

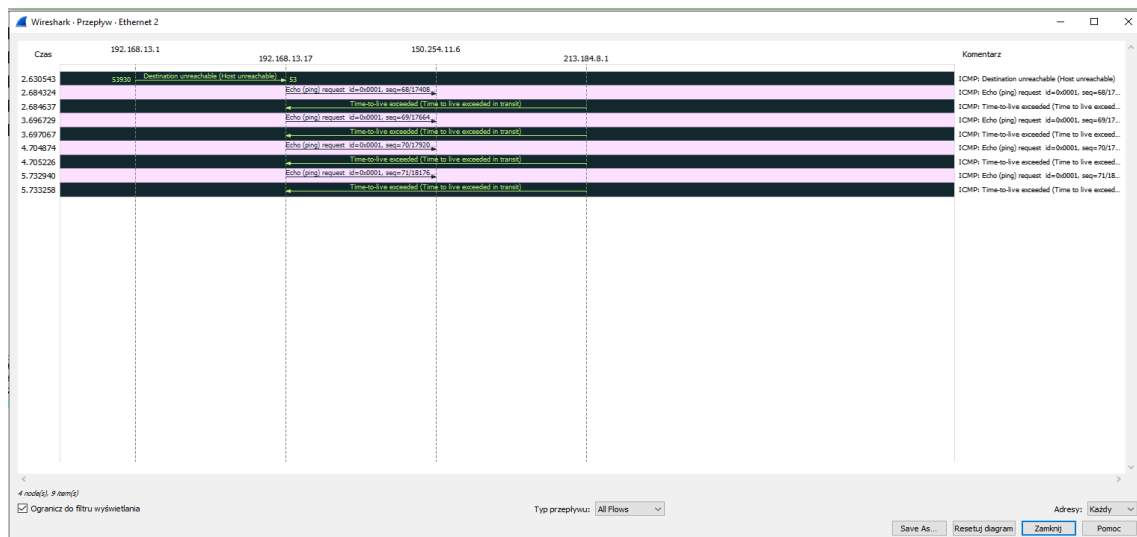
02/04/2023

4.1

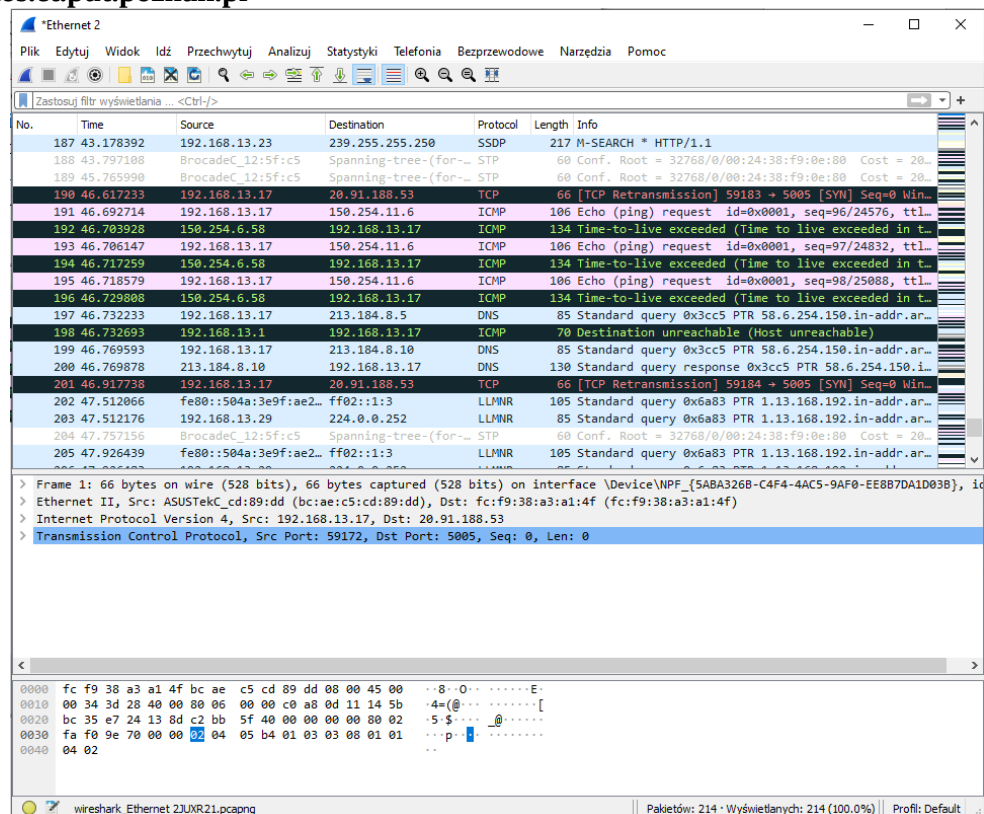
- d) Adres IPv4 jest adresem logicznym nadawanym każdemu hostowi w sieci. Adres MAC jest adresem fizycznym urządzenia sieciowego, jest nadawany przez producenta na etapie produkcji.
- e) f) Parametr TTL (ang. Time To Live) definiuje jak długo pakiet danych może krążyć w sieci przechodząc od jednego routera do drugiego.
TTL = 128
- g) Ramka ethernetowa nie zawiera pola o podobnym znaczeniu. Czas jej życia wynosi ok. 10 minut, jeżeli została skutecznie przesłana i nie zawierała błędów. Jeżeli natomiast zawierała błędy, nie została dostarczona do adresata, tylko od razu utracona. Do weryfikacji błędów w ramce ethernetowej służy pole „suma kontrolna”. Pole to pośrednio decyduje o żywotności ramki.
- h) Komputer wysłał 4 wiadomości, a otrzymał 5. Otrzymane wiadomości były typu „Time-to-live exceeded (Time to live exceeded in transit)”. Parametr TTL przyjmuje wartość 2 (poprzednio było to 128). Wniosek jest taki, że dopisanie opcji „-i 2” na końcu polecenia „ping” powoduje skrócenie czasu życia pakietu do zadanej wartości, w naszym przypadku do 2.

i)

4.2



tracert helios.et.put.poznan.pl



icmp

No.	Time	Source	Destination	Protocol	Length	Info
124	29.859982	192.168.13.17	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=87/22272, ttl...
125	29.870500	212.191.224.18	192.168.13.17	ICMP	70	Time-to-live exceeded (Time to live exceeded in t...
126	29.872624	192.168.13.17	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=88/22528, ttl...
127	29.884403	212.191.224.18	192.168.13.17	ICMP	70	Time-to-live exceeded (Time to live exceeded in t...
128	29.885670	192.168.13.17	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=89/22784, ttl...
129	29.897010	212.191.224.18	192.168.13.17	ICMP	70	Time-to-live exceeded (Time to live exceeded in t...
131	29.899759	192.168.13.1	192.168.13.17	ICMP	70	Destination unreachable (Host unreachable)
144	35.470294	192.168.13.17	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=90/23040, ttl...
145	35.481257	150.254.163.27	192.168.13.17	ICMP	70	Time-to-live exceeded (Time to live exceeded in t...
146	35.483410	192.168.13.17	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=91/23296, ttl...
147	35.494285	150.254.163.27	192.168.13.17	ICMP	70	Time-to-live exceeded (Time to live exceeded in t...
148	35.496254	192.168.13.17	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=92/23552, ttl...
149	35.507041	150.254.163.27	192.168.13.17	ICMP	70	Time-to-live exceeded (Time to live exceeded in t...
151	35.509743	192.168.13.1	192.168.13.17	ICMP	70	Destination unreachable (Host unreachable)
170	41.080778	192.168.13.17	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=93/23808, ttl...
171	41.092275	150.254.4.68	192.168.13.17	ICMP	134	Time-to-live exceeded (Time to live exceeded in t...
172	41.094301	192.168.13.17	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=94/24064, ttl...
173	41.105544	150.254.4.68	192.168.13.17	ICMP	134	Time-to-live exceeded (Time to live exceeded in t...
174	41.107369	192.168.13.17	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=95/24320, ttl...
175	41.118101	150.254.4.68	192.168.13.17	ICMP	134	Time-to-live exceeded (Time to live exceeded in t...
177	41.120959	192.168.13.1	192.168.13.17	ICMP	70	Destination unreachable (Host unreachable)
191	46.692714	192.168.13.17	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=96/24576, ttl...
192	46.703928	150.254.6.58	192.168.13.17	ICMP	134	Time-to-live exceeded (Time to live exceeded in t...
193	46.706147	192.168.13.17	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=97/24832, ttl...
194	46.717259	150.254.6.58	192.168.13.17	ICMP	134	Time-to-live exceeded (Time to live exceeded in t...
195	46.718579	192.168.13.17	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=98/25088, ttl...
196	46.729808	150.254.6.58	192.168.13.17	ICMP	134	Time-to-live exceeded (Time to live exceeded in t...
198	46.732693	192.168.13.1	192.168.13.17	ICMP	70	Destination unreachable (Host unreachable)
211	52.332812	192.168.13.17	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=99/25344, ttl...
213	55.449943	150.254.6.58	192.168.13.17	ICMP	134	Destination unreachable (Host unreachable)

> Frame 4: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{5ABA326B-C4F4-4AC5-9AF0-EE8B7DA1D03B}

> Ethernet II, Src: ASUSTekC_cd:89:dd (bc:ae:c5:cd:89:dd), Dst: fc:f9:38:a3:a1:4f (fc:f9:38:a3:a1:4f)

> Internet Protocol Version 4, Src: 192.168.13.17, Dst: 150.254.11.6

```

0000  fc f9 38 a3 a1 4f bc ae c5 cd 89 dd 08 00 45 00  ..8..0...E..
0010  00 5c 98 49 00 00 01 01 00 00 c0 a8 0d 11 96 fe  .\..I...A....
0020  0b 06 08 00 f7 b6 00 01 00 48 00 00 00 00 00 00  .H.....
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0050  00 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 00  .....

```

Internet Control Message Protocol: Protocol | Pakietów: 214 · Wyświetlanych: 71 (33.2%) · Porzuconych: 0 (0.0%) | Profil: Default

- Komputer wysłał 28 wiadomości typu „Echo (ping) request ...”
- Komputer odebrał 43 wiadomości typu: „Time-to-live exceeded (Time to live exceeded in transit)” oraz „Destination unreachable (Host unreachable)” oraz „Destination unreachable (Port unreachable)”.
- Ethernet II, Src: ASUSTekC_cd:89:dd (bc:ae:c5:cd:89:dd), Dst: fc:f9:38:a3:a1:4f (fc:f9:38:a3:a1:4f); Internet Protocol Version 4, Src: 192.168.13.17, Dst: 150.254.11.6
- TTL zaczyna się od wartości 1 a kończy się na wartości 10. Najpierw komputer wysłał 3 wiadomości z TTL=1, potem 3 wiadomości z TTL=2 itd.

Czas	192.168.13.17	150.254.11.6	192.168.13.1	213.184.8.1	10.1.3.1	10.1.1.194	Komentarz
7.481562	137			137			ICMP: Destination unreachable (Port unreachable)
8.993781	137			137			ICMP: Destination unreachable (Port unreachable)
10.497877	137			137			ICMP: Destination unreachable (Port unreachable)
13.024003							ICMP: Echo (ping) request id=0x0001, seq=78/1996
13.024854							ICMP: Time-to-live exceeded (Time to live exceeded in transit)
13.025483							ICMP: Time-to-live exceeded (Time to live exceeded in transit)
13.025742							ICMP: Echo (ping) request id=0x0001, seq=79/2022
13.026572							ICMP: Time-to-live exceeded (Time to live exceeded in transit)
13.027152							ICMP: Time-to-live exceeded (Time to live exceeded in transit)
13.027346							ICMP: Echo (ping) request id=0x0001, seq=80/2048
13.028200							ICMP: Time-to-live exceeded (Time to live exceeded in transit)
13.028543							ICMP: Time-to-live exceeded (Time to live exceeded in transit)
13.030836							ICMP: Destination unreachable (Host unreachable)
18.635569							ICMP: Echo (ping) request id=0x0001, seq=81/2073
18.637377							ICMP: Time-to-live exceeded (Time to live exceeded in transit)
18.639439							ICMP: Echo (ping) request id=0x0001, seq=82/2099
18.643760							ICMP: Time-to-live exceeded (Time to live exceeded in transit)
18.645776							ICMP: Echo (ping) request id=0x0001, seq=83/2124
18.647570							ICMP: Time-to-live exceeded (Time to live exceeded in transit)
18.650384							ICMP: Destination unreachable (Host unreachable)
24.233173							ICMP: Echo (ping) request id=0x0001, seq=84/2150
24.254341							ICMP: Time-to-live exceeded (Time to live exceeded in transit)
24.256452							ICMP: Echo (ping) request id=0x0001, seq=85/2176
24.289677							ICMP: Time-to-live exceeded (Time to live exceeded in transit)
24.291729							ICMP: Echo (ping) request id=0x0001, seq=86/2201
24.303253							ICMP: Time-to-live exceeded (Time to live exceeded in transit)
24.306129							ICMP: Destination unreachable (Host unreachable)
29.859982							ICMP: Echo (ping) request id=0x0001, seq=87/2227
29.870500							ICMP: Time-to-live exceeded (Time to live exceeded in transit)

5.3 Analiza działania polecenia pathping

```
C:\Users\local>pathping helios.et.put.poznan.pl

Tracing route to helios.et.put.poznan.pl [150.254.11.6]
over a maximum of 30 hops:
  0  DESKTOP-718DGH2.wmii.local [192.168.13.17]
  1  192.168.13.1
  2  213.184.8.1
  3  10.1.3.1
  4  10.1.1.194
  5  z-olsztyna.poznan-gw3.10Gb.rtr.pionier.gov.pl [212.191.224.41]
  6  z-poznan-gw3.poznan.10Gb.rtr.pionier.gov.pl [212.191.224.18]
  7  pp-piotrowo-gw.man.poznan.pl [150.254.163.27]
  8  PUTNET-FW-V.put.poznan.pl [150.254.4.68]
  9  PUTNET-X450A-A3-2.put.poznan.pl [150.254.6.58]
 10  PUTNET-X450A-A3-2.put.poznan.pl [150.254.6.58]  reports: Destination host unreachable.

Computing statistics for 250 seconds...

Hop  RTT      Source to Here   This Node/Link   Address
  0                               DESKTOP-718DGH2.wmii.local [192.168.13.17]
  1    0ms      0/ 100 = 0%      0/ 100 = 0%      192.168.13.1
  2    2ms      0/ 100 = 0%      0/ 100 = 0%      213.184.8.1
  3    ---     100/ 100 =100%   100/ 100 =100%   10.1.3.1
  4    ---     100/ 100 =100%   100/ 100 =100%   10.1.1.194
  5   11ms      0/ 100 = 0%      0/ 100 = 0%      z-olsztyna.poznan-gw3.10Gb.rtr.pionier.gov.pl [212.191.224.41]
  6   12ms      0/ 100 = 0%      0/ 100 = 0%      z-poznan-gw3.poznan.10Gb.rtr.pionier.gov.pl [212.191.224.18]
  7   12ms      0/ 100 = 0%      0/ 100 = 0%      pp-piotrowo-gw.man.poznan.pl [150.254.163.27]
  8   11ms      0/ 100 = 0%      0/ 100 = 0%      PUTNET-FW-V.put.poznan.pl [150.254.4.68]
  9   11ms      0/ 100 = 0%      0/ 100 = 0%      PUTNET-X450A-A3-2.put.poznan.pl [150.254.6.58]
 10    ---     100/ 100 =100%   0/ 100 = 0%      DESKTOP-718DGH2 [0.0.0.0]

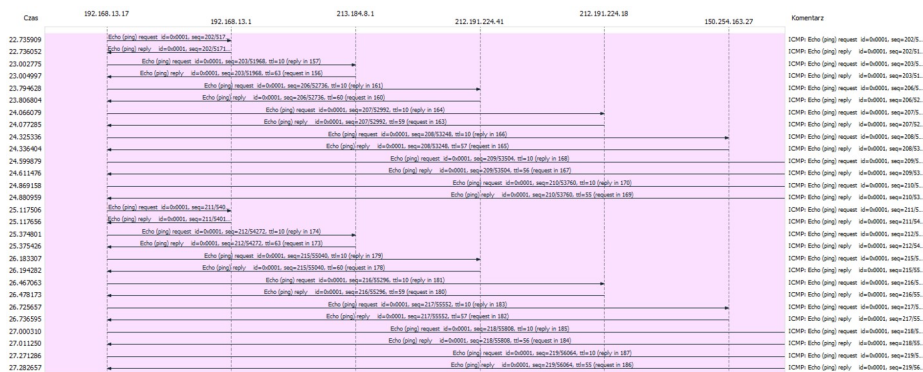
Trace complete.

C:\Users\local>
```

No.	Time	Source	Destination	Protocol	Length	Info
3	1.382780	192.168.13.17	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=192/49152, ttl=1 (no res...
4	1.382905	192.168.13.1	192.168.13.17	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
24	5.909955	192.168.13.17	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=193/49408, ttl=2 (no res...
25	5.910269	213.184.8.1	192.168.13.17	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
29	5.912239	213.184.8.1	192.168.13.17	ICMP	70	Destination unreachable (Port unreachable)
35	7.410478	213.184.8.1	192.168.13.17	ICMP	70	Destination unreachable (Port unreachable)
41	8.916842	213.184.8.1	192.168.13.17	ICMP	70	Destination unreachable (Port unreachable)
49	10.418883	192.168.13.17	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=194/49664, ttl=3 (no res...
50	10.419698	10.1.3.1	192.168.13.17	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
51	10.419959	10.1.3.1	192.168.13.17	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
61	14.949689	192.168.13.17	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=195/49920, ttl=4 (no res...
62	14.951327	10.1.1.194	192.168.13.17	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
74	18.964063	192.168.13.1	192.168.13.17	ICMP	70	Destination unreachable (Host unreachable)
77	19.488244	192.168.13.17	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=196/50176, ttl=5 (no res...
78	19.489424	212.191.224.41	192.168.13.17	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
79	19.502758	192.168.13.17	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=197/50432, ttl=6 (no res...
80	19.513367	212.191.224.18	192.168.13.17	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
81	19.517938	192.168.13.17	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=198/50688, ttl=7 (no res...
82	19.528709	150.254.163.27	192.168.13.17	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
83	19.532061	192.168.13.17	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=199/50944, ttl=8 (no res...
84	19.543664	150.254.4.68	192.168.13.17	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
85	19.547532	192.168.13.17	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=200/51200, ttl=9 (no res...
86	19.558715	150.254.6.58	192.168.13.17	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
87	19.562557	192.168.13.17	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=201/51456, ttl=10 (no re...
93	20.858785	192.168.13.1	192.168.13.17	ICMP	70	Destination unreachable (Host unreachable)
153	22.728994	150.254.6.58	192.168.13.17	ICMP	134	Destination unreachable (Host unreachable)
154	22.735909	192.168.13.17	192.168.13.1	ICMP	106	Echo (ping) request id=0x0001, seq=202/51712, ttl=10 (reply...
155	22.736052	192.168.13.1	192.168.13.17	ICMP	106	Echo (ping) reply id=0x0001, seq=202/51712, ttl=64 (reque...
156	23.002775	192.168.13.17	213.184.8.1	ICMP	106	Echo (ping) request id=0x0001, seq=203/51968, ttl=10 (reply...
157	23.004997	213.184.8.1	192.168.13.17	ICMP	106	Echo (ping) reply id=0x0001, seq=203/51968, ttl=63 (reque...
158	23.260825	192.168.13.17	10.1.3.1	ICMP	106	Echo (ping) request id=0x0001, seq=204/52224, ttl=10 (no re...

- Komputer wysłał ok. 800 wiadomości typu „Echo (ping) request ...”
- Komputer otrzymał 25 wiadomości typu: „Destination unreachable (Host unreachable)” lub „Destination unreachable (Port unreachable)” oraz ok. 800 wiadomości typu: „Echo (ping) reply ...”
W sumie wiadomości wysłanych i odebranych (ICMP) było: 1635
- Dla wiadomości typu „Echo (ping) request ...” TTL rośnie od 1 do 10 i potem się nie zmienia. Dla wiadomości typu „Echo (ping) reply ...” oscyluje w okolicach 60
- Najpierw wysyłany jest „Echo (ping) request ...”, potem otrzymywany jest „Echo (ping) reply ...”, na podstawie wysłanych i otrzymanych wiadomości wyznaczana jest optymalna trasa od urządzenia, które wysyła request do urządzenia docelowego.
-

e)



5.4 Analiza działania protokołów telnet oraz ssh

Nie udało się połączyć z żadnym serwerem za pomocą protokołu telnet (ani ze wskazanym w podręczniku serwerem helios.et.put.poznan.pl , ani z naszym uczelnianym orfi.uwm.edu.pl).

SSH (orfi.uwm.edu.pl)

*Ethernet 2

Plik Edytuj Widok Idź Przechwytyj Analizuj Statystyki Telefonia Bezprzewodowe Narzędzia Pomoc

ssh

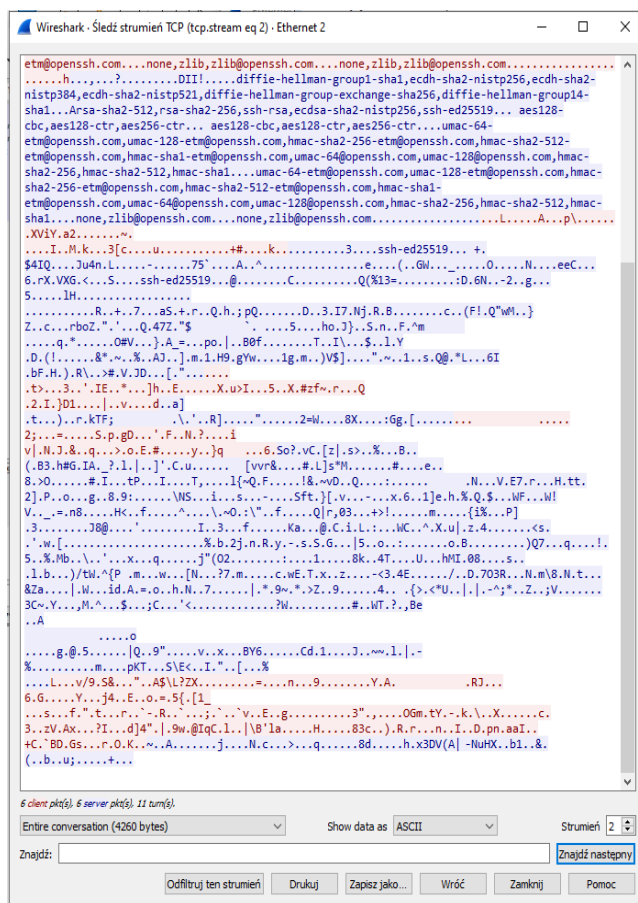
No.	Time	Source	Destination	Protocol	Length	Info
8	0.970313	192.168.13.17	213.184.8.9	SSHv2	82	Client: Protocol (SSH-2.0-PuTTY_Release_0.76)
10	0.980439	213.184.8.9	192.168.13.17	SSHv2	86	Server: Protocol (SSH-2.0-OpenSSH_8.4p1 Debian-5)
11	0.984304	192.168.13.17	213.184.8.9	SSHv2	1310	Client: Key Exchange Init
12	0.985078	213.184.8.9	192.168.13.17	SSHv2	870	Server: Key Exchange Init
13	0.990730	192.168.13.17	213.184.8.9	SSHv2	134	Client: Elliptic Curve Diffie-Hellman Key Exchange Init
15	0.995082	213.184.8.9	192.168.13.17	SSHv2	582	Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys,...
16	1.014116	192.168.13.17	213.184.8.9	SSHv2	134	Client: New Keys, Encrypted packet (len=64)
17	1.014791	213.184.8.9	192.168.13.17	SSHv2	118	Server: Encrypted packet (len=64)
27	6.075406	192.168.13.17	213.184.8.9	SSHv2	134	Client: Encrypted packet (len=80)
28	6.096832	213.184.8.9	192.168.13.17	SSHv2	998	Server: Encrypted packet (len=944)
36	10.107349	192.168.13.17	213.184.8.9	SSHv2	326	Client: Encrypted packet (len=272)
52	12.698845	213.184.8.9	192.168.13.17	SSHv2	134	Server: Encrypted packet (len=80)

> Frame 8: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \Device\NPF_{5ABA326B-C4F4-4AC5-9AF0-EE8B7DA1D03B}, id 0
> Ethernet II, Src: ASUSTekCd:89:dd (bc:ae:c5:cd:89:dd), Dst: fc:f9:38:a3:a1:4f (fc:f9:38:a3:a1:4f)
> Internet Protocol Version 4, Src: 192.168.13.17, Dst: 213.184.8.9
> Transmission Control Protocol, Src Port: 60425, Dst Port: 22, Seq: 1, Ack: 1, Len: 28
> SSH Protocol

0000 fc f9 38 a3 a1 4f bc ae c5 cd 89 dd 00 00 45 00 ..8..0.....E.
0010 00 44 f7 ad 40 00 80 06 00 00 c0 a8 0d 11 d5 b8 .D..@.....

SSH Protocol: Protocol

Pakietów: 61 • Wyświetlanych: 12 (19.7%) • Porzuconych: 0 (0.0%) | Profil: Default



a) przedstawia zapis konwersacji pomiędzy naszym urządzeniem a serwerem, z którym próbujemy się połączyć.

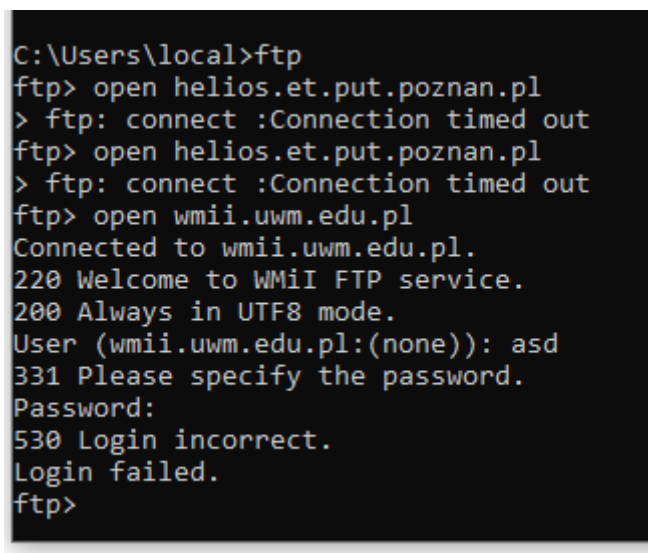
b) SSH (ang. Secure Shell) – protokół stosowany przez administratorów do zarządzania serwerami znajdującymi się często w odległych od miejsca pracy lokalizacjach. Protokół SSH jest następcą protokołu TELNET (najstarszy protokół warstwy aplikacji, **nie szyfruje** komunikacji między klientem a serwerem)

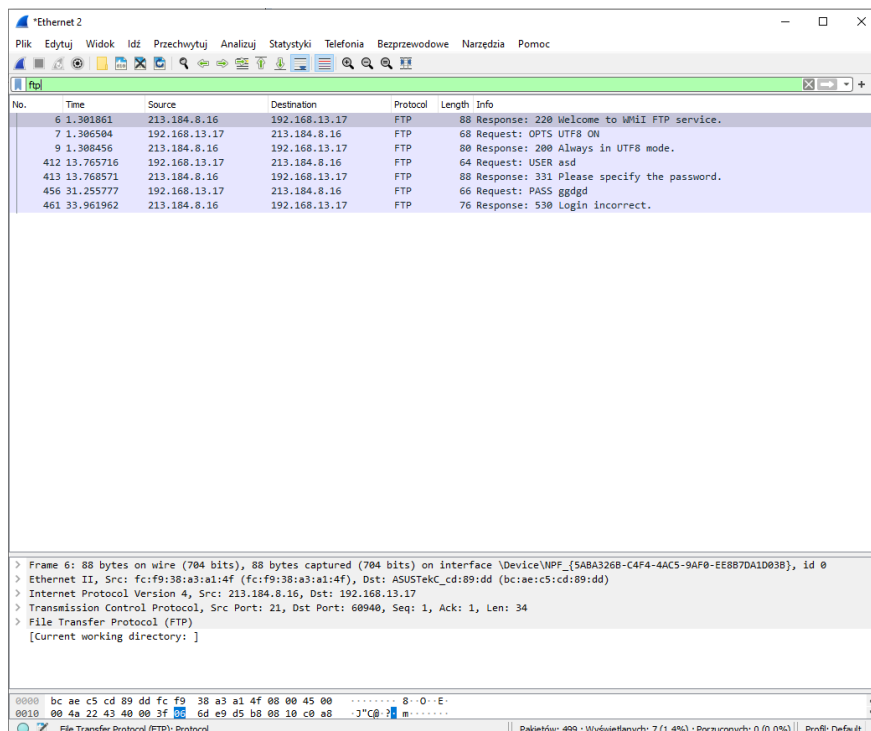
c) login i hasło przesyłane są w sposób zaszyfrowany.

d) Bardziej bezpieczny sposób łączenia z serwerem to połączenie za pomocą protokołu SSH, ponieważ szyfruje on dane wymieniane między klientem a serwerem.

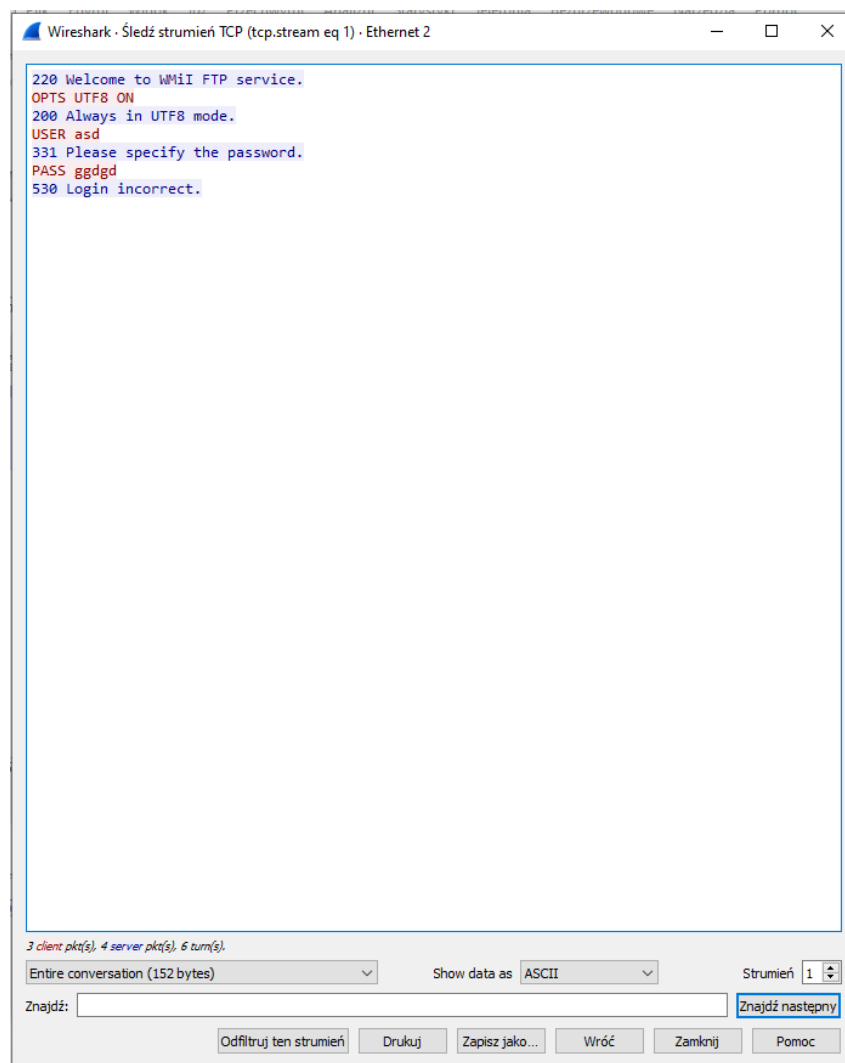
5.5 Analiza działania protokołu FTP

open wmii.uwm.edu.pl





No.	Time	Source	Destination	Protocol	Length	Info
6	1.381861	213.184.8.16	192.168.13.17	FTP	88	Response: 220 Welcome to WMI FTP service.
7	1.386594	192.168.13.17	213.184.8.16	FTP	68	Request: OPTS UTF8 ON
9	1.388456	213.184.8.16	192.168.13.17	FTP	80	Response: 200 Always in UTF8 mode.
412	13.765716	192.168.13.17	213.184.8.16	FTP	64	Request: USER asd
413	13.768571	213.184.8.16	192.168.13.17	FTP	88	Response: 331 Please specify the password.
456	31.255777	192.168.13.17	213.184.8.16	FTP	66	Request: PASS ggddg
461	35.961962	213.184.8.16	192.168.13.17	FTP	76	Response: 530 Login incorrect.



```

220 Welcome to WMI FTP service.
OPTS UTF8 ON
200 Always in UTF8 mode.
USER asd
331 Please specify the password.
PASS ggddg
530 Login incorrect.
  
```

a) Po wyborze opcji Follow TCP Stream (Śledź strumień TCP) program przedstawia informacje w postaci niezaszyfrowanej (informacje takie jak login i hasło oraz odpowiedzi serwera).

b) Protokół FTP (ang. File Transfer Protocol) jest protokołem nieszyfrowanym.

c) Login i hasło nie jest zaszyfrowane.

Czy istnieje bezpieczniejszy od FTP sposób przesyłania plików?

Tak.

SFTP (ang. SSH File Transfer Protocol). Jest to protokół zabezpieczający przesyłane dane za pomocą szyfrowania. FTPS – funkcjonuje na bazie protokołu FTP, dodaje szyfrowanie TLS/SSL (zabezpiecza połączenie między klientem a serwerem)

AS2 – protokół opracowany i licencjonowany przez IBM, jest bardziej skomplikowany niż FTP, ale bezpieczniejszy, żeby go używać trzeba wykupić licencję. HTTPS – HyperText Transfer Protocol Secure- zabezpieczenie połączenia za pomocą SSL/TLS

MFT-zastrzeżony protokół IBM