

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

**Fakulta elektrotechnická**

PROJEKT Č. 4

## **Analýza aplikačních protokolů**

**Vypracoval:** Jan HLÍDEK

**V rámci předmětu:** Komunikace v datových sítích (X32KDS)

**Měřeno:** 28. 4. 2008

**Cvičení:** pondělí od 11:00 do 12:30

# 1. CÍL ÚLOHY

Seznámit se s podstatou analýzy protokolů na aplikační úrovni. Jedná se o protokoly DHCP, FTP, TFTP, SMTP a POP3

## 2. ZMĚŘENÉ VÝSTUPY A ROZBOR

Následují vždy jednotlivé úkoly, které měly být provedeny a zachyceny ve Wiresharku. Informace k nim jsou také hodnotícího charakteru – v závěru již nebude každý bod zvlášť komentován.

Odpovědi pramení většinou z webové encyklopedie Wikipedia a také z knihy „Data Communications, Computer Networks and Open Systems“.

V programu TFTPd32 v záložce DHCP server bylo pro naši skupinu nastaveno:

- IP pool starting address: 10.1.36.36
- WINS/DNS Server: 10.1.36.136
- Default router: 10.1.36.76

V programu HomeFTPserver byl vytvořen účet:

- User name: po11-6
- Password: po11-6-heslo

No. -	Time	Source	Destination	Protocol	Info
1	0.000000	AsustekC_00:f5:7f	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.36
2	3.999631	AsustekC_00:f5:7f	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.36
3	7.394453	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x78eb6e75
4	7.396737	10.1.36.36	10.1.36.38	ICMP	Echo (ping) request
5	7.890854	10.1.36.36	10.1.36.38	ICMP	Echo (ping) request
6	8.390318	10.1.36.36	10.1.36.38	ICMP	Echo (ping) request
7	8.892225	10.1.36.36	255.255.255.255	DHCP	DHCP Offer - Transaction ID 0x78eb6e75
8	8.892623	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x78eb6e75
9	8.895157	10.1.36.36	10.1.36.38	ICMP	Echo (ping) request
10	9.390284	10.1.36.36	10.1.36.38	ICMP	Echo (ping) request
11	9.891176	10.1.36.36	10.1.36.38	ICMP	Echo (ping) request
12	10.392150	10.1.36.36	255.255.255.255	DHCP	DHCP ACK - Transaction ID 0x78eb6e75
13	10.396455	AsustekC_00:f4:c1	Broadcast	ARP	Gratuitous ARP for 10.1.36.38 (Request)
14	10.999572	AsustekC_00:f5:7f	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.36
15	11.222221	AsustekC_00:f4:c1	Broadcast	ARP	Gratuitous ARP for 10.1.36.38 (Request)
16	12.222208	AsustekC_00:f4:c1	Broadcast	ARP	Gratuitous ARP for 10.1.36.38 (Request)
17	12.499387	AsustekC_00:f5:7f	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.36
18	13.252571	10.1.36.38	224.0.0.22	IGMP	v3 Membership Report
19	13.254095	AsustekC_00:f4:c1	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.38
20	13.999343	AsustekC_00:f5:7f	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.36
21	14.222166	10.1.36.38	224.0.0.22	IGMP	v3 Membership Report
22	14.800282	AsustekC_00:f4:c1	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.38
23	15.530569	10.1.36.36	10.1.255.255	NBNS	Name query NB U47.ESET.COM<00>
24	16.280542	10.1.36.36	10.1.255.255	NBNS	Name query NB U47.ESET.COM<00>
25	16.300206	AsustekC_00:f4:c1	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.38

  

```

+ Frame 3 (342 bytes on wire, 342 bytes captured)
+ Ethernet II, Src: AsustekC_00:f4:c1 (00:13:d4:00:f4:c1), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
+ Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
  Version: 4
  Header length: 20 bytes
+ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
  Total Length: 328
  Identification: 0x42f8 (17144)
+ Flags: 0x00
  Fragment offset: 0
  Time to live: 128
  Protocol: UDP (0x11)
+ Header checksum: 0xf6ad [correct]
  Source: 0.0.0.0 (0.0.0.0)
  Destination: 255.255.255.255 (255.255.255.255)
+ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
+ Bootstrap Protocol

```

  

```

0010  01 48 42 f8 00 00 80 11 f6 ad 00 00 00 00 ff ff .HB.....
0020  ff ff 00 44 00 43 01 34 9c c0 01 01 06 00 78 eb .D.C.4....x.
0030  6e 75 00 00 00 00 00 00 00 00 00 00 00 00 00 nu.....
0040  00 00 00 00 00 00 00 13 d4 00 f4 c1 00 00 00 00 .....
0050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00a0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

```

Obr. 1 Přidělování IP adresy DHCP serverem

Obr. 1 ukazuje jak je přidělována IP adresa. Zpráva DHCP discover poslaná do sítě od PC-vpravo se šíří jako broadcast. Tím žádá o to, aby se ohlásily DHCP servery, které jsou momentálně dostupné. Odpověď od DHCP serveru je formou DHCP Offer zprávy posílané unicastem, v níž se PC-vpravo nabízí adresy, které mu mohou být přiděleny. PC-vpravo odpoví broadcastem, že chce danou adresu. Toto opět mohou „slyšet“ všechny do sítě připojené stanice. Následně DHCP server potvrdí přidělení dané adresy zprávou DHCP Ack.

No. -	Time	Source	Destination	Protocol	Info
66	47.560986	AsustekC_00:f5:7f	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.36
67	54.560924	AsustekC_00:f5:7f	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.36
68	55.231746	AsustekC_00:f4:c1	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.38
69	56.060732	AsustekC_00:f5:7f	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.36
70	57.560697	AsustekC_00:f5:7f	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.36
71	59.091925	10.1.36.36	10.1.255.255	NBNS	Name query NB U46.ESET.COM<00>
72	59.220829	AsustekC_00:f4:c1	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.38
73	59.841911	10.1.36.36	10.1.255.255	NBNS	Name query NB U46.ESET.COM<00>
74	60.591888	10.1.36.36	10.1.255.255	NBNS	Name query NB U46.ESET.COM<00>
75	61.359167	AsustekC_00:f5:7f	Broadcast	ARP	who has 10.1.36.76? Tell 10.1.36.36
76	62.983219	10.1.36.38	10.1.36.36	ICMP	Echo (ping) request
77	62.983376	10.1.36.36	10.1.36.38	ICMP	Echo (ping) reply
78	63.220721	AsustekC_00:f4:c1	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.38
79	63.970699	10.1.36.38	10.1.36.36	ICMP	Echo (ping) request
80	63.970848	10.1.36.36	10.1.36.38	ICMP	Echo (ping) reply
81	64.389806	AsustekC_00:f5:7f	Broadcast	ARP	who has 10.1.36.76? Tell 10.1.36.36
82	64.970661	10.1.36.38	10.1.36.36	ICMP	Echo (ping) request
83	64.970803	10.1.36.36	10.1.36.38	ICMP	Echo (ping) reply
84	65.986280	10.1.36.38	10.1.36.36	ICMP	Echo (ping) request
85	65.986437	10.1.36.36	10.1.36.38	ICMP	Echo (ping) reply
86	70.220755	AsustekC_00:f4:c1	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.38
87	70.404095	AsustekC_00:f5:7f	Broadcast	ARP	who has 10.1.36.76? Tell 10.1.36.36
88	71.720433	AsustekC_00:f4:c1	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.38
89	73.220391	AsustekC_00:f4:c1	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.38
90	74.751586	10.1.36.38	10.1.255.255	NBNS	Name query NB U32.ESET.COM<00>

  

⊕ Frame 76 (74 bytes on wire, 74 bytes captured)	
⊖ Ethernet II, Src: AsustekC_00:f4:c1 (00:13:d4:00:f4:c1), Dst: AsustekC_00:f5:7f (00:13:d4:00:f5:7f)	
⊕ Destination: AsustekC_00:f5:7f (00:13:d4:00:f5:7f)	
⊕ Source: AsustekC_00:f4:c1 (00:13:d4:00:f4:c1)	
Type: IP (0x0800)	
⊖ Internet Protocol, Src: 10.1.36.38 (10.1.36.38), Dst: 10.1.36.36 (10.1.36.36)	
Version: 4	
Header length: 20 bytes	
⊕ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)	
Total Length: 60	
Identification: 0x432c (17196)	
⊕ Flags: 0x00	
Fragment offset: 0	
Time to live: 128	
Protocol: ICMP (0x01)	
⊕ Header checksum: 0x9b49 [correct]	
source: 10.1.36.38 (10.1.36.38)	
destination: 10.1.36.36 (10.1.36.36)	
⊕ Internet Control Message Protocol	

  

0000	00 13 d4 00 f5 7f 00 13 d4 00 f4 c1 08 00 45 00	.....E.
0010	00 3c 43 2c 00 00 80 01 9b 49 0a 01 24 26 0a 01	<C,... .I..\$&.
0020	24 24 08 00 4a 5c 02 00 01 00 61 62 63 64 65 66	\$\$..J\.. ..abcdef
0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
0040	77 61 62 63 64 65 66 67 68 69	wabcdefg hi

**Obr. 2** Posílání „ping“ – ověření spojení mezi PC vlevo a vpravo po získání nové adresy z DHCP serveru

Přidávají se odpovědi na položené otázky:

1. *Proč se zpráva DHCP Request šíří jako broadcast, když již ve zprávě DHCP offer klientská stanice zjistí IP adresu DHCP serveru?*

Je totiž třeba, aby byly informovány i ostatní DHCP servery, že právě tomu PC byla přidělena adresa a již není třeba se o něj starat. Svoje DHCP Offers tím pádem již nepošlou.

2. *Proč stanice, která pomocí DHCP protokolu obdrží IP adresu, se vzápětí protokolem ARP dotazuje, kdo vlastní tuto adresu?*

Jedná se o jakýsi bezpečnostní mechanismus pro ochranu před kolizemi. Mohlo by se totiž stát, že daná adresa již byla přidělena například při manuálním nastavování adres někde jinde v dané síti.

### 3. Jaký protokol na transportní vrstvě používají protokoly DHCP, TFTP a SMTP?

Protokol DHCP používá na transportní vrstvě UDP (User Datagram Protocol), který nezaručuje bezchybný přenos dat. V případě nedoručení je datagram jednoduše zahozen a UDP se nestará o přeposílání. Důkazem je výpis z Wiresharku a oranžově zarámovaná oblast na Obr. 1. UDP používá také TFTP protokol. Na druhou stranu protokol SMTP užívá protokol TCP často označovaný také jako spojově orientovaný – stará se o zajištění spolehlivého přenosu s případným opětovným přeposíláním ztracených dat. Vždy je nutné nějak potvrdit, že datagram dorazil úspěšně/neúspěšně.

### 4. Na jakých portech probíhá komunikace protokolů DHCP a TFTP (klient i server)

Komunikace probíhá u DHCP serveru dle Obr. 3 na portech 68 a 67. Pakety, které odesílá klient mají jako zdrojový port 68 a jako cílový 67. Pakety odeslané serverem mají zdrojový port 67 a cílový 68.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	AsustekC_00:f5:7f	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.36
2	3.999631	AsustekC_00:f5:7f	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.36
3	7.394453	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x78eb6e75
4	7.396737	10.1.36.36	10.1.36.38	ICMP	Echo (ping) request
5	7.890854	10.1.36.36	10.1.36.38	ICMP	Echo (ping) request
6	8.390318	10.1.36.36	10.1.36.38	ICMP	Echo (ping) request
7	8.892225	10.1.36.36	255.255.255.255	DHCP	DHCP Offer - Transaction ID 0x78eb6e75
8	8.892623	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x78eb6e75
9	8.895157	10.1.36.36	10.1.36.38	ICMP	Echo (ping) request
10	9.390284	10.1.36.36	10.1.36.38	ICMP	Echo (ping) request
11	9.891176	10.1.36.36	10.1.36.38	ICMP	Echo (ping) request
12	10.392150	10.1.36.36	255.255.255.255	DHCP	DHCP ACK - Transaction ID 0x78eb6e75

  

Frame 3 (342 bytes on wire (342 bytes captured) on interface 0)	
Ethernet II, Src: AsustekC_00:f4:c1 (00:13:d4:00:f4:c1), Dst: Broadcast (ff:ff:ff:ff:ff:ff)	
Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)	
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)	
Source port: bootpc (68)	
Destination port: bootps (67)	
Length: 308	
Checksum: 0x9cc0 [correct]	
Bootstrap Protocol	

  

0010	01 48 42 18 00 00 80 11 10 40 00 00 00 00 11 11	..P.....
0020	ff ff 00 44 00 43 01 34 9c c0 01 01 06 00 78 eb	...D.C.4...X.
0030	6e 75 00 00 00 00 00 00 00 00 00 00 00 00 00	nu.....

Obr. 3 Komunikace protokolu DHCP – porty 67 a 68

TFTP protokol se musí sám postarat o garantované spojení, protože to za něj UDP neudělá. Pracuje na portu 69, jak dokládá Obr. 4. Při vytváření si klient zvolí TID (Transfer Identifier) – číslo spojení a posílá ho na „běžný“ port 69 na serveru. Server pak pošle odpověď z portu 69 jako svého zdrojového, přičemž cílovým je port s číslem TID klienta, které zůstává stejné dokud není spojení zrušeno. Každý paket má přiřazena dvě TID – jedno zdrojové a druhé cílové, což dokládá Obr. 5.

71.279306	AsustekC_00:f5:7f	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.36
71.313554	10.1.36.38	10.1.255.255	NBNS	Name query NB U30.ESET.COM<00>
72.064351	AsustekC_00:f4:c1	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.38
72.342024	AsustekC_00:f5:7f	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.36
73.478529	10.1.36.38	10.1.36.36	TFTP	Read Request, File: test.abc, Transfer type: 0
73.486451	10.1.36.36	10.1.36.38	TFTP	Option Acknowledgement, tsize=9
73.486635	10.1.36.38	10.1.36.36	TFTP	Acknowledgement, Block: 0
73.486803	10.1.36.36	10.1.36.38	TFTP	Data Packet, Block: 1 (last)
73.486925	10.1.36.38	10.1.36.36	TFTP	Acknowledgement, Block: 1
73.841761	AsustekC_00:f5:7f	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.36
75.341692	AsustekC_00:f5:7f	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.36
76.064351	AsustekC_00:f4:c1	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.38

  

Frame 53 (67 bytes on wire, 67 bytes captured)			
Ethernet II, Src: AsustekC_00:f4:c1 (00:13:d4:00:f4:c1), Dst: AsustekC_00:f5:7f (00:13:d4:00:f5:7f)			
Internet Protocol, Src: 10.1.36.38 (10.1.36.38), Dst: 10.1.36.36 (10.1.36.36)			
Version: 4			
Header length: 20 bytes			
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)			
Total Length: 53			
Identification: 0x4408 (17416)			
Flags: 0x00			
Fragment offset: 0			
Time to live: 128			
Protocol: UDP (0x11)			
Header checksum: 0x9a64 [correct]			
Source: 10.1.36.38 (10.1.36.38)			
Destination: 10.1.36.36 (10.1.36.36)			
User Datagram Protocol, Src Port: 1535 (1535), Dst Port: tftp (69)			
Trivial File Transfer Protocol			

  

0000	00 13 d4 00 f5 7f 00 13 d4 00 f4 c1 08 00 45 00	.....E.
0010	00 35 44 08 00 00 80 11 9a 64 0a 01 24 26 0a 01	.5D.....d.\$&..
0020	24 24 05 ff 00 45 00 21 6c b2 00 01 74 65 73 74	\$.E.!l..test
0030	2e 61 62 63 00 6f 63 74 65 74 00 74 73 69 7a 65	.abc.oct et.tsize
0040	00 30 00	.0.

Obr. 4 Komunikace protokolu TFTP – port 69

57.343003	AsustekC_00:f5:7f	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.36
58.282720	AsustekC_00:f4:c1	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.38
61.342095	AsustekC_00:f5:7f	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.36
65.282685	AsustekC_00:f4:c1	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.38
65.342023	AsustekC_00:f5:7f	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.36
66.782440	AsustekC_00:f4:c1	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.38
68.282396	AsustekC_00:f4:c1	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.38
69.779346	AsustekC_00:f5:7f	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.36
69.813602	10.1.36.38	10.1.255.255	NBNS	Name query NB U30.ESET.COM<00>
70.563583	10.1.36.38	10.1.255.255	NBNS	Name query NB U30.ESET.COM<00>
71.279306	AsustekC_00:f5:7f	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.36
71.313554	10.1.36.38	10.1.255.255	NBNS	Name query NB U30.ESET.COM<00>
72.064351	AsustekC_00:f4:c1	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.38
72.342024	AsustekC_00:f5:7f	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.36
73.478529	10.1.36.38	10.1.36.36	TFTP	Read Request, File: test.abc, Transfer
73.486451	10.1.36.36	10.1.36.38	TFTP	Option Acknowledgement, tsize=9
73.486635	10.1.36.38	10.1.36.36	TFTP	Acknowledgement, Block: 0
73.486803	10.1.36.36	10.1.36.38	TFTP	Data Packet, Block: 1 (last)
73.486925	10.1.36.38	10.1.36.36	TFTP	Acknowledgement, Block: 1
73.841761	AsustekC_00:f5:7f	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.36
75.341692	AsustekC_00:f5:7f	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.36
76.064351	AsustekC_00:f4:c1	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.38

  

Frame 56 (60 bytes on wire, 60 bytes captured)			
Ethernet II, Src: AsustekC_00:f5:7f (00:13:d4:00:f5:7f), Dst: AsustekC_00:f4:c1 (00:13:d4:00:f4:c1)			
Internet Protocol, Src: 10.1.36.36 (10.1.36.36), Dst: 10.1.36.38 (10.1.36.38)			
User Datagram Protocol, Src Port: 2130 (2130), Dst Port: 1535 (1535)			
Source port: 2130 (2130)			
Destination port: 1535 (1535)			
Length: 21			
Checksum: 0xec8e [correct]			
Trivial File Transfer Protocol			

Obr. 5 Ukázka TID

5. V záznamu komunikace protokolem FTP nalezněte a popište (kdo komunikaci iniciuje, kdo volí čísla portů...) inicializaci spojení pro přenos dat v aktivním a pasivním režimu.

Postup při navazování komunikace mezi serverem a klientem v aktivním režimu ukazuje Obr. 6. FTP server pošle data na port a adresu zadanou klientem. Spojení je navázáno tak, že na portu 21 je server a na 1546 je klient. Dále se přenesou následující zprávy:

- USER – uživatelské jméno
- PASS – heslo
- SYST – pro k zjištění typu systému, na kterém pracuje FTP server
- FEAT – jaké funkce jsou podporované
- PWD – zjištění aktuálního pracovního adresáře
- TYPE – určuje typ reprezentace dat, např. text nebo binární
- PORT – specifikuje port, na kterém klient očekává datové spojení – v tomto případě jde o port 1547
- LIST – získání seznamu souborů

No.	Time	Source	Destination	Protocol	Info
3	3.999922	AsustekC_00:f5:7f	Broadcast	ARP	who has 10.1.36.136? tell 10.1.36.36
4	4.250153	10.1.36.38	10.1.36.36	TCP	1546 > ftp [SYN] Seq=0 Len=0 MSS=1460
5	4.250310	10.1.36.36	10.1.36.38	TCP	ftp > 1546 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
6	4.250331	10.1.36.38	10.1.36.36	TCP	1546 > ftp [ACK] Seq=1 Ack=1 Win=65535 [TCP CHECKSUM INCORRECT]
7	4.251018	10.1.36.36	10.1.36.38	FTP	Response: 220 Test
8	4.268587	10.1.36.38	10.1.36.36	FTP	Request: USER po11-6
9	4.268975	10.1.36.36	10.1.36.38	FTP	Response: 331 User name okay, need password.
10	4.284127	10.1.36.38	10.1.36.36	FTP	Request: PASS po11-6-heslo
11	4.284580	10.1.36.36	10.1.36.38	FTP	Response: 230 User logged in, proceed.
12	4.299679	10.1.36.38	10.1.36.36	FTP	Request: SYST
13	4.299977	10.1.36.36	10.1.36.38	FTP	Response: 215 UNIX Type: L8
14	4.315519	10.1.36.38	10.1.36.36	FTP	Request: FEAT
15	4.316074	10.1.36.36	10.1.36.38	FTP	Response: 211-Extensions supported:
16	4.362101	10.1.36.38	10.1.36.36	FTP	Request: PWD
17	4.362409	10.1.36.36	10.1.36.38	FTP	Response: 257 "/" is working directory.
18	4.409342	10.1.36.38	10.1.36.36	FTP	Request: TYPE A
19	4.409695	10.1.36.36	10.1.36.38	FTP	Response: 200 Type set to A.
20	4.426994	10.1.36.38	10.1.36.36	FTP	Request: PORT 10,1,36,38,6,11
21	4.427532	10.1.36.36	10.1.36.38	FTP	Response: 200 PORT Command successful.
22	4.440454	10.1.36.38	10.1.36.36	FTP	Request: LIST -IT
23	4.441154	10.1.36.36	10.1.36.38	FTP	Response: 125 Opening ASCII mode data connection for /bin/ls.
24	4.441386	10.1.36.36	10.1.36.38	TCP	2134 > 1547 [SYN] Seq=0 Len=0 MSS=1460
25	4.441431	10.1.36.38	10.1.36.36	TCP	1547 > 2134 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460

  

Frame 20 (76 bytes on wire, 76 bytes captured)	
Ethernet II, Src: AsustekC_00:f4:c1 (00:13:d4:00:f4:c1), Dst: AsustekC_00:f5:7f (00:13:d4:00:f5:7f)	
Internet Protocol, Src: 10.1.36.38 (10.1.36.38), Dst: 10.1.36.36 (10.1.36.36)	
Transmission Control Protocol, Src Port: 1546 (1546), Dst Port: ftp (21), Seq: 58, Ack: 644, Len: 22	
File Transfer Protocol (FTP)	
PORT 10,1,36,38,6,11\r\n	
Request command: PORT	
Request arg: 10,1,36,38,6,11	
Active IP address: 10.1.36.38 (10.1.36.38)	
Active port: 1547	

  

0000	00 13 d4 00 f5 7f 00 13 d4 00 f4 c1 08 00 45 00	.....E.
0010	00 3e 44 f6 40 00 80 06 59 78 0a 01 24 26 0a 01	.>D.@...Yx..\$&..
0020	24 24 06 0a 00 15 8b 0b 9d 33 9e ff a0 f6 50 18	\$\$.....3....P.
0030	fd 7c 5c 7c 00 00 50 4f 52 54 20 31 30 2c 31 2c	. N ..PORT 10,1,
0040	33 36 2c 33 38 2c 36 2c 31 31 0d 0a	36,38,6,11..

Obr. 6 Inicializace spojení klient-server při využití protokolu FTP

- RETR – příkaz užitý k přenosu souboru ze serveru. Ilustruje ho Obr. 7.

45	14.673616	AsustekC_00:f4:c1	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.38
46	15.530707	10.1.36.36	10.1.255.255	NBNS	Name query NB U44.ESET.COM<00>
47	15.924514	10.1.36.38	10.1.36.36	FTP	Request: TYPE I
48	15.924936	10.1.36.36	10.1.36.38	FTP	Response: 200 Type set to I.
49	15.941055	10.1.36.38	10.1.36.36	FTP	Request: PORT 10,1,36,38,6,13
50	15.941578	10.1.36.36	10.1.36.38	FTP	Response: 200 PORT Command successful.
51	15.955700	10.1.36.38	10.1.36.36	FTP	Request: RETR test.abc
52	15.956342	10.1.36.36	10.1.36.38	FTP	Response: 150 File status okay; about to open data connection.
53	15.956578	10.1.36.36	10.1.36.38	TCP	2135 > 1549 [SYN] Seq=0 Len=0 MSS=1460
54	15.956621	10.1.36.38	10.1.36.36	TCP	1549 > 2135 [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0 MSS=1460
55	15.956724	10.1.36.36	10.1.36.38	TCP	2135 > 1549 [ACK] Seq=1 Ack=1 win=65535 Len=0
56	15.956860	10.1.36.36	10.1.36.38	TCP	2135 > 1549 [PSH, ACK] Seq=1 Ack=1 win=65535 Len=9
57	15.956949	10.1.36.36	10.1.36.38	TCP	2135 > 1549 [FIN, ACK] Seq=10 Ack=1 win=65535 Len=0
58	15.956966	10.1.36.38	10.1.36.36	TCP	1549 > 2135 [ACK] Seq=1 Ack=11 win=65526 [TCP CHECKSUM INCORRECT]
59	15.958888	10.1.36.38	10.1.36.36	TCP	1549 > 2135 [FIN, ACK] Seq=1 Ack=11 win=65526 [TCP CHECKSUM INCORRECT]
60	15.958992	10.1.36.36	10.1.36.38	TCP	2135 > 1549 [ACK] Seq=11 Ack=2 win=65535 Len=0
61	16.095429	10.1.36.38	10.1.36.36	TCP	1546 > ftp [ACK] Seq=135 Ack=861 win=64675 [TCP CHECKSUM INCORRECT]
62	16.095566	10.1.36.36	10.1.36.38	FTP	Response: 226 Closing data connection.

  

Frame 51 (69 bytes on wire, 69 bytes captured)

- Ethernet II, Src: AsustekC\_00:f4:c1 (00:13:d4:00:f4:c1), Dst: AsustekC\_00:f5:7f (00:13:d4:00:f5:7f)
- Internet Protocol, Src: 10.1.36.38 (10.1.36.38), Dst: 10.1.36.36 (10.1.36.36)
- Transmission Control Protocol, Src Port: 1546 (1546), Dst Port: ftp (21), Seq: 120, Ack: 807, Len: 15
- File Transfer Protocol (FTP)
  - RETR test.abc\r\n
    - Request command: RETR
    - Request arg: test.abc

  

0000	00 13 d4 00 f5 7f 00 13 d4 00 f4 c1 08 00 45 00	.....E.
0010	00 37 45 1a 40 00 80 06 59 5b 0a 01 24 26 0a 01	.7E.@...Y[..\$&..
0020	24 24 06 0a 00 15 8b 0b 9d 71 9e ff a1 99 50 18	\$\$.....q....P.
0030	fc d9 5c 75 00 00 52 45 54 52 20 74 65 73 74 2e	..\.u..RE TR test.
0040	61 62 63 0d 0a	abc..

Obr. 7 Přenos souboru test.abc z FTP serveru

Pokud se má vytvořit spojení protokolem FTP na základě **pasivního** režimu, tak ho vytváří klient na port, který mu přidělí server a kde mu také následně budou poskytnuta data. Místo příkazu PORT je užito PASV. PASV znamená žádost serveru o pasivní režim. Tuto situaci ukazuje Obr. 8 s tím, že je vidět připojení klienta na port 1024.



No.	Time	Source	Destination	Protocol	Info
96	49.457228	10.1.36.36	10.1.36.38	TCP	ftp > 1553 [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0 MSS=1460
97	49.457249	10.1.36.38	10.1.36.36	TCP	1553 > ftp [ACK] Seq=1 Ack=1 win=65535 [TCP CHECKSUM INCORRE
98	49.457954	10.1.36.36	10.1.36.38	FTP	Response: 220 Test
99	49.470425	10.1.36.38	10.1.36.36	FTP	Request: USER poll-6
100	49.470816	10.1.36.36	10.1.36.38	FTP	Response: 331 User name okay, need password.
101	49.485996	10.1.36.38	10.1.36.36	FTP	Request: PASS poll-6-heslo
102	49.486471	10.1.36.36	10.1.36.38	FTP	Response: 230 User logged in, proceed.
103	49.501944	10.1.36.38	10.1.36.36	FTP	Request: SYST
104	49.502231	10.1.36.36	10.1.36.38	FTP	Response: 215 UNIX Type: L8
105	49.517189	10.1.36.38	10.1.36.36	FTP	Request: FEAT
106	49.517741	10.1.36.36	10.1.36.38	FTP	Response: 211-Extensions supported:
107	49.563929	10.1.36.38	10.1.36.36	FTP	Request: PWD
108	49.564240	10.1.36.36	10.1.36.38	FTP	Response: 257 "/" is working directory.
109	49.611264	10.1.36.38	10.1.36.36	FTP	Request: TYPE A
110	49.611581	10.1.36.36	10.1.36.38	FTP	Response: 200 Type set to A.
111	49.626625	10.1.36.38	10.1.36.36	FTP	Request: PASV
112	49.628640	10.1.36.36	10.1.36.38	FTP	Response: 227 Entering Passive Mode (10,1,36,36,4,0).
113	49.629882	10.1.36.38	10.1.36.36	TCP	1554 > 1024 [SYN] Seq=0 Len=0 MSS=1460
114	49.630021	10.1.36.36	10.1.36.38	TCP	1024 > 1554 [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0 MSS=1460
115	49.630040	10.1.36.38	10.1.36.36	TCP	1554 > 1024 [ACK] Seq=1 Ack=1 win=65535 [TCP CHECKSUM INCORRE
116	49.642388	10.1.36.38	10.1.36.36	FTP	Request: LIST -lT
117	49.643145	10.1.36.36	10.1.36.38	FTP	Response: 125 Opening ASCII mode data connection for /bin/l
118	49.643372	10.1.36.36	10.1.36.38	FTP-DATA	FTP Data: 9 bytes
119	49.654836	10.1.36.36	10.1.36.38	FTP-DATA	FTP Data: 73 bytes
120	49.654871	10.1.36.38	10.1.36.36	TCP	1554 > 1024 [ACK] Seq=1 Ack=84 win=65453 [TCP CHECKSUM INCOR
121	49.654964	10.1.36.38	10.1.36.36	TCP	1554 > 1024 [FIN, ACK] Seq=1 Ack=84 win=65453 [TCP CHECKSUM ]
122	49.655063	10.1.36.36	10.1.36.38	TCP	1024 > 1554 [ACK] Seq=84 Ack=2 win=65535 Len=0
123	49.783269	10.1.36.38	10.1.36.36	TCP	1553 > ftp [ACK] Seq=74 Ack=742 win=64794 [TCP CHECKSUM INCO
124	49.783396	10.1.36.36	10.1.36.38	FTP	Response: 226 Closing data connection.
125	50.000691	10.1.36.38	10.1.36.36	TCP	1553 > ftp [ACK] Seq=74 Ack=772 win=64764 [TCP CHECKSUM INCO
126	50.453813	AsustekC_00:f4:c1	Broadcast	ARP	who has 10.1.36.136? Tell 10.1.36.38
127	51.985010	10.1.36.38	10.1.255.255	NBNS	Name query NB U35.ESET.COM<00>
128	52.734984	10.1.36.38	10.1.255.255	NBNS	Name query NB U35.ESET.COM<00>

  

Frame 112 (99 bytes on wire, 99 bytes captured)

- ⊕ Ethernet II, Src: AsustekC\_00:f5:7f (00:13:d4:00:f5:7f), Dst: AsustekC\_00:f4:c1 (00:13:d4:00:f4:c1)
- ⊕ Internet Protocol, Src: 10.1.36.36 (10.1.36.36), Dst: 10.1.36.38 (10.1.36.38)
- ⊕ Transmission Control Protocol, Src Port: ftp (21), Dst Port: 1553 (1553), Seq: 644, Ack: 64, Len: 45
- ⊖ File Transfer Protocol (FTP)
  - ⊖ 227 Entering Passive Mode (10,1,36,36,4,0).\r\n
    - Response code: Entering Passive Mode (227)
    - Response arg: Entering Passive Mode (10,1,36,36,4,0).
    - Passive IP address: 10.1.36.36 (10.1.36.36)
    - Passive port: 1024

  

0000	00 13 d4 00 f4 c1 00 13 d4 00 f5 7f 08 00 45 00	.....E.
0010	00 55 b1 e7 40 00 80 06 ec 6f 0a 01 24 24 0a 01	.U..@...o..\$\$..
0020	24 26 00 15 06 11 fb 38 10 2f f7 a5 1c 56 50 18	\$&.....8 ./...VP.
0030	ff c0 0e 2c 00 00 32 32 37 20 45 6e 74 65 72 69	.....22 7 Enteri
0040	6e 67 20 50 61 73 73 69 76 65 20 4d 6f 64 65 20	ng Passi ve Mode
0050	28 31 30 2c 31 2c 33 36 2c 33 36 2c 34 2c 30 29	(10,1,36 ,36,4,0)
0060	2e 0d 0a	...

Obr. 8 FTP pasivní mód provozu - navázání

### 6. Jak u protokolu POP3 pozná klient, že server pochopil a zpracoval jeho příkaz?

Každá odpověď od serveru musí začínat potvrzením, že příkaz byl zpracován a to sice tak, že indikuje stav operace +OK. Ukazuje to

No. -	Time	Source	Destination	Protocol	Info
47	29.999362	Cisco_93:43:c2	Cisco_93:43:c2	LOOP	Reply
48	30.093340	10.20.1.222	10.20.1.59	TCP	pop3 > 1581 [ACK] Seq=108 Ack=19 win
49	30.953920	10.20.1.59	10.20.1.222	POP	Request: -
50	31.094976	10.20.1.222	10.20.1.59	TCP	pop3 > 1581 [ACK] Seq=108 Ack=20 win
51	31.360670	10.20.1.59	10.20.1.222	POP	Request: 2
52	31.495521	10.20.1.222	10.20.1.59	TCP	pop3 > 1581 [ACK] Seq=108 Ack=21 win
53	34.161529	10.20.1.59	10.20.1.222	POP	Request:
54	34.163484	10.20.1.222	10.20.1.59	POP	Response: +OK 6 messages (1087 octet
55	34.277614	10.20.1.59	10.20.1.222	TCP	1581 > pop3 [ACK] Seq=23 Ack=138 win
56	37.459174	10.20.1.59	10.20.1.222	POP	Request: L
57	37.604662	10.20.1.222	10.20.1.59	TCP	pop3 > 1581 [ACK] Seq=138 Ack=24 win
58	37.701072	10.20.1.59	10.20.1.222	POP	Request: I
59	37.804929	10.20.1.222	10.20.1.59	TCP	pop3 > 1581 [ACK] Seq=138 Ack=25 win
60	37.910129	10.20.1.59	10.20.1.222	POP	Request: S
61	38.105438	10.20.1.222	10.20.1.59	TCP	pop3 > 1581 [ACK] Seq=138 Ack=26 win
62	38.246565	10.20.1.59	10.20.1.222	POP	Request: T
63	38.415002	10.20.1.222	10.20.1.59	TCP	pop3 > 1581 [ACK] Seq=138 Ack=27 win
64	38.990005	10.20.1.59	10.20.1.222	POP	Request:
65	38.991216	10.20.1.222	10.20.1.59	POP	Response: +OK scan listing follows
66	39.199352	10.20.1.59	10.20.1.222	TCP	1581 > pop3 [ACK] Seq=29 Ack=164 win
67	39.199983	10.20.1.222	10.20.1.59	POP	Continuation
68	39.418080	10.20.1.59	10.20.1.222	TCP	1581 > pop3 [ACK] Seq=29 Ack=209 win
69	39.999180	Cisco_93:43:c2	Cisco_93:43:c2	LOOP	Reply
70	43.816627	10.20.1.59	10.20.1.222	POP	Request: R
71	44.014328	10.20.1.222	10.20.1.59	TCP	pop3 > 1581 [ACK] Seq=209 Ack=30 win
72	44.025571	10.20.1.59	10.20.1.222	POP	Request: E
73	44.215248	10.20.1.222	10.20.1.59	TCP	pop3 > 1581 [ACK] Seq=209 Ack=31 win
74	44.631170	10.20.1.59	10.20.1.222	POP	Request: T
75	44.815495	10.20.1.222	10.20.1.59	TCP	pop3 > 1581 [ACK] Seq=209 Ack=32 win
76	44.840119	10.20.1.59	10.20.1.222	POP	Request: R
77	45.015818	10.20.1.222	10.20.1.59	TCP	pop3 > 1581 [ACK] Seq=209 Ack=33 win
78	49.135102	10.20.1.59	10.20.1.222	POP	Request:
79	49.322329	10.20.1.222	10.20.1.59	TCP	pop3 > 1581 [ACK] Seq=209 Ack=34 win
80	49.624346	10.20.1.59	10.20.1.222	POP	Request: 1
81	49.823011	10.20.1.222	10.20.1.59	TCP	pop3 > 1581 [ACK] Seq=209 Ack=35 win
82	49.998987	Cisco_93:43:c2	Cisco_93:43:c2	LOOP	Reply
83	51.129133	10.20.1.59	10.20.1.222	POP	Request:
84	51.130621	10.20.1.222	10.20.1.59	POP	Response: +OK message 1 (193 octets)
85	51.238628	10.20.1.59	10.20.1.222	TCP	1581 > pop3 [ACK] Seq=27 Ack=227 win

  

Ethernet II, Src: CnetTech_6c:47:f1 (00:08:a1:6c:47:f1), Dst: AsustekC_00:f4:c1 (00:13:d4:c	
Internet Protocol, Src: 10.20.1.222 (10.20.1.222), Dst: 10.20.1.59 (10.20.1.59)	
Transmission Control Protocol, Src Port: pop3 (110), Dst Port: 1581 (1581), Seq: 138, Ack:	
Post Office Protocol	
+OK scan listing follows\r\n	
Response indicator: +OK	
Response description: scan listing follows	

  

```

0000 00 13 d4 00 f4 c1 00 08 a1 6c 47 f1 08 00 45 00  ....G...E.
0010 00 42 f2 e5 00 00 80 06 30 90 0a 14 01 de 0a 14  .B.....0.....
0020 01 3b 00 6e 06 2d a6 6d 75 5b f9 be e9 a1 50 18  .;.n.-.m u[....P.
0030 ff e3 5a 18 00 00 2b 4f 4b 20 73 63 61 6e 20 6c  ..Z...+OK scan l
0040 69 73 74 69 6e 67 20 66 6f 6c 6c 6f 77 73 0d 0a  isting follows..

```

Obr. 9 POP3 potvrzování +OK

### 7. K čemu slouží zpráva HELO u protokolu SMTP a jak na ní server reaguje?

Klient je touto zprávou identifikován. Je to vlastně zahájení konverzace. Pokud klient zadá správné přihlašovací údaje, je mu potvrzeno jako „250 OK“. Pak je možno odesílat e-maily.

### 3. ZÁVĚR

Vyzkoušení několika aplikačních protokolů a jejich analýza byly vcelku názorné. Osobní přínos bych viděl v pochopení rozdílu mezi aktivním a pasivním režimem např. při používání Total Commanderu k připojení pomocí FTP protokolu na server. V některých případech totiž není aktivní propojení, které bývá v Total Commanderu defaultně nastaveno, možno uskutečnit, a tak komunikace uvázne na mrtvém bodě a spojení není navázáno. Je tedy nutné mód provozu změnit a napodobit tak funkci webového prohlížeče, který také pracuje v pasivním módu.

Ověřili jsme také některé teoretické předpoklady např. z přednášek – funkce DHCP serveru při přidělování adresy apod.

Všechny ostatní komentáře k úloze jsou již uvedeny výše v rozboru změřených výstupů.