Ľubomír Dlhý, ID: 102897

ANALYZÁTOR SIEŤOVEJ KOMUNIKÁCIE

Ľubomír Dlhý, ID: 102897

ZADANIE ÚLOHY

Navrhnite a implementujte programový analyzátor Ethernet siete, ktorý analyzuje komunikácie v sieti zaznamenané v .pcap súbore a poskytuje nasledujúce informácie o komunikáciách.
Vypracované zadanie musí spĺňať nasledujúce body:

1) Výpis všetkých rámcov v hexadecimálnom tvare postupne tak, ako boli zaznamenané v súbore.
Pre každý rámec uveďte:

a) Poradové číslo rámca v analyzovanom súbore.
b) Dĺžku rámca v bajtoch poskytnutú pcap API, ako aj dĺžku tohto rámca prenášaného po médiu.
c) Typ rámca – Ethernet II, IEEE 802.3 (IEEE 802.3 s LLC, IEEE 802.3 s LLC a SNAP, IEEE 802.3 – Raw).
d) Zdrojovú a cieľovú fyzickú (MAC) adresu uzlov, medzi ktorými je rámec prenášaný. Vo výpise jednotlivé bajty rámca usporiadajte po 16 alebo 32 v jednom riadku. Pre prehľadnosť výpisu je vhodné použiť neproporcionálny (monospace) font.

2) Pre rámce typu Ethernet II a IEEE 802.3 vypíšte vnorený protokol. Študent musí vedieť vysvetliť, aké informácie sú uvedené v jednotlivých rámcoch Ethernet II, t.j. vnáranie protokolov ako aj ozrejmiť dĺžky týchto rámcov.
3) Analýzu cez vrstvy vykonajte pre rámce Ethernet II a protokoly rodiny TCP/IPv4: Na konci výpisu z bodu 1) uveďte pre IPv4 pakety:

a) Zoznam IP adries všetkých prijímajúcich uzlov,
b) IP adresu uzla, ktorý sumárne prijal (bez ohľadu na odosielateľa) najväčší počet paketov a koľko paketov prijal (berte do úvahy iba IPv4 pakety).

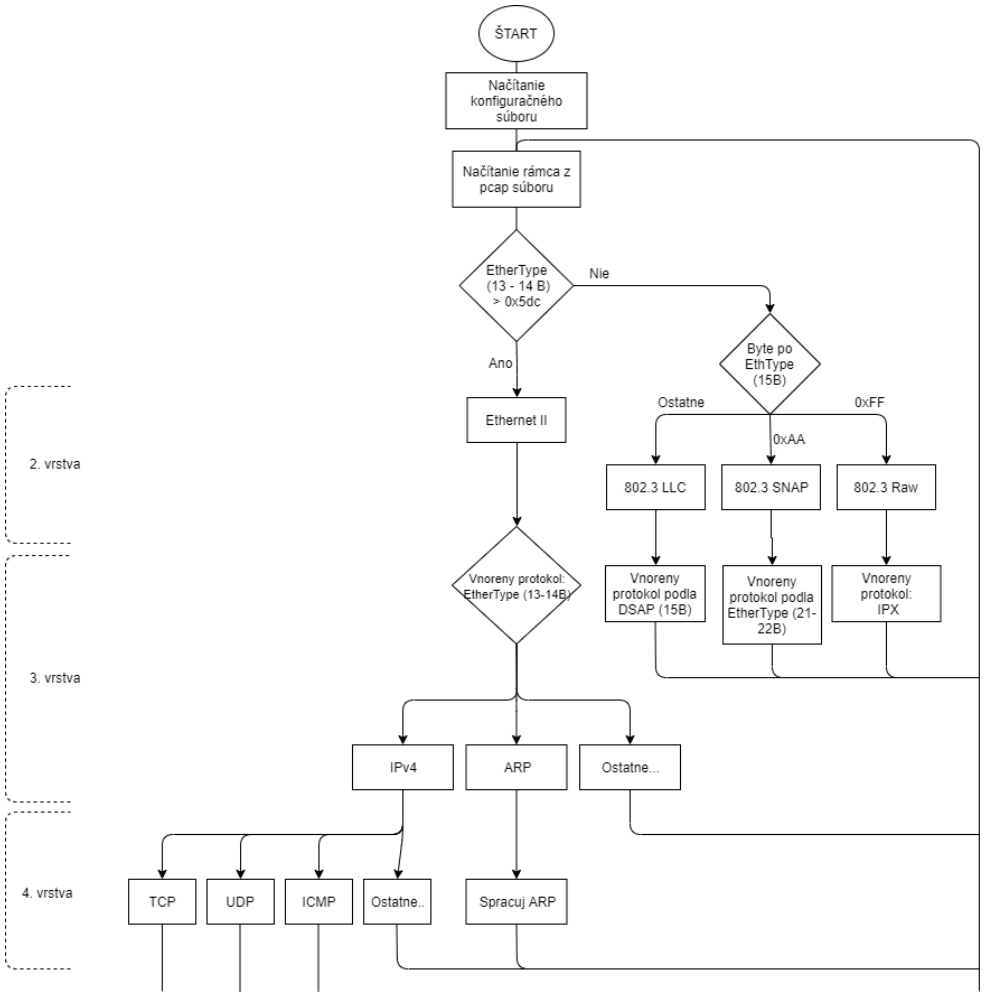
IP adresy a počet poslaných paketov sa musia zhodovať s IP adresami vo výpise Wireshark -> Statistics -> IPv4 Statistics -> Source and Destination Addresses.
4) V danom súbore analyzujte komunikácie pre zadané protokoly:

a) HTTP
b) HTTPS
c) TELNET
d) SSH
e) FTP riadiace
f) FTP dátové
g) TFTP, uveďte všetky rámce komunikácie, nielen prvý rámec na UDP port 69
h) ICMP, uveďte aj typ ICMP správy (pole Type v hlavičke ICMP), napr. Echo request, Echo reply, Time exceeded, a pod.
i) Všetky ARP dvojice (request – reply), uveďte aj IP adresu, ku ktorej sa hľadá MAC (fyzická) adresa a pri ARP-Reply uveďte konkrétny pár - IP adresa a nájdená MAC adresa. V prípade, že bolo poslaných viacero rámcov ARP-Request na rovnakú IP adresu, vypíšte všetky. Ak sú v súbore rámce ARP-Request bez korešpondujúceho ARP-Reply (alebo naopak ARP- Reply bez ARP-Request), vypíšte ich samostatne.

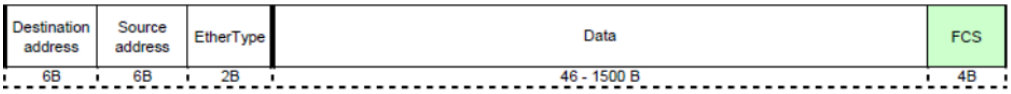
Ľubomír Dlhý, ID: 102897

NÁVRH FUNGOVANIA RIEŠENIA

.



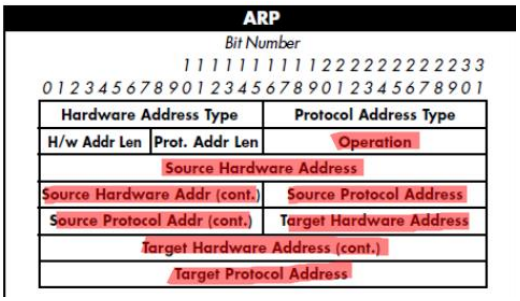
Program sa začne načítaním protokolov z konfiguračného súboru. Následne sa začne načítavať pcap súbor po rámcoch. Najprv sa získa informácie o dĺžke paketu zo štruktúry Pkthdr, potom sa získajú MAC Adresy. Zdrojová MAC Adresa sa nachádza na prvých 6 byteoch, cieľová na nasledujúcich 6 byteoch.

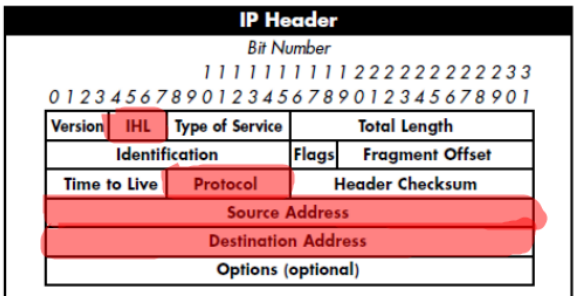


Identifikuje sa 2. vrstva – Linková vrstva podľa poľa EtherType (13-14B), prípadne bajtu po poli EtherType (ak ide o IEEE 802.3). O Ethernet II ide, ak je pole EtherType väčšie ako hodnota 0x5DC, inak ide o IEEE 802.3. Ďalej treb špecifikovať typ IEEE 802.3, to sa robí podľa bajtu za EtherType poľom. IEEE 802.3 RAW má hodnotu tohto bajtu 0xFF, 802.3 SNAP 0xAA a všetky ostatné hodnoty patria 802.3 LLC. Pre všetky rámce sa zistí vnorený protokol z možných protokolov nachádzajúcich sa v konfiguračnom súbore – pre Ethernet II a 802.3 SNAP podľa poľa EtherType, pre 802.3 LLC podľa LSAP, 802.3 RAW ma vždy vnorený protokol IPX.

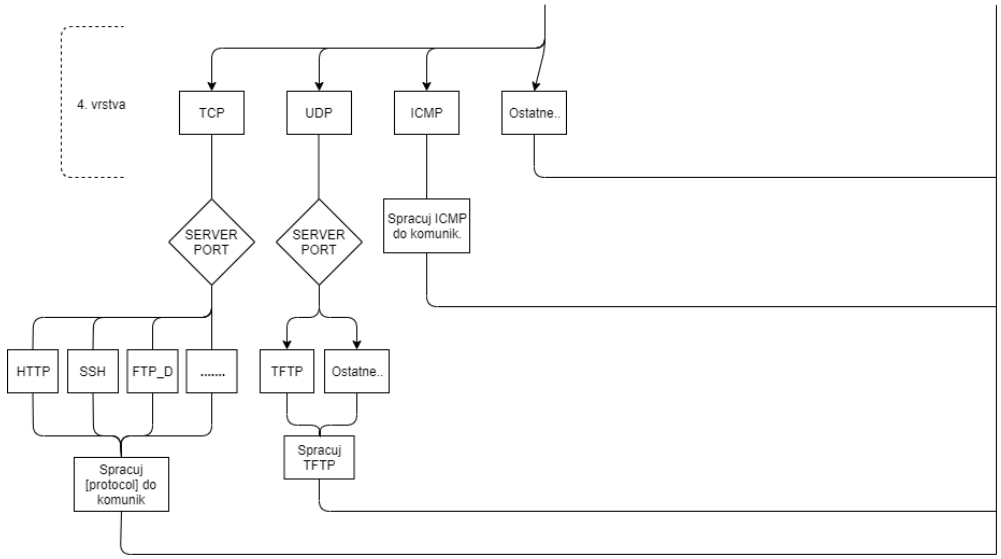
Ľubomír Dlhý, ID: 102897

Pre Ethernet II sa ďalej analyzuje IPv4 protokol a ARP. ARP rámce sa analyzujú a zoskupujú do komunikácií. V ARP hlavičke sú dôležité hodnoty *Operation, Source MAC, Source IP, Target Mac a Target IP*. Podľa *Operation* rozlišujeme, či ide o žiadosť alebo o odpoveď. IP adresy slúžia na zlúčenie do komunikácií.

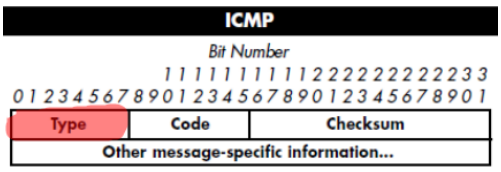


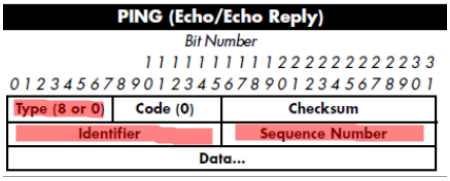


Z IPv4 hlavičky zistíme IP Adresy (zdrojovú a cieľovú), vnorený protokol na transportnej vrstve a veľkosť IP hlavičky (keďže jej veľkosť sa mení) pomocou IHL, ktorý určuje počet 4-bajtových slov v hlavičke.



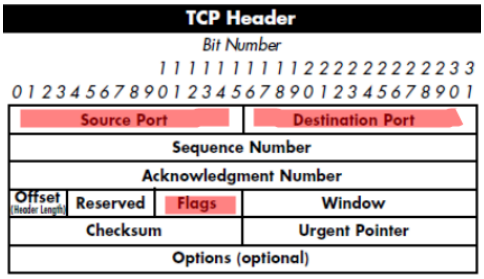
Na transportnej vrstve sa ďalej rozoberajú pakety s TCP, UDP a ICMP protokolom.

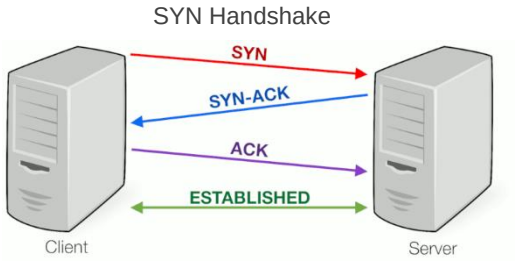




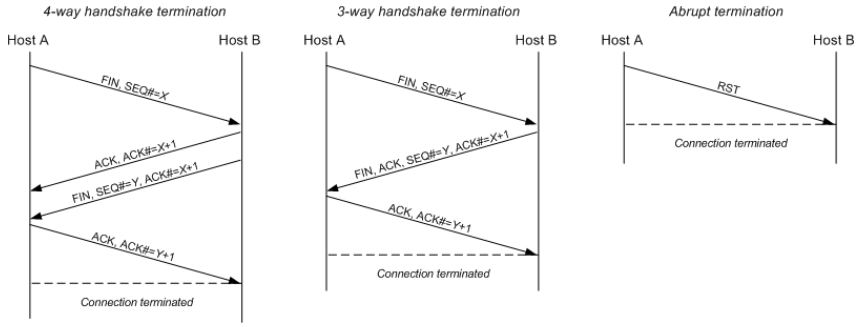
V ICMP je vo všeobecnosti dôležité pole *Type*, ktoré určuje typ ICMP paketu. Pre hodnoty 8 a 0 ide o špeciálny typ Echo (Ping), kde sa páruje do komunikácie request (8) a reply (0) podľa poľa *Identifier* a *Sequence Number*. Ostatné typy ICMP paketov sa zoskupujú iba podľa IP adries.

Ľubomír Dlhý, ID: 102897

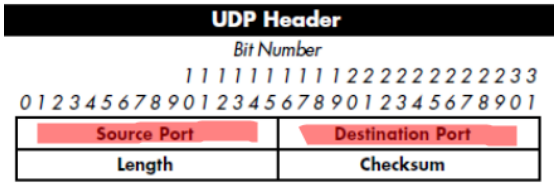


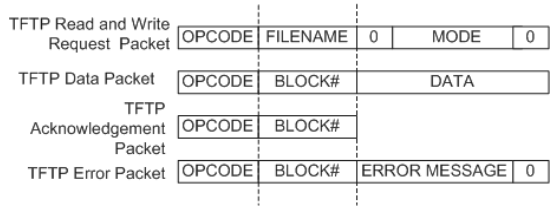


Pre TCP sa podľa server portu (menšieho portu zo zdrojového alebo cieľového) určuje vnorený (aplikačný) protokol, porty sa ukladajú. Konkrétne protokoly sa spracúvajú do TCP komunikácií podľa spojenia, kde treba sledovať pole Flags v TCP hlavičke. Pri komunikácii treba spojenie otvoriť pomocou tzv. SYN Handshake, v ktorom sú 3 pakety s flagmi v nasledujúcej postupnosti : SYN, SYN+ACK, ACK.



Ukončenie komunikácie prebieha pomocou 4-way alebo 3-way handshake-u, prípadne resetom. Komunikácia sa považuje za kompletnú, ak je otvorená i zatvorená. Iba otvo rená komunikácia je nekompletná.





Pre UDP sa tiež podľa server portu určí vnorený protokol, porty sa taktiež uložia. Analyzuje sa ďalej TFTP protokol, ktorý funguje na rôznych portoch (na porte 69 sa začne komunikácia, samotná komunikácia prebieha na inom, náhodne zvolenom porte). V TFTP hlavičke je 2-bajtové pole *OPCODE*, ktoré určuje jeden z 5 typov TFTP paketu.

Po kompletnej analýze rámca a uložení dôležitých informácií sa prejde na ďalší paket z pcap súboru.

Ľubomír Dlhý, ID: 102897

ŠTRUKTÚRA EXTERNÝCH SÚBOROV

Konfiguračný súbor s protokolmi má nasledovnú štruktúru:

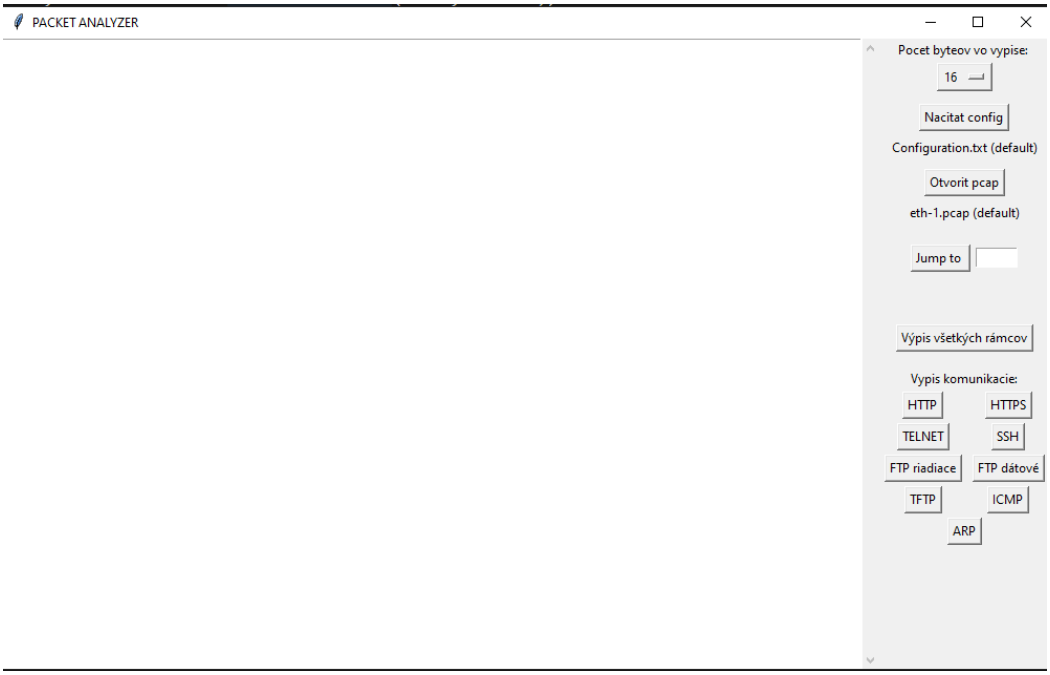
```
#Ethertypes
0x0800 IPv4
0x0806 ARP
0x86dd IPv6

#LSAPs
0x42 STP
0xaa SNAP
0xe0 IPX

#IPs
0x01 ICMP
0x06 TCP
0x11 UDP

#TCPs
0x0016 SSH
0x0050 HTTP
0x1bb HTTPS
0x17 TELNET
0x15 FTP RIADIACE
0x15 FTP DATOVE

#UDPs
0x0035 DNS
0x0045 TFTP
```

Textový súbor je zložený z 5 blokov pre jednotlivé skupiny a v každom bloku sa nachádza zoznam protokolov v tvare číslo protokolu v hexadecimálnej sústave a názov protokolu oddelený medzerou.

POUŽÍVATEĽSKÉ ROZHRANIE

Po spustení programu sa otvorí grafické rozhranie, v ktorom na ľavej strane sa nachádza časť, kde sa vypisujú jednotlivé informácie a na pravej strane je menu s ovládaním.

V GUI je možné:
- nastaviť počet byte-ov vypísaných v jednom riadku pri výpise packetu
- načítať konfiguračný súbor s číslami protokolov
- načítať pcap súbor
- vypísať všetky rámce z pcap súboru
- vypísať jednotlivé komunikácie
- skočiť na rámec so zadaným číslom vo výpise



Pre správne fungovanie je potrebné načítať konfiguračný súbor a pcap súbor. Potom po stlačení tlačidiel na výpis sa vypíšu na textovú plochu zanalyzované informácie.

IMPLEMENTAČNÉ PROSTREDIE

Použitý programovací jazyk:	Python 3.8.5
Použité knižnice:	pcapy – načítanie pcap súborov
	tkinter – vytvorenie GUI
	os – práca so súbormi