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.

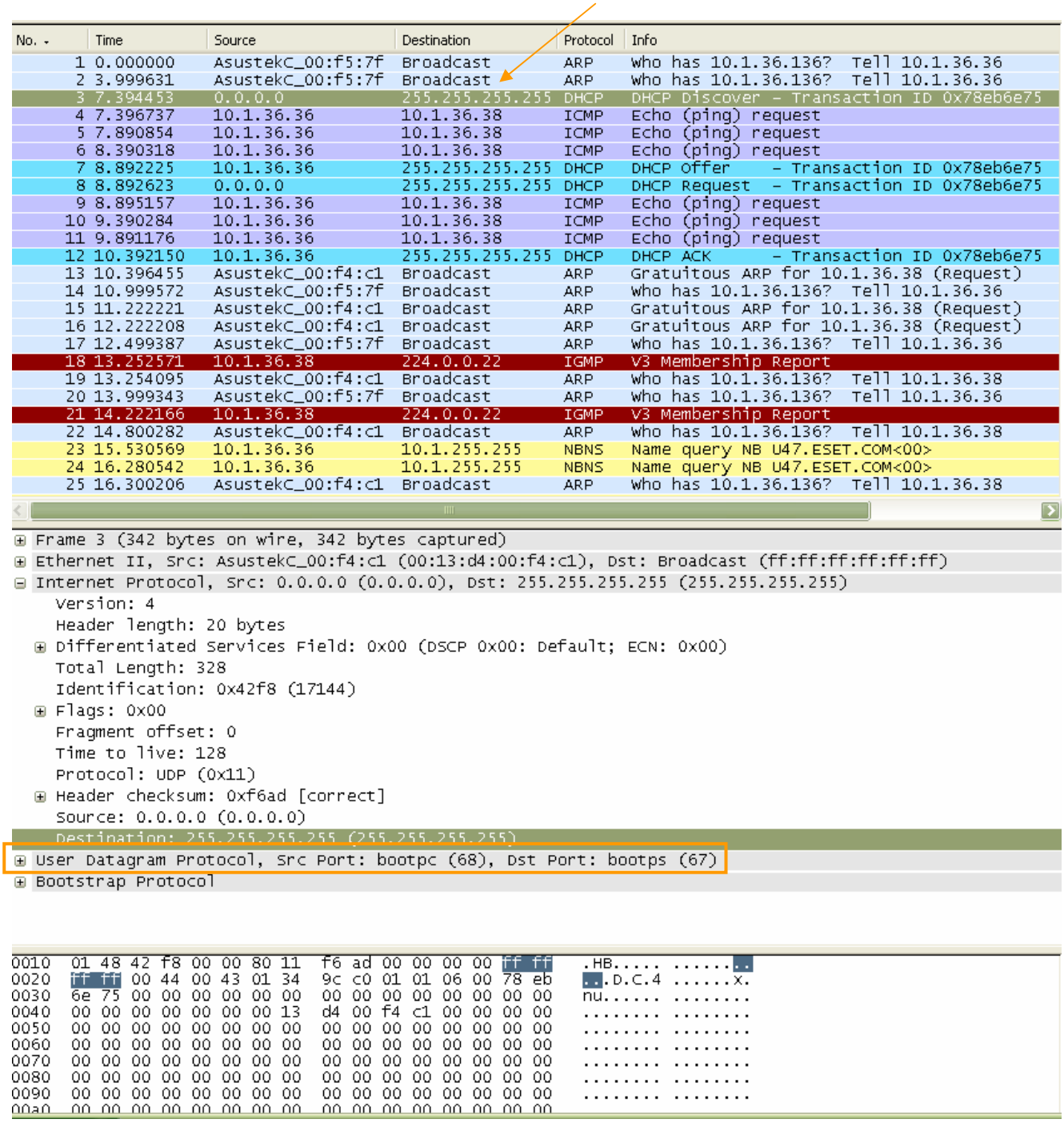
Odpovědi pramení většinou z webové encyklopedie Wikipedia a také z knihy „Data Communications, Computer Networks and Open Systems“.

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

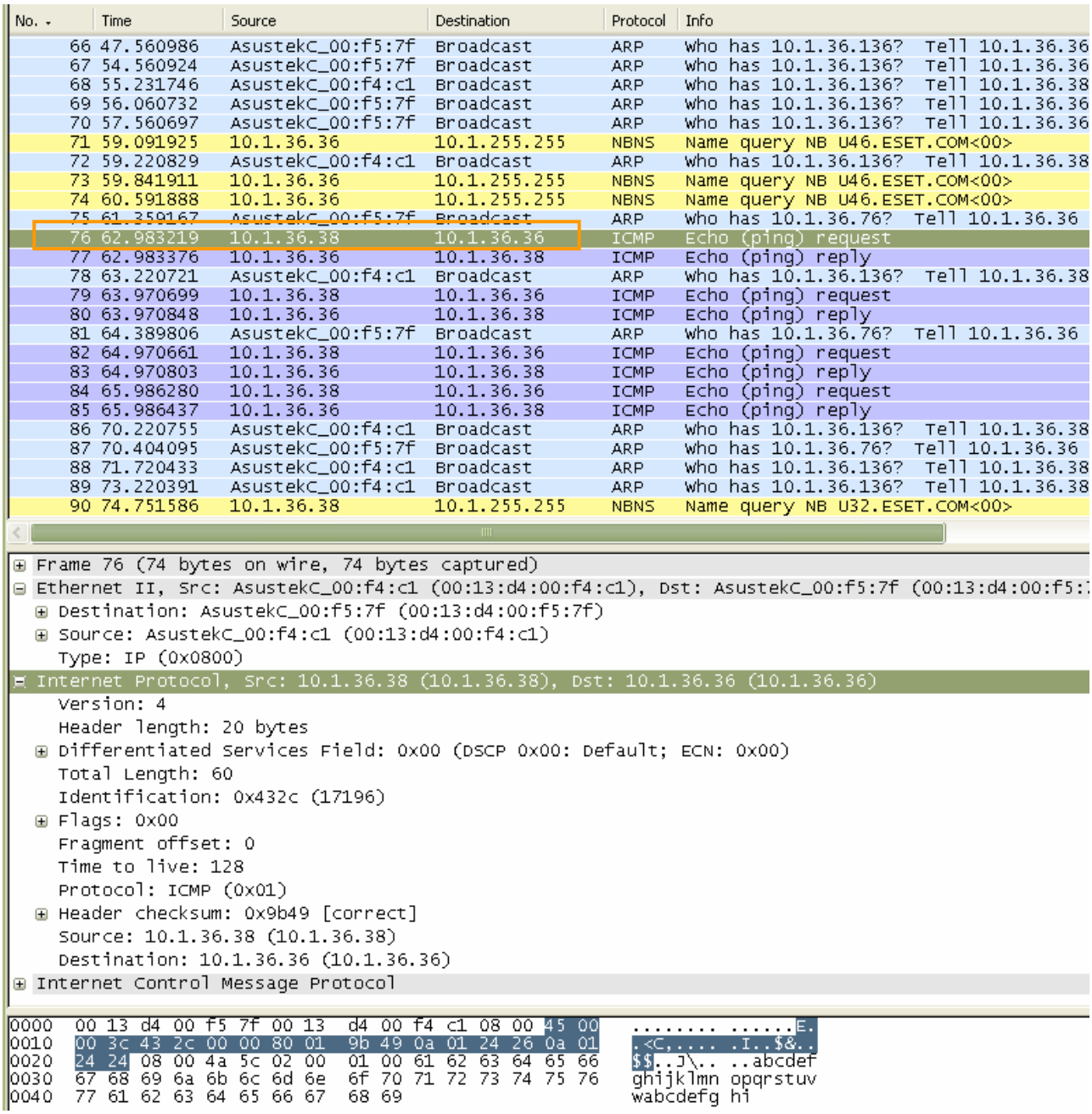
V programu HomeFTPserver byl vytvořen účet:

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



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.



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?*

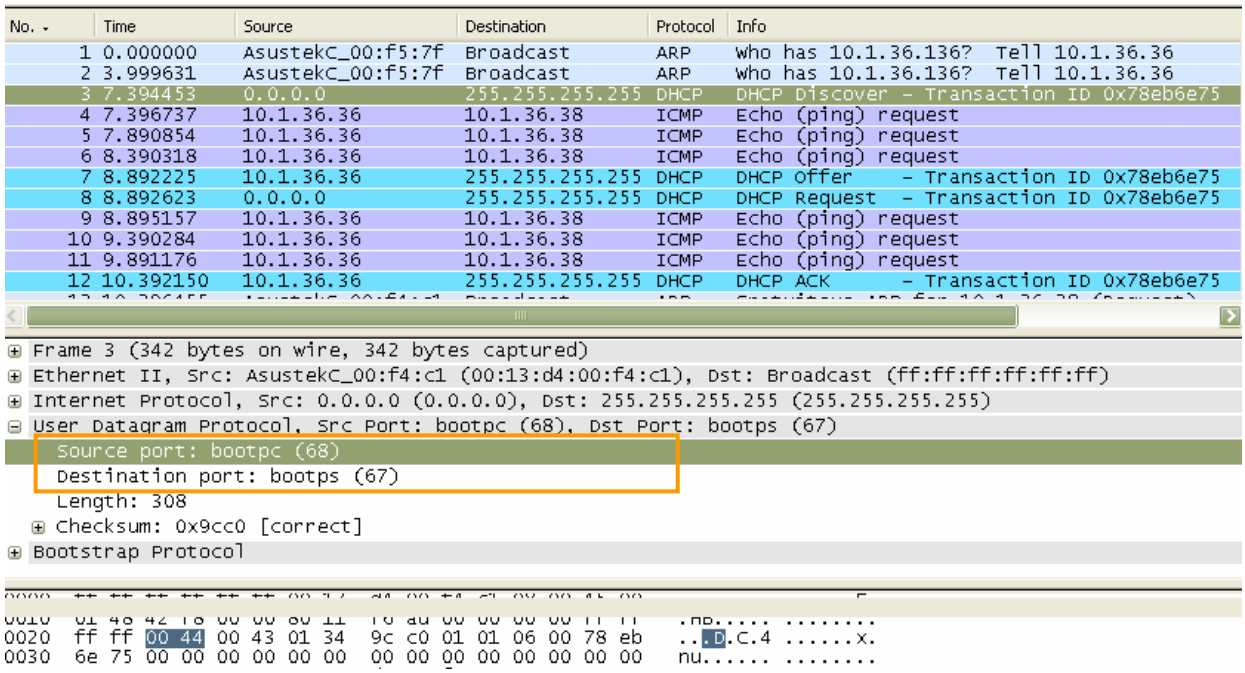
Jedná se o jakýsi bezpečnostní mechanismus pro ochranu před kolizemi. Mohlo by se totiž stát, že daná adresa již byla přidělena například při manuálním nastavování adres někde jinde v dané síti.

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.

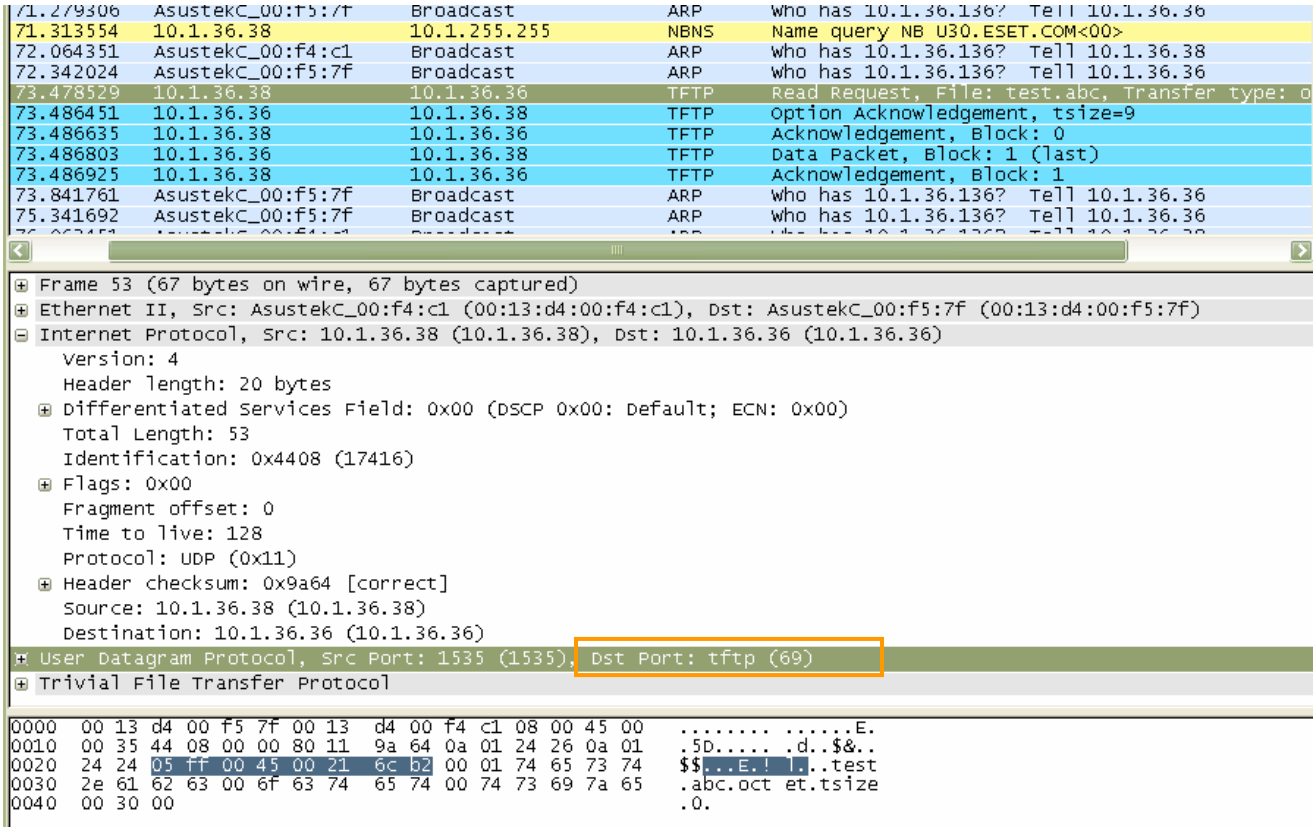
4. Na jakých portech probíhá komunikace protokolů DHCP a TFPT (klient i server)

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 odesílané serverem mají zdrojový port 67 a cílový 68.

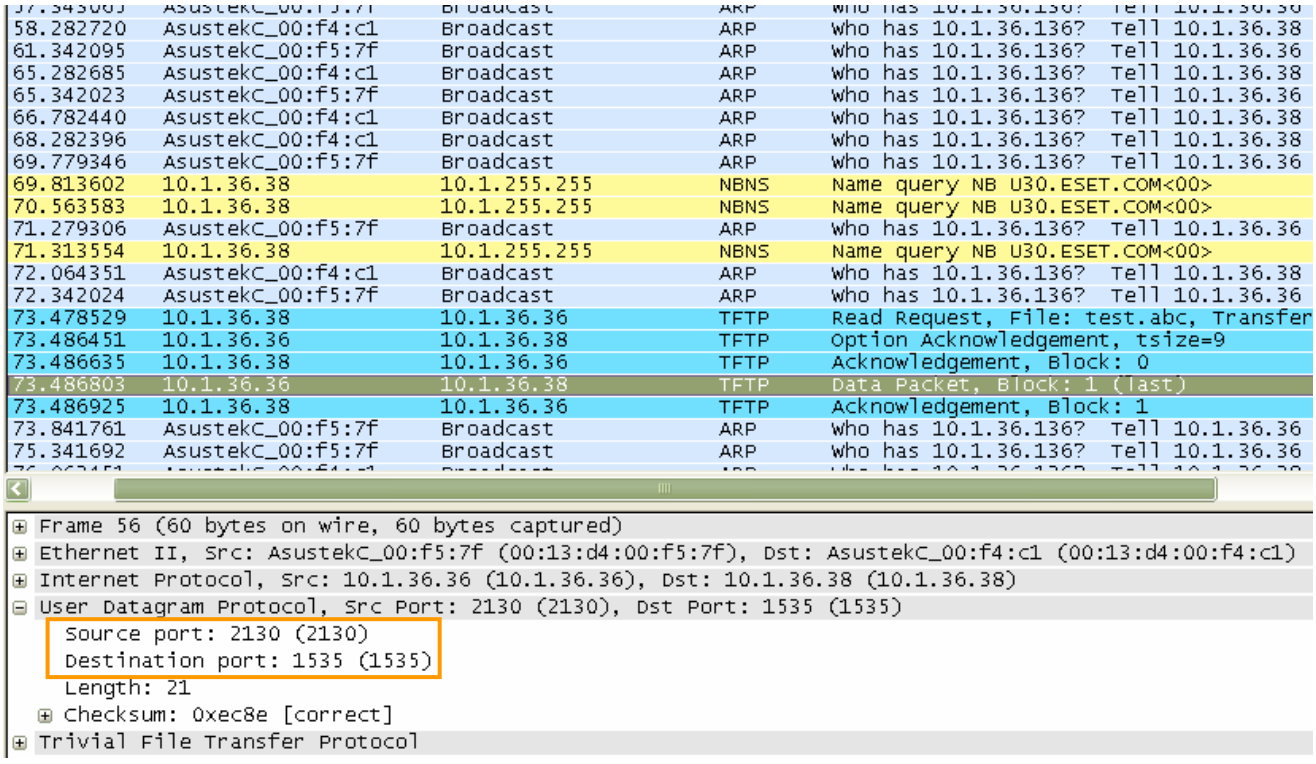


Obr. 3 Komunikace protokolu DHCP – porty 67 a 68

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.



Obr. 4 Komunikace protokolu TFTP – port 69

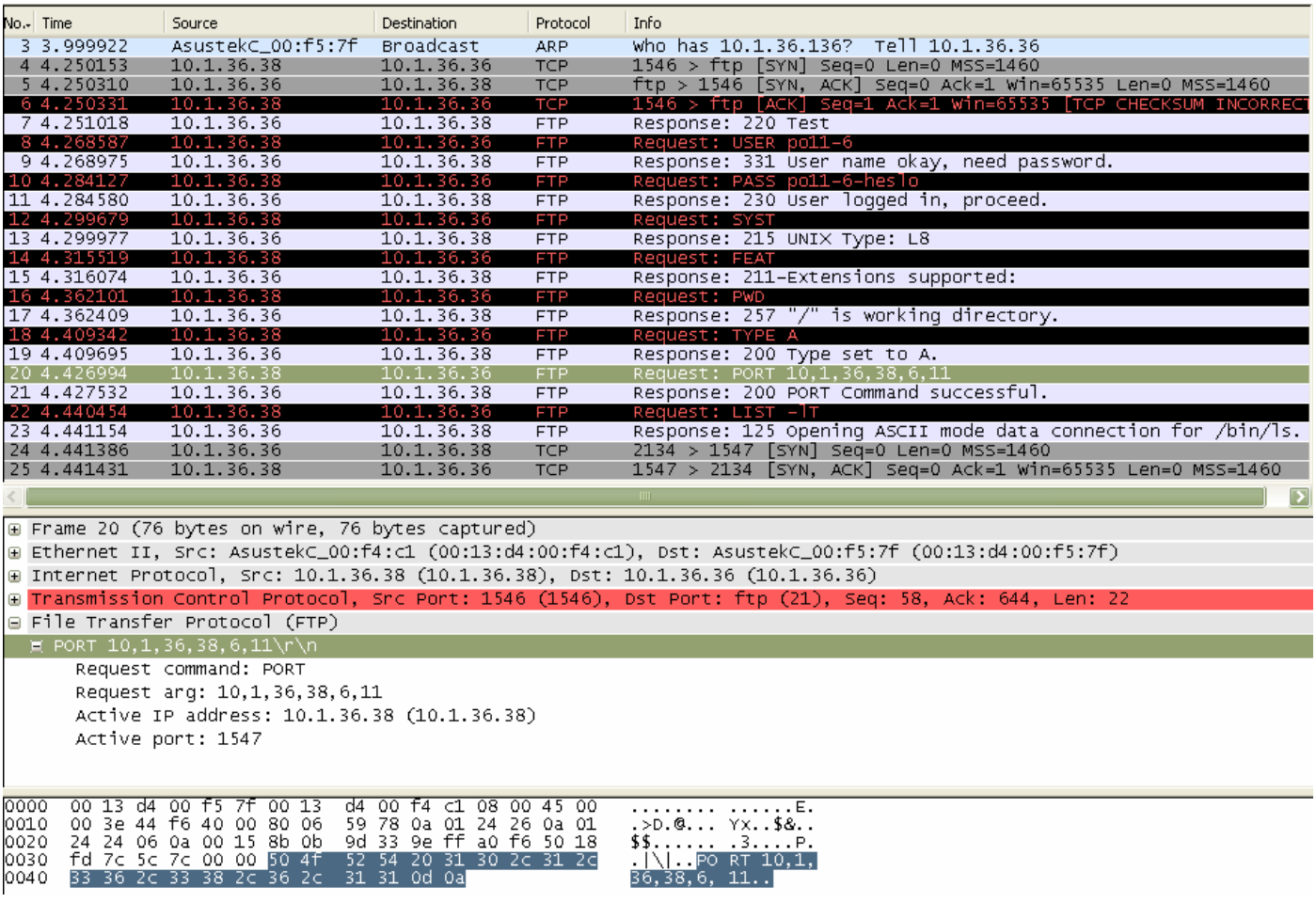


Obr. 5 Ukázka TID

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.*

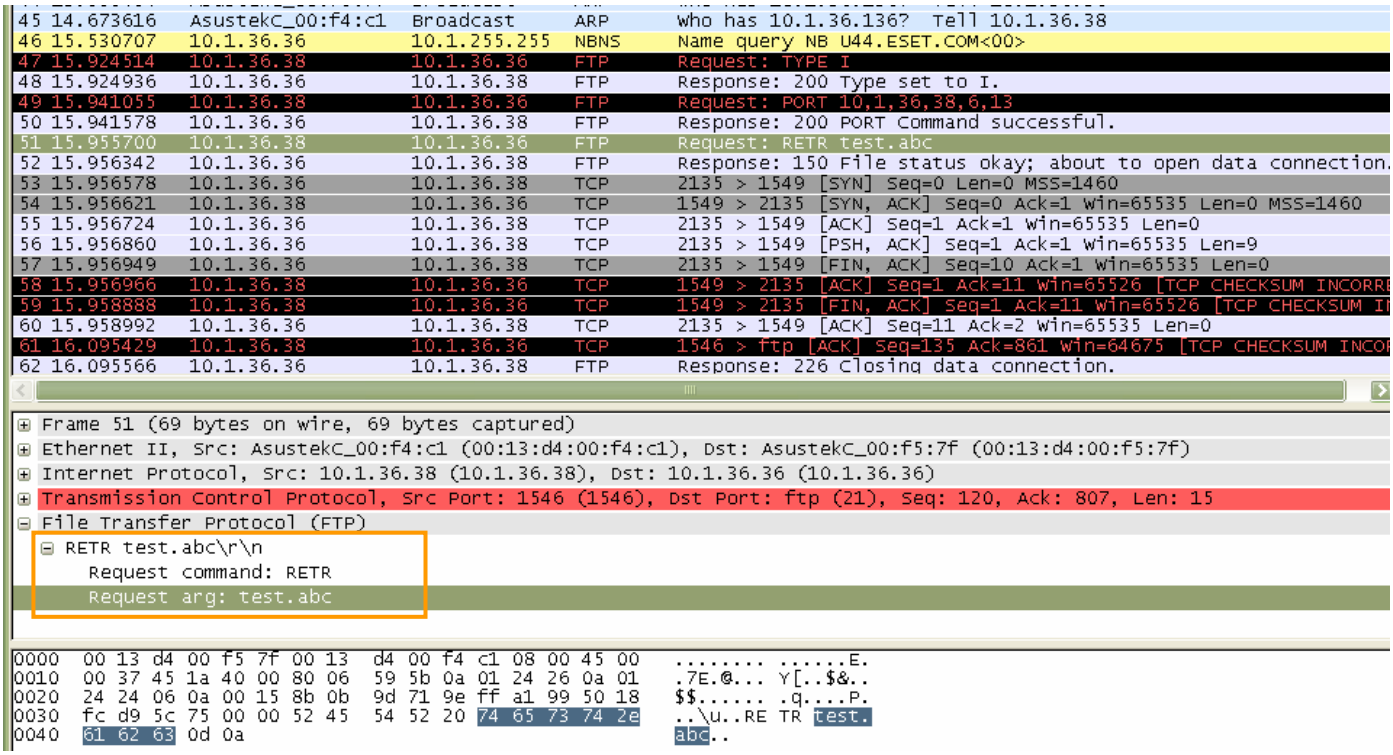
Postup při navazování komunikace mezi serverem a klientem v aktivním režimu ukazuje Obr. 6. FTP server pošle data na port a adresu zadanou klientem. Spojení je navázáno tak, že na portu 21 je server a na 1546 je klient. Dále se přenesou následující zprávy:

- 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



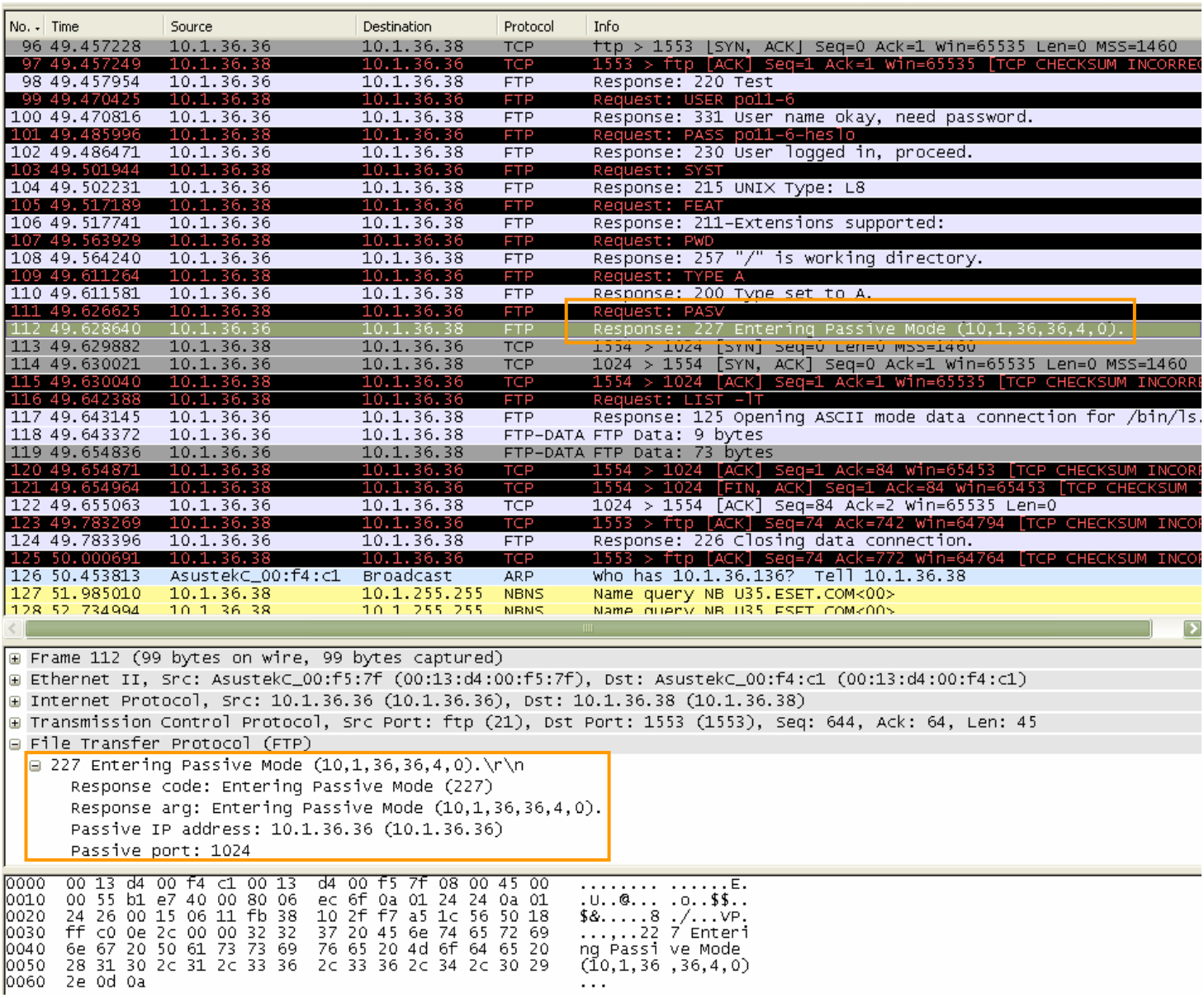
Obr. 6 Inicializace spojení klient-server při využití protokolu FTP

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



Obr. 7 Přenos souboru test.abc z FTP serveru

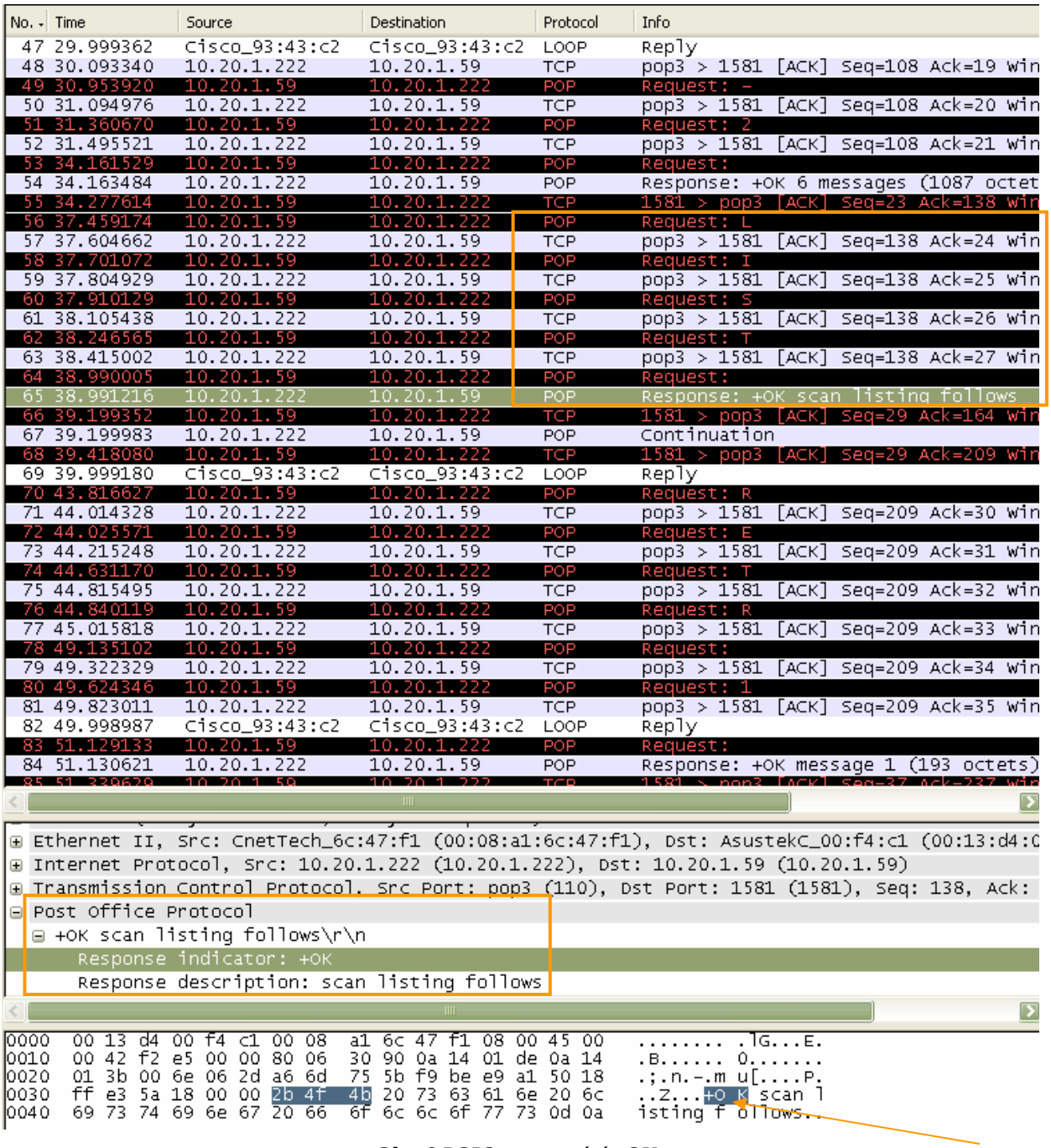
Pokud se má vytvořit spojení protokolem FTP na základě **pasivního** režimu, tak ho vytváří klient na port, který mu přidělí server a kde mu také následně budou poskytnuta data. Místo příkazu PORT je užito PASV. PASV znamená žádost serveru o pasivní režim. Tuto situaci ukazuje Obr. 8 s tím, že je vidět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



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



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.