KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Sieťová a komunikačná bezpečnosť

11 Monitoring počítačovej siete

KCKB UPJS CSIRT UPJS

KCKB UPJS
UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Monitoring počítačovej siete

- monitoring počítačovej siete.
- analýza sieťového toku (flow)

Monitoring počítačovej siete (I.)

- priebežné sledovanie stavu, výkonu a bezpečnosti siete
- cieľ: dostupnosť, spoľahlivosť a včasné odhalenie problémov
- poskytuje prehľad o prevádzke a vyťažení zariadení
- podklad pre plánovanie kapacity a riešenie incidentov
- dôležitý zdroj údajov pre bezpečnostné systémy

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

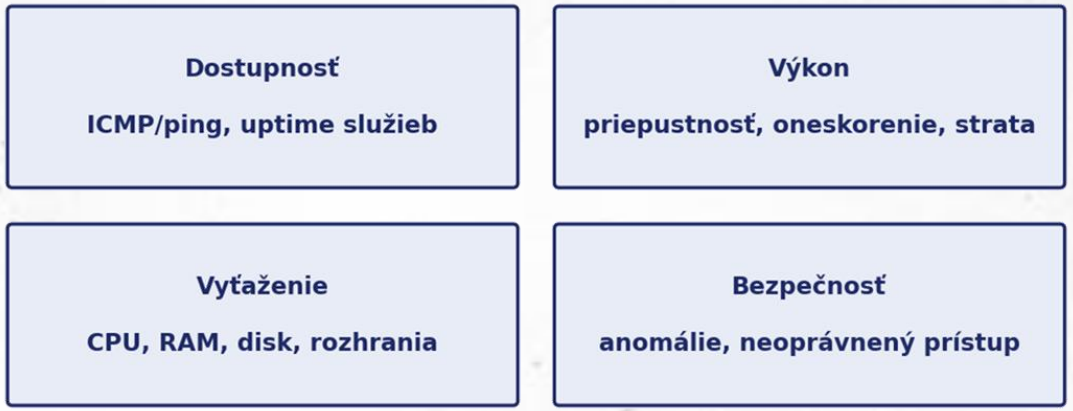
Monitoring počítačovej siete (II.)

- Dôvody monitorovania počítačovej siete:
  - včasná detekcia výpadkov a anomálií
  - identifikácia úzkych miest a preťaženia
  - podpora dodržania SLA (úroveň služby)
  - ddhalenie bezpečnostných incidentov v prevádzke
  - dáta pre rozhodovanie a optimalizáciu siete

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Monitoring počítačovej siete (III.)

- **Obsah/predmet monitorovania:**
  - dostupnosť zariadení a služieb (ping, uptime)
  - výkon - priepustnosť, oneskorenie, strata paketov
  - vyťaženie - CPU, pamäť, disk, sieťové rozhrania
  - chyby rozhraní a stav liniek
  - bezpečnostné anomálie a neobvyklú prevádzku



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Metódy monitorovania

- **aktívny monitoring** - generovanie testovacej prevádzky (ping, probe)
- **pasívny monitoring** - pozorovanie reálnej prevádzky
- agentový a bezagentový zber údajov
- tokový monitoring (NetFlow/IPFIX) – kto s kým komunikuje
- hĺbková analýza paketov (packet capture)

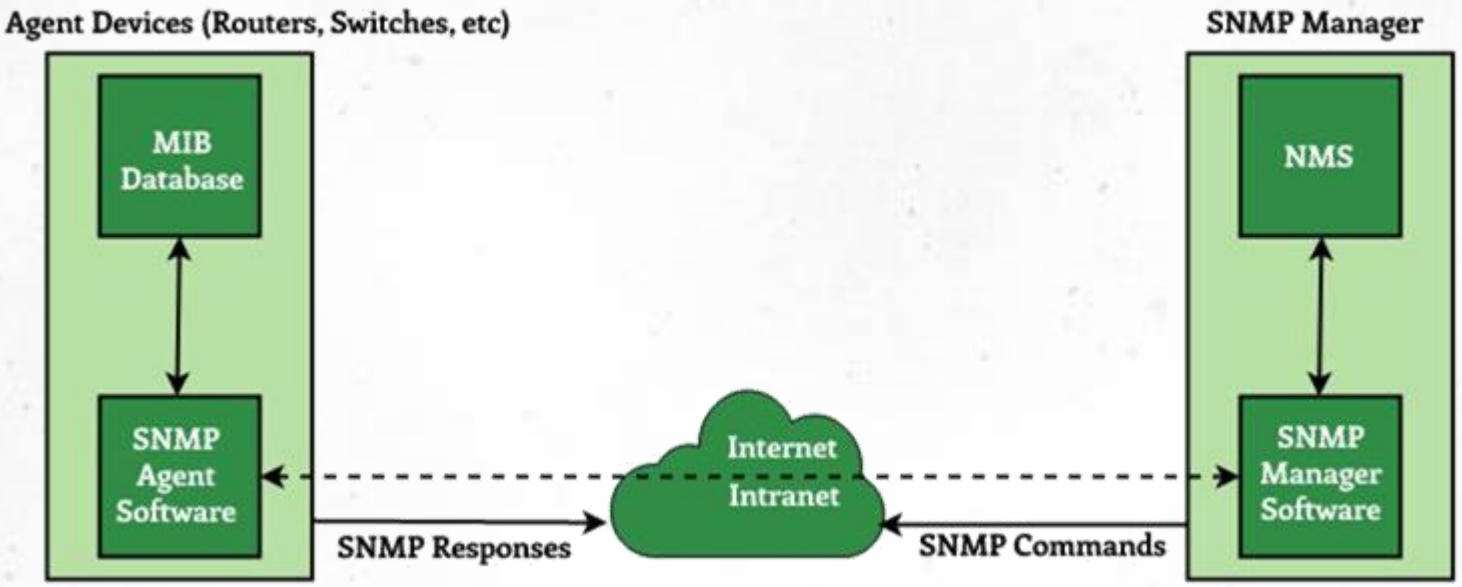
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Protokol SNMP (I.)

- SNMP (Simple Network Management Protocol) - správa zariadení
- polling - pravidelné dotazovanie hodnôt (OID v MIB)
- trapy - zariadenie samo hlási udalosť
- SNMPv3 prináša autentizáciu a šifrovanie
- staršie verzie (v1/v2c) sú nezabezpečené

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Protokol SNMP (II.)



Zdroj: https://www.geeksforgeeks.org/computer-networks/simple-network-management-protocol-snmp/

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Monitorovanie sieťového toku

- zaznamenáva metadáta o tokoch (adresy, porty, objem)
- neukladá obsah, ale prehľad o komunikácii
- vhodný na detekciu anomálií a analýzu prevádzky
- štandardy: NetFlow, IPFIX, sFlow
- nižšia réžia než plný packet capture

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

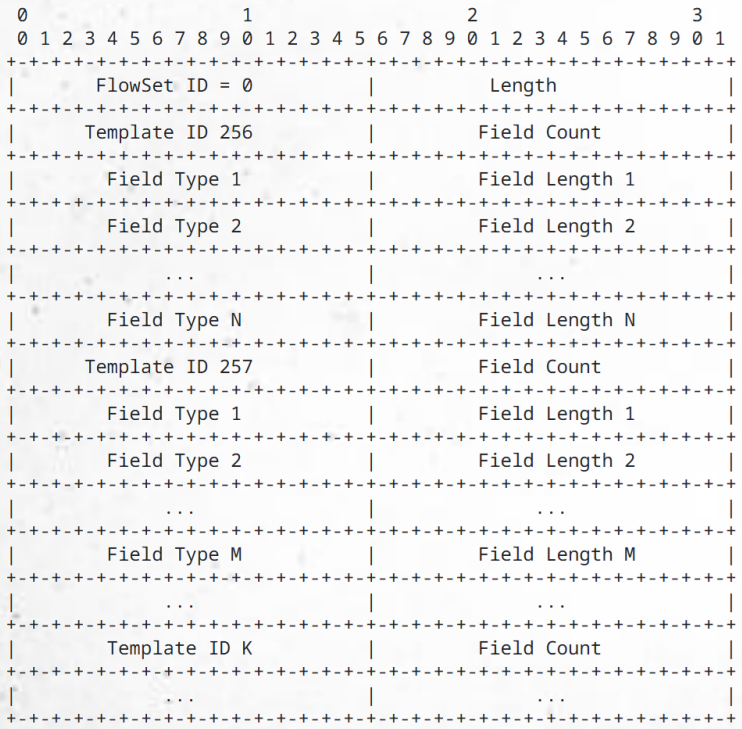
Netflow (I.)

- je technológia monitorovania prevádzky vyvinutá spoločnosťou Cisco Networks.

- toky (flows) sú jednosmerné / obojsmerné a obsahujú údaje týkajúce sa pripojenia, ako napríklad:
  - zdrojová a cieľová IP adresa
  - zdrojový a cieľový port
  - zdroj a miesto určenia AS.
  - protokol (TCP, UDP, ICMP atď.)
  - príznaky protokolu TCP (TCP flags)
  - logické vstupné a výstupné rozhrania
  - počet bajtov a paketov

Netflow (II.)

- **RFC**
  - RFC 3954 - Cisco Systems NetFlow Services Export Version 9
  - RFC 7011 - Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information
  - RFC 7012 - Information Model for IP Flow Information Export (IPFIX)



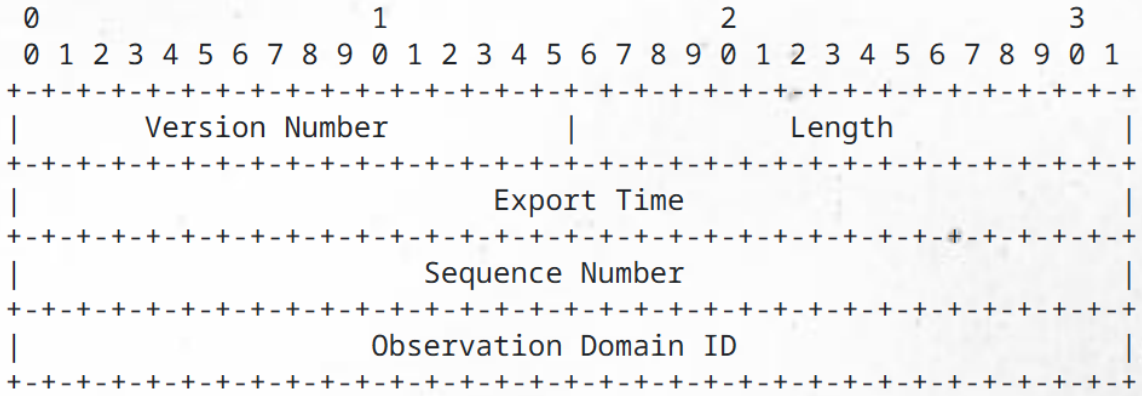
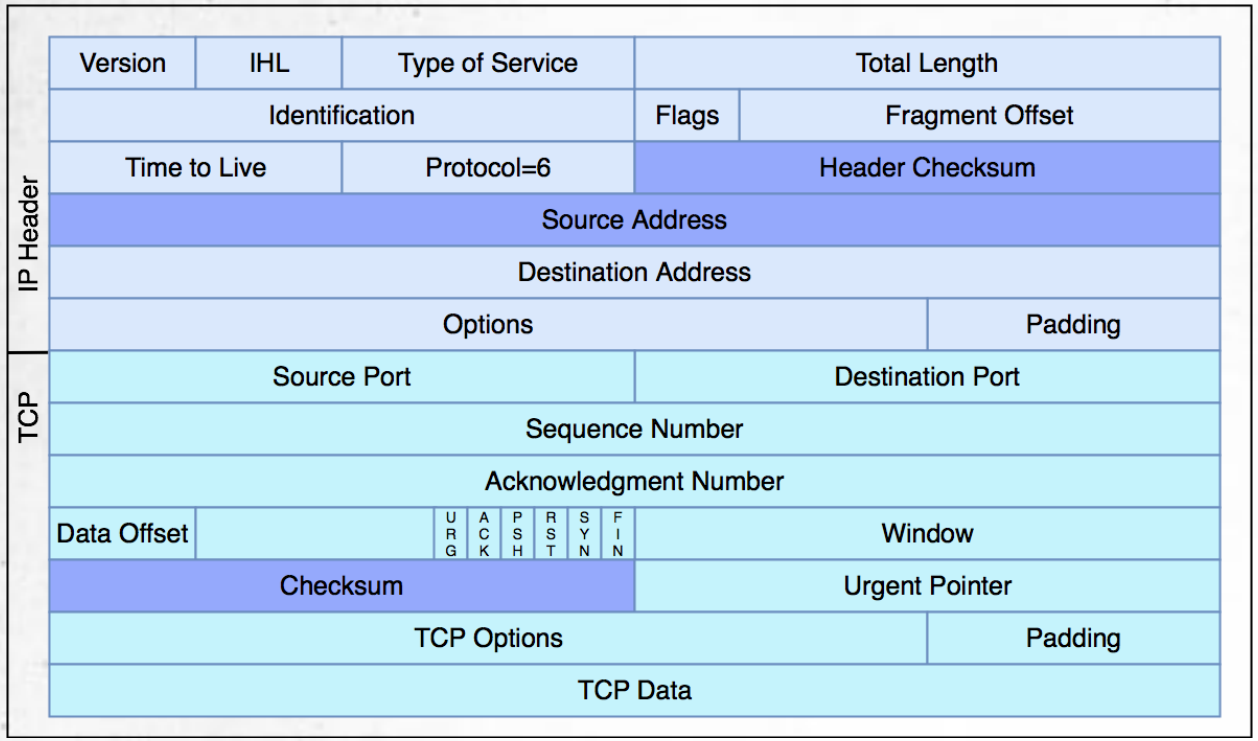
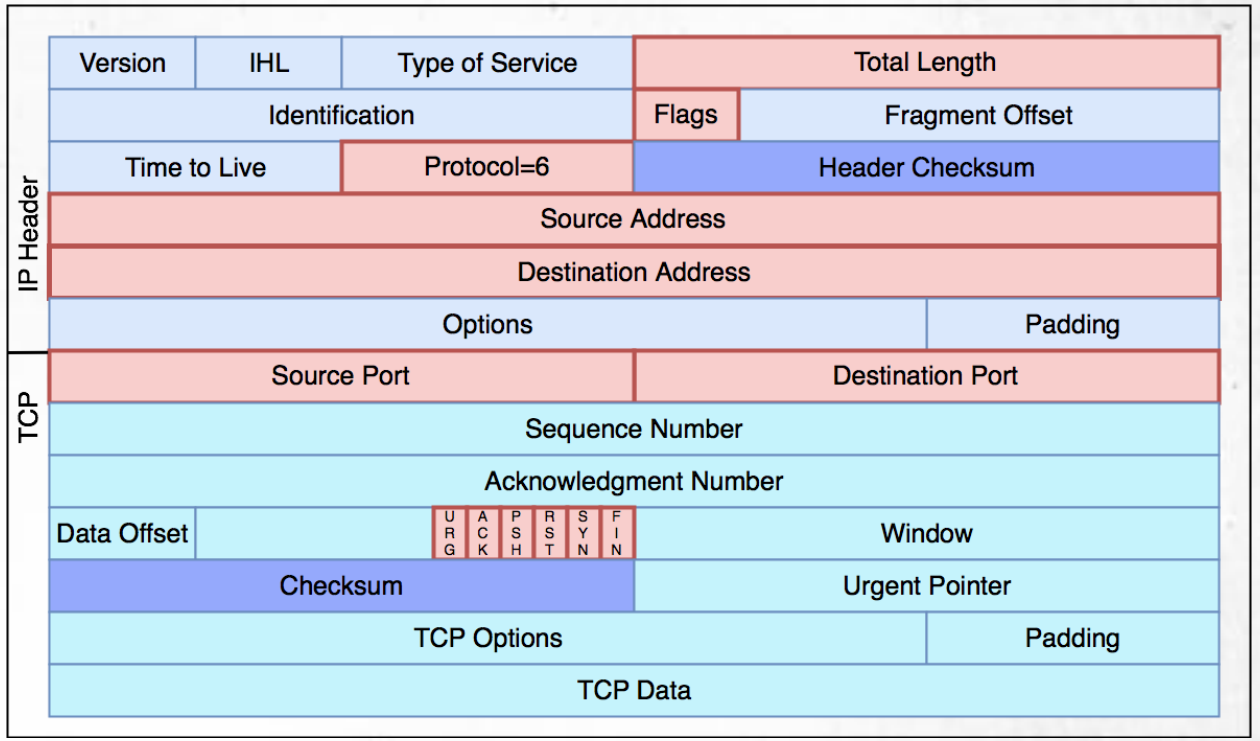


Figure F: IPFIX Message Header Format

Netflow (III.)

- Packet vs. netflow





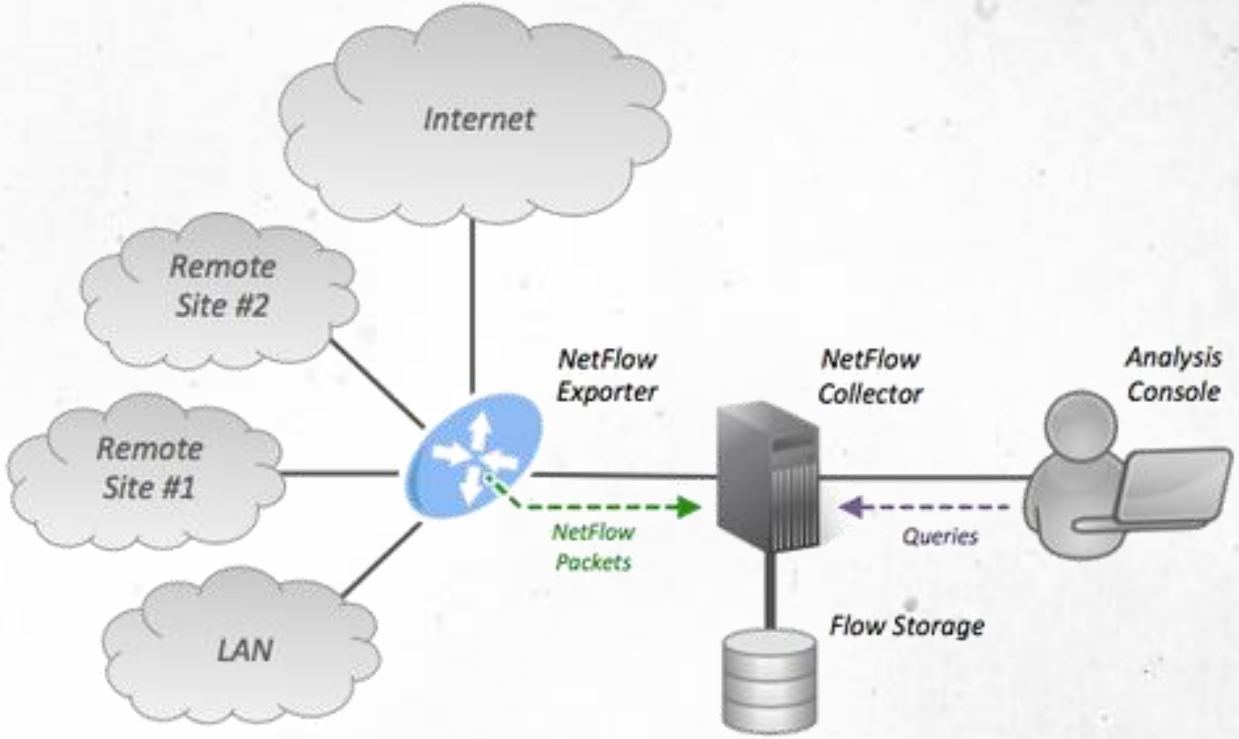
Netflow (IV.)

Verzia	Popis
v1	Prvá implementácia, obmedzená iba na IPv4 (bez IP masky a AS čísla).
v2	Interná verzia spoločnosti Cisco, nikdy neuvoľnená.
v3	Interná verzia spoločnosti Cisco, nikdy neuvoľnená.
v4	Interná verzia spoločnosti Cisco, nikdy neuvoľnená.
v5	Najbežnejšia verzia, ktorá je dostupná (od roku 2009) na mnohých sieťových smerovačoch rôznych značiek, ale obmedzená na toky protokolu IPv4.
v6	Cisco už nepodporuje. Informácie o zapuzdrení
v7	Rovnako ako verzia 5 so zdrojovým smerovačom
v8	Niekoľko agregačných spôsobov, ale iba pre informácie, ktoré sú už v záznamoch verzie 5
v9	Dostupná od roku 2009 na niektorých nových sieťových smerovačoch. Väčšinou sa používa na hlásenie tokov ako IPv6, MPLS, alebo dokonca obyčajný protokol IPv4 s ďalšou službou BGP.
v10	Používa sa na identifikáciu IPFIX.

Zdroj: https://en.wikipedia.org/wiki/NetFlow

Netflow (V.)

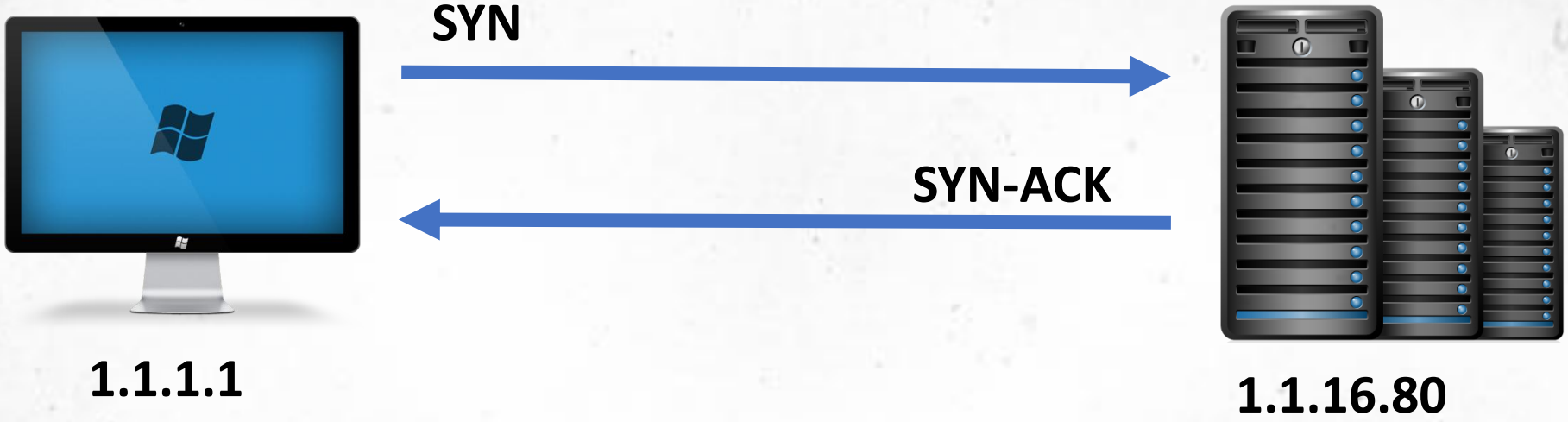
- **Architektúra**
  - **exportér toku** (flow exporter) - agreguje pakety do tokov a exportuje záznamy tokov do jedného alebo viacerých kolektorov.
  - **kolektor tokov** (flow collector) - zodpovedá za príjem, uskladnenie a predbežné spracovanie údajov o tokoch získaných od exportéra toku.
  - **analytická aplikácia** (analysis application) - analyzuje prijaté dáta toku napríklad v súvislosti s detekciou narušenia alebo profilovaním sieťovej prevádzky



Zdroj: https://en.wikipedia.org/wiki/NetFlow

Netflow (VI.)

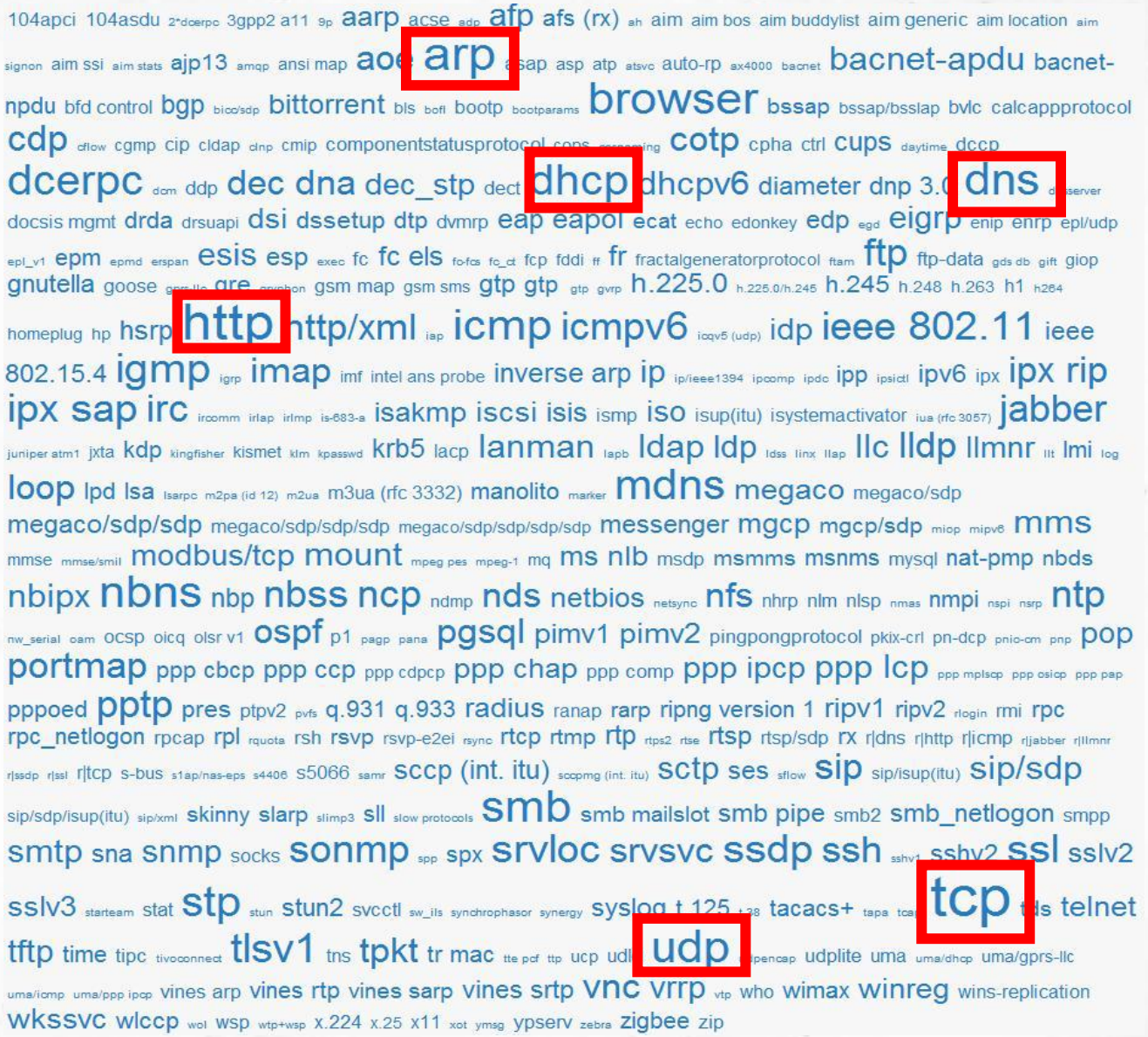
Príklad



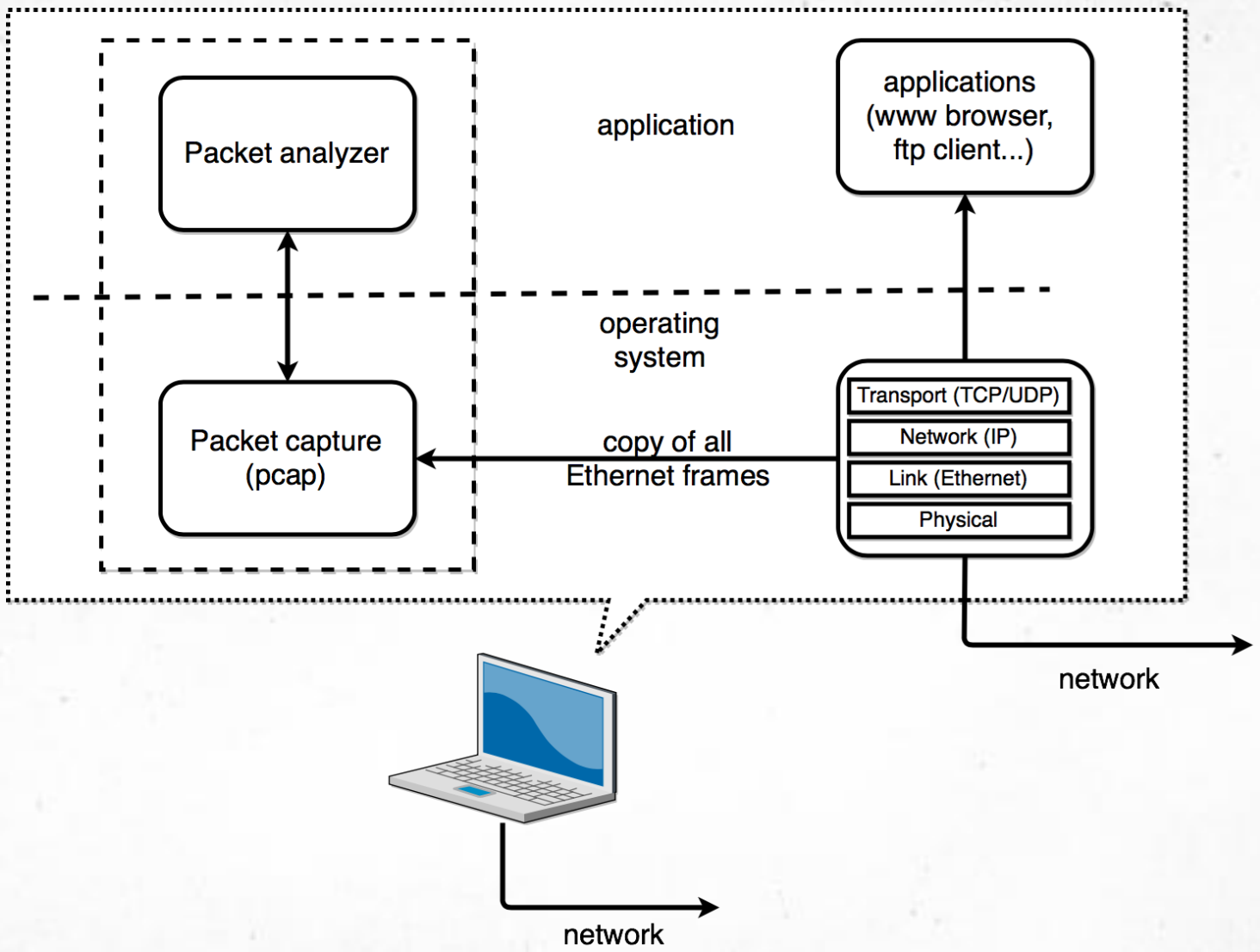
Date flow start	Duration	Proto	Src Ip addr:port	Dst IP addr:port	Flags	Packets	Bytes
2018-05-07	14:00:24.320	TCP	1.1.1.1:11266 ->	1.1.16.80:80	.....S	10	840
2018-05-07	14:00:24.370	TCP	1.1.16.80:80 ->	1.1.1.1:11266	A....S	12	12444

Zdroj: http://www.pngmart.com/image/tag/pc

Analýza packetov (I.)



Analýza packetov (II.)



Analýza packetov (III.)

- analýza komunikácie na úrovni jednotlivých paketov
- využitie: vyšetrovanie incidentov, troubleshooting, detekcia anomálií
- výhoda: vysoká granularita dát
- nevýhoda: veľký objem dát a potreba správneho filtrovania

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Analýza packetov (IV.)

- **tcpdump** - textový nástroj na zachytávanie paketov (servery, prostredie bez GUI)
- **WinDump** - historická verzia tcpdumpu pre operačný systém Windows
- **TShark** - terminálová verzia Wiresharku (skriptovanie a automatizácia)
- **tcpdump** vypisuje pakety podľa filtrovacej podmienky
- **TShark** dokáže zachytávať aj čítať uložené capture súbory

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

TCPdump (I.)

- syntax kombinuje voľby programu a filter expression
- voľby určujú rozhranie, súbor, počet paketov a úroveň detailu
- výraz na konci príkazu určuje, čo sa má zachytiť
- **tcpdump [options] [filter expression]**

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

TCPdump (II.)

- -i – výber rozhrania
- -w – zápis paketov do súboru, -r – čítanie capture súboru
- -n – vypnutie prekladu mien (zrýchľuje analýzu)
- -v, -vv, -vvv – zvyšovanie detailnosti výstupu

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

TCPdump (III.)

- tcpdump -D – zoznam dostupných rozhraní
- zachytávanie konkrétneho alebo všetkých rozhraní
- verbose režimy (-v / -vv / -vvv) pridávajú detaily o pakete
- pri forenznej analýze dokumentovať príkaz aj čas zachytávania

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

TCPdump (IV.)

- -X a -XX – zobrazenie paketu v hex a ASCII podobe
- -w – uchovanie dôkazu v .pcap súbore
- -r – neskoršia analýza bez opätovného zachytávania
- -n – ponechá pôvodné IP adresy (bez DNS lookupu)
- -s 65535 – plná dĺžka paketu pri starších verziách

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

TCPdump (V.)

- host – filtrovanie podľa konkrétnej IP adresy
- net – analýza segmentu alebo VLAN
- port – služby ako SMTP, DNS, HTTP alebo SSH
- kombinácia protokolu a portu zvyšuje presnosť zachytávania

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

TCPdump (VI.)

- and – zúženie výberu paketov
- or – rozšírenie výberu
- not – vylúčenie šumu (napr. ARP, DNS)
- zložité filtre uvádzať v úvodzovkách

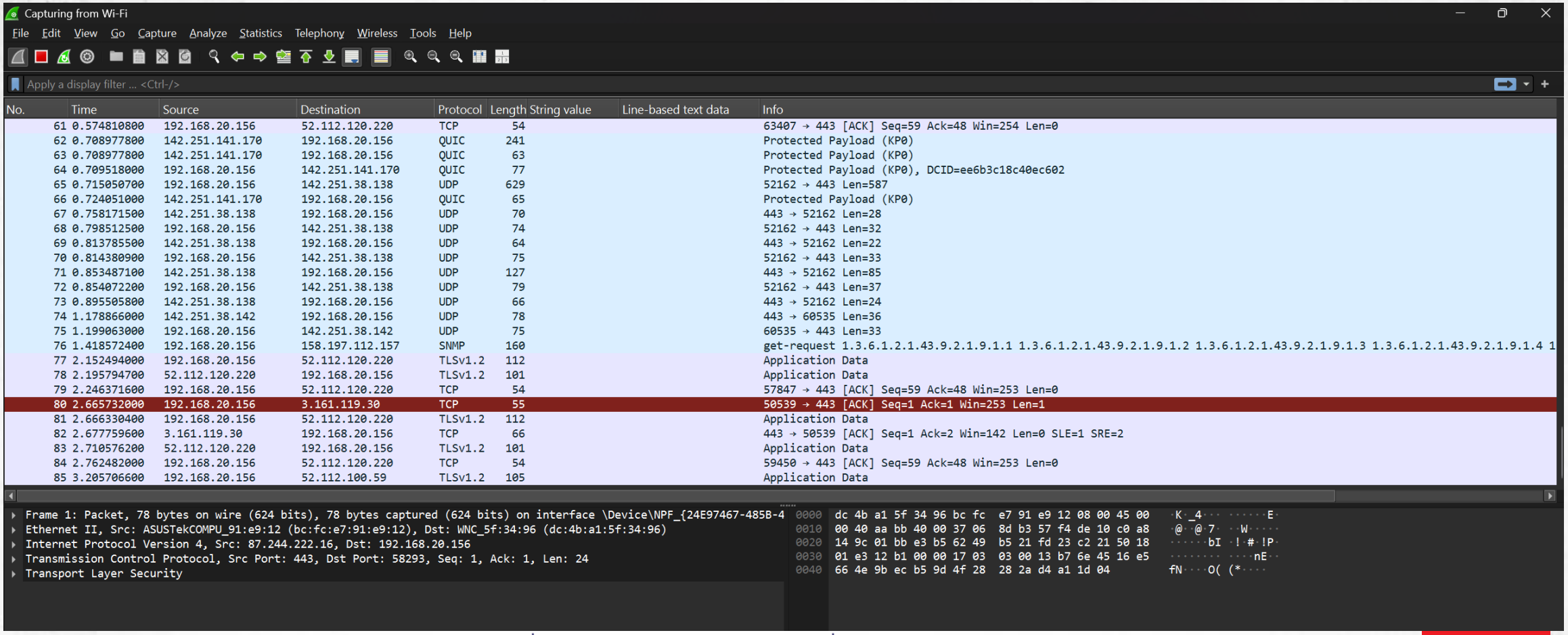
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Wireshark (I.)

- grafický nástroj na zachytávanie a analýzu paketov
- detailné skúmanie jednotlivých vrstiev protokolov
- vhodný na forenznú analýzu, troubleshooting aj výučbu
- kombinácia filtrov, štatistík a vizuálnych nástrojov
- https://www.wireshark.org/

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Wireshark (II.)



Wireshark – rozhranie

- Packet List – prehľad zachytených paketov
- Packet Details – protokolové vrstvy a polia
- Packet Bytes – surové dáta v hex a ASCII podobe
- Status Bar – kontext o výbere a capture súbore

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Wireshark – Status Bar

- zobrazuje stav analýzy a informácie o vybranom pakete
- počet paketov a aktuálny profil
- rozdiel medzi captured a displayed packets
- dôležité pri použití display filtrov

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

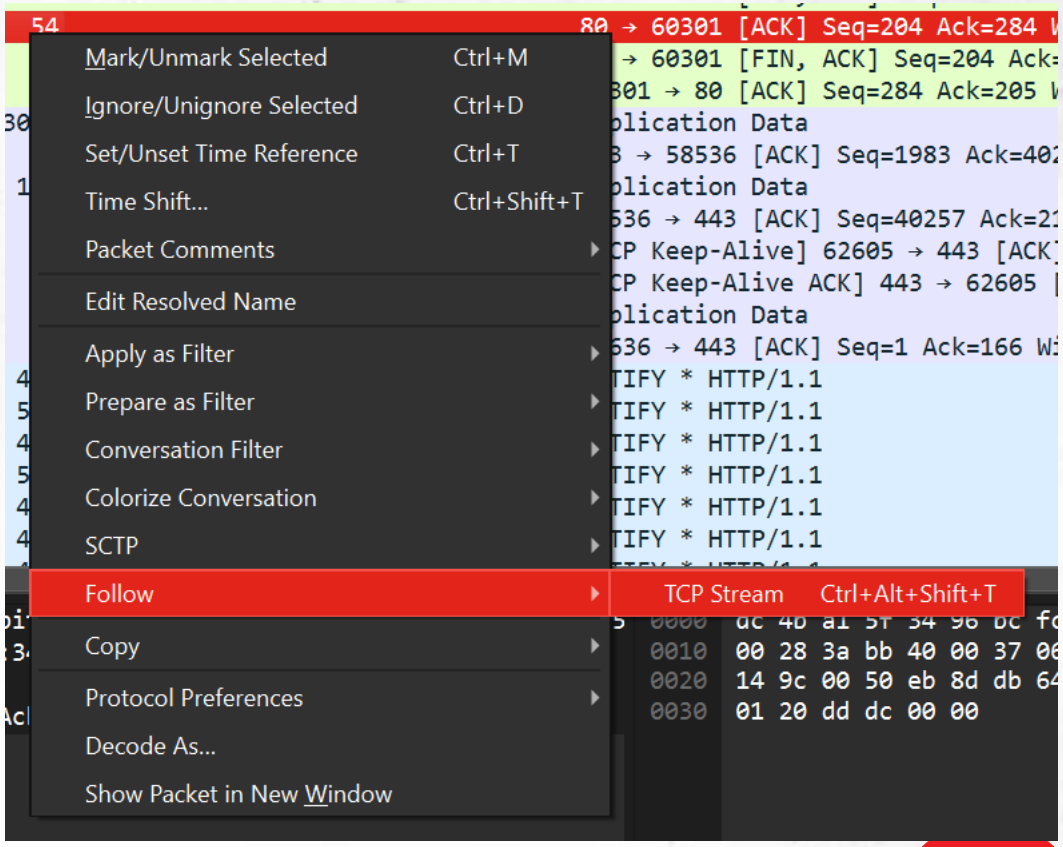
Wireshark – filtre

- **capture filtre** - určujú, čo sa vôbec zachytí
- **display filtre** - určujú, čo sa zobrazí zo zachytených paketov
- display filtre sú vhodné na iteratívnu analýzu
- príklady: ip.addr, tcp.port, http.request, tcp.flags.reset

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Wireshark – Follow TCP Stream (I.)

- rekonštrukcia komunikácie v jednom TCP spojení
- využitie pri HTTP, FTP a nešifrovaných protokoloch
- automatické aplikovanie filtra na konkrétny tok
- rýchla analýza obsahu komunikácie

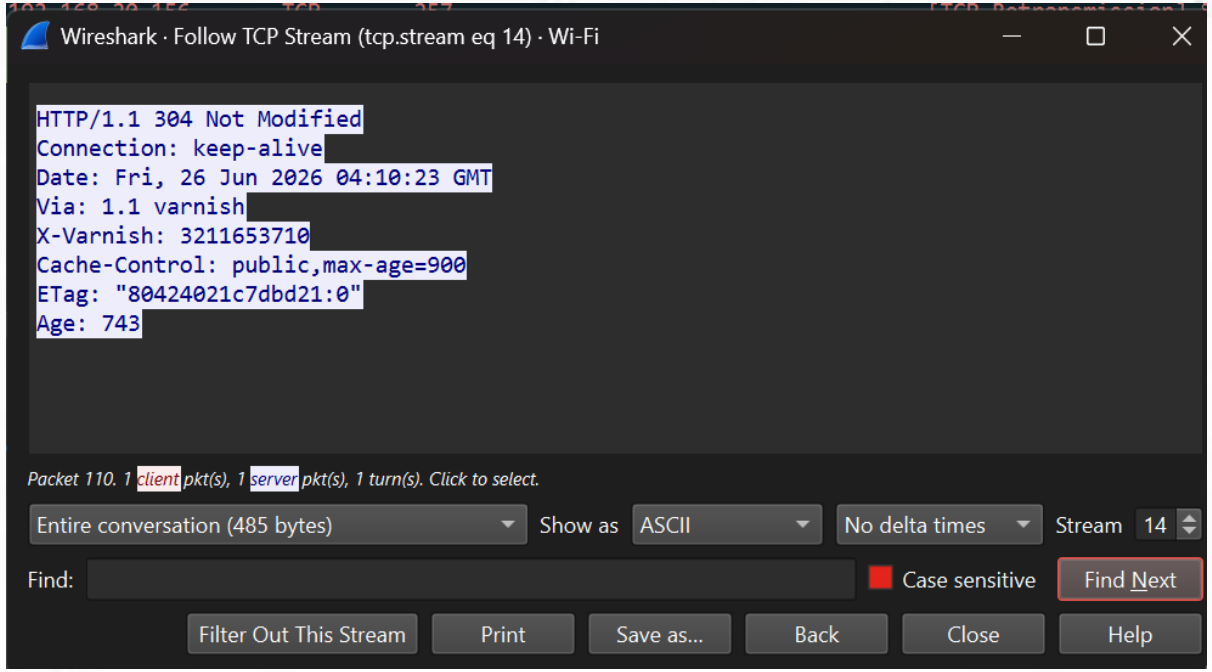


Wireshark – Follow TCP Stream (II.)

- výstup ukazuje komunikáciu klienta a servera čitateľnejšie
- pri HTTP vidno požiadavky, hlavičky a obsah odpovede
- pri šifrovaní je obsah bez kľúčov nečitateľný
- farby odlišujú smer komunikácie

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Wireshark – Follow TCP Stream (III.)



Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

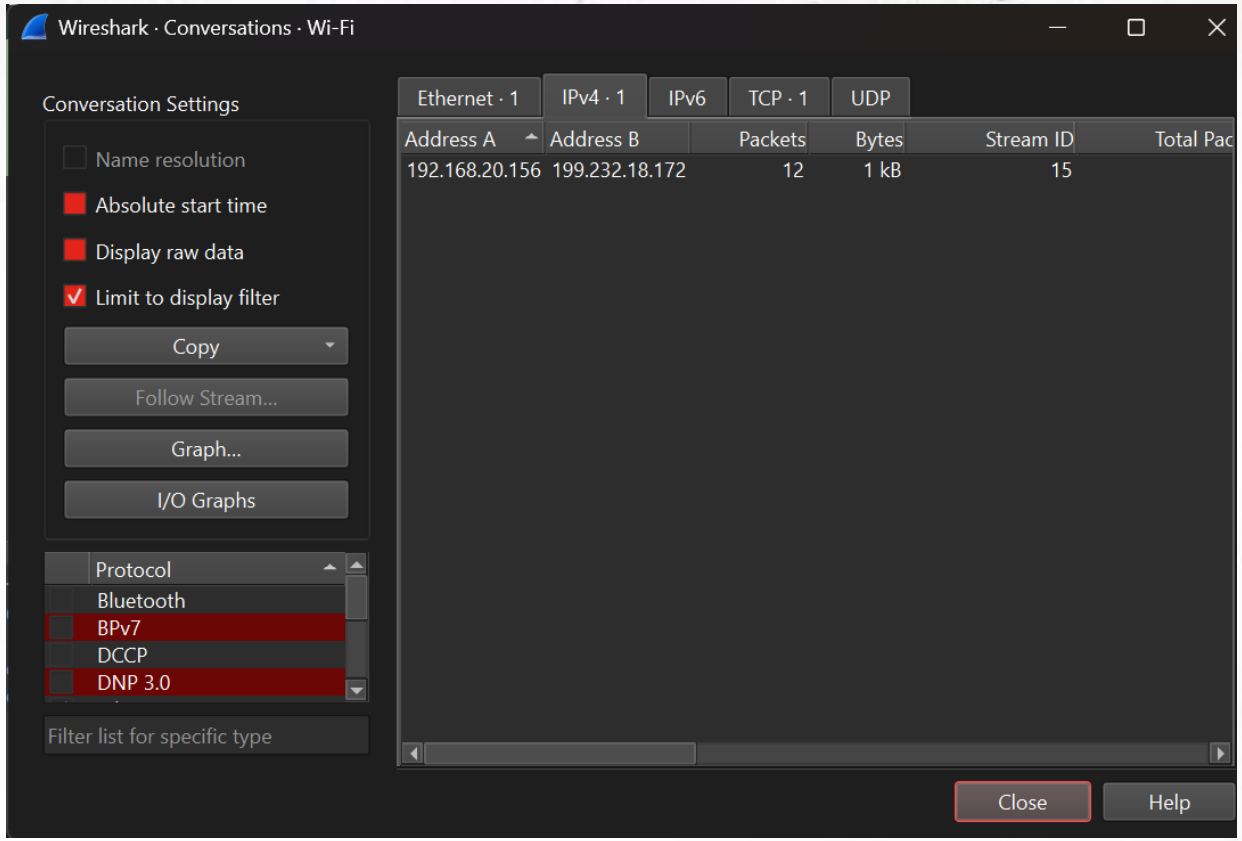
Wireshark – štatistiky (I.)

- **Protocol hierarchy** - zastúpenie protokolov
- **Conversations** - komunikujúce dvojice
- **I/O Graph** - vývoj prevádzky v čase
- rýchle pochopenie charakteru capture súboru

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

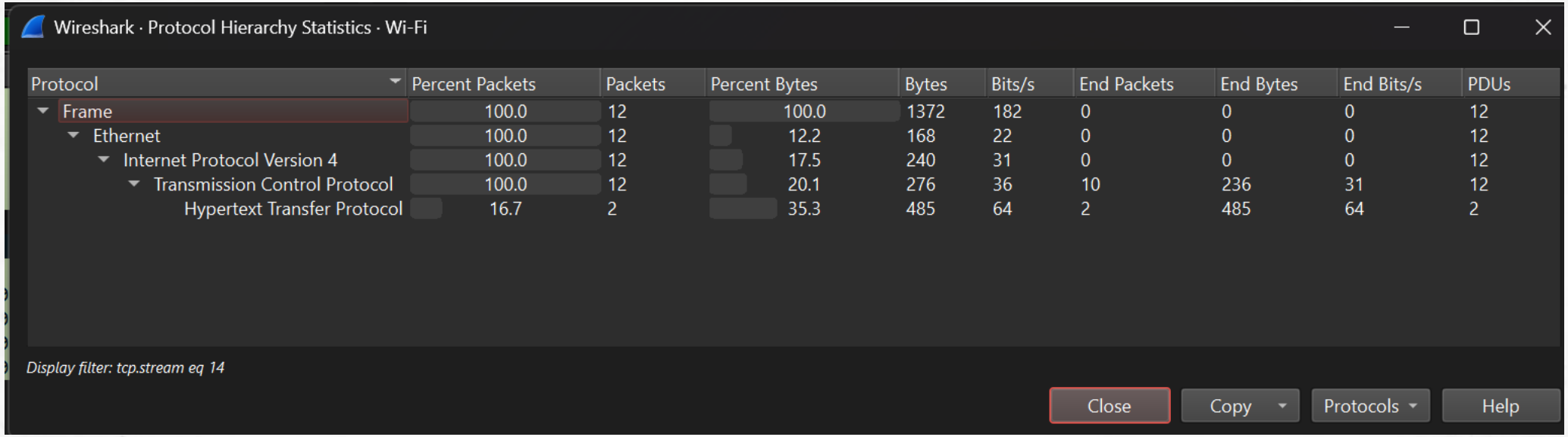
Wireshark – štatistiky (II.)

- **Conversations**



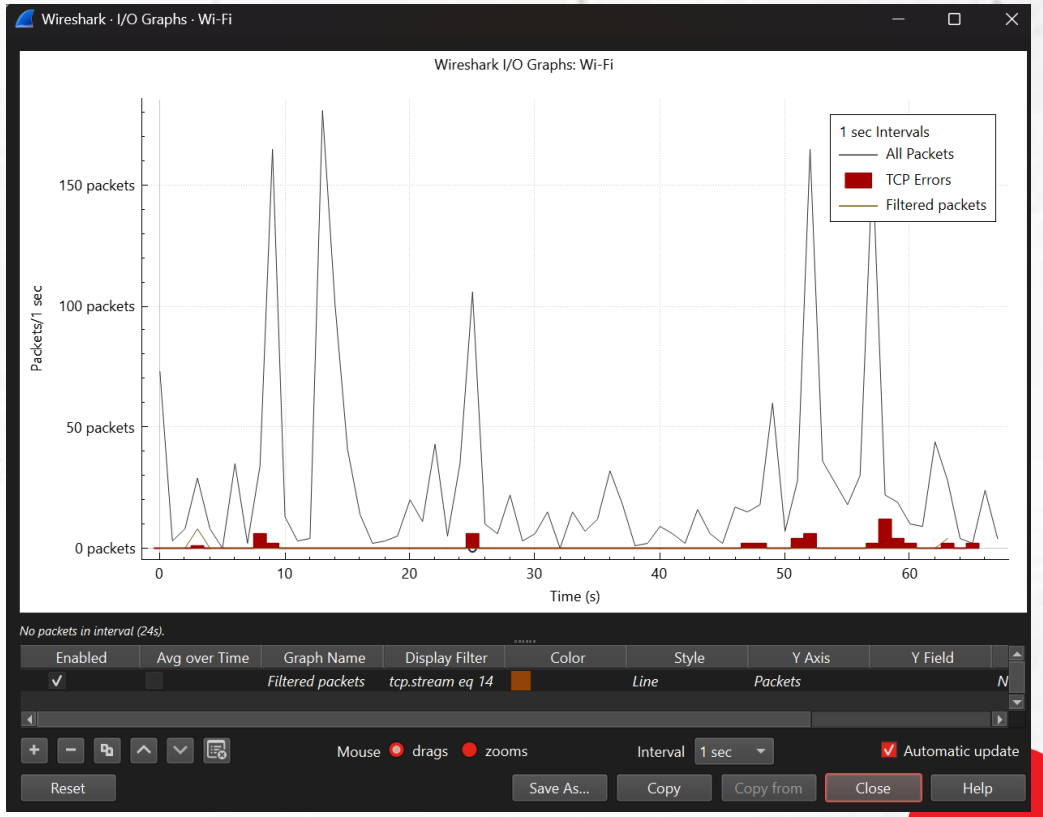
Wireshark – štatistiky (III.)

- **Protocol hierarchy**



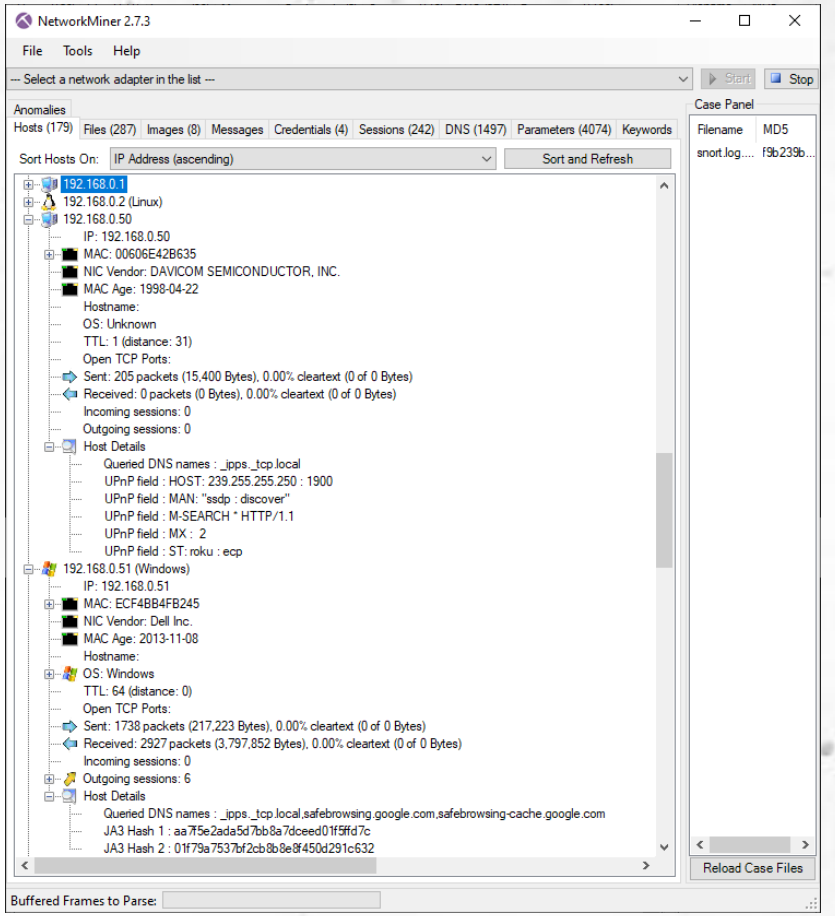
Wireshark – štatistiky (IV.)

- **I/O Graph**
  - vizualizácia objemu prevádzky v čase
  - identifikácia špičiek, výpadkov a anomálií
  - možnosť kombinácie s display filtrami
  - určenie časového okna pre detailnú analýzu



NetworkMiner

- nástroj orientovaný na sieťovú forenznú analýzu (network forensics)
- extrakcia artefaktov z PCAP – súbory, obrázky, e-maily, prihlasovacie údaje
- vhodný doplnok k Wiresharku
- rýchly prehľad hostov a prenášaného obsahu



Zdroj: https://www.netresec.com/?page=NetworkMiner

Wireshark – praktické úlohy

- PING – ICMP komunikácia
- DNS – preklad názvu na IP adresu
- TCP handshake – začiatok spojenia
- footprinting a extrakcia súborov – prepojenie s forenznou analýzou

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Ďakujeme za pozornosť