-they-used-for/
   b. **Koristeći naredbu Netstat kako bi pretražili Portove i PID u Windowsima**
      https://helpdeskgeek.com/how-to/use-netstat-to-see-listening-ports-and-pid-in-windows/
      Command prompt: >netstat -a -n -o
      Task Manager - Details – PID
      https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers
      https://www.wireshark.org/docs/dfref/
      https://www.site24x7.com/find-ip-address-of-web-site.html

5. **Testiranje dijela mogućnosti Wireshark programa**

1. pokrenuti snimanje paketa i otvoriti neku web stranicu, pa u filtar upisati "dns". Potražiti što radi DNS protokol
2.
3. tcp contains tsrb ili koju ste već stranicu otvorili

4. filtar: ip.addr ==192.168.1.xx
5. filtar: ip.src ==192.168.1.xx
6. filtar: ip.dst==192.168.1.xx
7. filtar: tcp.port==443
8. filtar: frame contains tsrb
9. menu: statistics - endpoints --> možete vidjeti koliko je paket/bajta pojedina ip adresa primila/poslala
10. filtar: utipkati "tcp" i OK, a zatim desni klik na redak (frame), odabrati Apply as filter – Selected
11. da biste povezali jednu (cijelu) konverzaciju i sastavili poruku od svih frejmova u konverzaciji, selektirati frame, desni klik i odabrati Follow - TCP stream, ili UDP stream...
12. filtar: udp contains tsrb ili odabrana web stranica
13. Potom odabrati frame sa Standard query .....U srednjem prozoru odabrati najniži red Domain Name System (query), uočiti da DNS protokol ide preko UDP protokola
14. U frameu Standard query Response.....se može u srednjem prozoru, pod Domain Name System pronaći Answers i IP adresa koju vraća DNS
15. filtar: arp , provjerite tko pita, što pita i tko odgovara, destination može biti jedan uređaj ili broadcast! Potražiti što radi ARP protokol, pronaći razliku između Unicast, Multicast i Broadcast
16. Uočite da se traži MAC adresa za poznatu IP adresu...
17. Provjerite u srednjem prozoru, pod Ethernet II, Destination : Broadcast ff:ff:ff:ff:ff:ff, što znači da se upit šalje na sve portove, odnosno na sva računala u mreži