Vaše jméno	Tomáš Batelka
VUT ID	243511
Vypracovaný lab (označení)	Pondeli 13-16 Caha.pcap

BPC-KOM

Projekt

Zimní semestr 2023/2024

ICMP komunikace (pakety 1-8)

No.	Time	Source	Destination	Protocol	Length	TTL	Info
1	0.000000	100.64.130.233	217.31.205.50	ICMP	142	3	Echo (ping) request id=0x0001, seq=16/4096, ttl=3 (no response found!)
2	0.002852	147.229.253.233	100.64.130.233	ICMP	170	62,1	Time-to-live exceeded (Time to live exceeded in transit)
3	1.007574	100.64.130.233	217.31.205.50	ICMP	142	3	Echo (ping) request id=0x0001, seq=17/4352, ttl=3 (no response found!)
4	1.012131	147.229.253.233	100.64.130.233	ICMP	170	62,1	Time-to-live exceeded (Time to live exceeded in transit)
5	2.020500	100.64.130.233	217.31.205.50	ICMP	142	3	Echo (ping) request id=0x0001, seq=18/4608, ttl=3 (no response found!)
6	2.024827	147.229.253.233	100.64.130.233	ICMP	170	62,1	Time-to-live exceeded (Time to live exceeded in transit)
7	3.041087	100.64.130.233	217.31.205.50	ICMP	142	3	Echo (ping) request id=0x0001, seq=19/4864, ttl=3 (no response found!)
8	3.045496	147.229.253.233	100.64.130.233	ICMP	170	62,1	Time-to-live exceeded (Time to live exceeded in transit)

Obrázek 1: ICMP komunikace

Pakety 1 až 8 obsahují komunikaci pomocí ICMP. ICMP protokol rodiny TCP/IP je protokol pracující na síťové vrstvě a slouží k odesílání chybových zpráv a služebních informací indikujících úspěch nebo chybu. Nejčastěji je však používán příkazem `ping`, jež byl použit v této analyzované komunikaci, a příkazem `tracert`/`traceroute`. Tato komunikace má původ ve fyzickém zařízení (usuzuji tak na základě MAC adresy klienta).

Protokol aplikační vrstvy

Žádný

Protokol transportní vrstvy a adresy komunikujících stran

Žádný

Protokol síťové vrstvy a adresy komunikujících stran

ICMP IP adresa klienta: 100.64.130.233

IP adresa odpovědi (pravděpodobně směrovače vzdáleného 3 skoky): 147.229.253.233

IP adresa cíle: 217.31.205.50

Popis průběhu komunikace

Během této komunikace dochází ke komunikaci během které ICPM echo request nestihne dosáhnout cílové adresy dříve než hodnota TTL dosáhne nuly. Proto odpovídá třetí účastník komunikace – směrovač, který posílá zprávu o překročení limitu TTL (příznak type s hodnotou 11 – Time Exceeded) a paket zahodí. To, že byl paket odeslán 4x, což je jedna z indícií (i když nesměrodatná), že klientský operační systém je Widnows. Příkaz ping v operačním systému odešle ve výchozí konfiguraci právě 4 pakety, zatímco v GNU/Linux odesílá požadavky až do terminace příkazu. Také si myslím, že k této komunikaci došlo provedením příkazu `ping 217.31.205.50 -l 142 -i 3`, kde parametr `-l` nastavuje délku a `-i` nastavuje hodnotu TTL.

Zabezpečení přenášených dat proti modifikaci a odposlechu při přenosu

Data nejsou šifrována, protože ani nemusí – nepřenášejí žádné citlivé informace. Obsahují totiž jen výplň, aby byla velikost rámce 142 bajtů. Přenášená data lze modifikovat.

Obsah případné datové části

Datová část je vyplněna opakováním řetězce `a-z` dokud není rámec dlouhý dle zadané délky.

DNS komunikace (pakety 9-12)

No.	Time	Source	Destination	Protocol	Length	TTL	Info
9	0.000000	147.229.208.38	1.1.1.1	DNS	69	128	Standard query 0x000f AAAA cesnet.cz
10	0.006514	1.1.1.1	147.229.208.38	DNS	97	58	Standard query response 0x000f AAAA cesnet.cz AAAA 2001:718:1:1f:50:56ff:feee:46
11	1.(182417…	147.229.208.38	1.1.1.1	DNS	69	128	Standard query 0x0010 AAAA cesnet.cz
12	2.829029	1.1.1.1	147.229.208.38	DNS	140	58	Standard query response 0x0010 AAAA cesnet.cz AAAA 2001:718:1:1f:50:56ff:feee:46

Obrázek 2: DNS komunikace

Pakety 9 až 12 obsahují dva dotazy a dvě odpovědi pro překlad doménového jména. Protože po nich následují další DNS dotazy s jiným doménovým jménem usuzuji, že se jednalo o dotaz vytvořený nějakým nástrojem. Nejprve mě napadlo, že by se mohlo jednat o příkaz `nslookup -type=AAAA cesnet.cz 1.1.1.1`. Tento příkaz ale posílá navíc dotaz na PTR záznam pro zjištění doménového jména dotazovaného serveru.

Protokol aplikační vrstvy

DNS

Protokol transportní vrstvy a adresy komunikujících stran

UDP Port klienta: 63236

Port serveru: 53

Protokol síťové vrstvy a adresy komunikujících stran

IPv4 IP adresa klienta: 147.229.253.233

IP adresa serveru: 1.1.1.1 (Cloudflare)

Popis průběhu komunikace

Nejprve je odeslán požadavek na překlad doménového jména *cesnet.cz* na DNS server 1.1.1.1 (Cloudflare), který odpovídá odpovědí nesoucí DNS záznam typu AAAA (IPv6). 11. paket nese stejný dotaz ovšem odpověď je delší. To je způsobeno tím, že rámec nenese pouze odpověď jako u předchozí odpovědi, ale i trailer a FCS (Frame check sequence).

Zabezpečení přenášených dat proti modifikaci a odposlechu při přenosu

Přenášená data jsou nešifrovaná. Pro poskytnutí šifrování obsahu lze použít protokol DoH (DNS-over-HTTPS) nebo DoT (DNS-over-TLS). Prenášená data by bylo možné modifikovat.

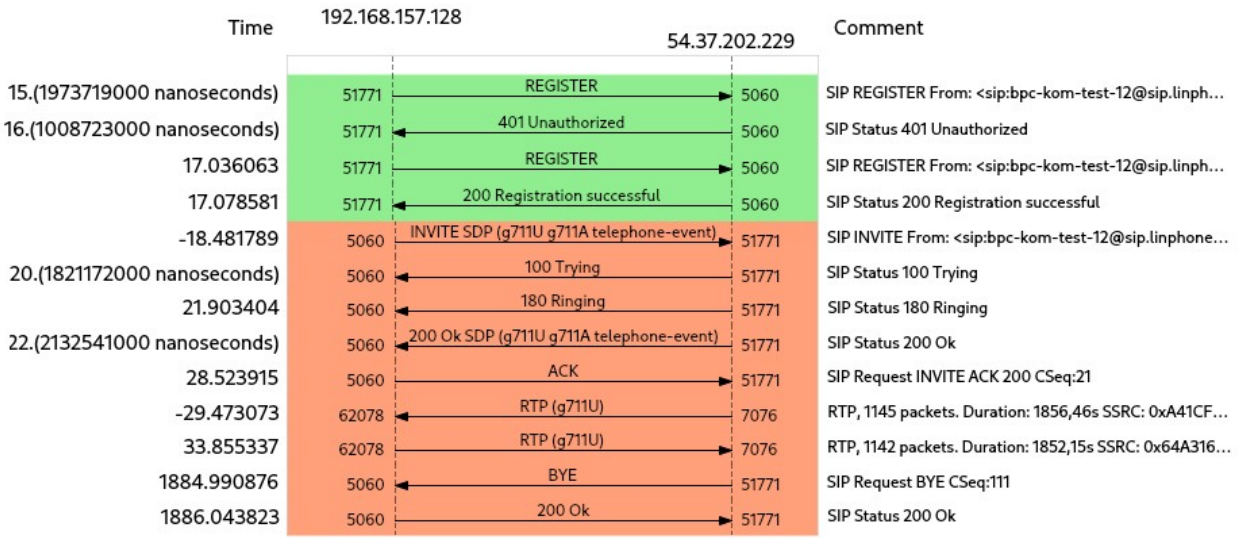
Obsah případné datové části

Obsahem datové části DNS dotazu je doména, u kterou chceme přeložit a typ DNS záznamu, který chceme obdržet (v tomto případě AAAA – IPv6). Obsahem odpovědi je dotaz i DNS záznam typu AAAA.

Do části fragmentu náležící traileru a FCS odpovědi na paket č. 11 a FCS byla uměle vložena zpráva (< *USE google maps* > *50 5‘13“N 14 25‘14“E*) se souřadnicemi 50°5'13"N 14°25'14"E, což jsou souřadnice Staroměstské radnice a Orloje (odkaz zde).

Internetová telefonie (pakety 13 – 2361)

Pakety č. 13 až paket č. 2361 slouží ke zprostředkování internetového hovorou. Internetový hovor je zahájen pomocí série SIP signalizací. V jedné z nich se můžeme dočíst, že klientská stanice používá operační systém Windows 10 a SIP klient Linphone (3.12.0-273-g20efb4ad4) využívající knihovnu belle-sip (1.6.3) implementující protokol SIP dle RFC3261. Operační systém klienta běží jako virtuální stroj hypervisoru VMware.



Obrázek 3: SIP flow

Protokol aplikační vrstvy

DNS, SIP, SDP, RTP, RTCP

Protokol transportní vrstvy a adresy komunikujících stran

UDP DNS – Klient: 63236, 63237, 51774, 51775, 51776, 51777, 51778, 58916 & server: 53

SIP/SDP – Klient: 51771 & server: 5060

RTP – Klient: 7076 & server: 62078

RTCP – Klient: 7077 & server: 62079

STUN – Klient: 7076, 7077 & server: 62078, 62079

Protokol síťové vrstvy a adresy komunikujících stran

IPv4 Volaný klient (monitorovaný): 192.168.157.128

SIP server (SIP proxy, REGISTRAR): 54.37.202.229 (sip6.linphone.org)

Volající klient: 192.168.1.108

Popis průběhu komunikace

DNS (pakety 13 až 24)

13	-2.003168	192.168.157.128	8.8.8.8	DNS	86	128 Standard query 0x62b8 SRV _sip._udp.sip.linphone.org
14	-3.985939	8.8.8.8	192.168.157.128	DNS	160	128 Standard query response 0x62b8 SRV _sip._udp.sip.linphone.org SRV 0 100 5060 sip6.linphone.org
15	5.(130965500…	192.168.157.128	8.8.8.8	DNS	77	128 Standard query 0xc97b A sip6.linphone.org
16	6.310209	192.168.157.128	8.8.8.8	DNS	77	128 Standard query 0x435f AAAA sip6.linphone.org
17	6.311527	192.168.157.128	8.8.8.8	DNS	77	128 Standard query 0x8fff A sip1.linphone.org
18	-7.687899	192.168.157.128	8.8.8.8	DNS	77	128 Standard query 0x16ab AAAA sip1.linphone.org
19	9.(161693900…	192.168.157.128	8.8.8.8	DNS	77	128 Standard query 0x994b AAAA sip1.linphone.org
20	10.619690	8.8.8.8	192.168.157.128	DNS	93	128 Standard query response 0xc97b A sip6.linphone.org A 54.37.202.229
21	11.619690	8.8.8.8	192.168.157.128	DNS	105	128 Standard query response 0x435f AAAA sip6.linphone.org AAAA 2001:41d0:700:789::2020
22	11.621173	8.8.8.8	192.168.157.128	DNS	93	128 Standard query response 0x8fff A sip1.linphone.org A 91.121.209.194
23	12.621173	8.8.8.8	192.168.157.128	DNS	137	128 Standard query response 0x16ab AAAA sip1.linphone.org SOA ns1.gandi.net
24	-13.368196	8.8.8.8	192.168.157.128	DNS	137	128 Standard query response 0x994b AAAA sip1.linphone.org SOA ns1.gandi.net

Nejdříve je odeslán SRV dotaz, který slouží ke zjištění adresy serveru a portu aplikace pro signalizaci SIP. Načež následuje odpověď se dvěma cíli `sip6.linphone.org` a sip1.linphone.org` a se standartními porty pro SIP – 5060.

```
_sip._udp.sip.linphone.org: type SRV, class IN
  Service: _sip
  Protocol: _udp
  Name: sip.linphone.org
  Type: SRV (33) (Server Selection)
  Class: IN (0x0001)
  Time to live: 3302 (55 minutes, 2 seconds)
  Data length: 25
  Priority: 0
  Weight: 100
  Port: 5060
  Target: sip6.linphone.org
_sip._udp.sip.linphone.org: type SRV, class IN
  Service: _sip
  Protocol: _udp
  Name: sip.linphone.org
  Type: SRV (33) (Server Selection)
  Class: IN (0x0001)
  Time to live: 3302 (55 minutes, 2 seconds)
  Data length: 25
  Priority: 10
  Weight: 100
  Port: 5060
  Target: sip1.linphone.org
```

Obrázek 4: SRV dotaz

Poté následují pět DNS dotazů (s tím, že pátý – p. č. 19 – je redundantní) na přeložení obou cílů získaných v předchozím dotazu SRV na adresu IPv4 (záznam typu A) a IPv6 (záznam typu AAAA).

Na těchto pět dotazů poté DNS server odešle odpovědi obsahující přeložená doménová jména (sip1.linphone.org a sip2.linphone.org) na IP adresy. Poslední dvě odpovědi obsahují ještě záznam SOA, který nese informace o autoritativním DNS serveru domény (linphone.org).

SIP a SDP (1/2) (pakety 25 až 32 a paket 39)

Následuje komunikace pomocí signalizačních protokolů SIP a SDP.

```
25 15.(19737190… 192.168.157.128      54.37.202.229        SIP        978    128 Request: REGISTER sip:sip.linphone.org  (1 binding) |
26 16.(10087230… 54.37.202.229        192.168.157.128      SIP        546    128 Status: 401 Unauthorized |
27 17.036063     192.168.157.128      54.37.202.229        SIP       1253    128 Request: REGISTER sip:sip.linphone.org  (1 binding) |
28 17.078581     54.37.202.229        192.168.157.128      SIP        879    128 Status: 200 Registration successful (REGISTER)  (1 binding) |
29 -18.481789    54.37.202.229        192.168.157.128      SIP/SDP   1140    128 Request: INVITE sip:bpc-kom-test-12@192.168.1.108:51944 |
30 20.(18211720… 192.168.157.128      54.37.202.229        SIP        385    128 Status: 100 Trying |
31 21.903404     192.168.157.128      54.37.202.229        SIP        539    128 Status: 180 Ringing |
32 22.(21325410… 192.168.157.128      54.37.202.229        SIP/SDP   1091    128 Status: 200 Ok (INVITE) |
```

Obrázek 5: Část komunikace pomocí signalizačních protokolů SIP a SDP

Nejprve je z klienta (UAC – User Agent Client) na server (REGISTRAR) odeslána SIP žádost REGISTER, kterou REGISTRAR server zařadí jej do lokalizační databáze koncových UA (tzv. lokolizační služba). Tato databáze obsahuje SIP URI a IP adresy jednotlivých UAC. Tato zpráva obsahuje veřejnou identitu a lokaci uživatele. Jinými slovy zaznamenává současnou polohu UA.

```
REGISTER sip:sip.linphone.org SIP/2.0
Via: SIP/2.0/UDP 192.168.157.128:51771;branch=z9hG4bK.ANnq1thk3;rport
From: <sip:bpc-kom-test-12@sip.linphone.org>;tag=JEFigbZTf
To: sip:bpc-kom-test-12@sip.linphone.org
CSeq: 20 REGISTER
Call-ID: NDEf6M7SCD
Max-Forwards: 70
Supported: replaces, outbound
Accept: application/sdp
Accept: text/plain
Accept: application/vnd.gsma.rcs-ft-http+xml
Contact: <sip:bpc-kom-test-12@192.168.157.128:51771;app-id=par02p.notify.windows.com;pn-type=w10;pn-
tok=aHR0cHM6Ly9wYXIwMnAubm90aWZ5LndpbmRvd3MuY29tLz90b2tlbj1Bd1lBQUFBZ0Nra08lMmZKd041RVBDTlVGZWxtOWs5U1ZHaGdZQ1phJTJiY3RUaG9jdUds
NDZaJTJmSHhpUXJZTHUwYWpJaFhiaGI2cyUyYlhjZWpmNnlVdThrWTBjMjRBbDQ5VVdOUEJiNE9tVCUyYjVLa1BWNERKRzRYTlBKWllSbE9ER3NseUQ0QjZwMEJMc21qaG
RuZTVObVowaGdNQTVMNEc1;transport=udp>;+sip.instance="<urn:uuid:263fe820-6f82-4164-b014-f758d8253ead>"
Expires: 28800
User-Agent: LinphoneW10/3.12.0-273-g20efb4ad4 (belle-sip/1.6.3)
```

Data 1: Obsah požadavku SIP – REGISTER

Protože tento požadavek neobsahoval žádné autentifikační údaje server odpoví stavovou zprávou `401 Unauthorized`.

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP 192.168.157.128:51771;branch=z9hG4bK.ANnq1thk3;rport=51944;received=46.39.165.147
From: <sip:bpc-kom-test-12@sip.linphone.org>;tag=JEFigbZTf
To: <sip:bpc-kom-test-12@sip.linphone.org>;tag=jeNBKjF7KB7yH
Call-ID: NDEf6M7SCD
CSeq: 20 REGISTER
Server: Flexisip/2.0.2-2-ga776b7d9 (sofia-sip-nta/2.0)
WWW-Authenticate: Digest realm="sip.linphone.org", nonce="2apP4wAAAABbIkvwAAD+4Fc/FjgAAAAA", opaque="+GNywA==", algorithm=MD5, qop="auth"
Content-Length: 0
```

Data 2: Obsah stavové zprávy SIP – 401 Unauthorized

Tato odpověď též obsahuje v poli WWW-Authenticate parametry autentifikace, které by měl klient použít.

Poté klient odešle ještě druhou žádost REGISTER, která již obsahuje v poli *Authorization* autentifikační údaje pomocí vyžádané metody (digest - klient odesílá zahešovaný přístupový klíč).

```
REGISTER sip:sip.linphone.org SIP/2.0
Via: SIP/2.0/UDP 192.168.157.128:51771;branch=z9hG4bK.bo~nVU5CO;rport
From: <sip:bpc-kom-test-12@sip.linphone.org>;tag=JEFigbZTf
To: sip:bpc-kom-test-12@sip.linphone.org
CSeq: 21 REGISTER
Call-ID: NDEf6M7SCD
Max-Forwards: 70
Supported: replaces, outbound
Accept: application/sdp
Accept: text/plain
Accept: application/vnd.gsma.rcs-ft-http+xml
Contact: <sip:bpc-kom-test-12@46.39.165.147:51944;app-id=par02p.notify.windows.com;pn-type=w10;pn-
tok=aHR0cHM6Ly9wYXIwMnAubm90aWZ5LndpbmRvd3MuY29tLz90b2tlbj1Bd1lBQUFBZ0Nra08lMmZKd041RVBDTlVGZWxtOWs5U1ZHaGdZQ1phJTJiY3RUaG9jdUds
NDZaJTJmSHhpUXJZTHUwYWpJaFhiaGI2cyUyYlhJZWpmNnlVdThrWTBjMjRBbDQ5VVdOUEJiNE9tVCUyYjVLa1BWNERKRzRYTlBKWllSbE9ER3NseUQ0QjZwMEJMc21qaGR
uZTVObVowaGdNQTVMNEc1;transport=udp>;+sip.instance="<urn:uuid:263fe820-6f82-4164-b014-f758d8253ead>"
Expires: 28800
User-Agent: LinphoneW10/3.12.0-273-g20efb4ad4 (belle-sip/1.6.3)
Authorization:  Digest realm="sip.linphone.org", nonce="2apP4wAAAABbIkvwAAD+4Fc/FjgAAAAA", algorithm=MD5, opaque="+GNywA==", username="bpc-kom-
test-12",  uri="sip:sip.linphone.org", response="1125ef401c0b625bdb3dc7c5153e1d5a", cnonce="FzxTUMuvHgj0av9t", nc=00000001, qop=auth
```

Data 3: Obsah požadavku SIP – REGISTER

Odpovědí na tuto žádost je stavová zpráva `200 Registration successful (REGISTERED)`.

```
SIP/2.0 200 Registration successful
Via: SIP/2.0/UDP 192.168.157.128:51771;branch=z9hG4bK.bo~nVU5CO;rport=51944;received=46.39.165.147
From: <sip:bpc-kom-test-12@sip.linphone.org>;tag=JEFigbZTf
To: <sip:bpc-kom-test-12@sip.linphone.org>;tag=pjtetyjN8e09F
Call-ID: NDEf6M7SCD
CSeq: 21 REGISTER
Contact: <sip:bpc-kom-test-12@192.168.1.108:51944;app-id=par02p.notify.windows.com;pn-type=w10;pn-
tok=aHR0cHM6Ly9wYXIwMnAubm90aWZ5LndpbmRvd3MuY29tLz90b2tlbj1Bd1lBQUFBZ0Nra08lMmZKd041RVBDTlVGZWxtOWs5U1ZHaGdZQ1phJTJiY3RUaG9jdUds
NDZaJTJmSHhpUXJZTHUwYWpJaFhiaGI2cyUyYlhJZWpmNnlVdThrWTBjMjRBbDQ5VVdOUEJiNE9tVCUyYjVLa1BWNERKRzRYTlBKWllSbE9ER3NseUQ0QjZwMEJMc21qaGR
uZTVObVowaGdNQTVMNEc1>;+sip.instance="<urn:uuid:263fe820-6f82-4164-b014-f758d8253ead>"
Expires: 28800
Server: Flexisip/2.0.2-2-ga776b7d9 (sofia-sip-nta/2.0)
Content-Length: 0
```

Data 4: Obsah stavové zprávy SIP – 200 Registration successful

V tento okamžik začíná zahajování hovoru. Nejprve se odešle SIP zpráva INVITE, která slouží k zahájení spojení a obsahuje mimo jiné i veřejnou identitu volaného. S touto zprávou se pomocí porotokolu SDP (Session Description Protocol) odesílají i parametry spojení (kodeky, IP adresy a porty pro příjem RTP paketů).

```
INVITE sip:bpc-kom-test-12@192.168.1.108:51944 SIP/2.0
Via: SIP/2.0/UDP 54.37.202.229;rport;branch=z9hG4bK.1m8KFtBKFB17DF5Ky0v0r63N6e
Via: SIP/2.0/UDP 192.168.110.129:60350;branch=z9hG4bK.UH0FpuJCk;rport=58304;received=147.229.146.74
Record-Route: <sip:54.37.202.229:5060;lr>
Max-Forwards: 69
From: <sip:bpc-kom-test-12@sip.linphone.org>;tag=yq7qrBbwg
To: <sip:bpc-kom-test-12@sip.linphone.org>
Call-ID: -TPwxCg9GI
CSeq: 21 INVITE
Contact: <sip:bpc-kom-test-12@147.229.146.74:58304>;+sip.instance="<urn:uuid:263fe820-6f82-4164-b014-f758d8253ead>"
User-Agent: LinphoneW10/3.12.0-273-g20efb4ad4 (belle-sip/1.6.3)
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO, UPDATE
Supported: replaces, outbound
Content-Type: application/sdp
Content-Length: 300

v=0
o=bpc-kom-test-12 3147 859 IN IP4 54.37.202.229
s=Talk
c=IN IP4 54.37.202.229
t=0 0
a=rtcp-xr:rcvr-rtt=all:10000 stat-summary=loss,dup,jitt,TTL voip-metrics
a=nortpproxy:yes
m=audio 62078 RTP/AVP 0 8 101
a=rtpmap:101 telephone-event/8000
a=rtcp-fb:* trr-int 5000
a=rtcp-fb:* ccm tmmbr
```

Data 5: Obsah požadavku SIP – INVITE a obsah SDP

Dále následují tři stavové pakety. První `100 Trying`, druhá `180 Ringing` (tyto dvě zprávy informují o doručení zprávy UA a o tom, že dochází k jejich zpracování) a třetí `200 Ok INVITE` (bez této zprávy není možné navázat spojení). Stavová zpráva `200 Ok INVITE` též obsahuje SIP zprávu INVITE a SDP obsahující parametry spojení (podobně jako žádost námi analyzovaného klienta).

SIP/2.0 100 Trying
Via: SIP/2.0/UDP 54.37.202.229;rport;branch=z9hG4bK.1m8KFtBKFB17DF5Ky0v0r63N6e
Via: SIP/2.0/UDP 192.168.110.129:60350;received=147.229.146.74;branch=z9hG4bK.UH0FpuJCk;rport=58304
From: <sip:bpc-kom-test-12@sip.linphone.org>;tag=yq7qrBbwg
To: sip:bpc-kom-test-12@sip.linphone.org
Call-ID: -TPwxCg9GI
CSeq: 21 INVITE

Data 6: Obsah stavové zprávy SIP – 100 Trying

SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 54.37.202.229;rport;branch=z9hG4bK.1m8KFtBKFB17DF5Ky0v0r63N6e
Via: SIP/2.0/UDP 192.168.110.129:60350;received=147.229.146.74;branch=z9hG4bK.UH0FpuJCk;rport=58304
From: <sip:bpc-kom-test-12@sip.linphone.org>;tag=yq7qrBbwg
To: <sip:bpc-kom-test-12@sip.linphone.org>;tag=Qs4kr~Y
Call-ID: -TPwxCg9GI
CSeq: 21 INVITE
User-Agent: LinphoneW10/3.12.0-273-g20efb4ad4 (belle-sip/1.6.3)
Supported: replaces, outbound
Record-route: <sip:54.37.202.229:5060;lr>

Data 7: Obsah stavové zprávy SIP – 180 Ringing

```
SIP/2.0 200 Ok
Via: SIP/2.0/UDP 54.37.202.229;rport;branch=z9hG4bK.1m8KFtBKFB17DF5Ky0v0r63N6e
Via: SIP/2.0/UDP 192.168.110.129:60350;received=147.229.146.74;branch=z9hG4bK.UH0FpuJCk;rport=58304
From: <sip:bpc-kom-test-12@sip.linphone.org>;tag=yq7qrBbwg
To: <sip:bpc-kom-test-12@sip.linphone.org>;tag=Qs4kr~Y
Call-ID: -TPwxCg9GI
CSeq: 21 INVITE
User-Agent: LinphoneW10/3.12.0-273-g20efb4ad4 (belle-sip/1.6.3)
Supported: replaces, outbound
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO, UPDATE
Contact: <sip:bpc-kom-test-12@46.39.165.147:51944;transport=udp>;+sip.instance="<urn:uuid:263fe820-6f82-4164-b014-f758d8253ead>"
Content-Type: application/sdp
Content-Length: 284
Record-route: <sip:54.37.202.229:5060;lr>

v=0
o=bpc-kom-test-12 3681 12 IN IP4 192.168.157.128
s=Talk
c=IN IP4 192.168.157.128
t=0 0
a=rtcp-xr:rcvr-rtt=all:10000 stat-summary=loss,dup,jitt,TTL voip-metrics
m=audio 7076 RTP/AVP 0 8 101
a=rtpmap:101 telephone-event/8000
a=rtcp-fb:* trr-int 5000
a=rtcp-fb:* ccm tmmbr
```

Data 8: Obsah stavové zprávy SIP – 200 Ok (INVITE)

Nakonec je klientovi doručena SIP zpráva metody ACK, která potvrzuje, že UAC přijal finální odpověď na zprávu INVITE. Zpráva ACK též obsahuje v poli Proxy-Authorization autentifikační údaje pro ověření autorizace.

```
ACK sip:bpc-kom-test-12@192.168.1.108:51944;verified SIP/2.0
Via: SIP/2.0/UDP 54.37.202.229;rport;branch=z9hG4bK.86Z0ec63ZUFpSt9j9Utp5jj8UB
Via: SIP/2.0/UDP 192.168.110.129:60350;rport=58304;branch=z9hG4bK.w~ZXhO-dZ;received=147.229.146.74
From: <sip:bpc-kom-test-12@sip.linphone.org>;tag=yq7qrBbwg
To: <sip:bpc-kom-test-12@sip.linphone.org>;tag=Qs4kr~Y
CSeq: 21 ACK
Call-ID: -TPwxCg9GI
Max-Forwards: 69
Proxy-Authorization: Digest realm="sip.linphone.org", nonce="3qpP4wAAAAD5MrsZAABUm/2Zkd8AAAAA", algorithm=MD5, opaque="+GNywA==", username="bpc-kom-test-12", uri="sip:bpc-kom-test-12@sip.linphone.org", response="2d1895aeacec91e10f96fba5745463fe", cnonce="sw60pV6rI0IFYoyb", nc=00000001, qop=auth
User-Agent: LinphoneW10/3.12.0-273-g20efb4ad4 (belle-sip/1.6.3)
Content-Length: 0
```

Data 9: Obsah zprávy SIP – ACK

Tabulka 1: Tabulka SIP odpovědí

Kód stavu	Popis
1xx	dočasná odpověď
2xx	ÚSPĚCH – finální odpověď
3xx	PŘESMĚROVÁNÍ – finální odpověď
4xx	CHYBA NA STRANĚ KLIENTA – finální odpověď
5xx	CHYBA NA STRANĚ SERVERU – finální odpověď
6xx	GLOBÁLNÍ CHYBA – finální odpověď

STUN komunikace (pakety 33 až 38 a pakety 42 až 43 a další)

No.	Time	Source	Destination	Protocol	Length	TTL	Info
33	23.(11332…	192.168.157.128	54.37.202.229	STUN	62	128	Binding Request
34	24.133323	192.168.157.128	54.37.202.229	STUN	62	128	Binding Request
35	24.188182	192.168.157.128	54.37.202.229	STUN	62	128	Binding Request
36	-25.811712	192.168.157.128	54.37.202.229	STUN	62	128	Binding Request
37	27.(15049…	54.37.202.229	192.168.157.128	STUN	62	128	Binding Request
38	28.505101	54.37.202.229	192.168.157.128	STUN	62	128	Binding Request
42	32.845847	54.37.202.229	192.168.157.128	STUN	62	128	Binding Request
43	33.845847	54.37.202.229	192.168.157.128	STUN	62	128	Binding Request
85	-74.(1093…	192.168.157.128	54.37.202.229	STUN	62	128	Binding Request
91	81.540021	54.37.202.229	192.168.157.128	STUN	62	128	Binding Request
138	-127.(105…	192.168.157.128	54.37.202.229	STUN	62	128	Binding Request
143	133.(1578…	54.37.202.229	192.168.157.128	STUN	62	128	Binding Request
190	-179.(100…	192.168.157.128	54.37.202.229	STUN	62	128	Binding Request
196	186.(1639…	54.37.202.229	192.168.157.128	STUN	62	128	Binding Request
242	232.030454	192.168.157.128	54.37.202.229	STUN	62	128	Binding Request
247	237.375031	54.37.202.229	192.168.157.128	STUN	62	128	Binding Request
293	283.(2064…	192.168.157.128	54.37.202.229	STUN	62	128	Binding Request
300	290.410290	54.37.202.229	192.168.157.128	STUN	62	128	Binding Request
347	337.(2117…	192.168.157.128	54.37.202.229	STUN	62	128	Binding Request
352	-341.8387…	54.37.202.229	192.168.157.128	STUN	62	128	Binding Request
399	388.855908	192.168.157.128	54.37.202.229	STUN	62	128	Binding Request
404	394.190595	54.37.202.229	192.168.157.128	STUN	62	128	Binding Request
450	440.(1889…	192.168.157.128	54.37.202.229	STUN	62	128	Binding Request
455	-444.(106…	54.37.202.229	192.168.157.128	STUN	62	128	Binding Request
501	490.628261	192.168.157.128	54.37.202.229	STUN	62	128	Binding Request
507	-496.(102…	54.37.202.229	192.168.157.128	STUN	62	128	Binding Request
555	545.(1975…	192.168.157.128	54.37.202.229	STUN	62	128	Binding Request
606	-595.2862…	192.168.157.128	54.37.202.229	STUN	62	128	Binding Request

Obrázek 6: STUN komunikace

STUN je protokol sloužící k umožnění komunikace skrz NAT. Jeho úkolem je zjištění veřejné IP adresy a portu zařízení za NAT bránou. Znalost veřejné adresy a portu umožní P2P spojení obou UAC. Jinými slovy první UAC bude moci posílat multimediální data přímo druhému UAC bez potřeby užití proxy. Toto spojení se ovšem nepodařilo navázat, proto bude v průběhu hovoru docházet k odesílání dalších zpráv `Binding Request`. Následkem nezdařeného spojení je i to, že veškerý provoz bude procházet přes SIP proxy (54.37.202.229).

RTP a RTCP komunikace (pakety 40 až 41, pakety 44 až 2357 a pakety 2359 až 2360)

No.	Time	Source	Destination	Protocol	Length	TTL	Info
40	-29.473073	192.168.157.128	54.37.202.229	RTP	214	128	PT=ITU-T G.711 PCMU, SSRC=0xA41CF215, Seq=0, Time=2640328734
41	31.(18415…	192.168.157.128	54.37.202.229	RTP	214	128	PT=ITU-T G.711 PCMU, SSRC=0xA41CF215, Seq=1, Time=2640328894
44	33.855337	54.37.202.229	192.168.157.128	RTP	214	128	PT=ITU-T G.711 PCMU, SSRC=0x64A31665, Seq=0, Time=54885798
45	-34.138815	192.168.157.128	54.37.202.229	RTP	214	128	PT=ITU-T G.711 PCMU, SSRC=0xA41CF215, Seq=2, Time=2640329054
46	-35.(1126…	54.37.202.229	192.168.157.128	RTP	214	128	PT=ITU-T G.711 PCMU, SSRC=0x64A31665, Seq=1, Time=54885958
47	37.(11779…	192.168.157.128	54.37.202.229	RTP	214	128	PT=ITU-T G.711 PCMU, SSRC=0xA41CF215, Seq=3, Time=2640329214
48	38.188121	54.37.202.229	192.168.157.128	RTP	214	128	PT=ITU-T G.711 PCMU, SSRC=0x64A31665, Seq=2, Time=54886118
49	38.196180	192.168.157.128	54.37.202.229	RTP	214	128	PT=ITU-T G.711 PCMU, SSRC=0xA41CF215, Seq=4, Time=2640329374
50	-39.791782	54.37.202.229	192.168.157.128	RTP	214	128	PT=ITU-T G.711 PCMU, SSRC=0x64A31665, Seq=3, Time=54886278

Obrázek 7: RTP a RTCP komunikace

Poté už probíhá samotný přenos multimediálních dat (v tomto případě pouze audio – kodek G.711). Mezi těmito daty se občas vyskytnou i řídící pakety protokolu RTCP. Protokol RTCP je používán pro kontrolu a řízení celého sezení. Protože je monitorovaný klient aktivním účastníkem relace, odesílá

se zpráva Sender Report (SR), která obsahuje statistické informace o přenosu. Dále je součástí RTCP paketu Source Description (SDES), který obsahuje CNAME (Canonical Name), což je jednoznačné jméno v rámci jedné RTP relace.

SIP komunikace 2/2 (pakety 40 až 41, pakety 44 až 2357 a pakety 2359 až 2360)

No.	Time	Source	Destination	Protocol	Length	TTL	Info
2358	1884.9908…	192.168.157.128	54.37.202.229	SIP	440	128	Request: BYE sip:bpc-kom-test-12@147.229.146.74:58304 |
2361	1886.0438…	54.37.202.229	192.168.157.128	SIP	427	128	Status: 200 Ok (BYE) |

Obrázek 8: SIP komunikace

K ukončení hovoru je odeslána SIP zpráva BYE, která ukončí probíhající relaci.

```
BYE sip:bpc-kom-test-12@147.229.146.74:58304 SIP/2.0
Via: SIP/2.0/UDP 192.168.157.128:51771;branch=z9hG4bK.Nbj~UF0wl;rport
From: <sip:bpc-kom-test-12@sip.linphone.org>;tag=Qs4kr~Y
To: <sip:bpc-kom-test-12@sip.linphone.org>;tag=yq7qrBbwg
CSeq: 111 BYE
Call-ID: -TPwxCg9GI
Max-Forwards: 70
Route: <sip:54.37.202.229:5060;lr>
User-Agent: LinphoneW10/3.12.0-273-g20efb4ad4 (belle-sip/1.6.3)
```

Data 10: Obsah požadavku SIP – BYE

Poté klient obdrží stavovou zprávu `200 Ok (BYE), která informuje o tom, že zpráva byla úspěšně zpracována druhým klientem. Zpráva také obsahuje metodu BYE.

```
SIP/2.0 200 Ok
Via: SIP/2.0/UDP 192.168.157.128:51771;received=46.39.165.147;branch=z9hG4bK.Nbj~UF0wl;rport=51944
From: <sip:bpc-kom-test-12@sip.linphone.org>;tag=Qs4kr~Y
To: <sip:bpc-kom-test-12@sip.linphone.org>;tag=yq7qrBbwg
Call-ID: -TPwxCg9GI
CSeq: 111 BYE
User-Agent: LinphoneW10/3.12.0-273-g20efb4ad4 (belle-sip/1.6.3)
Supported: replaces, outbound
Content-Length: 0
```

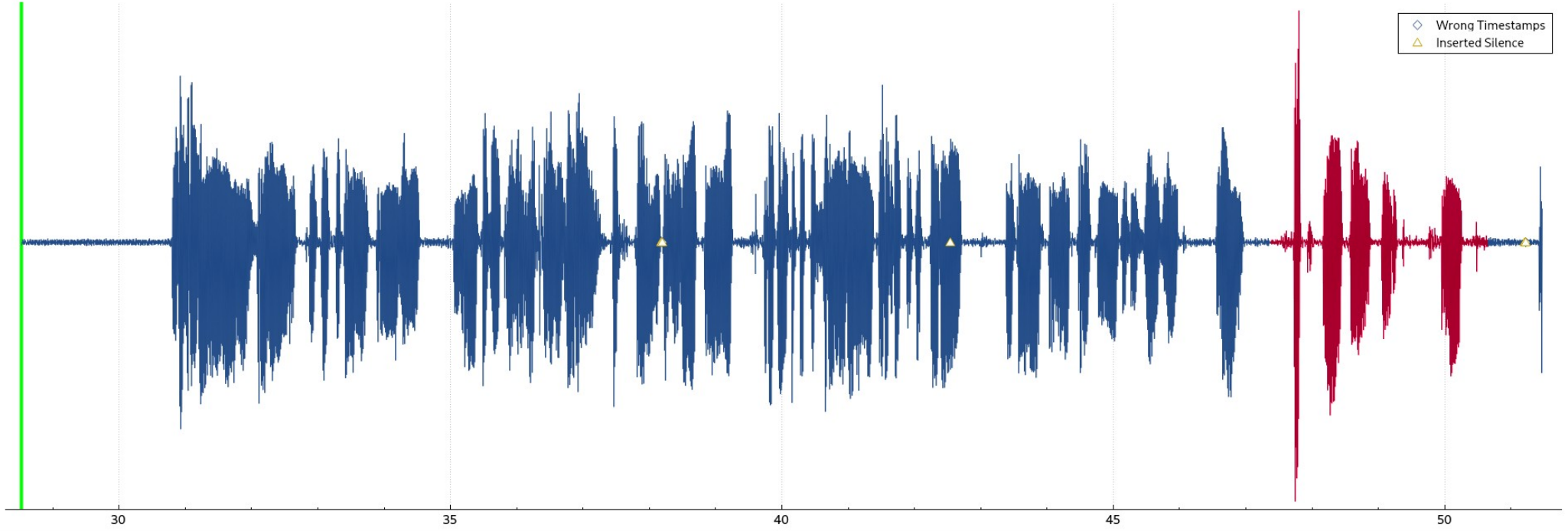
Data 11: Obsah stavové zprávy SIP – 200 Ok

Zabezpečení přenášených dat proti modifikaci a odposlechu při přenosu

Obsah není šifrován. Šifrované jsou pouze hesla a to pomocí hashovacího algoritmu MD5. Modifikace signalizačních paketů by dle mého názoru neměl být problém, neboť není komunikace šifrována a kromě registrace k REGISTRAR serveru není vyžadována žádná další autentifikace. Multimediální RTP stream lze též modifikovat, protože není šifrovaný.

Obsah případné datové části

Obsahem datové části je následující nešifrovaná hlasová zpráva kódována standardem G.711 obsahující mimo jiné i tajnou zprávu: `sip linphone org` (vyznačeno rudě). K poslechu hlasové nahrávky bylo třeba přepnout časování dle časové známky RTP.



Obrázek 9: Přenášená zvuková data pomocí protokolu RTP

FTP komunikace (pakety 2362 až 2417)

No.	Time	Delta	Source	Destination	Protocol	Length	TTL	Info
2362	-1886.(10…	-0.(1141…	160.216.225.122	160.216.225.129	TCP	66	128	56317 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2363	1888.(119…	0.000119	160.216.225.129	160.216.225.122	TCP	66	128	21 → 56317 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
2364	1889.1976…	0.000237	160.216.225.122	160.216.225.129	TCP	60	128	56317 → 21 [ACK] Seq=1 Ack=1 Win=1051136 Len=0
2365	1889.1981…	0.000559	160.216.225.129	160.216.225.122	FTP	197	128	Response: 220-FileZilla Server 0.9.60 beta
2366	-1890.786…	0.015756	160.216.225.122	160.216.225.129	FTP	71	128	Request: USER FTP_server
2367	1892.(150…	0.000495	160.216.225.129	160.216.225.122	FTP	92	128	Response: 331 Password required for ftp_server
2368	1893.5242…	0.014882	160.216.225.122	160.216.225.129	FTP	64	128	Request: PASS FTP
2369	1893.5246…	0.000429	160.216.225.129	160.216.225.122	FTP	69	128	Response: 230 Logged on
2370	-1894.460…	0.015213	160.216.225.122	160.216.225.129	FTP	60	128	Request: SYST
2371	1896.(183…	0.000555	160.216.225.129	160.216.225.122	FTP	86	128	Response: 215 UNIX emulated by FileZilla
2372	1897.8504…	0.014979	160.216.225.122	160.216.225.129	FTP	60	128	Request: FEAT
2373	1897.8509…	0.000512	160.216.225.129	160.216.225.122	FTP	176	128	Response: 211-Features:
2374	-1898.134…	0.014868	160.216.225.122	160.216.225.129	FTP	84	128	Request: CLNT Total Commander (UTF-8)
2375	-1899.(11…	0.000344	160.216.225.129	160.216.225.122	FTP	70	128	Response: 200 Don't care
2376	1901.(117…	0.015179	160.216.225.122	160.216.225.129	FTP	68	128	Request: OPTS UTF8 ON
2377	1902.1766…	0.000332	160.216.225.129	160.216.225.122	FTP	118	128	Response: 202 UTF8 mode is always enabled. No need to send this command.
2378	1902.2070…	0.030431	160.216.225.122	160.216.225.129	FTP	60	128	Request: PWD
2379	-1903.792…	0.000332	160.216.225.129	160.216.225.122	FTP	85	128	Response: 257 "/" is current directory.
2380	1905.(154…	0.045733	160.216.225.122	160.216.225.129	TCP	60	128	56317 → 21 [ACK] Seq=89 Ack=462 Win=1050624 Len=0

Obrázek 10: Část FTP komunikace

V této komunikaci se klient připojuje k FTP serveru. Jako FTP klient je použit software *Total Commander* a jako FTP server je použit software *FileZilla Server 0.9.60 beta*. Také dle MAC adresy serveru můžeme zjistit, že FTP server běží ve virtuálním prostředí VMware.

Protokol aplikační vrstvy

FTP

Protokol transportní vrstvy a adresy komunikujících stran

TCP

- FTP – Klient: 56317 & server: 21
- FTP-DATA – Klient: 56318 & server: 20

Protokol síťové vrstvy a adresy komunikujících stran

IPv4 Klient: 160.216.225.122

Server: 160.216.225.129

Popis průběhu komunikace

První dva pakety slouží k navázání (spolehlivého) TCP spojení. Klient odešle první paket s příznakem SYN a od serveru obdrží paket s příznaky SYN a ACK.

Poté probíhá samotná FTP komunikace. Pro zobrazení této komunikace jsem použil funkci `Follow TCP stream`.

Navázání spojení a autentifikace uživatele

Po navázání spojení server odesílá zprávu s kódem 220, který dává najevo, že server je připraven k připojení klienta:

```
220-FileZilla Server 0.9.60 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
```

Poté je pomocí příkazu **USER** odesláno jméno uživatele a obdrží zprávu s kódem 331, která dává klientovy vědět že je pro daného uživatele vyžadováno heslo.:

```
USER FTP_server
331 Password required for ftp_server
```

Poté je pomocí příkazu **PASS** v čitelném formátu odesláno heslo a server odesílá zprávu s kódem 230 oznamující úspěšné přihlášení:

```
PASS FTP
230 Logged on
```

Poté se klient pomocí příkazu **SYST** dotázal na typ systému a server mu odpoví zprávou s kódem 215 a jménem systému dle RFC1700:

```
SYST
215 UNIX emulated by FileZilla
```

Následuje dotaz klienta příkazem **FEAT** a odpověď serveru (s kódem 211) na seznam příkazů FTP serveru:

```
FEAT
211-Features:
 MDTM
 REST STREAM
 SIZE
 MLST type*;size*;modify*;
 MLSD
 UTF8
 CLNT
 MFMT
 EPSV
 EPRT
211 End
```

Následně klient příkazem **CLNT** odešle informace o klientském programu:

```
CLNT Total Commander (UTF-8)
200 Don't care
```

Poté klient zapne pomocí příkazu **OPT** kódování UTF8, které už je ovšem na serveru ve výchozím stavu zapnuté.

```
OPTS UTF8 ON
202 UTF8 mode is always enabled. No need to send this command.
```

Následně klient příkazem **PWD** zjistí absolutní cestu adresáře, ve kterém se nachází:

```
PWD
257 "/" is current directory.
```

Přenesení seznamu souborů v aktuálním adresáři

No.	Time	Delta	Source	Destination	Protocol	Length	TTL	Info
2385	1910.9057…	0.014934	160.216.225.122	160.216.225.129	FTP	60	128	Request: MLSD
2386	1910.9065…	0.000764	160.216.225.129	160.216.225.122	TCP	66	128	20 → 56318 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2387	-1911.093…	0.000321	160.216.225.122	160.216.225.129	TCP	66	128	56318 → 20 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
2388	-1912.(10…	0.000035	160.216.225.129	160.216.225.122	FTP	109	128	Response: 150 Opening data channel for directory listing of "/"
2389	1914.(120…	0.000017	160.216.225.129	160.216.225.122	TCP	54	128	20 → 56318 [ACK] Seq=1 Ack=1 Win=262656 Len=0
2390	1915.2024…	0.000558	160.216.225.129	160.216.225.122	FTP-DA…	390	128	FTP Data: 336 bytes (PORT) (MLSD)
2391	1915.2027…	0.000342	160.216.225.129	160.216.225.122	TCP	54	128	20 → 56318 [FIN, ACK] Seq=337 Ack=1 Win=262656 Len=0
2392	-1916.797…	0.000110	160.216.225.122	160.216.225.129	TCP	60	128	56318 → 20 [ACK] Seq=1 Ack=338 Win=1051136 Len=0
2393	1918.(149…	0.000202	160.216.225.129	160.216.225.122	FTP	88	128	Response: 226 Successfully transferred "/"
2394	1919.4981…	0.000091	160.216.225.122	160.216.225.129	TCP	60	128	56317 → 21 [ACK] Seq=133 Ack=599 Win=1050368 Len=0
2395	1919.5019…	0.003808	160.216.225.122	160.216.225.129	TCP	60	128	56318 → 20 [FIN, ACK] Seq=1 Ack=338 Win=1051136 Len=0
2396	-1920.498…	0.000052	160.216.225.129	160.216.225.122	TCP	54	128	20 → 56318 [ACK] Seq=338 Ack=2 Win=262656 Len=0

Obrázek 11: Přenesení seznamu souborů v aktuálním adresáři

Nejprve došlo příkazem **TYPE** k nastavení módu přenosu na ASCII a ze serveru přijde potvrzení o provedení příkazu:

```
TYPE A
200 Type set to A
```

Poté se příkazem **PORT** nastaví porty pro přenos dat a ze serveru přijde potvrzení o provedení příkazu:

```
PORT 160,216,225,122,219,254
200 Port command successful
```

Poté dojde k odeslání příkazu **MLSD**, který slouží k získání obsahu současného adresáře:

```
MLSD
```

Server vytvoří nové TCP spojení a odešle odpověď informující o otevření datového kanálu:

```
150 Opening data channel for directory listing of "/"
```

Poté server data odešle, spojení terminuje a odešle klientovi informaci o dokončení přenosu:

```
226 Successfully transferred "/"
```

Poté TCP spojení terminuje i klient.

Stažení souboru z FTP serveru

No.	Time	Delta	Source	Destination	Protocol	Length	TTL	Info
2397	-1921.443…	1.054460	160.216.225.122	160.216.225.129	FTP	62	128	Request: TYPE I
2398	1923.(185…	0.000324	160.216.225.129	160.216.225.122	FTP	73	128	Response: 200 Type set to I
2399	1924.8659…	0.014267	160.216.225.122	160.216.225.129	FTP	84	128	Request: PORT 160,216,225,122,219,255
2400	1924.8663…	0.000365	160.216.225.129	160.216.225.122	FTP	83	128	Response: 200 Port command successful
2401	-1925.117…	0.016080	160.216.225.122	160.216.225.129	FTP	74	128	Request: RETR Transfer2.txt
2402	-1926.(11…	0.000643	160.216.225.129	160.216.225.122	TCP	66	128	20 → 56319 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2403	1928.(117…	0.000374	160.216.225.129	160.216.225.122	FTP	130	128	Response: 150 Opening data channel for file download from server of "/Transfer2.txt"
2404	1929.1784…	0.000063	160.216.225.122	160.216.225.129	TCP	66	128	56319 → 20 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
2405	1929.1785…	0.000059	160.216.225.129	160.216.225.122	TCP	54	128	20 → 56319 [ACK] Seq=1 Ack=1 Win=262656 Len=0
2406	-1930.819…	0.001759	160.216.225.129	160.216.225.122	FTP-DA…	84	128	FTP Data: 30 bytes (PORT) (RETR Transfer2.txt)
2407	1932.(147…	0.000921	160.216.225.129	160.216.225.122	TCP	54	128	20 → 56319 [FIN, ACK] Seq=31 Ack=1 Win=262656 Len=0
2408	1933.4764…	0.000253	160.216.225.122	160.216.225.129	TCP	60	128	56319 → 20 [ACK] Seq=1 Ack=32 Win=1051136 Len=0
2409	1933.4766…	0.000193	160.216.225.129	160.216.225.122	FTP	101	128	Response: 226 Successfully transferred "/Transfer2.txt"
2410	-1934.523…	0.000157	160.216.225.122	160.216.225.129	TCP	60	128	56317 → 21 [ACK] Seq=191 Ack=770 Win=1050368 Len=0
2411	1936.(177…	0.001677	160.216.225.122	160.216.225.129	TCP	60	128	56319 → 20 [FIN, ACK] Seq=1 Ack=32 Win=1051136 Len=0
2412	1937.7734…	0.000044	160.216.225.129	160.216.225.122	TCP	54	128	20 → 56319 [ACK] Seq=32 Ack=2 Win=262656 Len=0

Obrázek 12: Stažení souboru z FTP serveru

Nejprve je příkazem **TYPE** nastaven mód přenosu na binární (image/binary):

```
TYPE I
200 Type set to I
```

Poté dojde pomocí příkazu PORT k nastavení portů pro přenos dat:

```
PORT 160,216,225,122,219,255
200 Port command successful
```

Poté klient odešle příkaz **RETR**, který slouží ke stažení souboru z FTP serveru (k nahrání souboru by byl použit příkaz **STOR** nebo **STOU**, které ovšem nejsou dostupné viz příkaz **FEAT**):

```
RETR Transfer2.txt
```

V tu chvíli server otevírá nové TCP spojení pro datový kanál, otevření datového kanálu je potvrzeno zprávou:

```
150 Opening data channel for file download from server of "/Transfer2.txt"
```

Poté je soubor datovým kanálem přenesen klientovi. Po přenosu server spojení terminuje a odešle zprávu o úspěšném přenosu:

```
226 Successfully transferred "/Transfer2.txt"
```

Poté i klient spojení terminuje

Ukončení spojení s FTP serverem

Pro ukončení FTP relace použije klient příkaz **QUIT** a server odpoví *221 Goodbye*:

```
QUIT
221 Goodbye
```

Poté je pomocí tří paketů ze strany serveru TCP spojení ukončeno. Server odeslal paket s příznaky FIN a ACK a klient odpovídá paketem s příznakem ACK a dále odesílá paket s příznaky RST a ACK.

Zabezpečení přenášených dat proti modifikaci a odposlechu při přenosu

Všechna přenesená data (port 20) i řídící příkazy (port 21) nebyly šifrovány. TCP protokol zajišťuje pouze spolehlivé doručení. Vzhledem k tomu lze dle mého názoru přenášené příkazy modifikovat. V takové situaci ovšem vyjde špatný kontrolní součet a došlo by tak k opětovnému odeslání všech paketů v současném okně nebo by bylo nutné upravit sekvenční čísla následujících paketů, odchytit TCP segment s příznakem ACK a upravit kontrolní součet. Také se domnívám, že i přenášená data by šla modifikovat. Ovšem v této komunikaci by bylo mnohem jednodušší odchytit autentifikační údaje uživatele a vytvořit novou FTP relaci.

Obsah případné datové části

Přenášený soubor `Transfer2.txt` obsahuje nešifrovanou zprávu: `hidden message: RELACNI VRSTVA`.

```
FTP Data (30 bytes data)
[Setup frame: 2399]
[Setup method: PORT]
[Command: RETR Transfer2.txt]
Command frame: 2401
[Current working directory: /]
Line-based text data (1 lines)
  hidden message: RELACNI VRSTVA
```

Obrázek 13: Obsah souboru Transfer2.txt