



# Siet'ová a komunikačná bezpečnosť

## 11 Monitoring počítačovej siete



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



**PLÁN [OBNOVY]**





# Monitoring počítačovej siete (II.)

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



# 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

**Dostupnosť**  
ICMP/ping, uptime služieb

**Výkon**  
priepustnosť, oneskorenie, strata

**Vyťaženie**  
CPU, RAM, disk, rozhrania

**Bezpečnosť**  
anomálie, neoprávnený prístup





# 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)



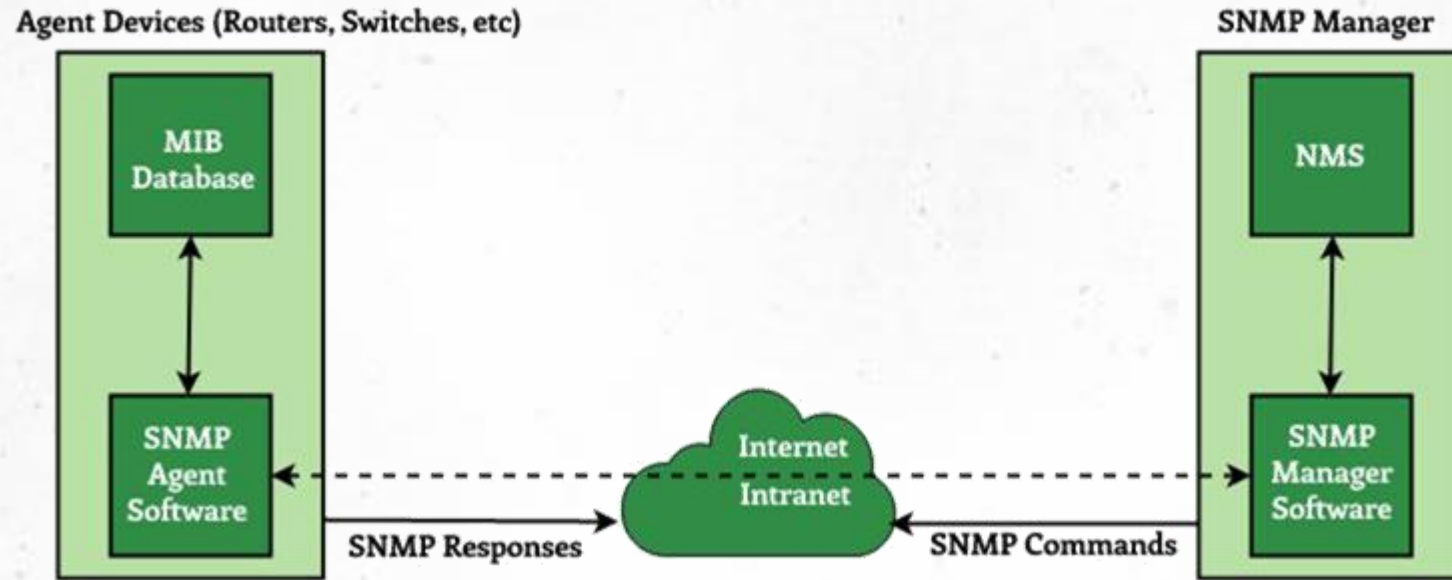


# Protokol SNMP (I.)

- 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



# Protokol SNMP (II.)



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





# 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



**PLÁN [OBNOVY]**



# 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)

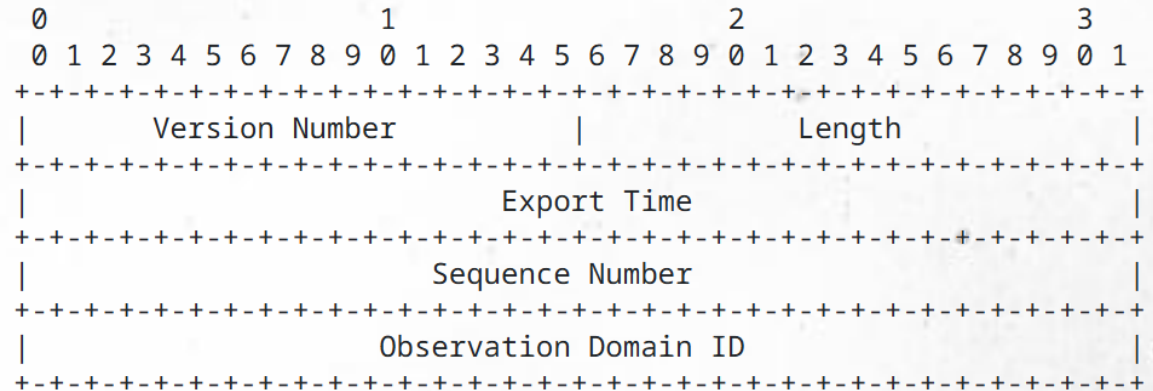
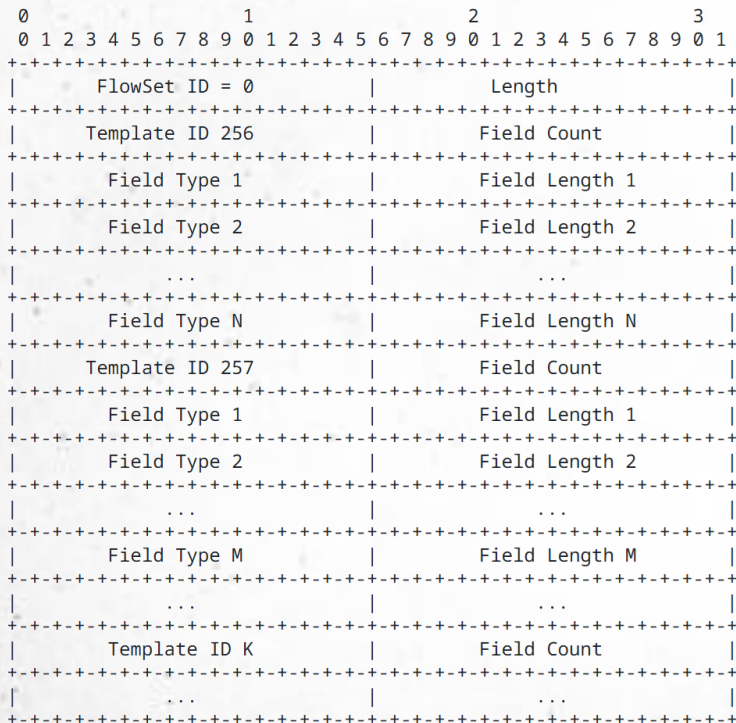


Figure F: IPFIX Message Header Format

# Netflow (III.)

- Packet vs. netflow

IP Header	Version	IHL	Type of Service	Total Length																			
	Identification			Flags	Fragment Offset																		
	Time to Live	Protocol=6		Header Checksum																			
	Source Address																						
	Destination Address																						
	Options				Padding																		
	TCP	Source Port			Destination Port																		
Sequence Number																							
Acknowledgment Number																							
Data Offset		<table border="1"> <tr> <td>U</td><td>A</td><td>P</td><td>R</td><td>S</td><td>F</td> </tr> <tr> <td>R</td><td>C</td><td>S</td><td>S</td><td>S</td><td>I</td> </tr> <tr> <td>G</td><td>K</td><td>H</td><td>T</td><td>N</td><td>N</td> </tr> </table>		U	A	P	R	S	F	R	C	S	S	S	I	G	K	H	T	N	N	Window	
U		A	P	R	S	F																	
R		C	S	S	S	I																	
G		K	H	T	N	N																	
Checksum			Urgent Pointer																				
TCP Options				Padding																			
TCP Data																							

IP Header	Version	IHL	Type of Service	Total Length																			
	Identification			Flags	Fragment Offset																		
	Time to Live	Protocol=6		Header Checksum																			
	Source Address																						
	Destination Address																						
	Options				Padding																		
	TCP	Source Port			Destination Port																		
Sequence Number																							
Acknowledgment Number																							
Data Offset		<table border="1"> <tr> <td>U</td><td>A</td><td>P</td><td>R</td><td>S</td><td>F</td> </tr> <tr> <td>R</td><td>C</td><td>S</td><td>S</td><td>S</td><td>I</td> </tr> <tr> <td>G</td><td>K</td><td>H</td><td>T</td><td>N</td><td>N</td> </tr> </table>		U	A	P	R	S	F	R	C	S	S	S	I	G	K	H	T	N	N	Window	
U		A	P	R	S	F																	
R		C	S	S	S	I																	
G		K	H	T	N	N																	
Checksum			Urgent Pointer																				
TCP Options				Padding																			
TCP Data																							

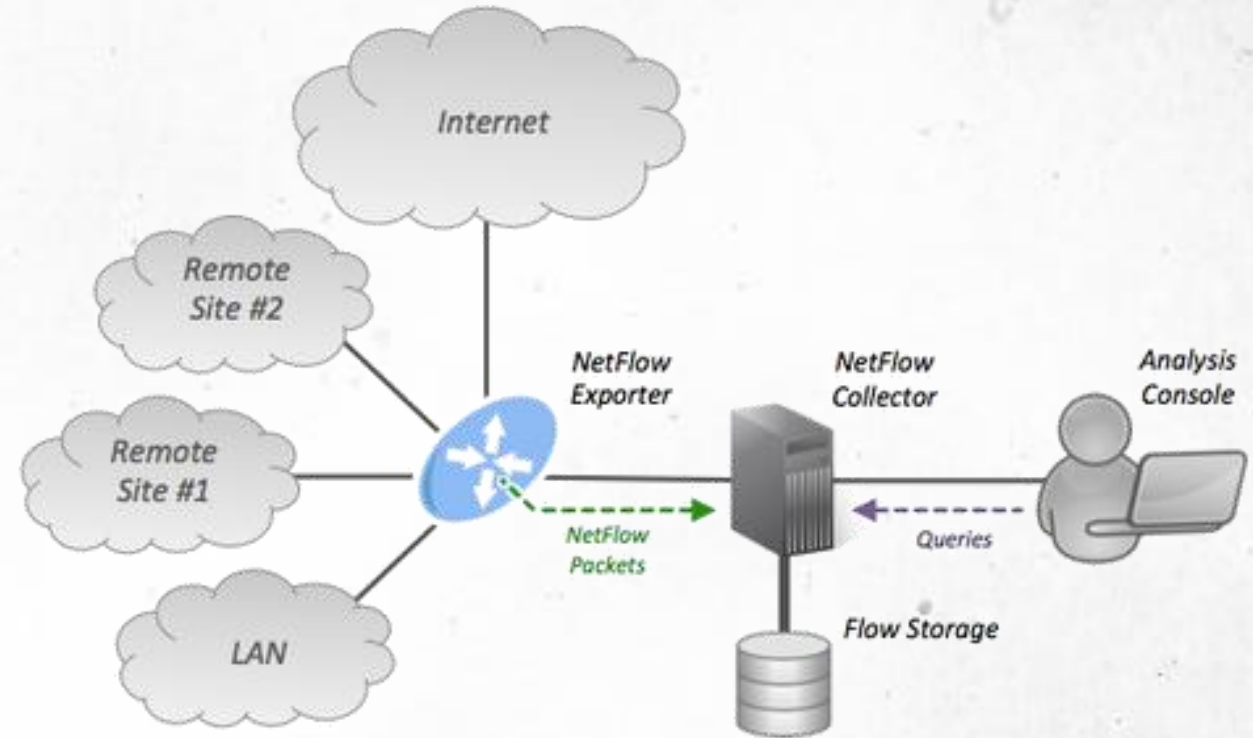
# Netflow (IV.)

Verzia	Popis
<b>v1</b>	Prvá implementácia, obmedzená iba na IPv4 (bez IP masky a AS čísla).
<b>v2</b>	Interná verzia spoločnosti Cisco, nikdy neuvolnená.
<b>v3</b>	Interná verzia spoločnosti Cisco, nikdy neuvolnená.
<b>v4</b>	Interná verzia spoločnosti Cisco, nikdy neuvolnená.
<b>v5</b>	Najbežnejšia verzia, ktorá je dostupná (od roku 2009) na mnohých sieťových smerovačoch rôznych značiek, ale obmedzená na toky protokolu IPv4.
<b>v6</b>	Cisco už nepodporuje. Informácie o zapuzdrení
<b>v7</b>	Rovnako ako verzia 5 so zdrojovým smerovačom
<b>v8</b>	Niekoľko agregáčnych spôsobov, ale iba pre informácie, ktoré sú už v záznamoch verzie 5
<b>v9</b>	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.
<b>v10</b>	Používa sa na identifikáciu IPFIX.

# Netflow (V.)

## Architektúra

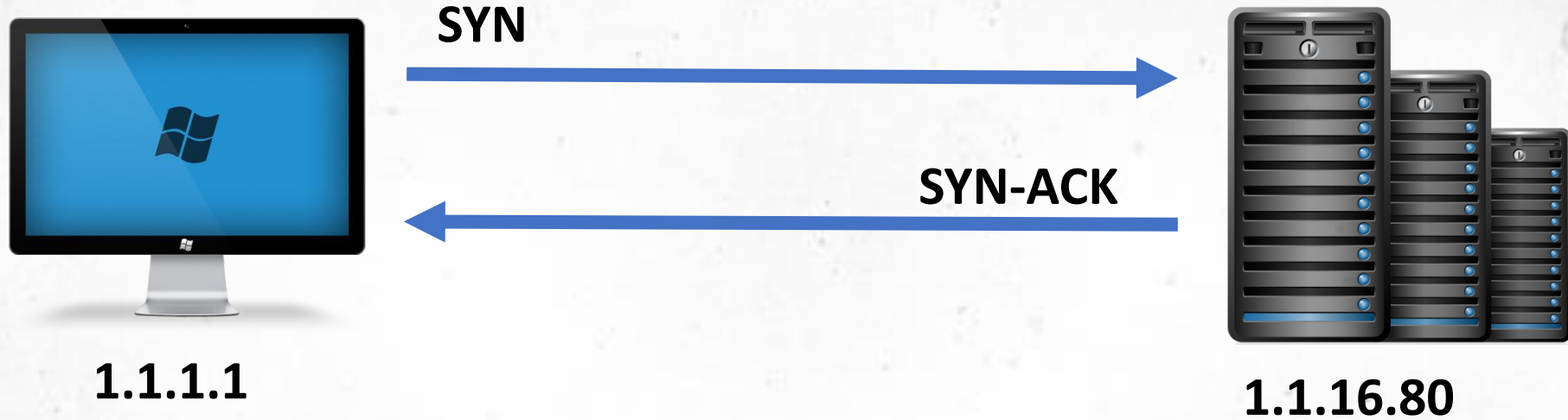
- **exportér toku** (flow exporter) - agreguje pakety do tokov a exportuje záznamy tokov do jedného alebo viacerých kolektorov.
- **kolektor tokov** (flow collector) - zodpovedá za príjem, uskladnenie a predbežné spracovanie údajov o tokoch získaných od exportéra toku.
- **analytická aplikácia** (analysis 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



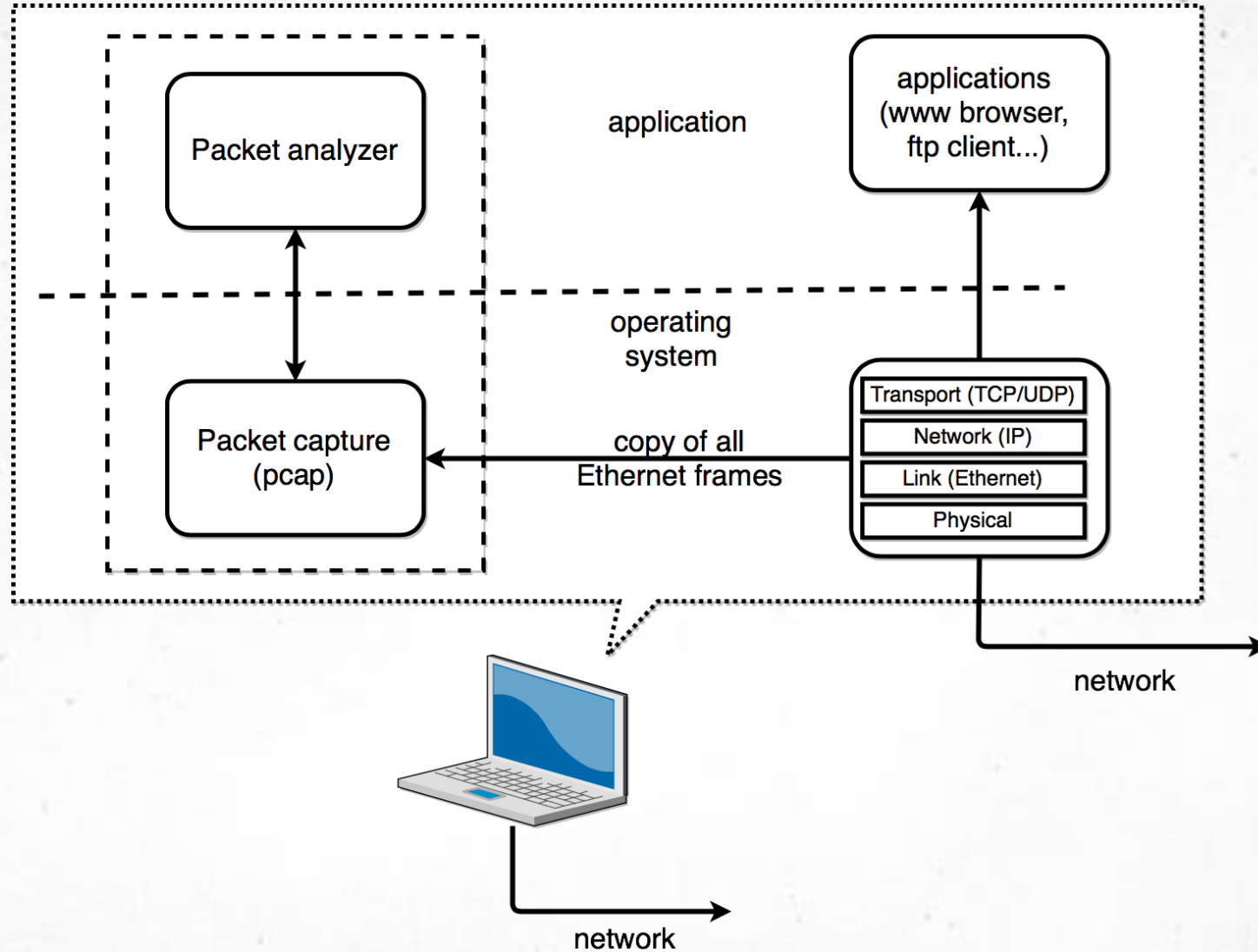
Date flow start	Duration	Proto	Src Ip addr:port	Dst IP addr:port	Flags	Packets	Bytes
2018-05-07	14:00:24.320	TCP	1.1.1.1:11266 ->	1.1.16.80:80	.....S	10	840
2018-05-07	14:00:24.370	TCP	1.1.16.80:80 ->	1.1.1.1:11266	A....S	12	12444



# Analýza packetov (I.)

104apci 104asdu 2\*doerpc 3gpp2 a11 9p aarp acse adp afp afs (rx) ah aim aim bos aim buddylist aim generic aim location aim  
 signon aim ssi aim stats **ajp13** amqp ansi map aoe **arp** asap asp atp atsvc auto-rp ax4000 bacnet **bacnet-apdu** bacnet-  
 npdu bfd control bgp bicc/sdp bittorrent bls bofi bootp bootparams **browser** bssap bssap/bsslap bvlc calcappprotocol  
 cdp cflow cgmp cip cdap dnp cmip componentstatusprotocol cons **cotp** cpha ctrl cups daytime dccc  
 dcerpc dcm ddp **dec dna dec\_stp** dect **dhcp** dhcpv6 diameter dnp 3.0 **dns** d\_server  
 docsis mgmt drda drsuapi dsi dssetup dtp dvmp eap eapol ecat echo edonkey edp egd eigrp enip enrtp epl/udp  
 epl\_v1 epmd erpans **esis esp** exec fc fc els fo-fcs fo\_ct fcp fddi ff fr fractalgeneratorprotocol ftam **ftp** ftp-data gds db gift giop  
 gnutella goose **gre** gre-ssh gsm map gsm sms gtp gtp gtp gvrp h.225.0 h.225.0/h.245 h.245 h.248 h.263 h1 h264  
 homeplug hp hsrp **http** http/xml iap **icmp icmpv6** icqv5 (udp) idp ieee 802.11 ieee  
 802.15.4 **igmp** igmp imap imf intel ans probe inverse arp ip ip/ieee1394 ipcomp ipdc ipp ipsidc ipv6 ipx **ipx rip**  
**ipx sap irc** ircomm irlap irlmp is-683-a isakmp iscsi isis ismp iso isup(itu) isystemactivator iua (rfc 3057) **jabber**  
 juniper atm1 jxta kdp kingfisher kismet klm kpasswd krb5 lacp lanman lapb **ldap ldap** ldsd linux llap **llc lldp llmnr** llmnr llm  
**loop** lpd lsa lsrpc m2pa (id 12) m2ua m3ua (rfc 3332) manolito marker **mdns** megaco megaco/sdp  
 megaco/sdp/sdp megaco/sdp/sdp/sdp megaco/sdp/sdp/sdp/sdp messenger mgcp mgcp/sdp miop mipv6 **mms**  
 mmse mmse/smil **modbus/tcp** mount mpeg pes mpeg-1 mq ms nlb msdp msmms msnms mysql nat-pmp nbds  
**nbipx nbns** nbp **nbss ncp** ndmp **nds** netbios netsync **nfs** nhrp nlm nlsip nmas **nmpi** nsip nsrp **ntp**  
 nw\_serial oam OCSP oicq olsr v1 **ospf** p1 pagp pana **pgsql** pimv1 pimv2 pingpongprotocol pkix-ctrl pn-dcp pnic-om pnp **pop**  
**portmap** ppp cbcp ppp ccp ppp cdpcp ppp chap ppp comp ppp ipcp ppp lcp ppp mplsccp ppp osicp ppp pap  
 pppoad **pptp** pres ptpv2 pvt q.931 q.933 radius ranap rarp ripng version 1 ripv1 ripv2 rlogin rmi rpc  
 rpc\_netlogon rpcap rpl rquota rsh rsvp rsvp-e2ei rsync rtcp rtmp rtp rtp2 rtpse **rtsp** rtsp/sdp rx rjdns rjhttp rjicmp rjabber rjllmnr  
 rjssdp rjssl rjtcp S-BUS s1ap/nas-eps s4406 S5066 samr **sctp** (int. itu) sccpmg (int. itu) **sctp** ses sflow **sip** sip/isup(itu) **sip/sdp**  
 sip/sdp/isup(itu) sip/xml **skinny** slarp slimp3 **sl** slow protocols **smb** smb mailslot smb pipe smb2 **smb\_netlogon** smpp  
**smtp** sna snmp socks **sonmp** spp spx **srvloc** srsvsc **ssdp** ssh sshv1 **sshv2** **ssl** sslv2  
 sslv3 starteam stat **stp** stun stun2 svcctl sw\_its synchrophasor synergy syslog t 125 t28 tacacs+ tapa tca **tcp** tds telnet  
 tftp time tipc tivooconnect **tlsv1** tns **tpkt** tr mac tte pdf ttp ucp udl **udp** upencap udplite uma uma/dhcp uma/gprs-llc  
 uma/icmp uma/ppp ipcp vines arp vines rtp vines sarp vines srtp **VNC** vrrp vtp who wimax winreg wins-replication  
**wkssvc** wlccp wol wsp wtp+wsp X.224 X.25 X11 xot ymsg ypserv zebra **zigbee** zip

# Analýza packetov (II.)



# Analýza packetov (III.)

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





# 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





# 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]**





# 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



# 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



# 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





# 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





# TCPdump (VI.)

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





# Wireshark (I.)

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





# Wireshark (II.)

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	String value	Line-based text data	Info
61	0.574810800	192.168.20.156	52.112.120.220	TCP	54			63407 → 443 [ACK] Seq=59 Ack=48 Win=254 Len=0
62	0.708977800	142.251.141.170	192.168.20.156	QUIC	241			Protected Payload (KP0)
63	0.708977800	142.251.141.170	192.168.20.156	QUIC	63			Protected Payload (KP0)
64	0.709518000	192.168.20.156	142.251.141.170	QUIC	77			Protected Payload (KP0), DCID=ee6b3c18c40ec602
65	0.715050700	192.168.20.156	142.251.38.138	UDP	629			52162 → 443 Len=587
66	0.724051000	142.251.141.170	192.168.20.156	QUIC	65			Protected Payload (KP0)
67	0.758171500	142.251.38.138	192.168.20.156	UDP	70			443 → 52162 Len=28
68	0.798512500	192.168.20.156	142.251.38.138	UDP	74			52162 → 443 Len=32
69	0.813785500	142.251.38.138	192.168.20.156	UDP	64			443 → 52162 Len=22
70	0.814380900	192.168.20.156	142.251.38.138	UDP	75			52162 → 443 Len=33
71	0.853487100	142.251.38.138	192.168.20.156	UDP	127			443 → 52162 Len=85
72	0.854072200	192.168.20.156	142.251.38.138	UDP	79			52162 → 443 Len=37
73	0.895505800	142.251.38.138	192.168.20.156	UDP	66			443 → 52162 Len=24
74	1.178866000	142.251.38.142	192.168.20.156	UDP	78			443 → 60535 Len=36
75	1.199063000	192.168.20.156	142.251.38.142	UDP	75			60535 → 443 Len=33
76	1.418572400	192.168.20.156	158.197.112.157	SNMP	160			get-request 1.3.6.1.2.1.43.9.2.1.9.1.1 1.3.6.1.2.1.43.9.2.1.9.1.2 1.3.6.1.2.1.43.9.2.1.9.1.3 1.3.6.1.2.1.43.9.2.1.9.1.4 1
77	2.152494000	192.168.20.156	52.112.120.220	TLSv1.2	112			Application Data
78	2.195794700	52.112.120.220	192.168.20.156	TLSv1.2	101			Application Data
79	2.246371600	192.168.20.156	52.112.120.220	TCP	54			57847 → 443 [ACK] Seq=59 Ack=48 Win=253 Len=0
80	2.665732000	192.168.20.156	3.161.119.30	TCP	55			50539 → 443 [ACK] Seq=1 Ack=1 Win=253 Len=1
81	2.666330400	192.168.20.156	52.112.120.220	TLSv1.2	112			Application Data
82	2.677759600	3.161.119.30	192.168.20.156	TCP	66			443 → 50539 [ACK] Seq=1 Ack=2 Win=142 Len=0 SLE=1 SRE=2
83	2.710576200	52.112.120.220	192.168.20.156	TLSv1.2	101			Application Data
84	2.762482000	192.168.20.156	52.112.120.220	TCP	54			59450 → 443 [ACK] Seq=59 Ack=48 Win=253 Len=0
85	3.205706600	192.168.20.156	52.112.100.59	TLSv1.2	105			Application Data

Frame 1: Packet, 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF\_{24E97467-485B-4... dc 4b a1 5f 34 96 bc fc e7 91 e9 12 08 00 45 00 ·K\_4 ······ E  
 Ethernet II, Src: ASUSTekCOMPU\_91:e9:12 (bc:fc:e7:91:e9:12), Dst: WNC\_5f:34:96 (dc:4b:a1:5f:34:96) 0010 00 40 aa bb 40 00 37 06 8d b3 57 f4 de 10 c0 a8 @·@·7··W·  
 Internet Protocol Version 4, Src: 87.244.222.16, Dst: 192.168.20.156 0020 14 9c 01 bb e3 b5 62 49 b5 21 fd 23 c2 21 50 18 ······bI·!#·!P·  
 Transmission Control Protocol, Src Port: 443, Dst Port: 58293, Seq: 1, Ack: 1, Len: 24 0030 01 e3 12 b1 00 00 17 03 03 00 13 b7 6e 45 16 e5 ··········nE·  
 Transport Layer Security 0040 66 4e 9b ec b5 9d 4f 28 28 2a d4 a1 1d 04 fN····O( (\*····



# 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





# 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





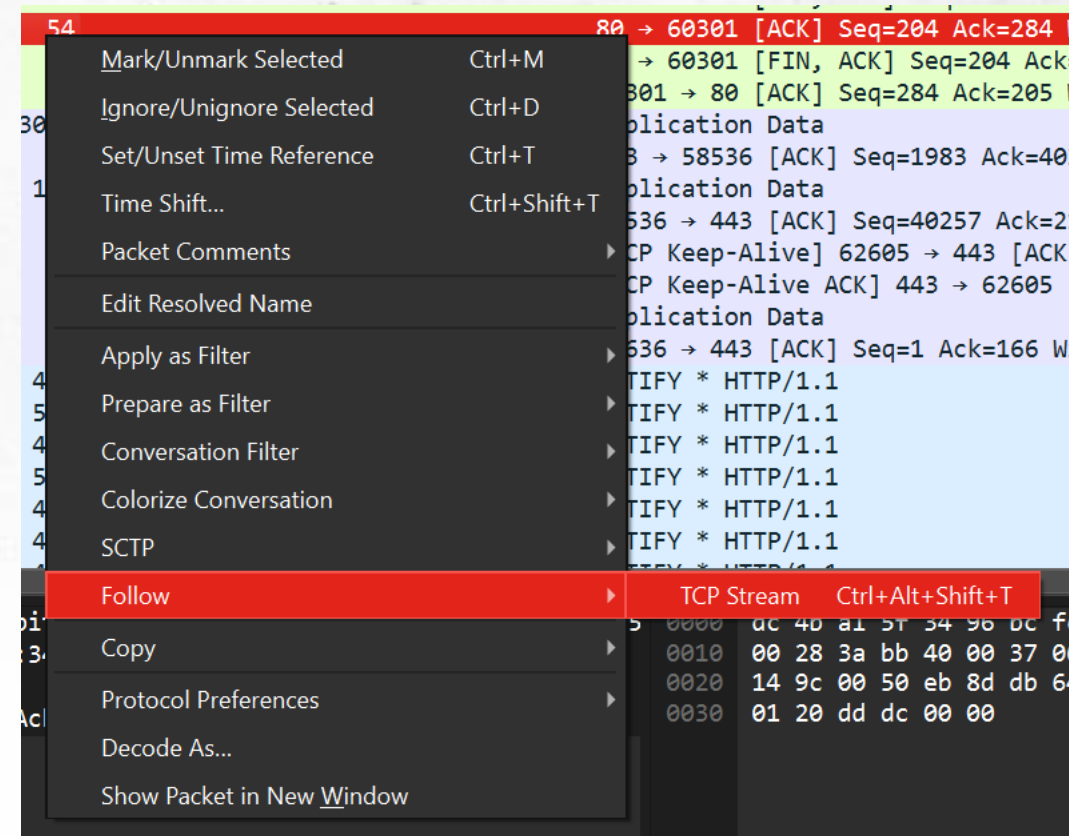
# Wireshark – filtre

- **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



# 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



# Wireshark – Follow TCP Stream (III.)

```
Wireshark · Follow TCP Stream (tcp.stream eq 14) · Wi-Fi

HTTP/1.1 304 Not Modified
Connection: keep-alive
Date: Fri, 26 Jun 2026 04:10:23 GMT
Via: 1.1 varnish
X-Varnish: 3211653710
Cache-Control: public,max-age=900
ETag: "80424021c7dbd21:0"
Age: 743

Packet 110. 1 client pkt(s), 1 server pkt(s), 1 turn(s). Click to select.

Entire conversation (485 bytes) Show as ASCII No delta times Stream 14
Find: Case sensitive Find Next
Filter Out This Stream Print Save as... Back Close Help
```





# Wireshark – štatistiky (I.)

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



# Wireshark – štatistiky (II.)

## ■ Conversations

Wireshark · Conversations · Wi-Fi

Conversation Settings

- Name resolution
- Absolute start time
- Display raw data
- Limit to display filter

Copy

Follow Stream...

Graph...

I/O Graphs

Ethernet · 1	IPv4 · 1	IPv6	TCP · 1	UDP	
Address A	Address B	Packets	Bytes	Stream ID	Total Pac
192.168.20.156	199.232.18.172	12	1 kB	15	

Protocol

- Bluetooth
- BPv7
- DCCP
- DNP 3.0

Filter list for specific type

Close Help



# Wireshark – štatistiky (III.)

## ■ Protocol hierarchy

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	12	100.0	1372	182	0	0	0	12
Ethernet	100.0	12	12.2	168	22	0	0	0	12
Internet Protocol Version 4	100.0	12	17.5	240	31	0	0	0	12
Transmission Control Protocol	100.0	12	20.1	276	36	10	236	31	12
Hypertext Transfer Protocol	16.7	2	35.3	485	64	2	485	64	2

Display filter: tcp.stream eq 14

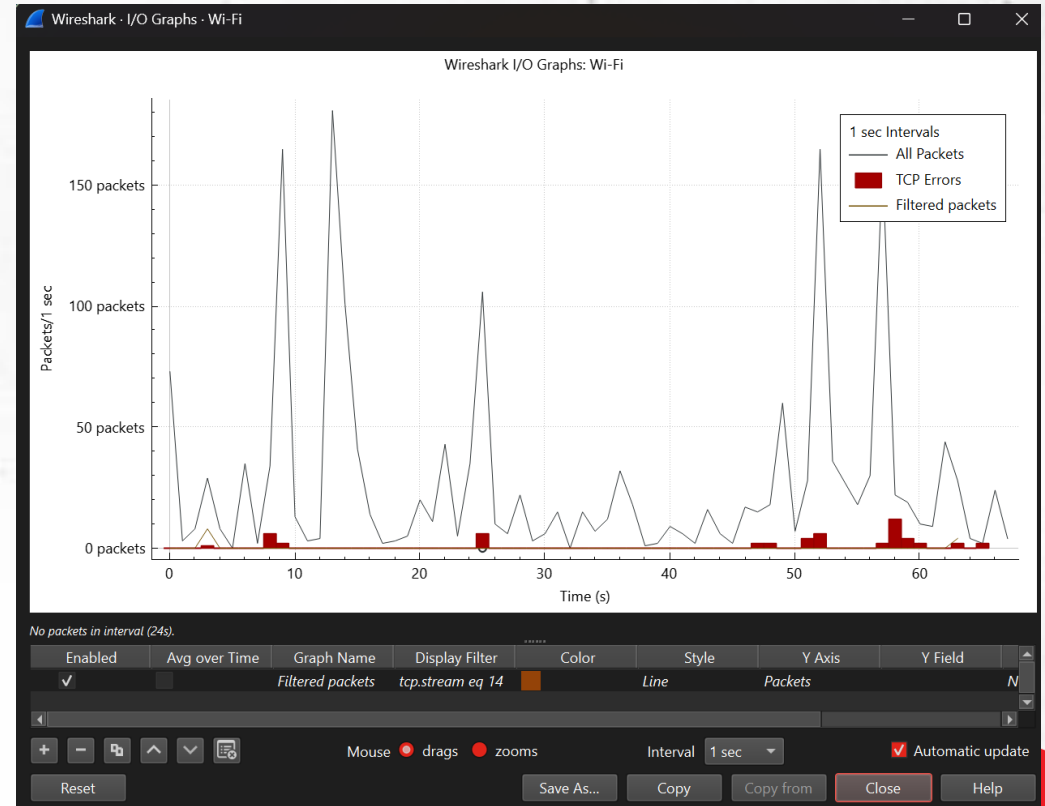
Close Copy Protocols Help



# Wireshark – štatistiky (IV.)

## ■ I/O Graph

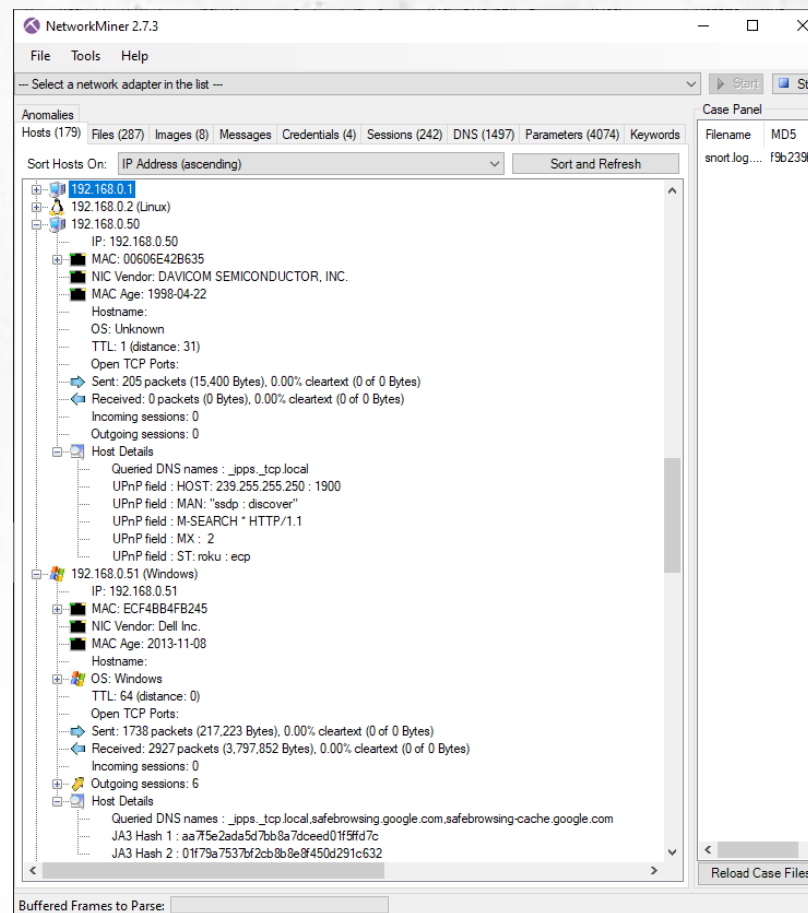
- vizualizácia objemu prevádzky v čase
- identifikácia špičiek, výpadkov a anomálií
- možnosť kombinácie s display filtrami
- určenie časového okna pre detailnú analýzu



# 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





UNIVERZITA  
PAVLA JOZEFA ŠAFÁRIKA  
V KOŠICIACH



Financované  
Európskou úniou  
NextGenerationEU

---

**PLÁN [OBNOVY]**

---



MINISTERSTVO  
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA  
A INFORMATIZÁCIE  
SLOVENSKEJ REPUBLIKY

**Ďakujeme za pozornosť**

