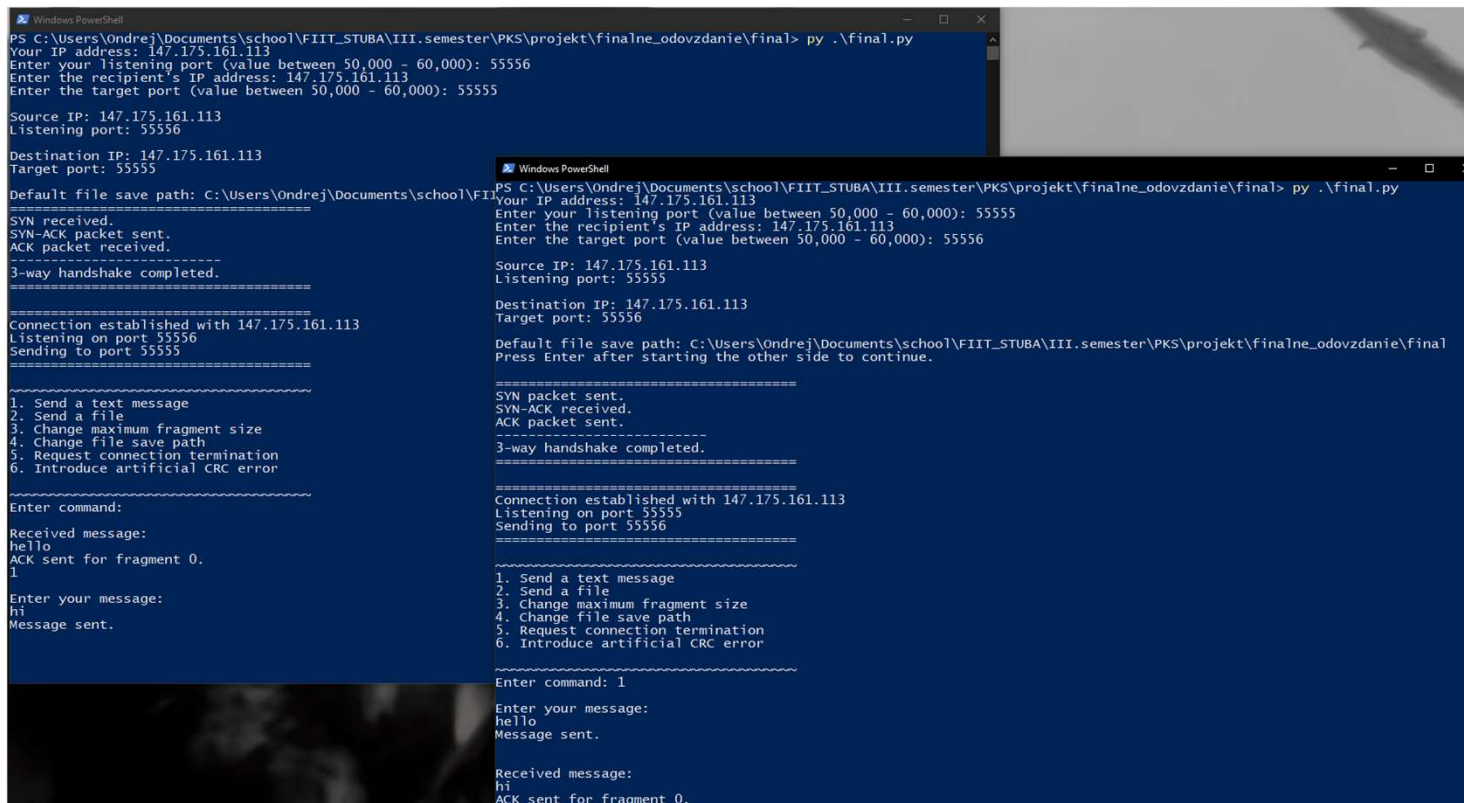


Test Custom UDP protokolu

Ondrej Krajčovič



Inicializácia, a poslanie text správy z oboch strán



```
PS C:\Users\Ondrej\Documents\school\FIIT_STUBA\III.semester\PKS\projekt\finalne_odovzdanie\final> py .\final.py
Your IP address: 147.175.161.113
Enter your listening port (value between 50,000 - 60,000): 55556
Enter the recipient's IP address: 147.175.161.113
Enter the target port (value between 50,000 - 60,000): 55555

Source IP: 147.175.161.113
Listening port: 55556

Destination IP: 147.175.161.113
Target port: 55555

Default file save path: C:\Users\Ondrej\Documents\school\FIIT_STUBA\III.semester\PKS\projekt\finalne_odovzdanie\final
Press Enter after starting the other side to continue.

=====
SYN received.
SYN-ACK packet sent.
ACK packet received.
3-way handshake completed.
=====

Connection established with 147.175.161.113
Listening on port 55556
Sending to port 55555
=====

1. Send a text message
2. Send a file
3. Change maximum fragment size
4. Change file save path
5. Request connection termination
6. Introduce artificial CRC error
=====
Enter command:
Received message:
hello
ACK sent for fragment 0.
1
Enter your message:
hi
Message sent.

=====
PS C:\Users\Ondrej\Documents\school\FIIT_STUBA\III.semester\PKS\projekt\finalne_odovzdanie\final> py .\final.py
Your IP address: 147.175.161.113
Enter your listening port (value between 50,000 - 60,000): 55555
Enter the recipient's IP address: 147.175.161.113
Enter the target port (value between 50,000 - 60,000): 55556

Source IP: 147.175.161.113
Listening port: 55555

Destination IP: 147.175.161.113
Target port: 55556

Default file save path: C:\Users\Ondrej\Documents\school\FIIT_STUBA\III.semester\PKS\projekt\finalne_odovzdanie\final
Press Enter after starting the other side to continue.

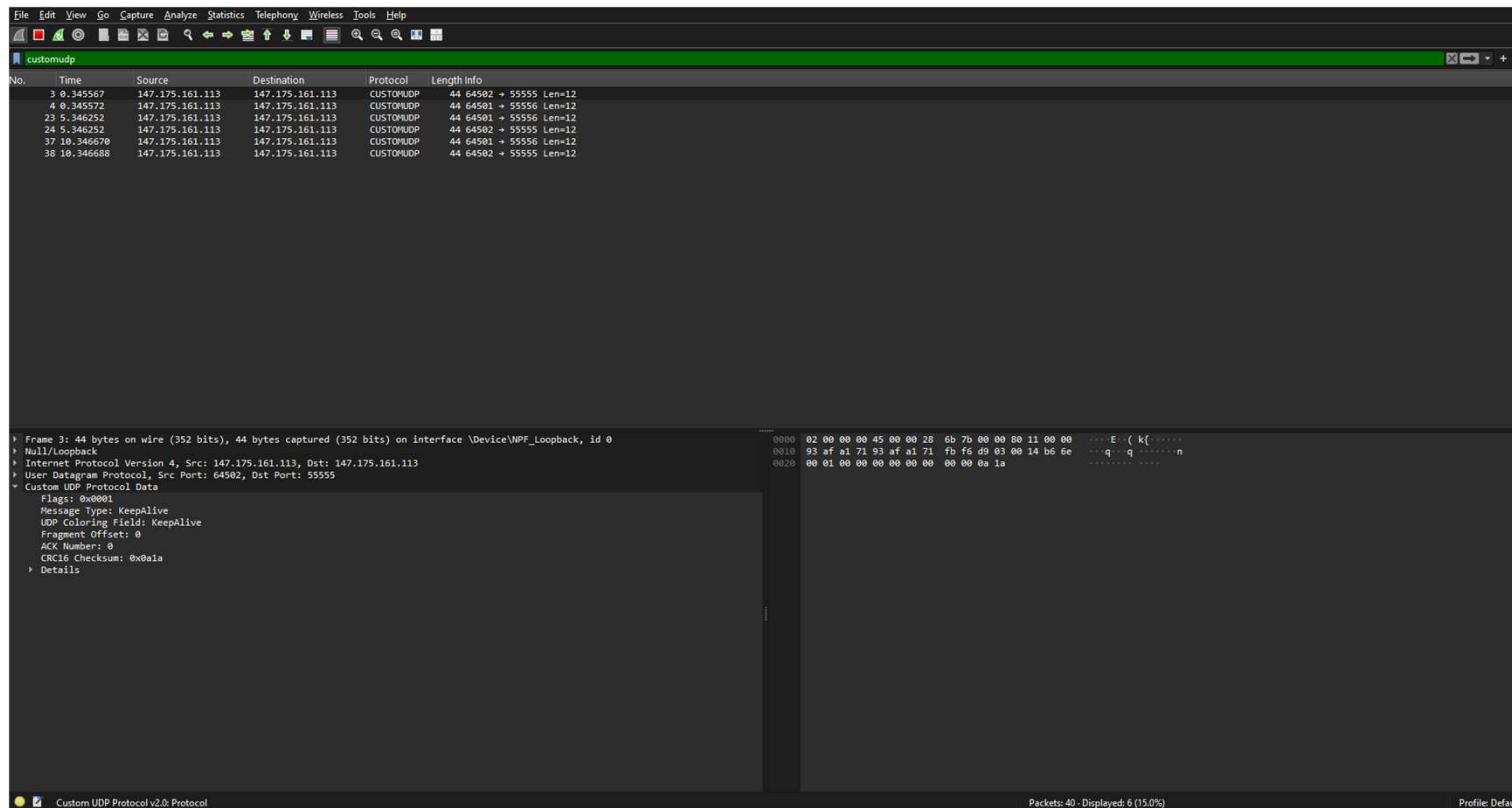
=====
SYN packet sent.
SYN-ACK received.
ACK packet sent.
3-way handshake completed.
=====

Connection established with 147.175.161.113
Listening on port 55555
Sending to port 55556
=====

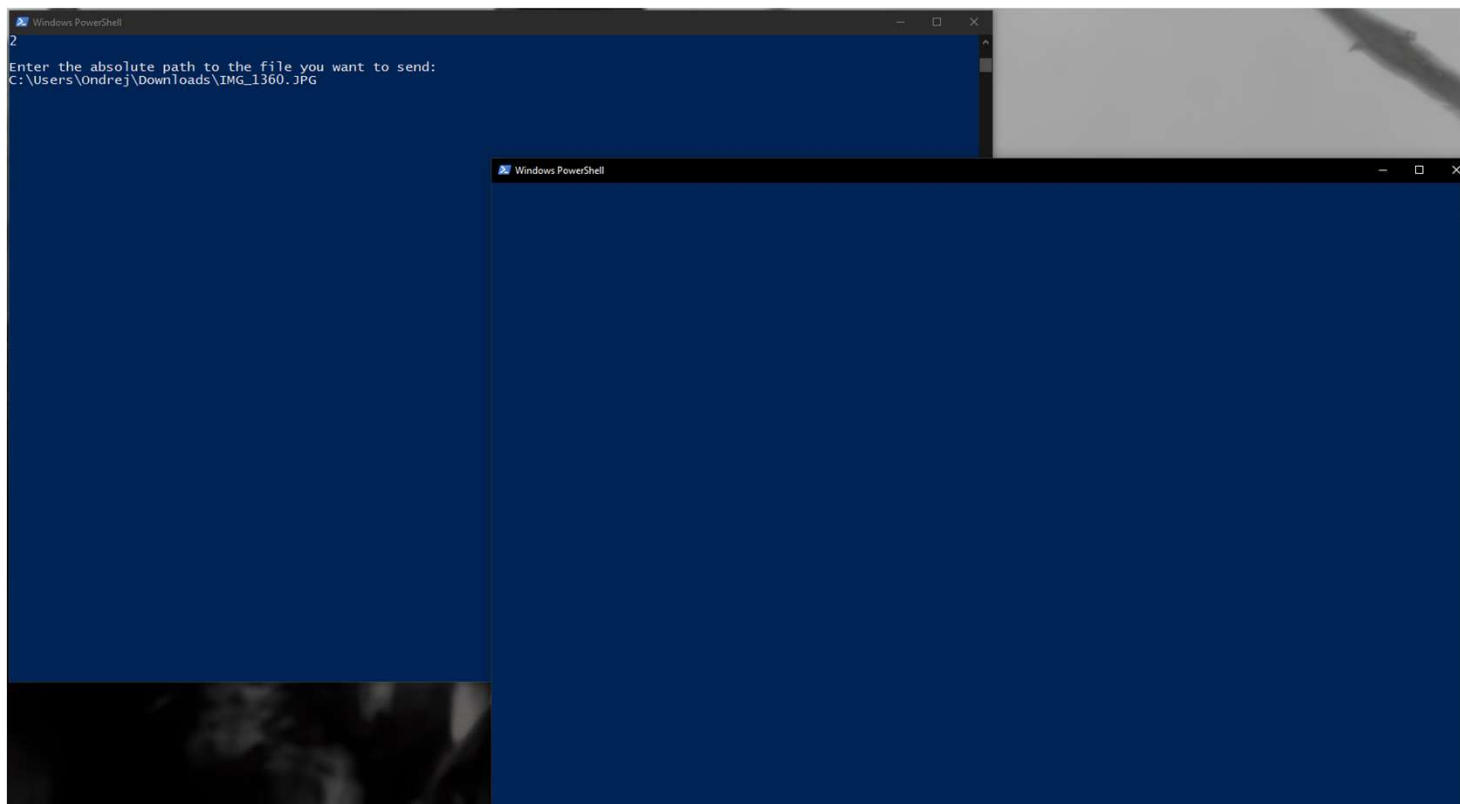
1. Send a text message
2. Send a file
3. Change maximum fragment size
4. Change file save path
5. Request connection termination
6. Introduce artificial CRC error
=====
Enter command: 1
Enter your message:
hello
Message sent.

Received message:
hi
ACK sent for fragment 0.
```

Keepalive odchytený po štarte



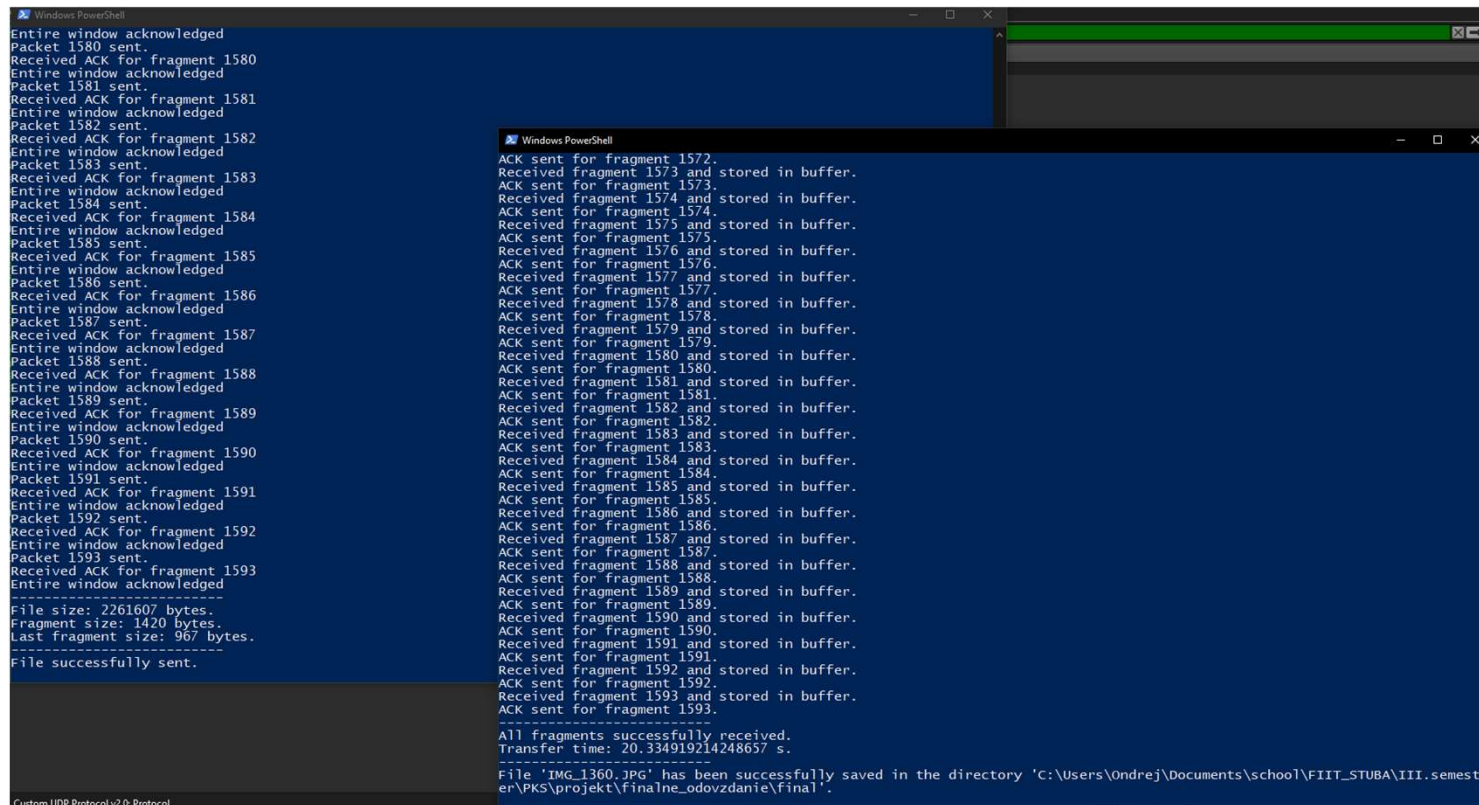
Inicializácia posielanie ~2MB file-u



Detail UI: informácia o dokončení posielania okna

```
Packet 1550 sent.  
Received ACK for fragment 1550  
Entire window acknowledged  
  
Sending window 32/32. Packets in window: 43.  
-----  
Packet 1551 sent.  
Received ACK for fragment 1551  
Entire window acknowledged  
Packet 1552 sent.  
Received ACK for fragment 1552  
Entire window acknowledged  
Packet 1553 sent.  
Received ACK for fragment 1553  
Entire window acknowledged
```

Posielanie packetov file-u



```
Windows PowerShell
Entire window acknowledged
Packet 1580 sent.
Received ACK for fragment 1580
Entire window acknowledged
Packet 1581 sent.
Received ACK for fragment 1581
Entire window acknowledged
Packet 1582 sent.
Received ACK for fragment 1582
Entire window acknowledged
Packet 1583 sent.
Received ACK for fragment 1583
Entire window acknowledged
Packet 1584 sent.
Received ACK for fragment 1584
Entire window acknowledged
Packet 1585 sent.
Received ACK for fragment 1585
Entire window acknowledged
Packet 1586 sent.
Received ACK for fragment 1586
Entire window acknowledged
Packet 1587 sent.
Received ACK for fragment 1587
Entire window acknowledged
Packet 1588 sent.
Received ACK for fragment 1588
Entire window acknowledged
Packet 1589 sent.
Received ACK for fragment 1589
Entire window acknowledged
Packet 1590 sent.
Received ACK for fragment 1590
Entire window acknowledged
Packet 1591 sent.
Received ACK for fragment 1591
Entire window acknowledged
Packet 1592 sent.
Received ACK for fragment 1592
Entire window acknowledged
Packet 1593 sent.
Received ACK for fragment 1593
Entire window acknowledged
-----
File size: 2261607 bytes.
Fragment size: 1420 bytes.
Last fragment size: 967 bytes.
-----
File successfully sent.

Custom UDP Protocol v2.0 Protocol

Windows PowerShell
ACK sent for fragment 1572.
Received fragment 1573 and stored in buffer.
ACK sent for fragment 1573.
Received fragment 1574 and stored in buffer.
ACK sent for fragment 1574.
Received fragment 1575 and stored in buffer.
ACK sent for fragment 1575.
Received fragment 1576 and stored in buffer.
ACK sent for fragment 1576.
Received fragment 1577 and stored in buffer.
ACK sent for fragment 1577.
Received fragment 1578 and stored in buffer.
ACK sent for fragment 1578.
Received fragment 1579 and stored in buffer.
ACK sent for fragment 1579.
Received fragment 1580 and stored in buffer.
ACK sent for fragment 1580.
Received fragment 1581 and stored in buffer.
ACK sent for fragment 1581.
Received fragment 1582 and stored in buffer.
ACK sent for fragment 1582.
Received fragment 1583 and stored in buffer.
ACK sent for fragment 1583.
Received fragment 1584 and stored in buffer.
ACK sent for fragment 1584.
Received fragment 1585 and stored in buffer.
ACK sent for fragment 1585.
Received fragment 1586 and stored in buffer.
ACK sent for fragment 1586.
Received fragment 1587 and stored in buffer.
ACK sent for fragment 1587.
Received fragment 1588 and stored in buffer.
ACK sent for fragment 1588.
Received fragment 1589 and stored in buffer.
ACK sent for fragment 1589.
Received fragment 1590 and stored in buffer.
ACK sent for fragment 1590.
Received fragment 1591 and stored in buffer.
ACK sent for fragment 1591.
Received fragment 1592 and stored in buffer.
ACK sent for fragment 1592.
Received fragment 1593 and stored in buffer.
ACK sent for fragment 1593.
-----
All fragments successfully received.
Transfer time: 20.334919214248657 s.

File 'IMG_1360.JPG' has been successfully saved in the directory 'C:\Users\Ondrej\Documents\schoo1\FIIT_STUBA\III.semest
er\PKS\projekt\finalne_odovzanie\final'.
```

Posielanie File-u, detail na prvý packet (filename packet)

The image shows a Wireshark packet capture window titled "customudp". The packet list on the left shows 32 packets, all of type CUSTOMUDP, sent from 147.175.161.113 to 147.175.161.113. The packet details pane on the right shows the structure of the first packet (No. 3):

- Frame 105: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface \\Device\\NPF_{...}, id 0
- Null/loopback
- Internet Protocol Version 4, Src: 147.175.161.113, Dst: 147.175.161.113
- User Datagram Protocol, Src Port: 64502, Dst Port: 55555
- Custom UDP Protocol Data
 - Flags: 0x000c
 - Message Type: Fragmented Data
 - UDP Coloring Field: Fragmented_Data
 - Fragment Offset: 0
 - ACK Number: 0
 - Data: 494d475f313336302e4a5047
 - CRC16 Checksum: 0x3045
 - Details
 - Flag Details
 - Message Type: Fragmented Data
 - Decoded Data: IMG_1360.JPG

The packet bytes pane on the right shows the raw data of the packet, including the file name "IMG_1360.JPG" in the data field.

Keep alive počas posielania file-u

No.	Time	Source	Destination	Protocol	Length	Info
416	35.283707	147.175.161.113	147.175.161.113	CUSTOMUDP	1464	64502 → 55555 Len=1432
417	35.285629	147.175.161.113	147.175.161.113	CUSTOMUDP	44	64501 → 55556 Len=12
418	35.294587	147.175.161.113	147.175.161.113	CUSTOMUDP	1464	64502 → 55555 Len=1432
419	35.296963	147.175.161.113	147.175.161.113	CUSTOMUDP	44	64501 → 55556 Len=12
420	35.305422	147.175.161.113	147.175.161.113	CUSTOMUDP	1464	64502 → 55555 Len=1432
421	35.308307	147.175.161.113	147.175.161.113	CUSTOMUDP	44	64501 → 55556 Len=12
422	35.322446	147.175.161.113	147.175.161.113	CUSTOMUDP	1464	64502 → 55555 Len=1432
423	35.324544	147.175.161.113	147.175.161.113	CUSTOMUDP	44	64501 → 55556 Len=12
424	35.333535	147.175.161.113	147.175.161.113	CUSTOMUDP	1464	64502 → 55555 Len=1432
425	35.335738	147.175.161.113	147.175.161.113	CUSTOMUDP	44	64501 → 55556 Len=12
426	35.346938	147.175.161.113	147.175.161.113	CUSTOMUDP	1464	64502 → 55555 Len=1432
427	35.349005	147.175.161.113	147.175.161.113	CUSTOMUDP	44	64501 → 55556 Len=12
428	35.349843	147.175.161.113	147.175.161.113	CUSTOMUDP	44	64501 → 55556 Len=12
429	35.349870	147.175.161.113	147.175.161.113	CUSTOMUDP	44	64502 → 55555 Len=12
430	35.357395	147.175.161.113	147.175.161.113	CUSTOMUDP	1464	64502 → 55555 Len=1432
431	35.359329	147.175.161.113	147.175.161.113	CUSTOMUDP	44	64501 → 55556 Len=12
432	35.369107	147.175.161.113	147.175.161.113	CUSTOMUDP	1464	64502 → 55555 Len=1432
433	35.371385	147.175.161.113	147.175.161.113	CUSTOMUDP	44	64501 → 55556 Len=12
434	35.381507	147.175.161.113	147.175.161.113	CUSTOMUDP	1464	64502 → 55555 Len=1432
435	35.383443	147.175.161.113	147.175.161.113	CUSTOMUDP	44	64501 → 55556 Len=12
436	35.392368	147.175.161.113	147.175.161.113	CUSTOMUDP	1464	64502 → 55555 Len=1432
437	35.395868	147.175.161.113	147.175.161.113	CUSTOMUDP	44	64501 → 55556 Len=12
438	35.403130	147.175.161.113	147.175.161.113	CUSTOMUDP	1464	64502 → 55555 Len=1432
439	35.405569	147.175.161.113	147.175.161.113	CUSTOMUDP	44	64501 → 55556 Len=12
440	35.413873	147.175.161.113	147.175.161.113	CUSTOMUDP	1464	64502 → 55555 Len=1432
441	35.415816	147.175.161.113	147.175.161.113	CUSTOMUDP	44	64501 → 55556 Len=12
442	35.424667	147.175.161.113	147.175.161.113	CUSTOMUDP	1464	64502 → 55555 Len=1432
443	35.427015	147.175.161.113	147.175.161.113	CUSTOMUDP	44	64501 → 55556 Len=12
444	35.435327	147.175.161.113	147.175.161.113	CUSTOMUDP	1464	64502 → 55555 Len=1432

Inicializácia umelej chyby + setup posialnia druhého file-u

```
6
Introduce Artificial CRC Error
Enter the packet ID (fragment number) you want to corrupt: 57
Packet 57 will have its CRC corrupted.
Now, please proceed to send your message or file.
Note: The CRC of packet with fragment number 57 will be corrupted.
2
Enter the absolute path to the file you want to send:
C:\Users\Ondrej\Downloads\civ.png
```

Detail NACK a preposielanie chybného packetu

```
Received ACK for fragment 49
Entire window acknowledged
Packet 50 sent.
Received ACK for fragment 50
Entire window acknowledged

Sending window 2/2. Packets in window: 10.
-----
Packet 51 sent.
Received ACK for fragment 51
Entire window acknowledged
Packet 52 sent.
Received ACK for fragment 52
Entire window acknowledged
Packet 53 sent.
Received ACK for fragment 53
Entire window acknowledged
Packet 54 sent.
Received ACK for fragment 54
Entire window acknowledged
Packet 55 sent.
Received ACK for fragment 55
Entire window acknowledged
Packet 56 sent.
Received ACK for fragment 56
Entire window acknowledged
Packet 57 sent.
Received NACK for fragment 57
Packet 57 lost or NACKed, regenerating and resending
Packet 58 sent.
Received ACK for fragment 57
Packet 58 lost or NACKed, regenerating and resending
Packet 59 sent.
Received ACK for fragment 58
Packet 59 lost or NACKed, regenerating and resending
Packet 60 sent.
Received ACK for fragment 59
Packet 60 lost or NACKed, regenerating and resending
-----
File size: 84284 bytes.
Fragment size: 1420 bytes.
Last fragment size: 504 bytes.
-----
File successfully sent.
Received ACK for fragment 60
Entire window acknowledged

-----
Received fragment 42 and stored in buffer.
ACK sent for fragment 42.
Received fragment 43 and stored in buffer.
ACK sent for fragment 43.
Received fragment 44 and stored in buffer.
ACK sent for fragment 44.
Received fragment 45 and stored in buffer.
ACK sent for fragment 45.
Received fragment 46 and stored in buffer.
ACK sent for fragment 46.
Received fragment 47 and stored in buffer.
ACK sent for fragment 47.
Received fragment 48 and stored in buffer.
ACK sent for fragment 48.
Received fragment 49 and stored in buffer.
ACK sent for fragment 49.
Received fragment 50 and stored in buffer.
ACK sent for fragment 50.
Received fragment 51 and stored in buffer.
ACK sent for fragment 51.
Received fragment 52 and stored in buffer.
ACK sent for fragment 52.
Received fragment 53 and stored in buffer.
ACK sent for fragment 53.
Received fragment 54 and stored in buffer.
ACK sent for fragment 54.
Received fragment 55 and stored in buffer.
ACK sent for fragment 55.
Received fragment 56 and stored in buffer.
ACK sent for fragment 56.
Checksum invalid for received packet.
NACK sent for fragment 57.
NACK sent for fragment 57.
Received fragment 57 and stored in buffer.
ACK sent for fragment 57.
Received fragment 58 and stored in buffer.
ACK sent for fragment 58.
Received fragment 59 and stored in buffer.
ACK sent for fragment 59.
Received fragment 60 and stored in buffer.
ACK sent for fragment 60.
-----
All fragments successfully received.
Transfer time: 0.7688682079315186 s.
-----
File 'civ.png' has been successfully saved in the directory 'C:\Users\Ondrej\Documents\school\FIIT_STUBA\III.semester\PK
S\projekt\finalne odovzdanie\final'.
Received fragment 60 and stored in buffer.
ACK sent for fragment 60.
```

Záver posielania umelej chyby - wireshark

The image shows a Wireshark packet capture of a network traffic. The top pane displays a list of 4673 packets, all of which are Custom UDP packets from 147.175.161.113 to 147.175.161.113. The selected packet is packet 4560, which is a FIN-ACK packet with sequence number 4560. The packet details pane shows the following information:

- Frame 4560: 44 bytes on wire (352 bits), 44 bytes captured (352 bits) on interface \Device\NPF_{...}_loopback, id 0
- Null/Loopback
- Internet Protocol Version 4, Src: 147.175.161.113, Dst: 147.175.161.113
- User Datagram Protocol, Src Port: 64502, Dst Port: 55555
- Custom UDP Protocol Data
 - Flags: 0x0050
 - Message Type: FIN-ACK
 - UDP Coloring Field: FIN-ACK
 - Fragment Offset: 0
 - ACK Number: 0
 - CRC16 Checksum: 0xed1e
- Details
 - Flag Details
 - ACK
 - FIN
 - Message Type: Finish Acknowledgment (FIN-ACK) Packet

The packet bytes pane shows the raw data of the packet, including the Ethernet II header, Internet Protocol Version 4 header, User Datagram Protocol header, and the Custom UDP Protocol Data.

Uzavretie spojenia

```
PS C:\Users\Ondrej\Documents\school\FIIT_STUBA\III.semester\PKS\projekt\finalne_odovzдание\final> py .\final.py
Your IP address: 147.175.161.113
Enter your listening port (value between 50,000 - 60,000): 55556
Enter the recipient's IP address: 147.175.161.113
Enter the target port (value between 50,000 - 60,000): 55555

Source IP: 147.175.161.113
Listening port: 55556

Destination IP: 147.175.161.113
Target port: 55555

Default file save path: C:\Users\Ondrej\Documents\school\FIIT_STUBA\III.semester\PKS\projekt\finalne_odovzдание\final
Press Enter after starting the other side to continue.

=====
SYN received.
SYN-ACK packet sent.
ACK packet received.
-----
3-way handshake completed.
=====

Connection established with 147.175.161.113
Listening on port 55556
Sending to port 55555
=====

1. Send a text message
2. Send a file
3. Change maximum fragment size
4. Change file save path
5. Request connection termination
6. Introduce artificial CRC error
=====
Enter command:
Received message:
hello
ACK sent for fragment 0.
1
Enter your message:
hi
Message sent.

=====
PS C:\Users\Ondrej\Documents\school\FIIT_STUBA\III.semester\PKS\projekt\finalne_odovzдание\final> py .\final.py
Your IP address: 147.175.161.113
Enter your listening port (value between 50,000 - 60,000): 55555
Enter the recipient's IP address: 147.175.161.113
Enter the target port (value between 50,000 - 60,000): 55556

Source IP: 147.175.161.113
Listening port: 55555

Destination IP: 147.175.161.113
Target port: 55556

Default file save path: C:\Users\Ondrej\Documents\school\FIIT_STUBA\III.semester\PKS\projekt\finalne_odovzдание\final
Press Enter after starting the other side to continue.

=====
SYN packet sent.
SYN-ACK received.
ACK packet sent.
-----
3-way handshake completed.
=====

Connection established with 147.175.161.113
Listening on port 55555
Sending to port 55556
=====

1. Send a text message
2. Send a file
3. Change maximum fragment size
4. Change file save path
5. Request connection termination
6. Introduce artificial CRC error
=====
Enter command: 1
Enter your message:
hello
Message sent.

Received message:
hi
ACK sent for fragment 0.
```

Ďakujem za pozornosť

