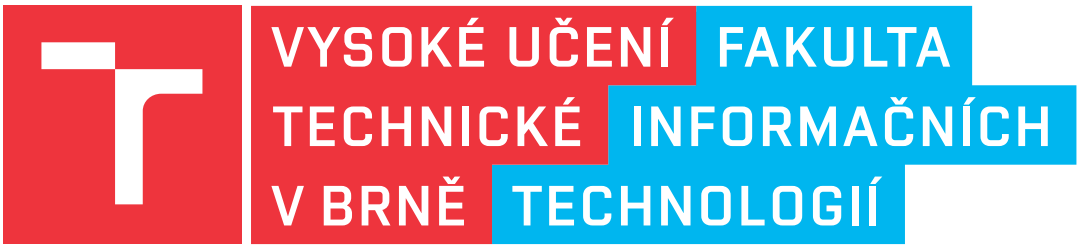


IPK projekt
ZETA: Sniffer paketov
Manuál

25. apríla 2021 Peter Močáry (xmocar00)

Obsah

1 Úvod 2

2 Teoretické základy 2

3 Implementácia 3

4 Testovanie programu 3

1 Úvod

Cieľom projektu je implementácia sieťového analyzátora, ktorý je schopný zachytávať a filtravať pakety na zvolenom sieťovom rozhraní. Program vypisuje zachytené pakety na štandardný výstup. Tento projekt nás zoznámi s problematikou zachytávania paketov a získavania dôležitých informácií z nich.

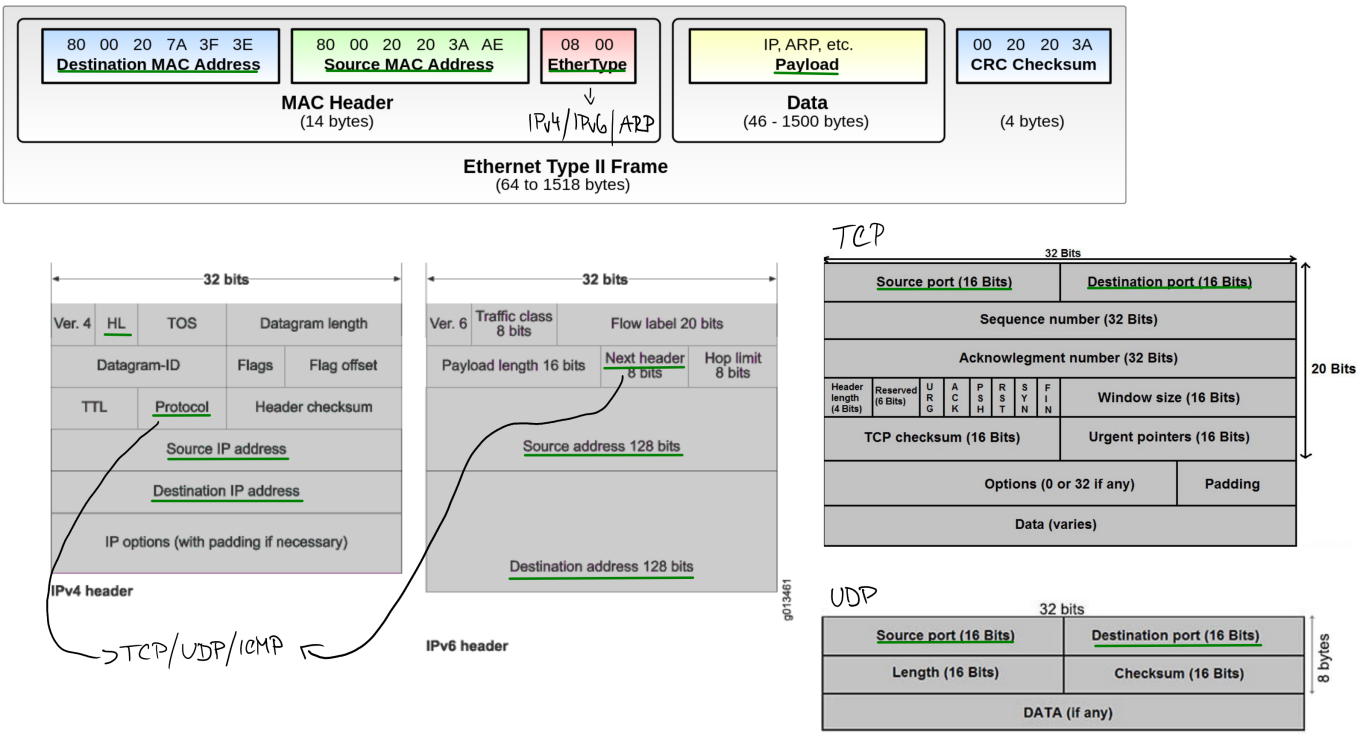
2 Teoretické základy

Pre pochopenie čo nás v projekte čaká si potrebujeme objasniť pár dôležitých pojmov. Na začiatku nás zaujíma čo to vlastne je paket?

Packet viz [5] je formátovaná jednotka dát prenášaná po sieti, ktorá nesie dáta od odosielateľa príjemcovi. Okrem dát však nesie aj hlavičku, ktorá v sebe skrýva potrebné informácie pre úspešnú dopravu k príjemcovi.

Ďalej je potrebné vedieť, že dáta nám budú po sieti prichádzať obalení vo viacerých vrstvách. Prvou je tzv. *Ethernetový rámec* [1], ktorý tvorí kompatibilnú vrstvu obalujúcu všetky pakety, ktoré nás pre tento projekt zaujímajú. Ethernetový rámec ďalej môže obsahovať rôzne typy protokolov. Určiť druh nasledujúceho protokolu vieme z hlavičky Ethernetového rámca pomocou *EtherType* [7] časti. Z nich filtrujeme IPv4 [6], IPv6 [8] a ARP [3]. Avšak, táto vrstva nie je posledná. Internetové protokoly v sebe ešte ukrývajú TCP [2], UDP [4] a ICMP [9]. Každý protokol má svoju hlavičku a pre naše potreby nás budú zaujímať časti vyznačené na obrázku 1.

Našou úlohou teda bude prečítať z týchto hlavičiek všetko potrebné a vypísať dané informácie užívateľovi podla toho aké argumenty programu zadal.



Obr. 1: Potrebné časti hlavičiek[1]

3 Implementácia

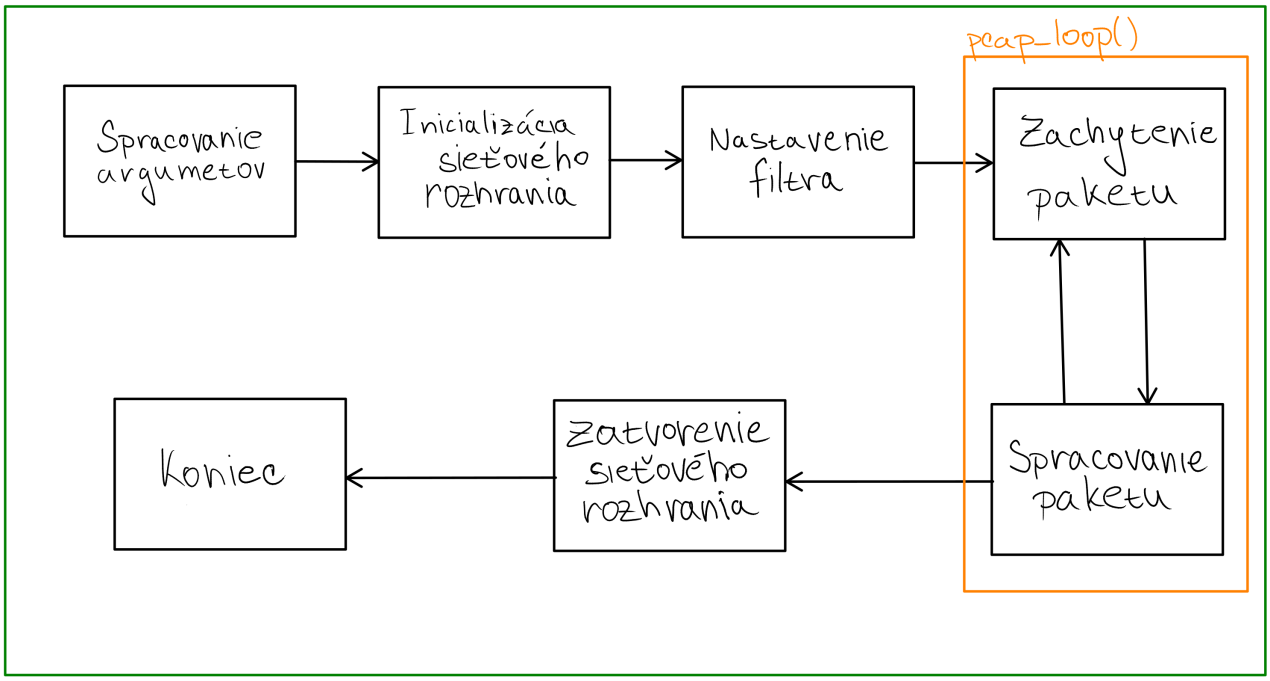
Projekt je implementovaný v jazyku C s využitím knižnice `libpcap` viz [?]. Program mmá jednoduchú štruktúru, ktorú môžete vidieť na obrázku 2.

Hneď po spracovaní argumentov programu zadaných užívateľom sa inicializuje sieťové rozhranie, ktoré má nastavené reagovanie na prečítaný packat ihneď ako ho prečíta pomocou funkcie `pcap_set_immediate_mode()`.

Nastavenie filtra prebieha vygenerovaním pseudokódu z argumentov, ktoré používateľ zadal. Ten je následne skompilovaný a nastavený ako filter paketov.

Nasleduje samotný „sniffing“ paketov, pre ktorý je využitá funkcia `pcap_loop()`, ktorá pri zachytení paketu zavolá obslužnú funkciu a vypíše požadovaný formát paketu na výstup viz obrázok 3.

Na záver nesmieme zabudnúť správne uzavrieť sieťové rozhranie a uvoľniť vymedzenú pamäť.

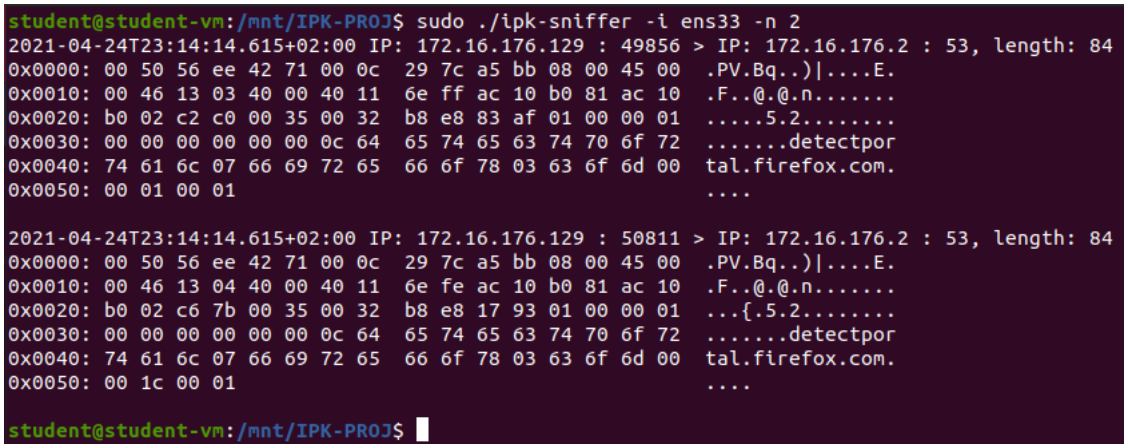


Obr. 2: Nastienenie fungovania programu (inšpirované [10])

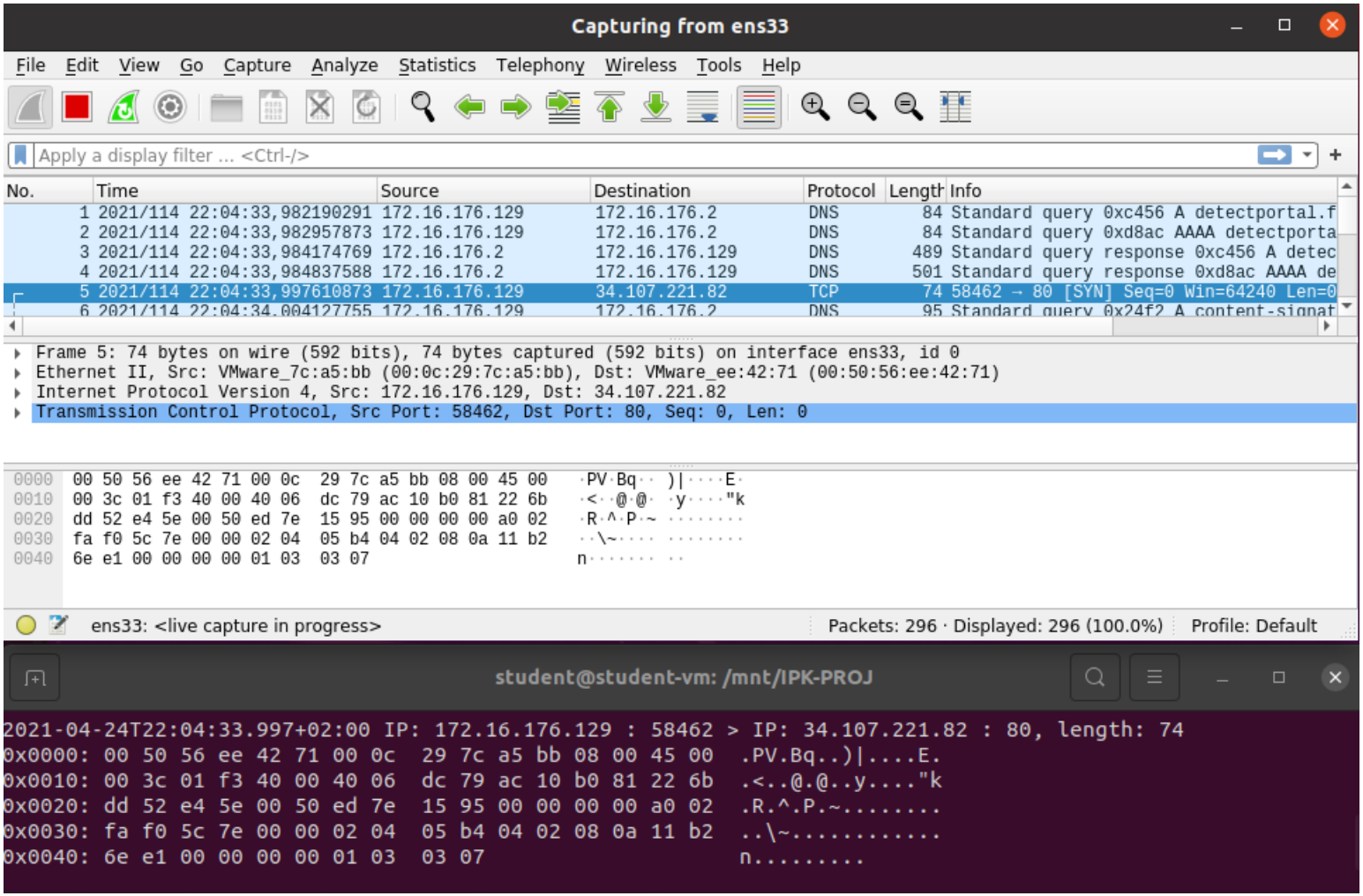
4 Testovanie programu

Testovanie prebehlo na referenčnom virtualnom stroji za použitia programu Wireshark jednoduchým porovnávaním výsledkov „sniffera“ a Wiresharku.

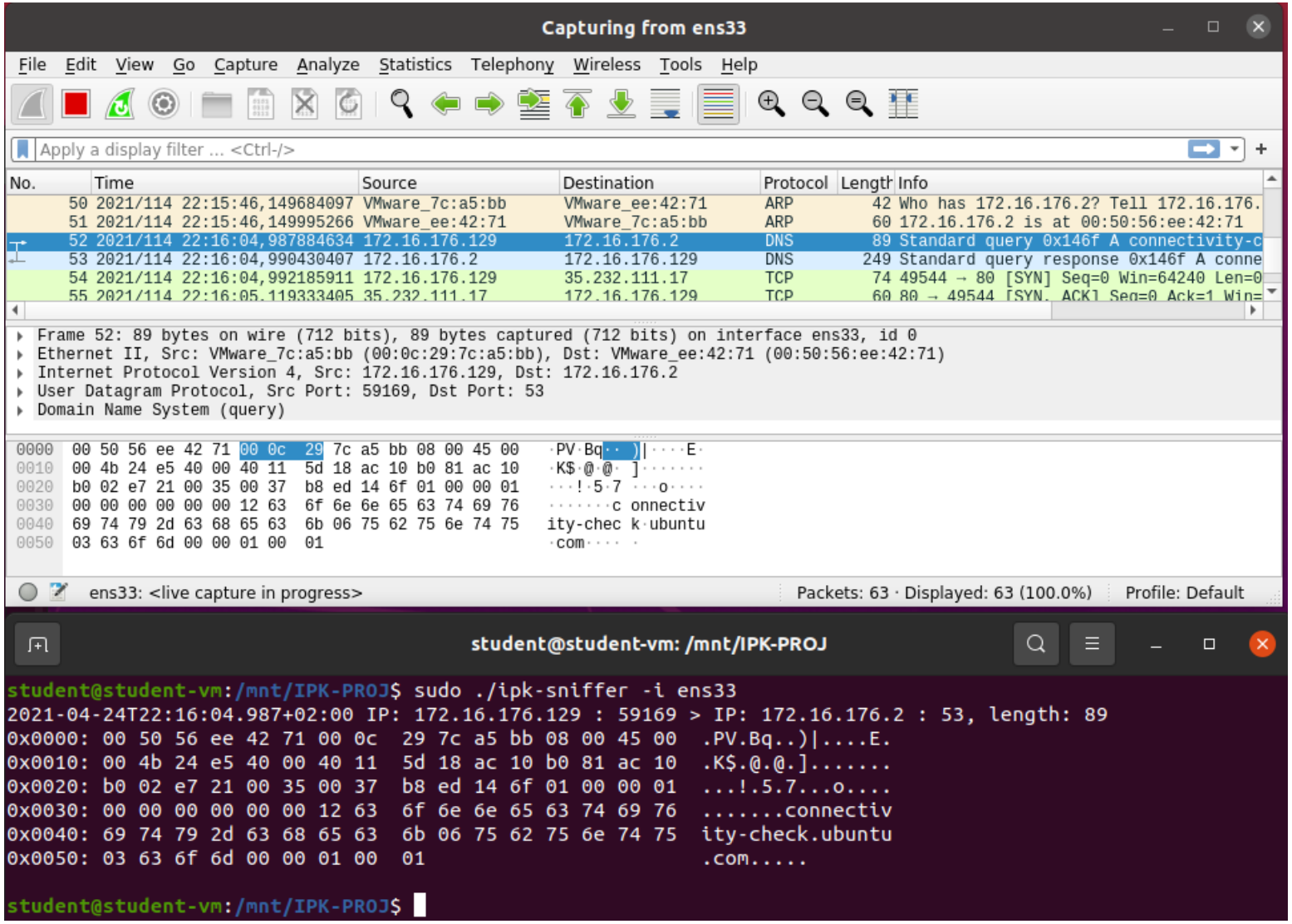
[1] Ďalšie použité zdroje viz [11] [12]



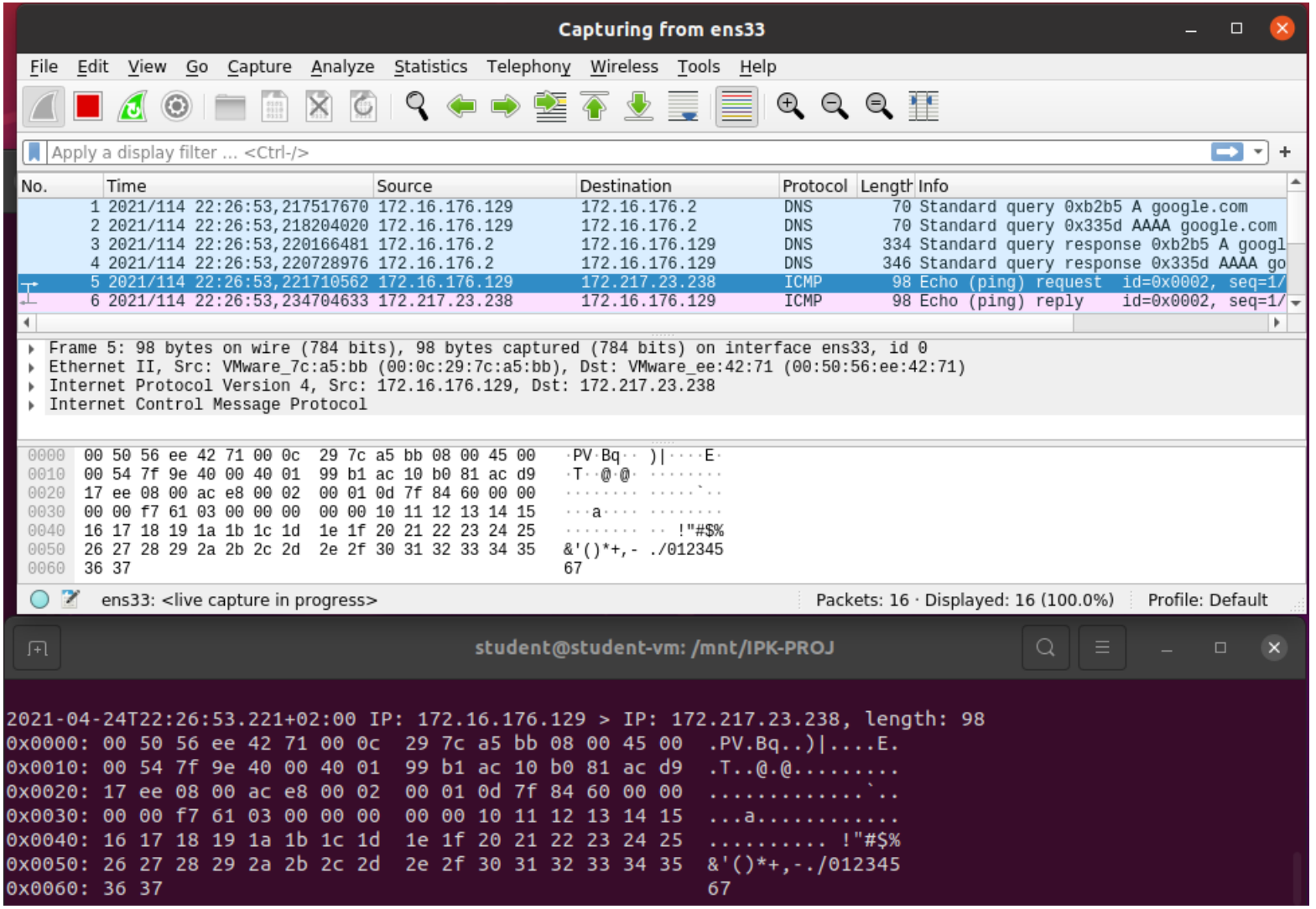
Obr. 3: Ukážka správneho výstupu



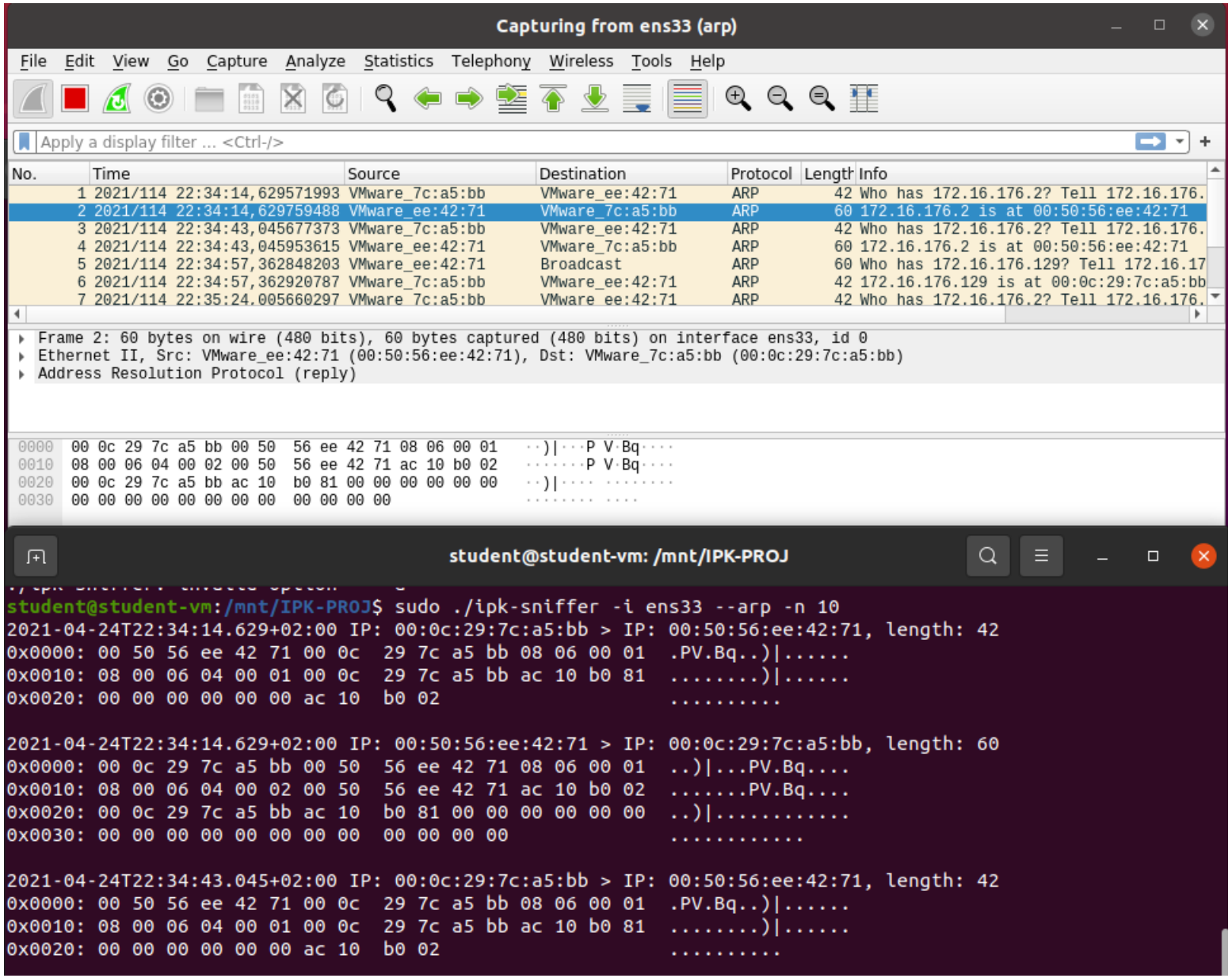
Obr. 4: Test TCP



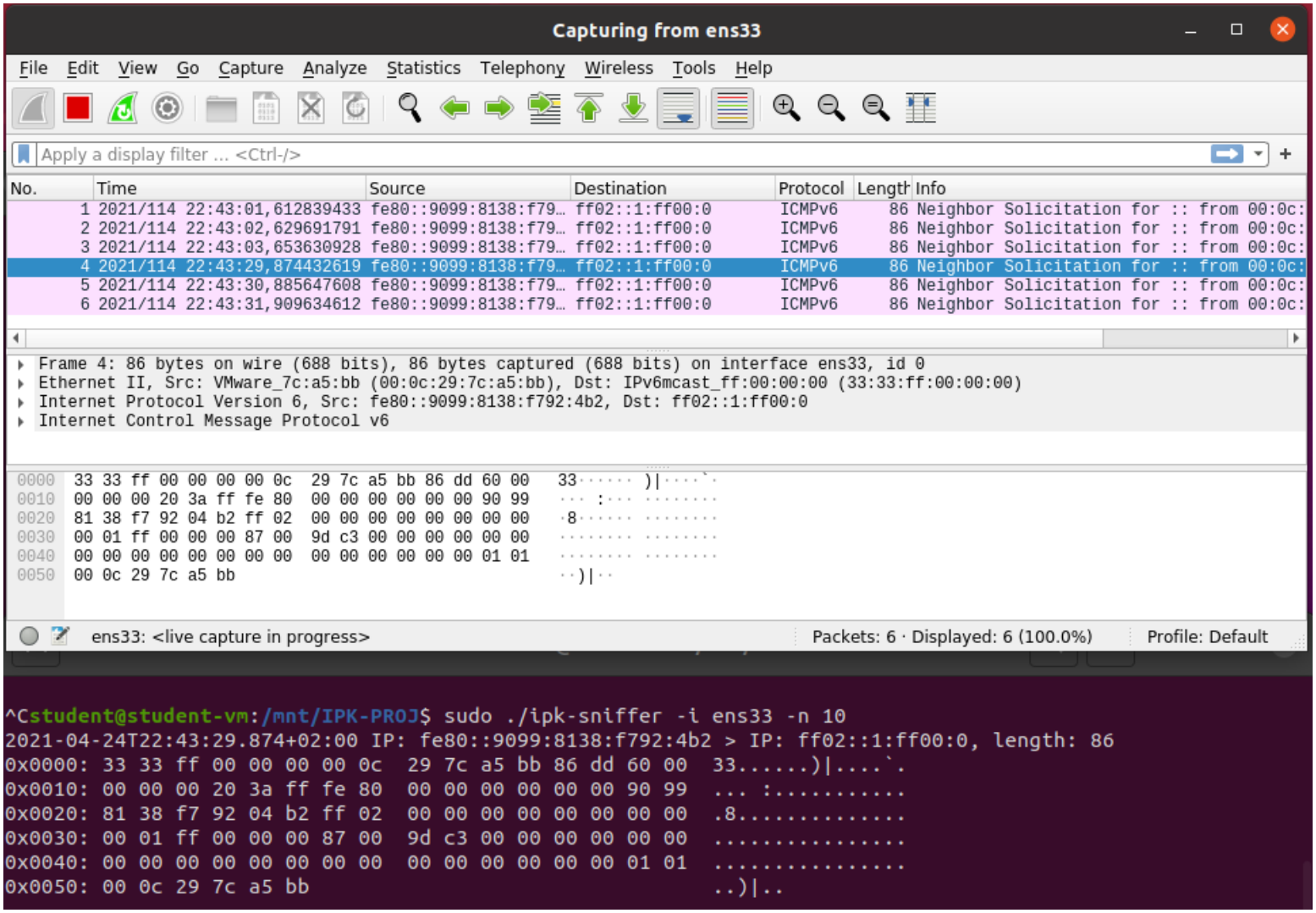
Obr. 5: Test UDP



Obr. 6: TEST ICMP



Obr. 7: TEST ARP



Obr. 8: TEST ICMPv6

Literatúra

[1] Ethernet frame. [online], Posledná modifikácia: 03. február 2021, [vid. 2021-04-20]. Dostupné z: https://en.wikipedia.org/wiki/Ethernet_frame

[2] Transmission Control Protocol. [online], Posledná modifikácia: 05. apríl 2021, [vid. 2021-04-21]. Dostupné z: https://en.wikipedia.org/wiki/Transmission_Control_Protocol

[3] Address Ressolution Protocol. [online], Posledná modifikácia: 07. apríl 2021, [vid. 2021-04-20]. Dostupné z: https://en.wikipedia.org/wiki/Address_Resolution_Protocol

[4] User Datagram Protocol. [online], Posledná modifikácia: 08. apríl 2021, [vid. 2021-04-21]. Dostupné z: https://en.wikipedia.org/wiki/User_Datagram_Protocol

[5] Network Packet. [online], Posledná modifikácia: 11. apríl 2021, [vid. 2021-04-20]. Dostupné z: https://en.wikipedia.org/wiki/Network_packet

[6] IPv4. [online], Posledná modifikácia: 12. apríl 2021, [vid. 2021-04-21]. Dostupné z: https://en.wikipedia.org/wiki/IPv4

[7] EtherType. [online], Posledná modifikácia: 16. január 2021, [vid. 2021-04-20]. Dostupné z: https://en.wikipedia.org/wiki/EtherType

[8] IPv6. [online], Posledná modifikácia: 17. apríl 2021, [vid. 2021-04-21]. Dostupné z: https://en.wikipedia.org/wiki/IPv6

[9] Internet Control Message Protocol. [online], Posledná modifikácia: 19. apríl 2021, [vid. 2021-04-21]. Dostupné z: https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol

[10] Garcia, L. M.: Programming with Libcap – Sniffing the Network From Our Own Appliction. *Hakin9*, ročník 3, č. 2, 2 2008: s. 39 – 43, ISSN 1733 – 7186. Dostupné z: http://recursos.aldabaknocking.com/libpcapHakin9LuisMartinGarcia.pdf

[11] Juniper Networks, I.: IPv6 Overview. [online], Posledná modifikácia: 13. august 2014, [vid. 2021-04-23]. Dostupné z: https://www.juniper.net/documentation/en_US/junose15.1/topics/concept/ipv6-overview.html

[12] Liang, K.: Explaining TCP/IP. [online], Posledná modifikácia: 18. jún 2018, [vid. 2021-04-23]. Dostupné z: https://kelvin.ink/2018/06/18/ExplainingTCP_IP/