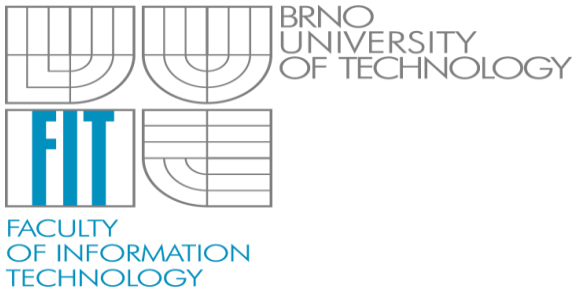
Analýza síťového provozu

Ing. Dominik Breitenbacher
ibreiten@fit.vutbr.cz
Mgr. Radim Janča
ijanca@fit.vutbr.cz

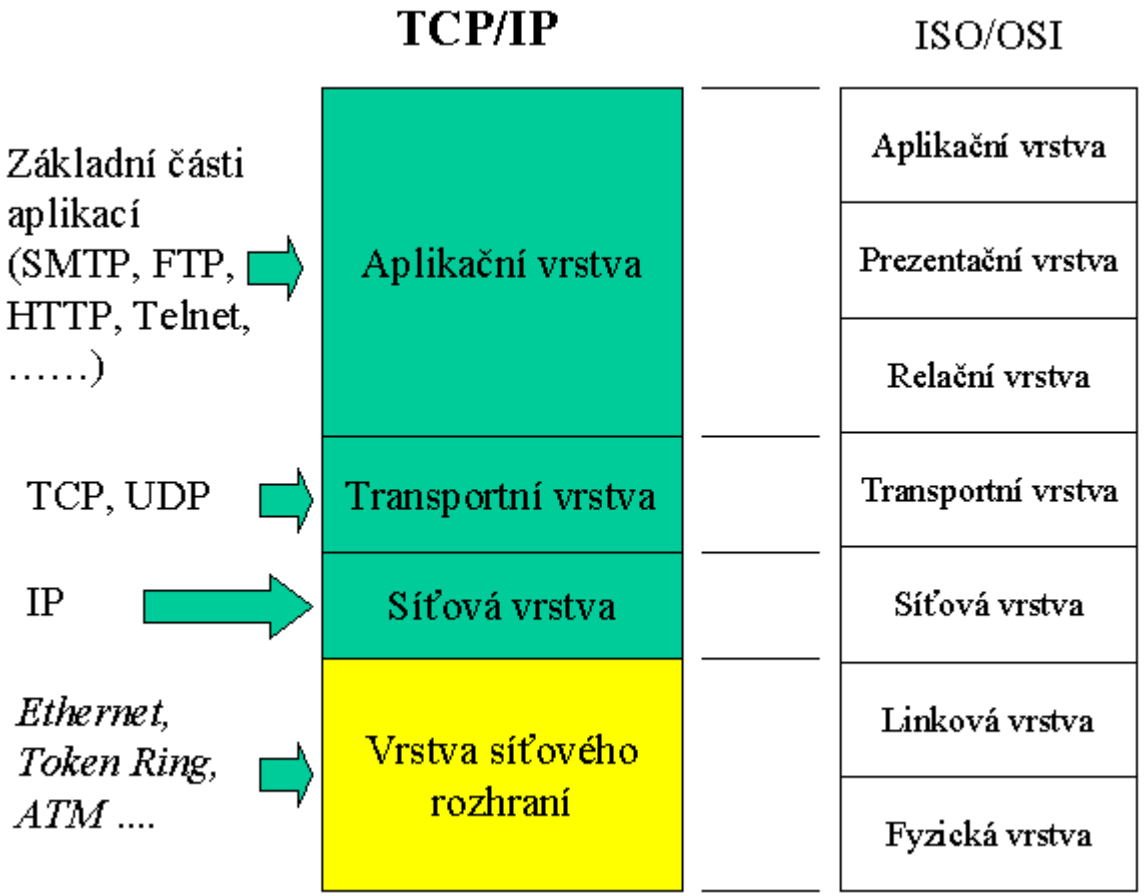


Obsah cvičení

- Komunikace na síti a internetu
- Ukázka nejčastějších protokolů na internetu
- Zachytávání a analýza síťového provozu

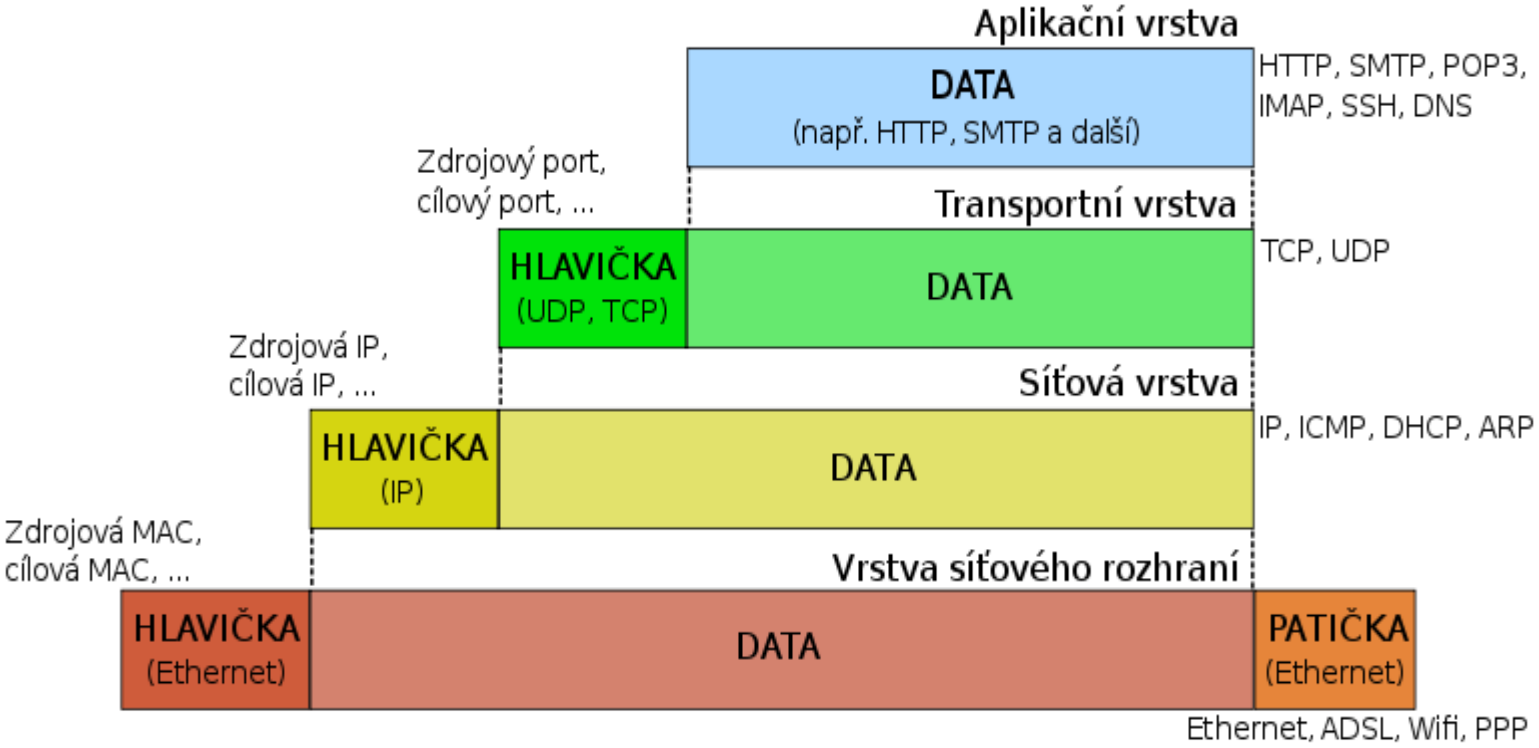
- MAC adresy (48 bitů)
  - 00-FF-9F-64-5E-9B
  - Poskytuje informaci o výrobci
  - Jedinečná
  - http://www.macvendorlookup.com/
- Každé PC má IP adresu
  - IPv4 – 147.229.8.52
  - IPv6 - 2001:0db8:85a3:08d3:1319:8a2e:0370:7344

- Komunikace pomocí:
  - Segmentů
  - Paketů
  - Rámců
- Komunikační protokol TCP/IP
- Výběr aplikace pomocí portů:
  - HTTP (WEB) – 80
  - SMTP – 25
  - POP3 – 110
  - SSH – 22
  - FTP – 20, 21
  - DNS – 53



zdroj: http://www.earchiv.cz/a708s600/a708s684.php3

- Zapouzdření na jednotlivých vrstvách



Zdroj: Wikipedia

- Kdo všechno může vidět přenášená data?
- tracert facebook.com (Windows) nebo traceroute facebook.com (Linux)

```
ibreiten@merlin: ~$ traceroute facebook.com
traceroute to facebook.com (69.171.230.5), 30 hops max, 60 byte packets
 1  bda-boz.fit.vutbr.cz (147.229.176.1)  0.629 ms  0.686 ms  0.743 ms
 2  pe-ant.net.vutbr.cz (147.229.254.205)  0.645 ms  1.048 ms  1.472 ms
 3  pe-kou.net.vutbr.cz (147.229.252.82)  0.685 ms  1.131 ms  1.499 ms
 4  rt-kou.net.vutbr.cz (147.229.252.114)  0.137 ms  0.135 ms  0.126 ms
 5  crs1.net.vutbr.cz (147.229.253.180)  3.558 ms  3.552 ms  3.540 ms
 6  195.113.235.89 (195.113.235.89)  7.119 ms  7.201 ms  7.189 ms
 7  cesnet.mx1.pra.cz.geant.net (62.40.124.29)  3.570 ms  3.563 ms  3.554 ms
 8  ae2.mx1.fra.de.geant.net (62.40.98.53)  10.003 ms  9.995 ms  9.932 ms
 9  ae1.br02.fra1.tfbnw.net (80.81.195.40)  17.183 ms  17.180 ms  17.209 ms
10  be19.bb02.fra2.tfbnw.net (31.13.30.14)  17.526 ms  17.654 ms  18.036 ms
11  ae2.bb02.ams2.tfbnw.net (74.119.78.92)  24.383 ms ae12.bb02.ams2.tfbnw.net (74.119.79.14)  23.375 ms ae2.bb02.ams2.tfbnw.net (74.119.78.92)  20.805 ms
12  ae4.bb01.bos2.tfbnw.net (204.15.23.57)  110.919 ms ae4.bb02.bos2.tfbnw.net (204.15.23.199)  100.464 ms  106.967 ms
13  be9.bb01.ewr2.tfbnw.net (31.13.27.59)  109.534 ms  111.596 ms be26.bb01.lga1.tfbnw.net (31.13.28.1)  115.029 ms
14  be29.bb01.dca1.tfbnw.net (74.119.78.78)  115.482 ms ae15.bb04.dca1.tfbnw.net (74.119.76.26)  113.156 ms be29.bb01.dca1.tfbnw.net (74.119.78.78)  115.884 ms
15  ae32.bb04.prn2.tfbnw.net (31.13.25.169)  196.161 ms  195.066 ms be28.bb01.prn2.tfbnw.net (31.13.31.65)  183.179 ms
16  ae0.dr11.prn1.tfbnw.net (31.13.25.163)  232.869 ms ae44.dr05.prn2.tfbnw.net (31.13.27.13)  174.599 ms ae3.dr10.prn1.tfbnw.net (31.13.27.123)  179.858 ms
17  * * *
18  * * *
19  * * *
20  * * *
21  edge-star-shv-17-prn1.facebook.com (69.171.230.5)  178.643 ms  179.138 ms  179.086 ms
```

- Open-source nástroj pro analýzu síťového provozu
- Zachytávání síťové komunikace na libovolném rozhraní
- Zobrazení obsahu paketů v závislosti na jejich typu
- K dispozici na www.wireshark.org

- Filtrování paketu dle IP
- ip.addr == X.X.X.X

Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	147.229.3.100	DNS	81	Standard query 0xafb0 A knot-win.fit.vutbr.cz
2	0.000111000	10.0.2.15	147.229.3.100	DNS	81	Standard query 0xfd4a AAAA knot-win.fit.vutbr.cz
3	0.008072000	147.229.3.100	10.0.2.15	DNS	287	Standard query response 0xafb0 A 147.229.8.52
4	0.008075000	147.229.3.100	10.0.2.15	DNS	299	Standard query response 0xfd4a AAAA 2001:67c:1220:808::93e5:834
5	0.008769000	10.0.2.15	147.229.8.52	TCP	74	51398→10000 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2376962 TSecr=0 WS=1024
6	0.017147000	147.229.8.52	10.0.2.15	TCP	60	10000→51398 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
7	0.017218000	10.0.2.15	147.229.8.52	TCP	54	51398→10000 [ACK] Seq=1 Ack=1 Win=29200 Len=0
8	0.017340000	10.0.2.15	147.229.8.52	HTTP/XMI	336	POST / HTTP/1.1
9	0.017456000	147.229.8.52	10.0.2.15	TCP	60	10000→51398 [ACK] Seq=1 Ack=283 Win=65535 Len=0
10	0.245911000	147.229.8.52	10.0.2.15	TCP	190	[TCP segment of a reassembled PDU]
11	0.246249000	10.0.2.15	147.229.8.52	TCP	54	51398→10000 [ACK] Seq=283 Ack=137 Win=30016 Len=0
12	0.258067000	147.229.8.52	10.0.2.15	HTTP/XMI	175	HTTP/1.0 200 OK
13	0.258229000	147.229.8.52	10.0.2.15	TCP	60	10000→51398 [FIN, ACK] Seq=258 Ack=283 Win=65535 Len=0
14	0.258474000	10.0.2.15	147.229.8.52	TCP	54	51398→10000 [ACK] Seq=283 Ack=258 Win=30016 Len=0
15	0.258774000	10.0.2.15	147.229.8.52	TCP	54	51398→10000 [FIN, ACK] Seq=283 Ack=259 Win=30016 Len=0
16	0.259187000	147.229.8.52	10.0.2.15	TCP	60	10000→51398 [ACK] Seq=259 Ack=284 Win=65535 Len=0
17	0.261162000	10.0.2.15	147.229.3.100	DNS	81	Standard query 0x0b9c A knot-win.fit.vutbr.cz
18	0.261421000	10.0.2.15	147.229.3.100	DNS	81	Standard query 0x27ed AAAA knot-win.fit.vutbr.cz
19	0.271613000	147.229.3.100	10.0.2.15	DNS	287	Standard query response 0x0b9c A 147.229.8.52
20	0.271798000	147.229.3.100	10.0.2.15	DNS	299	Standard query response 0x27ed AAAA 2001:67c:1220:808::93e5:834
21	0.272382000	10.0.2.15	147.229.8.52	TCP	74	51399→10000 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2377028 TSecr=0 WS=1024
22	0.282125000	147.229.8.52	10.0.2.15	TCP	60	10000→51399 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
23	0.282371000	10.0.2.15	147.229.8.52	TCP	54	51399→10000 [ACK] Seq=1 Ack=1 Win=29200 Len=0
24	0.283821000	10.0.2.15	147.229.8.52	HTTP/XMI	337	POST / HTTP/1.1
25	0.284377000	147.229.8.52	10.0.2.15	TCP	60	10000→51399 [ACK] Seq=1 Ack=284 Win=65535 Len=0
26	0.783598000	147.229.8.52	10.0.2.15	TCP	190	[TCP segment of a reassembled PDU]
27	0.783842000	10.0.2.15	147.229.8.52	TCP	54	51399→10000 [ACK] Seq=284 Ack=137 Win=30016 Len=0
28	0.789353000	147.229.8.52	10.0.2.15	HTTP/XMI	175	HTTP/1.0 200 OK
29	0.789441000	147.229.8.52	10.0.2.15	TCP	60	10000→51399 [FIN, ACK] Seq=258 Ack=284 Win=65535 Len=0
30	0.789563000	10.0.2.15	147.229.8.52	TCP	54	51399→10000 [ACK] Seq=284 Ack=258 Win=30016 Len=0
31	0.789710000	10.0.2.15	147.229.8.52	TCP	54	51399→10000 [FIN, ACK] Seq=284 Ack=259 Win=30016 Len=0
32	0.789930000	147.229.8.52	10.0.2.15	TCP	60	10000→51399 [ACK] Seq=259 Ack=285 Win=65535 Len=0
33	0.790236000	10.0.2.15	147.229.3.100	DNS	81	Standard query 0x043d A knot-win.fit.vutbr.cz
34	0.790377000	10.0.2.15	147.229.3.100	DNS	81	Standard query 0xea8c AAAA knot-win.fit.vutbr.cz
35	0.798666000	147.229.3.100	10.0.2.15	DNS	287	Standard query response 0x043d A 147.229.8.52
36	0.798754000	147.229.3.100	10.0.2.15	DNS	299	Standard query response 0xea8c AAAA 2001:67c:1220:808::93e5:834
37	0.799097000	10.0.2.15	147.229.8.52	TCP	74	51400→10000 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2377159 TSecr=0 WS=1024
38	0.808755000	147.229.8.52	10.0.2.15	TCP	60	10000→51400 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
39	0.808873000	10.0.2.15	147.229.8.52	TCP	54	51400→10000 [ACK] Seq=1 Ack=1 Win=29200 Len=0
40	0.809185000	10.0.2.15	147.229.8.52	HTTP/XMI	338	POST / HTTP/1.1

Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	SuperMic_0e:a4:12	Broadcast	ARP	60	Who has 147.229.8.1? Tell 147.229.8.52
2	77.6549060(	147.229.8.38	147.229.8.52	TCP	74	57048→10000 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1381301760 TSecr=0 WS=128
3	77.6551440(	SuperMic_0e:a4:12	Broadcast	ARP	60	Who has 147.229.8.38? Tell 147.229.8.52
4	77.6551590(	SuperMic_c8:a6:2b	SuperMic_0e:a4:12	ARP	42	147.229.8.38 is at 00:25:90:c8:a6:2b
5	77.6552750(	147.229.8.52	147.229.8.38	TCP	74	10000→57048 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=47145904 TSecr=1381301760
6	77.6553000(	147.229.8.38	147.229.8.52	TCP	66	57048→10000 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1381301760 TSecr=47145904
7	77.6553800(	147.229.8.38	147.229.8.52	HTTP/XMI	348	POST / HTTP/1.1
8	77.6577840(	147.229.8.52	147.229.8.38	HTTP/XMI	323	HTTP/1.0 200 OK
9	77.6578140(	147.229.8.52	147.229.8.38	TCP	66	10000→57048 [FIN, ACK] Seq=258 Ack=283 Win=66560 Len=0 TSval=47145905 TSecr=1381301760
10	77.6578370(	147.229.8.38	147.229.8.52	TCP	66	57048→10000 [ACK] Seq=283 Ack=258 Win=30336 Len=0 TSval=1381301760 TSecr=47145905
11	77.6581060(	147.229.8.38	147.229.8.52	TCP	66	57048→10000 [FIN, ACK] Seq=283 Ack=259 Win=30336 Len=0 TSval=1381301760 TSecr=47145905
12	77.6582200(	147.229.8.52	147.229.8.38	TCP	66	10000→57048 [ACK] Seq=259 Ack=284 Win=66560 Len=0 TSval=47145905 TSecr=1381301760
13	82.6627060(	SuperMic_c8:a6:2b	SuperMic_0e:a4:12	ARP	42	Who has 147.229.8.52? Tell 147.229.8.38
14	82.6628150(	SuperMic_0e:a4:12	SuperMic_c8:a6:2b	ARP	60	147.229.8.52 is at 00:25:90:0e:a4:12
15	124.002778(	SuperMic_0e:a4:12	Broadcast	ARP	60	Who has 147.229.8.1? Tell 147.229.8.52
16	204.886895(	147.229.8.38	147.229.8.52	TCP	74	57057→10000 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1381333568 TSecr=0 WS=128
17	204.887125(	SuperMic_0e:a4:12	Broadcast	ARP	60	Who has 147.229.8.38? Tell 147.229.8.52
18	204.887142(	SuperMic_c8:a6:2b	SuperMic_0e:a4:12	ARP	42	147.229.8.38 is at 00:25:90:c8:a6:2b
19	204.887213(	147.229.8.52	147.229.8.38	TCP	74	10000→57057 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=47158627 TSecr=1381333568
20	204.887242(	147.229.8.38	147.229.8.52	TCP	66	57057→10000 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1381333568 TSecr=47158627
21	204.887295(	147.229.8.38	147.229.8.52	HTTP/XMI	349	POST / HTTP/1.1
22	205.087477(	147.229.8.52	147.229.8.38	TCP	66	10000→57057 [ACK] Seq=1 Ack=284 Win=66560 Len=0 TSval=47158647 TSecr=1381333568
23	205.142963(	147.229.8.52	147.229.8.38	HTTP/XMI	323	HTTP/1.0 200 OK
24	205.142992(	147.229.8.52	147.229.8.38	TCP	66	10000→57057 [FIN, ACK] Seq=258 Ack=284 Win=66560 Len=0 TSval=47158653 TSecr=1381333568
25	205.143044(	147.229.8.38	147.229.8.52	TCP	66	57057→10000 [ACK] Seq=284 Ack=258 Win=30336 Len=0 TSval=1381333632 TSecr=47158653
26	205.143336(	147.229.8.38	147.229.8.52	TCP	66	57057→10000 [FIN, ACK] Seq=284 Ack=259 Win=30336 Len=0 TSval=1381333632 TSecr=47158653
27	205.143460(	147.229.8.52	147.229.8.38	TCP	66	10000→57057 [ACK] Seq=259 Ack=285 Win=66560 Len=0 TSval=47158653 TSecr=1381333632
28	209.894706(	SuperMic_c8:a6:2b	SuperMic_0e:a4:12	ARP	42	Who has 147.229.8.52? Tell 147.229.8.38
29	209.894827(	SuperMic_0e:a4:12	SuperMic_c8:a6:2b	ARP	60	147.229.8.52 is at 00:25:90:0e:a4:12
30	332.374849(	147.229.8.38	147.229.8.52	TCP	74	57061→10000 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1381365440 TSecr=0 WS=128
31	332.375088(	SuperMic_0e:a4:12	Broadcast	ARP	60	Who has 147.229.8.38? Tell 147.229.8.52
32	332.375102(	SuperMic_c8:a6:2b	SuperMic_0e:a4:12	ARP	42	147.229.8.38 is at 00:25:90:c8:a6:2b
33	332.375180(	147.229.8.52	147.229.8.38	TCP	74	10000→57061 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=47171375 TSecr=1381365440
34	332.375207(	147.229.8.38	147.229.8.52	TCP	66	57061→10000 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1381365440 TSecr=47171375
35	332.375270(	147.229.8.38	147.229.8.52	HTTP/XMI	350	POST / HTTP/1.1
36	332.417182(	147.229.8.52	147.229.8.38	HTTP/XMI	323	HTTP/1.0 200 OK
37	332.417212(	147.229.8.52	147.229.8.38	TCP	66	10000→57061 [FIN, ACK] Seq=258 Ack=285 Win=66560 Len=0 TSval=47171380 TSecr=1381365440
38	332.417233(	147.229.8.38	147.229.8.52	TCP	66	57061→10000 [ACK] Seq=285 Ack=258 Win=30336 Len=0 TSval=1381365450 TSecr=47171380
39	332.417433(	147.229.8.38	147.229.8.52	TCP	66	57061→10000 [FIN, ACK] Seq=285 Ack=259 Win=30336 Len=0 TSval=1381365450 TSecr=47171380
40	332.417485(	147.229.8.52	147.229.8.38	TCP	66	10000→57061 [ACK] Seq=259 Ack=286 Win=66560 Len=0 TSval=47171380 TSecr=1381365450

- HTTP - webové stránky, nezabezpečený
- HTTPS - webové stránky, zabezpečený
- SMTP, IMAP, POP3 – poštovní protokoly
- FTP - přenos souborů
- Telnet – jednoduchý komunikační protokol

- Zabezpečené protokoly typicky označeny S
  - FTPS – FTP tunelováno přes SSL/TLS
  - SFTP – FTP tunelováno přes SSH

TELNET

- Jednoduchý protokol pro komunikaci po síti přes TCP
- Specifikován roku 1969 v RFC 15
- Port 23
- Nezabezpečený
- Dnes používán především pro jednoduché testování otevřených portů, služeb …
- Příklad:
- http://wiki.wireshark.org/SampleCaptures?action=AttachFile&do=get&target=telnet-cooked.pcap

- File Transfer Protocol
- Jednoduchý protokol pro přenos dat
- Porty 21 (příkazy) a 20 (data)
- Specifikován roku 1985 v **RFC** 959
- Nezabezpečený
- FTPS zabezpečení pomocí TLS/SSL
- vsftp 2.3.4 – obsahuje zadní vrátka

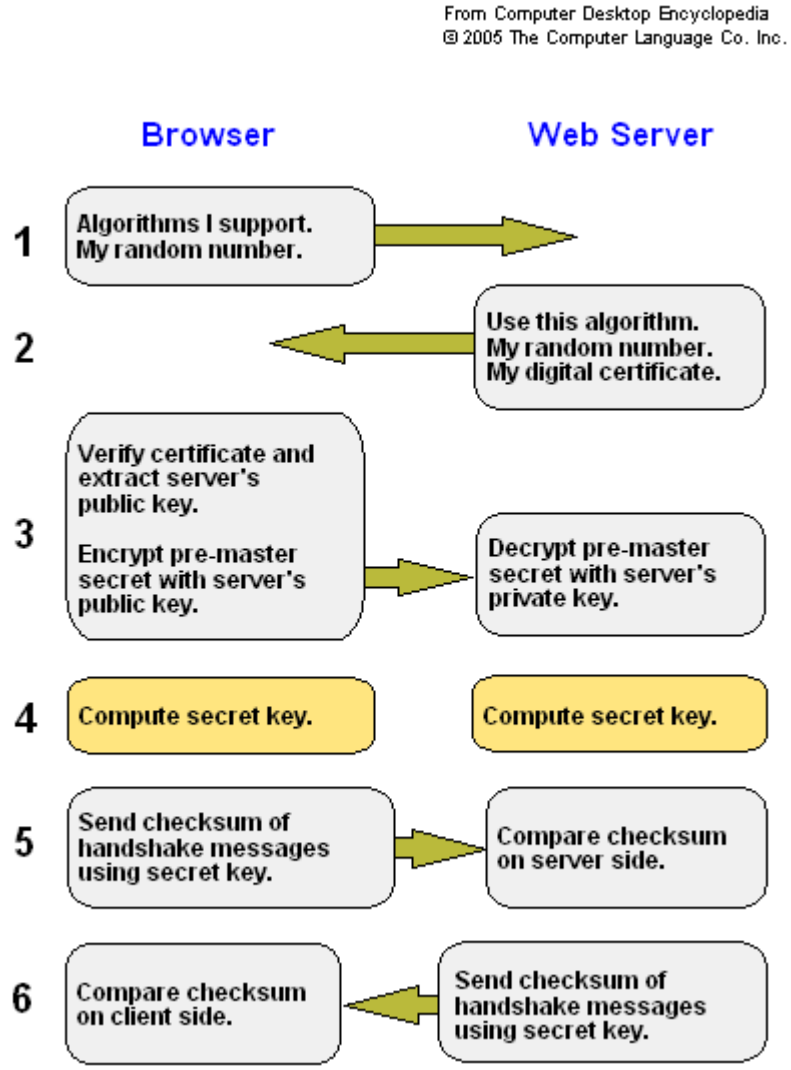
- Hypertext Transfer Protocol
- TCP port 80
- Data v otevřené podobě
- Nezajišťuje utajení ani integritu
- Základní příkazy:
  - GET – Požadavek na server
  - POST – Zaslání dat na server
- Pro šifrování a autentizaci HTTP + TLS\SSL-> HTTPS

- Transport Layer Security
- Secure Sockets Layer

- Protokoly zabezpečující autentizaci a šifrování
- Autentizace pomocí certifikátů
- Typické použití HTTPS, IMAP, SMTP, FTPS
- Nejčastěji pouze autentizace serveru vůči klientovi
  - Možná obousměrná autentizace
- Nejčastěji používané verze ~~SSL 3.0~~, TSL 1.1
  - SSL 3.0 obsahuje bezpečnostní chybu – Poodle Attack

(Padding Oracle On Downgraded Legacy Encryption)

- SSL handshake
- Příklad jednosměrné autentizace



Zdroj: http://www.mwclearning.com/?p=883

Poštovní protokoly

- SMTP, POP3, IMAP
- Bezpečné? Pouze za použití TLS/SSL
- Jinak lze login a heslo snadno získat z paketů + emaily v otevřené podobě
- TLS/SSL řeší připojení klient server, co ale pošta přeposílaná mezi servery?
- Řešení: TLS + šifrování pošty + certifikáty

Poštovní protokoly

- POP3 , IMAP
- Protokol určený ke stahování pošty ze poštovního serveru
  - Využívají je poštovní klienti (Outlook, Thunderbird…)
  - Porty POP3 110
    IMAP 143

- SMTP
- Protokol pro odesílání pošty z klienta na server
- Využívá se také pro přeposílání mezi servery
  - Port SMTP 25

tcpdump

```
[root@devonly ~]# tcpdump -i eth0 -X -nn -vvv -s0 src 192.168.122.14 and dst 192.168.122.98
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
10:21:40.874818 IP (tos 0x0, ttl 64, id 34874, offset 0, flags [DF], proto TCP (6), length 60)
    192.168.122.14.59104 > 192.168.122.98.110: Flags [S], cksum 0xd5a3 (correct), seq 3389733946, win 14600, options [mss 1460,sackOK,TS val 570471424 ecr 0,nop,wscale 4], length 0
        0x0000:  4500 003c 883a 4000 4006 3cc0 c0a8 7a0e  E..<.:@.@.<...z.
        0x0010:  c0a8 7a62 e6e0 006e ca0b 3c3a 0000 0000  ..zb...n..<:....
        0x0020:  a002 3908 d5a3 0000 0204 05b4 0402 080a  ..9.............
        0x0030:  2200 b400 0000 0000 0103 0304            "...........
10:21:40.875344 IP (tos 0x0, ttl 64, id 34875, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.122.14.59104 > 192.168.122.98.110: Flags [.], cksum 0x218c (correct), seq 3389733947, ack 2279230092, win 913, options [nop,nop,TS val 570471425 ecr 386019038], length 0
        0x0000:  4500 0034 883b 4000 4006 3cc7 c0a8 7a0e  E..4.;@.@.<...z.
        0x0010:  c0a8 7a62 e6e0 006e ca0b 3c3b 87da 4a8c  ..zb...n..<;..J.
        0x0020:  8010 0391 218c 0000 0101 080a 2200 b401  ....!.......".."...
        0x0030:  1702 2ede                                ....
10:21:40.880870 IP (tos 0x0, ttl 64, id 34876, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.122.14.59104 > 192.168.122.98.110: Flags [.], cksum 0x216d (correct), seq 0, ack 21, win 913, options [nop,nop,TS val 570471430 ecr 386019044], length 0
        0x0000:  4500 0034 883c 4000 4006 3cc6 c0a8 7a0e  E..4.<@.@.<...z.
        0x0010:  c0a8 7a62 e6e0 006e ca0b 3c3b 87da 4aa0  ..zb...n..<;..J.
        0x0020:  8010 0391 216d 0000 0101 080a 2200 b406  ....!m......"...
        0x0030:  1702 2ee4                                ....
10:21:40.881051 IP (tos 0x0, ttl 64, id 34877, offset 0, flags [DF], proto TCP (6), length 58)
    192.168.122.14.59104 > 192.168.122.98.110: Flags [P.], cksum 0x80d1 (correct), seq 0:6, ack 21, win 913, options [nop,nop,TS val 570471431 ecr 386019044], length 6
        0x0000:  4500 003a 883d 4000 4006 3cbf c0a8 7a0e  E..:.=@.@.<...z.
        0x0010:  c0a8 7a62 e6e0 006e ca0b 3c3b 87da 4aa0  ..zb...n..<;..J.
        0x0020:  8018 0391 80d1 0000 0101 080a 2200 b407  ............"...
        0x0030:  1702 2ee4 4341 5041 0d0a                 ....CAPA..
10:21:40.881516 IP (tos 0x0, ttl 64, id 34878, offset 0, flags [DF], proto TCP (6), length 64)
    192.168.122.14.59104 > 192.168.122.98.110: Flags [P.], cksum 0x770e (correct), seq 6:18, ack 100, win 913, options [nop,nop,TS val 570471431 ecr 386019044], length 12
        0x0000:  4500 0040 883e 4000 4006 3cb8 c0a8 7a0e  E..@.>@.@.<...z.
        0x0010:  c0a8 7a62 e6e0 006e ca0b 3c41 87da 4aef  ..zb...n..<A..J.
        0x0020:  8018 0391 770e 0000 0101 080a 2200 b407  ....w.......".."...
        0x0030:  1702 2ee4 5553 4552 2073 6d69 7468 0d0a  ....USER.smith..
10:21:40.882102 IP (tos 0x0, ttl 64, id 34879, offset 0, flags [DF], proto TCP (6), length 67)
    192.168.122.14.59104 > 192.168.122.98.110: Flags [P.], cksum 0x0ace (correct), seq 18:33, ack 105, win 913, options [nop,nop,TS val 570471432 ecr 386019045], length 15
        0x0000:  4500 0043 883f 4000 4006 3cb4 c0a8 7a0e  E..C.?@.@.<...z.
        0x0010:  c0a8 7a62 e6e0 006e ca0b 3c4d 87da 4af4  ..zb...n..<M..J.
        0x0020:  8018 0391 0ace 0000 0101 080a 2200 b408  ............"...
        0x0030:  1702 2ee5 5041 5353 2071 4277 5a48 7a4c  ....PASS.qBwZHzL
        0x0040:  310d 0a                                  1..
```

- ASCII reprezentace typicky binárních dat
- Často používané kódování (ne šifrování)
  - Využití např. u certifikátů, přílohy emailů MIME (Multi-Purpose Internet Mail Extensions), SMTP přenos hesla …
- Princip: Trojice bytů zakódována do čtyř ASCII znaků
  - 6tice bitů slouží jako index do tabulky znaků
  - `ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/`

Znak	M	a	n
ASCII	77	97	110
Řetězec Bitů	0 1 0 0 1 1 0 1	0 1 1 0 0 0 0 1	0 1 0 0 0 0 0 1

Index	19	22	5	1
Base64	T	W	F	B

Užitečné příkazy

- CMD
  - nslookup – překlad doménového jména <-> IP
    - nslookup Seznam.cz
  - tracert – trasování paket
    - Tracert Seznam.cz
  - Ipconfig /all – informace o nastavení síťových adaptérů v PC

Užitečné Wireshark filtry

- ip.addr == X.X.X.X filtrace paketů dle IP
- smtp filtrace paketů odchozí pošty
- pop filtrace paketů příchozí pošty
- imap filtrace paketů příchozí pošty
- ftp filtrace paketů protokolu FTP
- ssl filtrace paketů protokolu SSL/TLS

Děkuji za pozornost