# Instrukcja programu Wireshark (wersja 1.8.3) w zakresie TCP/IP

## I. <u>Na początek</u>

### Czym jest analizator sieciowy jakim jest Wireshark?

Analizator sieciowy pozwala na przechwytywanie i analizę danych, które są przesyłane przez sieć. W łatwy sposób możemy "obejrzeć" cały ruch w naszej sieci. Możemy sprawdzić jakie porty wykorzystuje dane oprogramowanie oraz wysyłany/odbierany ruch przez nasz komputer.

Wireshark jest najbardziej popularnym analizatorem sieciowym. To silne narzędzie dostarcza sieciowe i wyższych protokołów informacyjnych dotyczące zrzuconych danych w sieci.

Do roku 2006 Wireshark nosił nazwę Ethereal.

#### <u>Ważna uwaga:</u>

Jeśli szukasz programu do włamywania się, podrzucania wirusów, wykradania haseł czy czegoś w tym stylu - to NIE TO. Wireshark tylko wyświetla w czytelny sposób to co juz i tak dociera do twojego komputera (zwykle oznacza to tylko ruch własny). Nie spowoduje, że nagle zobaczysz hasło do banku swojego szefa, albo kody do odpalenia amerykańskich, czy rosyjskich rakiet balistycznych.

### Do czego może służyć Wireshark?

- Głównie do diagnostyki: np. nie można połączyć się z jakimś serwerem on nie działa, czy mój komputer w ogóle nie próbuje, a może DNS podał zły adres? To oznacza, że raczej trzeba już wiedzieć czego się szuka, a wtedy instrukcja obsługi nie jest potrzebna ;)
- Jest doskonałym narzędziem do nauki żaden wykład teoretyczny nie zastąpi popatrzenia sobie w praktyce jak te pakiety faktycznie wyglądają.
- No dobrze, można też podsłuchiwać. Jest to możliwe, kiedy komputer "słyszy" nie swoje pakiety. Dzieje się tak np. gdy mamy sieć zbudowaną na HUBach (a nie switchach), bezprzewodową (chociaż wtedy mogą być problemy z driverami i i tak się nie uda) lub nasz komputer robi za router ("udostępnia sieć" innym).

#### II. <u>Przechwytywanie</u>

Uruchom Wiresharka z prawami Administratora

S Window Window S Window	Otwórz lokalizację pliku <b>Otwórz</b>
📕 Window 🔮	Uruchom jako administrator
😨 Window 🛐	Zachomikuj
💟 Window 🚰 Window 🖾	🕽 Skanuj
📶 Wiresha 🖀	Add to archive
🤰 20Dollar	Add to "wireshark.rar"
Advance Akcesor	Compress and email
🔋 Ashamp	Compress to "wireshark.rar" and email
🔒 Autosta	Przypnij do paska zadań



Wybierz interfejs którym twój komputer łączy się z siecią (zwykle eth0) i naciśnij start.

	Description	IP	Packets	Packets/s	
🗌 😥 Microsoft		fe80::4c4e:b964:8bb1:ea10	0	0	Details
🗏 🙍 Microsoft		fe80::70f6:57ea:2354:6d98	0	0	Details
🗌 😥 Realtek PCI	e FE Family Controller	fe80::f850:ac2b:20c4:3c1a	99	4	Details
🛾 😥 Microsoft		fe80::4d93:9845:daa8:4ddf	0	0	Details
	£				
Help	Start	Stop	<u>O</u> ption	s	Close
<u>H</u> elp Wireshark: Capture	<u>Start</u> e Interfaces	Stop	Option Packets	s Packets/s	<u>C</u> lose
<u>H</u> elp Wireshark: Captur	<u>Start</u> e Interfaces Description	IP fe80::4c4e:b964:8bb1:ea10	Option Packets 0	s Packets/s 0	<u>C</u> lose
Help Wireshark: Captur Microsoft	<u>Start</u> e Interfaces Description	IP fe80::4c4e:b964:8bb1:ea10 fe80::70f6:57ea:2354:6d98	Option Packets 0 0	S Packets/s 0 0	<u>C</u> lose
Help Wireshark: Captur Microsoft	<u>Start</u> e Interfaces Description le FE Family Controller	IP fe80::4c4e:b964:8bb1:ea10 fe80::70f6:57ea:2354:6d98 fe80::f850:ac2b:20c4:3c1a	Option Packets 0 0 924	Packets/s 0 1	<u>C</u> lose
Help Wireshark: Capture Microsoft Microsoft Realtek PCI	<u>Start</u> e Interfaces Description le FE Family Controller	IP fe80::4c4e:b964:8bb1:ea10 fe80::70f6:57ea:2354:6d98 fe80::f850:ac2b:20c4:3c1a fe80::4d93:9845:daa8:4ddf	Option Packets 0 0 924 0	Packets/s 0 1 0	Close



#### Skończ chwytanie pakietów (Capture - Stop)

Capturing from Real	tek PCIe FE Family Contro	oller: \Devi	ce\NPF_{CE90751F-1E7E	8-4708-8548	-DD99E8AF1AA9} [Wir 💷 💷 🛑	×
<u>File Edit View Go</u>	<u>Capture</u> <u>Analyze</u> <u>St</u>	atistics	felephony <u>T</u> ools Inte	ernals <u>H</u> elp	)	
	Interfaces	Ctrl+I	■ ● ● 7 4		Q, Q, Q, 🖭   🌌 🗵 畅	>>
Filter:	Start	Ctrl+K Ctrl+E		Expression	. Clear Apply Save	
No. Time	Stop	Ctrl+E	ination	Protocol	Length Info	-
2451 115.17441	M Restart	Ctrl+R	2::c	SSDP	208 M-SEARCH * HTTP/1.1	
2452 115.49709		Con M	t_62:fa:dc	ARP	42 who has 192.168.123.1	?
2453 115.4976	Capture Filters		tronI_c6:15:c3	ARP	60 192.168.123.1 is at 0	)C
2454 116.33428	36 192.168.123.10	3 94	.127.76.120	TCP	54 49672 > http [RST, AC	K
2455 117.11040	9 192.168.123.1	23	9.255.255.250	SSDP	369 NOTIFY * HTTP/1.1	
2456 117.21708	31 192.168.123.1	23	9.255.255.250	SSDP	369 NOTIFY * HTTP/1.1	
2457 117. 32504	0 192, 168, 123, 1	23	9,255,255,250	SSDP	378 NOTIFY * HTTP/1.1	

Przefiltruj listę pakietów by zostawić tylko te opisujące komunikację z hostem www.onet.pl (IP: 213.180.141.140): w pasku "Filter" u góry okna programu wpisz: ip.addr == 213.180.141.140.

<b>R</b>	tealtek PCIe FE Fan	nily Controller: \Devi	ce\NPF_{CE90751F-1E7B-470B-8548	-DD99E8AF1AA9}	[Wireshark 1.8.4 (SV	
<u>F</u> ile	<u>E</u> dit <u>V</u> iew <u>G</u> o	o <u>C</u> apture <u>A</u> nalyz	e <u>S</u> tatistics Telephony <u>T</u> ools	<u>I</u> nternals <u>H</u> elp		
		i 🖻 🖬 🗶 🕯	🖱 占   🔍 🗢 🌳 🔷 7 ,	<u>2</u>   [] []	QQ 🖳 🔛 🛛 🗃	🗹 🔂 🚿
Filte	er: ip.addr == 213	.180.141.140		Expression	Clear Apply Save	
No.	Time	Source	Destination	Protocol Le	ngth Info	4
	555 14. 58214	60 192.168.123	.103 213.180.141.140	TCP	66.49636 > http	[SYN] Sec
	556 14.58313	60 192.168.123	.103 213.180.141.140	TCP	66 49637 > http	[SYN] Sec F
	574 14.62735	80 213.180.141	.140 192.168.123.103	TCP	66 http > 49636	[SYN, ACK
2	575 14.62742	40 192.168.123	.103 213.180.141.140	TCP	54 49636 > http	[ACK] Sec
	576 14.62801	90 213.180.141	.140 192.168.123.103	TCP	66 http > 49637	[SYN, ACK
5	577 14.62807	30 192.168.123	.103 213.180.141.140	TCP	54 49637 > http	[ACK] Sec
	584 14.69469	10192.168.123	.103 213.180.141.140	HTTP	904 GET / HTTP/1	.1
	589 14.72921	30 213.180.141	.140 192.168.123.103	TCP	60 http > 49636	[ACK] Sec
	590 14.73712	00 213.180.141	.140 192.168.123.103	HTTP	195 HTTP/1.1 301	Moved Per
2	591 14.73790	00192.168.123	.103 213.180.141.140	TCP	54 49636 > http	[FIN, ACK
	593 14.75801	30 213.180.141	.140 192.168.123.103	TCP	60 http > 49636	[FIN, ACK
	504 14 75800	80 102 168 123	103 213 180 141 140	TCP	54.49636 > bttn	TACKI Sec

### III. <u>Analiza pakietów</u>

- Okno Wireshark podzielone jest na trzy części:
  - $\succ$  górna część zawiera listę złapanych pakietów (przefiltrowanych przez filtr) 1
  - $\succ$  środkowa część to analiza wybranego pakietu 2
  - > dolna część to zawartość pakietu (binarna i reprezentacja ASCII) 3

Realtek PCIe FE Family Controller: \Device\NPF_(CE90	0751F-1E7B-470B-8548-DD99E8AF1AA9} [Wireshark 1.8.4 (SV 💷 💷 🔤	
<u>File Edit View Go Capture Analyze Statistics</u>	Telephony <u>I</u> ools Internals <u>H</u> elp	
	、 🌳 🌳 🖥 🛓   🗐 🗐   Q, Q, Q, 🗹   🖉 🖉 🥵 👒	
Filter: ip.addr == 213.180.141.140	Expression Clear Apply Save	
No. Time Source E	Destination Protocol Length Info	
555 14. 5821460 192. 168. 123. 103	213.180.141.140 TCP 66 49636 > http [SYN] Sec	
556 14.5831360 192.168.123.103	213.180.141.140 TCP 66 49637 > http [SYN] Sed	
574 14.6273580 213.180.141.140	192.168.123.103 TCP 66 http > 49636 [SYN, ACK	
575 14.6274240 192.168.123.103	213.180.141.140 TCP 54 49636 > http [ACK] Sec	
576 14.6280190 213.180.141.140	192.108.123.103 TCP 60 Http > 49637 [SYN, ACK	
5// 14.0200/ 50 192.108.125.105	213.180.141.140 HTTP 004 GET / HTTP/1 1	비니
589 14 7292130 213 180 141 140	192 168 123 103 TCP 60 http > 49636 [ACK] Sec	1
590 14, 7371200 213, 180, 141, 140	192.168.123.103 HTTP 195 HTTP/1.1 301 Moved Per	ημΞ
591 14,7379000 192,168,123,103	213.180.141.140 TCP 54 49636 > http [FIN. ACK	
593 14.7580130 213.180.141.140	192.168.123.103 TCP 60 http > 49636 [FIN, ACK	
594 14.7580980 192.168.123.103	213.180.141.140 TCP 54 49636 > http [ACK] Sec	
596 14.7594230 192.168.123.103	213.180.141.140 TCP 66 49638 > http [SYN] Sec	
597 14.7604360 192.168.123.103	213.180.141.140 TCP 66 49639 > http [SYN] Sec	
598 14.7804210 213.180.141.140	192.168.123.103 TCP 66 http > 49639 [SYN, ACK	
FOR 14 300E000 100 100 100 100 100 100 100 100 1		
∃ Frame 556: 66 bytes on wire (528 bi	ts), 66 bytes captured (528 bits) on interface 0	
Ethernet II, Src: wistronI_c6:15:c3     ■	(f0:de:f1:c6:15:c3), Dst: Amit_62:fa:dc (00:50:18:62:fa	
Internet Protocol Version 4, Src: 1	.92.168.123.103 (192.168.123.103), Dst: 213.180.141.140 (	┦┓╢
田 Transmission Control Protocol, Src     □	Port: 49637 (49637), Dst Port: http (80), Seq: 0, Len: 0	┐┻║
<	III. F	
0000 00 50 18 62 fa dc f0 de f1 c6 1	15 с3 08 00 45 00 .р.рЕ.	
0010 00 34 1a cc 40 00 80 06 00 00 c	c0 a8 7b 67 d5 b4 .4@{g	
0020 80 80 01 e5 00 50 96 ef 20 67 0	00 00 00 00 80 02P ,g	_  3
0040 04 02		
⊖ 🛃 File: "C:\Users\Patii\AppData\Local\Temp\ Ⅰ	Packets: 2544 Displayed: 85 Profile: Default	

#### • Zadania:

Realtek PCIe FE Family Controller: \Device\NPF_(CE90751F-1E7B-470B-8548-DD99E8AF1AA9)       [Wireshark 1.8.4 (SV         File       Edit       Yiew       Go       Gapture       Analyze       Statistics       Telephony       Iools       Internals       Help         Image: Statistic Statistic Statistics       Telephony       Iools       Internals       Help         Image: Statistic Statis
Eile       Edit       View       Go       Capture       Analyze       Statistics       Telephony       Iools       Internals       Help         Image: Image
Image: Second secon
Filter: ip.addr == 213.180.141.140
Filter: ip.addr == 213.180.141.140
No. Time Source Destination Protocol Length Info
555 14.5821460 192.168.123.103 213.180.141.140 TCP 66 49636 > http [SYN] sec
556 14.5831360 192.168.123.103 213.180.141.140 TCP 66 49637 > http [SYN] Sec =
575 14.6274240 192.168.123.103 213.180.141.140 TCP 54 49636 Shttp [ACK] sec
576 14.6280190 213.180.141.140 192.168.123.103 TCP 66 http > 49637 [SYN, ACK
577 14.6280730192.168.123.103 213.180.141.140 TCP 54 49637 > http [ACK] Sec
584 14.6946910 192.168.123.103 213.180.141.140 HTTP 904 GET / HTTP/1.1
589 14.7292130 213.180.141.140 192.168.123.103 TCP 60 http > 49636 [ACK] Sec
590 14.7371200 213.180.141.140 192.108.123.103 HTP 195 HTP/1.1 301 MOVED PER
593 14.7580130 213.180.141.140 192.168.123.103 TCP 60 http > 49636 [FIN, ACK
594 14.7580980 192.168.123.103 213.180.141.140 TCP 54 49636 > http [ACK] Sec
596 14.7594230 192.168.123.103 213.180.141.140 TCP 66 49638 > http [SYN] Sec
597 14.7604360 192.168.123.103 213.180.141.140 TCP 66 49639 > http [SYN] sec
598 14.7804210 213.180.141.140 192.168.123.103 TCP 66 http > 49639 [SYN, ACK -
Ethernet II, Src: Amit_62:fa:dc (00:50:18:62:fa:dc), Dst: WistronI_c6:15:c3 (f0:de:f1:c6:
Transmission Control Protocol, Src Port: http (80), Dst Port: 49636 (49636), Seq: 1, Ack
⊕ Hypertext Transfer Protocol
0000 f0 de f1 c6 15 c3 00 50 18 62 fa dc 08 00 45 00P .bE.
0010 00 b5 14 51 40 00 36 06 90 a1 d5 b4 8d 8c c0 a8 Q@.6
0030 00 20 ef e6 00 00 48 54 54 50 2f 31 2e 31 20 33HT TP/1.1 3
0040 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 01 Moved Permane
File: "C:\Users\Patii\AppData\Local\Temp\ Packets: 2544 Displayed: 85 Profile: Default
<ul> <li>B Frame 590: 195 bytes on wire (1560 bits), 195 bytes captured (1560 bits) on interface 0</li> <li>B Ethernet II, Src: Amit_62:fa:dc (00:50:18:62:fa:dc), Dst: WistronI_c6:15:c3 (f0:de:f1:c6:15:c3)</li> <li>B Internet Protocol Version 4, Src: 213.180.141.140 (213.180.141.140), Dst: 192.168.123.103 (192.168.123.10)</li> <li>B Transmission Control Protocol, Src Port: http (80), Dst Port: 49636 (49636), Seq: 1, Ack: 851, Len: 141</li> </ul>
Obejrzyj szczegółowe informacje w środkowej części okna.
Transmission Control Protocol, Src Port: http (80), Dst Port: 49636 (49636), Seq: 1, Ack: 851, Len: 141 Hypertext Transfer Protocol HTTP/1.1 301 Moved Permanently\r\n Expert Info (Chat/Sequence): HTTP/1.1 301 Moved Permanently\r\n]
Request Version: HTTP/1.1

Request Version: HTTP/1.1 Status Code: 301 Response Phrase: Moved Permanently location: http://www.onet.pl\r\n server: edgeserver\r\n Connection: keep-alive\r\n Transfer-Encoding: chunked\r\n \r\n ■ HTTP chunked response ■ End of chunked encoding Chunk size: 0 octets Chunk boundary Kliknij w Hypertext Transfer Protocol w środkowej części okna.

∃ Transmission Control Protocol, Src Port: http (80), Dst Port: 49636 (49636), Seq: 1, Ack: 851, Len: 141 🗐 H □ HTTP/1.1 301 Moved Permanently\r\n Request Version: HTTP/1.1 Status Code: 301 Response Phrase: Moved Permanently location: http://www.onet.pl\r\n server: edgeserver $r^n$ Connection: keep-alive\r\n Transfer-Encoding: chunked r nr nHTTP chunked response □ End of chunked encoding Chunk size: 0 octets Chunk boundary Obejrzyj które bajty w pakiecie odpowiadaja za zawartość HTTP, a które za nagłówki (Ethernet, IP, TCP). 🗆 Transmiss http (80), Dst Port: 49636 (49636), Ack: 851. Len: 141 Source port: http (80) Destination port: 49636 (49636) [Stream index: 19] Sequence number: 1 (relative sequence number) [Next sequence number: 142 (relative sequence number)] Acknowledgment number: 851 (relative ack number) Header length: 20 bytes Window size value: 32 [Calculated window size: 16384] [Window size scaling factor: 512] Ethernet II, Src: Amit\_62:fa:dc (00:50:18:62:fa:dc Dst: WistronI\_c6:15:c3 (f0:de:f1:c6:15:c3) Type: IP (0x0800) col Version 4, Src: 213.180.141.140 (213.180.141.140), Dst: 192.168.123.103 (192.168.123.103) Internet Proto Version: 4 Header length: 20 bytes B Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)) Total Length: 181 Identification: 0x1451 (5201) Image: Flags: 0x02 (Don't Fragment) Fragment offset: 0 Time to live: 54 Protocol: TCP (6) B Header checksum: 0x90a1 [correct] source: 213.180.141.140 (213.180.141.140) Destination: 192.168.123.103 (192.168.123.103) [Source GeoIP: Unknown] [Destination GeoIP: Unknown] Jaki jest lokalny numer portu? Jaki jest numer portu serwera?  $\geq$ Dst Port: 49636 (49636), Seq: 1. Ack: 851. Len: 141 Source port: http (80) Destination port: 49636 (49636) [Stream Index. 19 Sequence number: 1 (relative sequence number) . .

```
Znajdź pakiet z odpowiedzią serwera.
E Frame 590: 195 bytes on wire (1560 bits), 195 bytes captured (1560 bits) on interface 0
   Interface id: 0
    WTAP_ENCAP: 1
    Arrival Time: Dec 8, 2012 18:16:38.678479000 środkowoeuropejski czas stand.
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1354986998.678479000 seconds
    [Time delta from previous captured frame: 0.007907000 seconds]
    [Time delta from previous displayed frame: 0.007907000 seconds]
    [Time since reference or first frame: 14.737120000 seconds]
    Frame Number: 590
    Frame Length: 195 bytes (1560 bits)
   Capture Length: 195 bytes (1560 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ip:tcp:http:data]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80]
```

- Z jakiego portu została wysłana odpowiedź? Na jaki port w naszym hoście?
- Jaka jest zawartość odpowiedzi serwera?

#### IV. <u>Cache'owanie w HTTP</u>

Tą część trzeba wykonać z włączonym łapaniem pakietów [po wstępnym wybraniu interfejsu, łapanie pakietów można włączać przez Capture – Start]



#### Połącz się jeszcze raz z Onet.pl (lub inną wybraną stroną)



Ogranicz pakiety do http (filtr: http && ip.addr == 213.180.141.140)

Filter: http && ip.addr == 213.180.141.140

> Co zmieniło się w odpowiedzi serwera? Dlaczego serwer http mógł tak odpowiedzieć?

•

Capturing from Realtek PCIe FE Family Controller: \Device\NPF_(CE90751F-1E78-4708-8548-DD99E8AF1AA9) [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)]	
<u>File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help</u>	
Filter: http && ip.addr == 213.180.141.140   Expression Clear Apply Save	
No. Time Source Destination Protocol Length Info	
44 9.66981600192.168.123.103 213.180.141.140 HTTP 1085 GET / HTTP/1.1	
46 9.70327200 213.180.141.140 192.168.123.103 HTTP 195 HTTP/1.1 301 Moved Permanently	
50 9.70803600192.168.123.103 213.180.141.140 HTTP 1089 GET / HTTP/1.1	
146 9.94190900 213.100.141.140 192.108.123.103 mir 1314 [ICP Retraitsmission] mir/1.1 200 0K (text/)	
156 10 1486560 213 180 141 140 192 168 123 103 HTTP 577 HTTP/1 1 200 0K (text/javascript)	
205 10.1895010192.168.123.103 213.180.141.140 HTTP 566 POST / cdf/render HTTP/1.1 (application/x-w	ww-form-urlencode
236 10.2845960 213.180.141.140 192.168.123.103 HTTP 401 HTTP/1.1 200 OK (text/html)	
270 10.5043840 213.180.141.140 192.168.123.103 HTTP 401 [TCP Retransmission] HTTP/1.1 200 OK (text/	ntml)
Trame 44: 1085 butes on wine (8680 bits) 1085 butes contured (8680 bits) on interface 0	
E Ethempet II Sec: Wistoni Collsca (Godo Dits), 1003 Dytes captured (2000 Dits) on interface 0	<u>.</u>
Internet Protocol version 4, Src: 192,168,123,103 (192,168,123,103), DST: 213,180,141,140 (213,180,141,140)	-
0000 00 50 18 62 fa dc f0 dc f1 c6 15 c3 08 00 45 00 R b 5	
0010 04 2f 25 f3 40 00 80 06 00 00 c0 a8 7b 67 d5 b4 ./%.@	â
0020 8d 8c c2 70 00 50 a6 74 e3 6e ef 1c 0d 4a 50 18p.p.t njp.	
0040 2 31 2 0 0 0 47 45 54 20 2T 20 48 54 34 30	
0050 20 70 60 64 04 0 42 65 60 60 65 52 74 60 65 60 25 (1) con nortion	
Kealtek PCle FE Family Controller: \Device\N Packets: 1138 Displayed: 9 Marked: 0 Profile: Default	

#### V. TCP



• Nagłówek TCP (ta część wykonujemy z włączonym łapaniem pakietów) Wyłącz analizę protokołu HTTP (Analyze - Enabled Protocols). Ustaw filtr na protokół TCP i adres IP serwera www.onet.pl

The Wire	shark Network Analyzer [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)				
<u>File</u> dit	View Go Capture Analyze Statistics Telephony Tools Internals	<u>H</u> elp			
	🖌 🔐 🚵 🔚 🔚 🔛 💟 Display Filters	] ⊑] ≪ ≪ ≪ ⊠   ≝ ⊠ № %   ⊠			
Filter:	Apply as Column kpr	ession Clear Apply Save			
WIR	Apply as Filter Prepare a Filter Prepare a Filter Prepare a Filter M M M M M M M M M M M M M	ork Protocol Analyzer (-1.8)			
	Cap 💐 User Specified Decodes	Files Online			
<b>Wire</b> s	hark: Enabled Protocols - Profile: Default				
Enabled	l Protocols				
Status 4	Protocol	Description			
V	HP_ERM	HP encapsulated remote mirroring			
V	HPEXT	HP Extended Local-Link Control			
V	HPSW	HP Switch Protocol			
V	HPTEAM	HP NIC Teaming Heartbeat			
V	HSR	High-availability Seamless Redundancy (IEC62439 Part 3 Chapter 5)			
V	HSR_PRP_SUPERVISION	HSR/PRP Supervision (IEC62439 Part 3)			
	HSRP	Cisco Hot Standby Router Protocol			
V	нттр	Hypertext Transfer Protocol			
V	HyperSCSI	HyperSCSI			
V	12C	Inter-Integrated Circuit			
V	IAP	Information Access Protocol			
V	IAPP	Inter-Access-Point Protocol			
V	IAX2	Inter-Asterisk eXchange v2			
V	ICAP	Internet Content Adaptation Protocol			
V	ICBAAccoCB	ICBAAccoCallback			
V	ICBAAccoCB2	ICBAAccoCallback2			
	ICBAAccoMgt	ICBAAccoMgt			
	ICBAAccoMgt2	ICBAAccoMgt2 +			
<		m			
	Disabling a protocol prevents	higher layer protocols from being displayed			
		Enable All Disable All Invert			
He	lp	OK Apply Save Cancel			

Znajdź i zaznacz (Edit - Mark Packet) pakiet w którym przeglądarka przesyła żądanie  $\succ$ do serwera.

File Edit View Go Canture Analyze Statistics Telephony Tools Internals Heln	
Filter: tcp && ip.addr == 213.180.141.140   Expression Clear Apply Save	
No.         Time         Source         Destination         Protocol         Length         Info           3799         184, 057606         192, 168, 123, 103         211         140 <td>66 SAC 56 SAC 55 SAC 55=146 1 55=15 1 55=</td>	66 SAC 56 SAC 55 SAC 55=146 1 55=15 1 55=
0000       00       50       18       62       fa       dc       finit      E.         0010       00       34       31       b3       40       00       80       00       00       columna      E.         0020       84       cc       31       fo       50       00       00       columna	* E +

## > Co jest w nagłówku TCP? Jakie flagi są związane z żądaniem?

Capturing fro	m Realtek PCIe FE Family Controller	: \Device\NPF_{CE90751F-1E7	E7B-470B-8548-DD99E8AF1AA9} [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)]		
<u>Eile Edit Vie</u>	w <u>G</u> o <u>C</u> apture <u>A</u> nalyze <u>S</u> tatis	tics Telephony <u>T</u> ools Int	Internals Help		
		् 🗢 🔿 🖗 🕹	2   🗐 🖩   Q, Q, Q, 🖻   🖉 🕺 🧏 🞉   🙀		
Filter: http			Expression Clear Apply Save		
No. Time	Source	Destination	Protocol Length Info	*	
104 2.14	841800 213.180.141.140	192.168.123.103	HTTP 435 HTTP/1.1 200 OK (text/html)	*	
□ Line-bases DOCTY</p <html 1<="" p=""> <head> <me< p=""> &lt;</me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></me<></head></html>	<pre>Content-encoded entity body (gzip): 35156 bytes -&gt; 227658 bytes Line-based text data: text/html <!DOCTYPE html>    \n <html lang="pl">\n <html <="" html="" lang="pl">\n <html <="" html="" lang="pl">\n <html <="" html="" l<="" lang="pl" th=""></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></pre>				
A 10				P	
0000 f0 de 0010 01 a5 0020 7b 67	f1 c6 15 c3 00 50 18 c 19 75 40 00 37 06 89 8 00 50 c4 1c e3 c1 fa	52 fa dc 08 00 45 00 3d d5 b4 8d 8c c0 a8 11 7d 2c 46 87 50 18	0P .bE. 8u8.7 8 {g.P	4.1.4	
Frame (435 byte	s) Reassembled TCP (35421 bytes)	Uncompressed entity body (2	/ (227658 bytes)		
😑 💅 Frame (fi	ame), 435 bytes	Packets: 1910 Displayed: 40	406 Marked: 0 Profile: Default		

> Znajdź i zaznacz pakiet z odpowiedzią serwera zawierającą stronę internetową. Jakie flagi są ustawione? Czy jest to jedyna odpowiedź TCP serwera? Jeśli nie - dlaczego jest ich więcej? Czym różnią się pozostałe odpowiedzi?

```
Flags: 0x02 (Don't Fragment)
   0... = Reserved bit: Not set
   .1.. .... = Don't fragment: Set
   ..... = More fragments: Not set
 Fragment offset: 0
 Time to live: 128
 Protocol: TCP (6)
```

- Zestawianie i zamykanie połączenia TCP
  - > Przeanalizuj pakiety tcp poprzedzające pakiet z żądaniem http.

Ele Si (	Edit Yvew Go	Capture Analyze Statist	icz Telephony Iook In 🔍 🌳 🕸 🌄 🛃	temais Help	aaa		S 39	
Filter	http && ip.add	r == 213.380.141.140		Expression	Clear Apply	Save		
io.	Time	Source	Destination	Protocol 1	Length Info			
	44 9.6698100	0192.168.123.103	213-180.141.140	HTTP	1085 GET	(NTTP/1)1		
	46 9.7032720	0 213.180.141.140	192,168,123,103	HETP	195 HTTP/	1.1 301 Moved	Permanently	
	50 9.7080300	0192.168.123.103	211.180.141.140	HTTP	1089 GET	HTTP/1,1		
	48 9,9419090	30 218, 180, 141, 140	192,168,123,105	HTTP	1514 TCH	Retransmissio	n HTTP/1.1 200 OK	(text/html)
	10,088467	70 192.168.123.103	213.180.141.140	HILL	1071 GET /	cdf/clitent.1	s HTTP/111	
1	56 10.148656	50 213.180.141.140	192.168.123.103	HTTP	577 HTTP/	1.1 200 OK (	text/javascript)	
	05 10.189501	10 192.168.123.103	213.180.141.140	HITE	366 P05T	/_cdf /render	HTTP/1.1 (applicat	ion/x-www-form-urliencoder
2	36 10.284596	50 213.180.141.140	192.168.123.103	HTTP	401 HTTP/	1.1 200 OK (	text/html)	
1	170 10, 504354	40 213 189 141 140	192.168.127.103	HTTP	401 TCP	Retransmissio	n] HTTP/1.1 200.0K	(text/html)

- Ile jest takich pakietów?
- Kto inicjuje połączenie?

Source
192.168.121.101
213.180.141.140
192.168.123.101
211.180.141.140
192.168.12.1/10.
213.180.141.140
197.168.173.101
213.180.141.140
213.189.141.140

```
> Jakie flagi są ustawiane?

□ Flags: 0x02 (Don't Fragment)

0... = Reserved bit: Not set

.1. ... = Don't fragment: Set

..0. ... = More fragments: Not set

Fragment offset: 0

Time to live: 128

Protocol: TCP (6)
```

Przeanalizuj pakiety tcp po pakiecie z odpowiedzią http.

44 9,06981600 192.168,123.103	213,180,141,140	HITTP	1085-66T / HTTP/1-1
46 9,70327200 213,180,141,140	192.168.123.103	NTTP	195 HTTP/1.1 301 Moved Permanently
50 9, /0803600 192.168.123.103	213,180,141,140	HITE	1089 CLT / HTTP/1,1
148 9,94190900 211,180,141,140	192.168.123.103	HITE	1514 [TCP Retransmission] HTTP/1.1 200 OK (text/html)
150 10.0884070 192.168.123.103	213, 180, 141, 140	HITP	1073 GET /_cdf/client.15 HTTP/1.1
156 10.1486560 213.180.141.140	192.168.123.103	HTTP	577 HTTP/1.1 200 OK (text/javascript)
705 10.1895010 192.168.123.103	213,180,141,140	HTTP	360 POST /_cdf/render ATTP/1.1 (application/x-www-form-urlencode
236 10.2845960 213.180.141.140	192.168.123.103	HITP	401 HTTP/1,1 200 OK (text/html)
270 10 5012840 312 580 141 140	103 166 131 103	14 T T 10	101 TTEL BATE DOLLARS AND ATTACK TO 100 OF CLASS DISC.

- Ile jest takich pakietów?
- Kto zaczyna proces zamykania połączenie?

192,168,123,103 213,180,141,140 193,108,121,103 213,108,121,103 213,108,121,103 192,168,123,103	213,180,141,140
213,180,141,140 193,108,121,103 715,168,121,103 192,168,123,103	192.168.123.103
193.108.121.103 214.160.141.140 192.168.123.103	213, 180, 141, 140
192.168.121.103	192.108.121.103
192.168.123.103	213 160 141 140
	192.168.123.103
	213 140 141 140
192.168.123.103	192.168.123.103

```
Jakie flagi są ustawiane?
Flags: 0x02 (Don't Fragment)
    0... = Reserved bit: Not set
    .1.. .... = Don't fragment: Set
    ..... = More fragments: Not set
 Fragment offset: 0
 Time to live: 128
 Protocol: TCP (6)
```

• <u>Połączenia keep-alive w http</u> - zobaczymy jak przeglądarka i serwer obsługują strony wymagające więcej niż jednego żądania http. (Tą część wykonujemy z włączonym łapaniem pakietów)



Dzisiaj Pogoda | Horoskop | Program TV | Kina | Warszawa D Kursy walut | Giełda online | Wyniki Lotto

teraz -7°C C -5°C

jutro

# Znajdź i zaznacz pakiety zawierające dwa żądania http

Elle Edit View Go Capture Analyze Statistics Telephony Iools Internals Help         Image: Statistics Telephony Iools Internals Help	📶 Capturing from Realtek PCIe FE Family Controller: \Device\NPF_(CE90751F-1E7B-470B-8548-DD99E8AF1AA9) [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)]
Image: Source       Destination       Protocol Length Info         325 65,7133740 192,168,123,103       213,180,141,140       ITTP 1115 661 / ITTP/1.1       2000 (c)	Eile Edit <u>V</u> iew <u>Go</u> <u>Capture</u> <u>Analyze</u> <u>Statistics</u> Telephony <u>I</u> ools Internals <u>H</u> elp
Filter       http &&& ip.addr == 213.180.141.140       Epression Clear Apply Save         No.       Time       Source       Destination       Protocol Length Info       A         325 65.7133740192.168.123.103       213.180.141.140       HTTP       1115 GET / HTTP/1.1       Protocol Length Info       A         412 66.2662710 213.180.141.140       HTTP       1019 GET / cdf / client, is HTTP/1.1       HTTP       109 GET / cdf / client, is HTTP/1.1       A         420 66.3408530 213.180.141.140       HTTP       109 GET / cdf / client, is HTTP/1.1       (text/html)       A         436 69.2144320 213.180.141.140       HTTP       538 HTTP/1.1 200 oK (text/html)       E       A         558 69.4804509 213.180.141.140       HTTP       538 HTTP/1.1 200 oK (text/html)       E       A         1203 185.062280 192.168.123.103       HTTP       538 HTTP/1.1 200 oK (text/html)       A       A         1203 185.062280 192.168.123.103       HTTP       538 HTTP/1.1 200 oK (text/html)       A       A         1204 185 21122 102       213.180.141.140       HTTP       115 CeT / HTTP/1.1       A       A       A         1203 185.062280 192.168.123.103       HTTP       115 CeT / HTTP/1.1       A       A       A       A         1274 185 21127 312 180.141.140       HTTP       A	▩ ▩ ▩ ▩   == ;;
No.         Time         Source         Destination         Protocol Length Info           325         65,7133760192,165,123,103         213,180,141,140         HTTP         1115         GET / LTTP/1.1         412         66,2662710 213,180,141,140         HTTP         460 HTTP/1.1 200 0K (text/html)         ####################################	Filter: http && ip.addr == 213.180.141.140   Expression Clear Apply Save
23 05,7153,740 192,108,123,1140       123,180,141,140       117       113 GET / HTTP/1.1       100 0K (text/html)         412 66,2602710 213,180,141,140       192,168,123,103       HTTP       1099 GET /_cdf/client,js HTTP/1.1         420 66,3408530 213,180,141,140       192,168,123,103       HTTP       1099 GET /_cdf/render HTTP/1.1 (application/x-www-form-urlenco         440 69,2144320 213,180,141,140       192,168,123,103       HTTP       536 FOST /_cdf/render HTTP/1.1 (application/x-www-form-urlenco         440 69,2144320 213,180,141,140       192,168,123,103       HTTP       538 HTTP/1.1 200 0K (text/html)         558 69,4804690 213,180,141,140       192,168,123,103       HTTP       538 HTTP/1.1 200 0K (text/html)         1231 155,062849192,168,123,103       113,180,141,140       HTTP       115 GET / HTTP/1.1         1231 145,141,140       192,168,123,103       HTTP       473 HTTP/1.1         1231 145,141,140       192,168,123,103       HTTP       115 GET / HTTP/1.1         1231 145,141,140       192,168,123,103       HTTP       114,160,123,180,141,140       HTTP </td <td>No. Time Source Destination Protocol Length Info</td>	No. Time Source Destination Protocol Length Info
414 66.2804110192.168.123.103       213.180.141.140       HTTP       1099 GET /_cdf/client.js HTTP/1.1         420 66.3408530 213.180.141.140       192.168.123.103       HTTP       610 HTTP/1.1 200 0K (text/javascript)         436 69.21592840 213.180.141.140       192.168.123.103       HTTP       538 HTTP/1.1 (application/x-www-form-urlenco         440 69.2144320 213.180.141.140       192.168.123.103       HTTP       538 HTTP/1.1 200 0K (text/html)         538 69.4804690 213.180.141.140       192.168.123.103       HTTP       538 HTTP/1.1 200 0K (text/html)         1293 185.062849 192.168.123.103       123.180.141.140       192.168.123.103       HTTP       538 HTTP/1.1 200 0K (text/html)         1293 185.062849 192.168.123.103       123.180.141.140       192.168.123.103       HTTP       472 HTTD/1 1 200 0K (text/html)         1293 185.062849 192.168.123.103       192.168.123.103       HTTP       473 HTTD/1 1 200 0K (text/html)         1293 185.062849 192.168.123.103       192.168.123.103       HTTP       473 HTTD/1 1 200 0K (text/html)         1293 185.062849 192.168.123.103       192.168.123.103       HTTP       473 HTTD/1 1 200 0K (text/html)         1293 180.141.140       192.168.123.103       192.168.123.103       D10 0 K (100.150.18.162.168.103.104.10.100.190.190.190.190.190.190.190.190.	325 05./135/40192.105.123.103 213.180.141.140 H11P 1115 GET / H11P/1.1 412 66.2662710.213.180.141.140 192.168.123.103 HTTP 460 HTTP/1.1 200 0K (text/htm])
420 66.3408330 213.180.141.140       192.168.123.103       HTTP       610 HTTP/1.1 200 oK (text/javascript)         436 69.1592840 192.168.123.103       213.180.141.140       HTTP       566 POST /_cdf/render HTTP/1.1 (application/x-www-form-ur]enco         440 69.2143.180.141.140       192.168.123.103       HTTP       538 HTTP/1.1 200 oK (text/html)         558 69.4804690 213.180.141.140       192.168.123.103       HTTP       538 HTTP/1.1 200 oK (text/html)         1231 185.062849 192.168.123.103       HTTP       538 HTTP/1.1 200 oK (text/html)       123.180.141.140         1231 185.0123.110       HTTP       538 HTTP/1.1 200 oK (text/html)       123.180.141.140       HTTP         1231 185.1123.112       103       HTTP       538 HTTP/1.1 200 oK (text/html)       123.180.141.140         1231 185.1123.112       103       HTTP       538 HTTP/1.1 200 oK (text/html)       123.180.141.140         1231 185.1123.112       103       HTTP       123.180.141.140       HTTP       120.0 cK (text/html)         1231 180.1141.140       102 168 123.103       HTTP       120.0 cK (text/html)       120.168.123.103       121.120       120.0 cK (text/html)         1231 180.141.140       102 168 123.103       HTTP       120.168.123.103       131.160.141.140       120.168.123.103         1231 180.141.140       HTTP       120.168	414 66.2804110 192.168.123.103 213.180.141.140 HTTP 1099 GET /_cdf/client.js HTTP/1.1
436 69.1592840 192.168.123.103       213.180.141.140       HTTP       566 POST /_cdf/render HTTP/1.1 (application/x-www-form-urlenco         440 69.214.320 213.180.141.140       192.168.123.103       HTTP       538 HTTP/1.1 200 0K (text/html)         558 69.4804690 213.180.141.140       192.168.123.103       HTTP       538 HTTP/1.1 200 0K (text/html)         1233 185.062849 192.168.123.103       213.180.141.140       HTTP       115 GET / HTTP/1.1         1374 185 311272 213 180 141 140       102 168 123 103       HTTP       472 HTTP/1 1 200 0K (text/html)         ************************************	420 66.3408530 213.180.141.140 192.168.123.103 HTTP 610 HTTP/1.1 200 OK (text/javascript)
440 09, 114120, 113, 100, 141, 140       192, 108, 123, 103       HTTP       538 HTTP/1.1 200 0K (text/html)         1293 185, 062849 192, 168, 123, 103       HTTP       115 6ff / HTTP/1.1         1274 185, 1022 312       180, 141, 140       HTTP       115 6ff / HTTP/1.1         1374 185, 1022 312       180, 141, 140       HTTP       115 6ff / HTTP/1.1         1374 185, 1022 312       180, 141, 140       HTTP       115 6ff / HTTP/1.1         1374 185, 11272 312       180, 141, 140       HTTP       115 6ff / HTTP/1.1         ************************************	436 69.1592840 192.168.123.103 213.180.141.140 HTTP 566 POST /_cdf/render HTTP/1.1 (application/x-www-form-urlenco
1293 185.06284 192.168.123.103       213.180.141.140       HTTP       1115 GET / HTTP/1.1         1274 185 311272 213 180 141 140       102 168 123 103       HTTP       472 HTTP/1.1       100 ow (fevt/html)         #       #       #       #       472 HTTP/1.1       200 ow (fevt/html)       #         #       #       #       #       #       #       #       #       #         # <td>440 09.2144320213.180.141.140 192.108.123.103 HTP 538 HTP/1.1 200 0K (text/html) 558 60 4804690213 180 141 140 192 168 123 103 HTP 538 [tre pergammission] HTP/1 200 0K (text/html)</td>	440 09.2144320213.180.141.140 192.108.123.103 HTP 538 HTP/1.1 200 0K (text/html) 558 60 4804690213 180 141 140 192 168 123 103 HTP 538 [tre pergammission] HTP/1 200 0K (text/html)
1274 185 311272 213 180 141 140       102 168 123 102       HTTP       A72 HTTP/1 1 200 0V (fevt/html)         #       #       #       #       #       #         #       Frame 325: 1115 bytes on wire (8920 bits), 1115 bytes captured (8920 bits) on interface 0       #       #       #         #       Ethernet II, Src: WistronLc6:15:c3 (f0:de:f1:c6:15:c3), Dst: Amit_62:fa:dc (00:50:18:62:fa:dc)       #       #       #         #       Transmission Control Version 4, Src: 192.168.123.103 (192.168.123.103), Dst: 213.180.141.140 (213.180.141.140)       #       #       #         #       Transmission Control Protocol, Src Port: 50013 (50013), Dst Port: http (80), Seq: 1, Ack: 1, Len: 1061       #         #       Hypertext Transfer Protocol       #       #       #       #         0000       00 50 18 62 fa dc f0 de f1 c6 15 c3 08 00 45 00       .P.b       .P.b       #         010 04 4d 35 ba 40 00 80 06 00 00 c0 a8 7b 67 d5 b4       .MS.@       .MS.@       .       .         0200 8d 8c c3 5d 00 50 03 3c 56 87 8c 91 a2 39 50 18	1293 185.062849 192.168.123.103 213.180.141.140 HTTP 1115 GET / HTTP/1.1
m       m	137/ 185 211070 012 180 1/1 1/0 100 168 102 102 HTTP // 12 000 nr (+avt/html)
B Frame 325: 1115 bytes on wire (8920 bits), 1115 bytes captured (8920 bits) on interface 0 E thernet II, Src: WistronI_c6:15:c3 (f0:de:f1:c6:15:c3), Dst: Amt_62:fa:dc (00:50:18:62:fa:dc) B Internet Protocol Version 4, Src: 192.168.123.103 (192.168.123.103), Dst: 213.180.141.140 (213.180.141.140) Transmission Control Protocol, Src Port: 50013 (50013), Dst Port: http (80), Seq: 1, Ack: 1, Len: 1061 Hypertext Transfer Protocol Phypertext Transfer Protocol 2000 00 50 18 62 fa dc f0 de f1 c6 15 c3 08 00 45 00 .P.bE. 2010 04 4d 35 ba 40 00 80 06 00 00 co a8 7b 67 d5 b4 .M5.@{g} 2020 8d 8c c3 5d 00 50 03 3c 56 87 8c 91 a2 39 50 18], P.< V9P. 2030 01 00 a3 90 00 00 07 45 54 20 27 20 48 54 54 55 0GE / HTTP	
Definite 11, sic. wistorin_co.in.cs (inde_file(0,1).cs)(s), sic. All(c) (0,10,10,0,114,140)         Internet Protocol Version 4, src: 192.168.123.103 (192.168.123.103), ost: 213.180.141.140 (213.180.141.140)         Transmission Control Protocol, src Port: 50013 (50013), Dst Port: http (80), Seq: 1, Ack: 1, Len: 1061         Hypertext Transfer Protocol         2000 00 50 18 62 fa dc f0 de f1 c6 15 c3 08 00 45 00, b, c, e.         010 04 4d 35 ba 40 00 80 06 00 00 c0 a8 7b 67 d5 b4, Ms.@(g)         0200 8d 8c c3 5d 00 50 03 3c 56 87 8c 91 a2 39 50 18, pr.         0200 00 3a 90 00 00 47 45 54 20 27 20 48 54 54 55 0	B Frame 325: 1115 bytes on wire (8920 bits), 1115 bytes captured (8920 bits) on interface 0
Transmission Control Protocol, Src Port: 50013 (50013), Dst Port: http (80), Seq: 1, Ack: 1, Len: 1061 Hypertext Transfer Protocol           0000         00         50         18         62         fa         dc         f0         fa         f0         fa	The prefer Protocol Version 4. Src: 192, 168, 123, 103 (192, 168, 123, 103), DSt. 301 (00, 30, 150, 02, 168, 02)
Bypertext Transfer Protocol          0000       00       50       18       62       fa       dc       f0       de       f1       c6       15       c3       08       00       45       00	Transmission Control Protocol, Src Port: 50013 (50013), Dst Port: http (80), Seq: 1, Ack: 1, Len: 1061
0000       00       50       18       62       fa       dc       f0       de       f1       c6       15       c3       08       00       45       00	B Hypertext Transfer Protocol
0000       00       50       18       62       fa       dc       f0       de       f1       c6       15       c3       08       00       45       00       .P.b	
0000       00       50       18       62       fa       dc       f0       de       f1       c6       15       c3       08       00       45       00       .P.b	
0000       00       50       18       62       fa       dc       f0       de       f1       c6       15       c3       08       00       45       00       .P.b	
0000       00       50       18       62       fa       dc       f0       e       f1       c6       15       c3       08       00       45       00       .P.b        E.	
2000       00       50       18       62       fa       dc       f0       de       f1       c6       15       c3       08       00       45       00	
0000       00       50       18       62       fa       dc       f0       61       c6       15       c3       08       00       45       00       00       10       04       4d       35       ba       40       00       80       06       00       00       ca       a       76       76       b4	
0010 04 4d 35 ba 40 00 80 06 00 00 c0 a8 7b 67 d5 b4	0000 00 50 18 62 fa dr f0 de f1 r6 15 r3 08 00 45 00 P b
0020 8d 8c c3 5d 00 50 03 3c 56 87 8c 91 a2 39 50 18].P.< V9P. 0030 01 00 a3 90 00 00 47 45 54 20 2f 20 48 54 54 50GE T / HTTP	0010 04 4d 35 ba 40 00 80 6 00 06 00 c0 a8 7b 67 d5 b4
0030 01 00 ab 50 00 00 47 45 54 20 21 20 48 54 54 50 de 1 / http	0020 8d 8c c3 5d 00 50 03 3c 56 87 8c 91 a2 39 50 18].P.< V9P.
J040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 72 e /1.1Ho st: www.	0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e /i.i.Ho st: www.
NSS. 65 65 74 20 70 65 04 02 42 65 66 65 62 74 oppt n Conport M Reater VCle FF Finity Controller: Nevice N Packets: 402 Displayed: 16 Marked: 0 Profile: Default	0050, 5t 56 74 2a 70 5c 0d 0.5 42 56 56 55 274 connect and connect and the second sec

Czy dla każdego żądania nawiązywana była oddzielna sesja TCP, czy też oba żądania były obsłużone w jednej sesji?

Capturing from Realtek PCIe FE Family Controller: \Device\NPF_(CE90751F-1E7B-470B-8548-DD99E8AF1AA9) [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)]	the second se
Lie Edit View Go Capture Analyze Statistics Telephony Tools Internals Help	
≝ ≝ ≝ ≝ ≝ ≡ ≣ % 2° ≜ I °,	
Filter: http && ip.addr == 213.180.141.140	
No. Time Source Destination Protocol Length Info	
325 65.7133740192.168.123.103 213.180.141.140 HTTP 1115 GET / HTTP/1.1	
412 66.2662/10.213.180.141.140 192.168.123.103 HTTP 460 HTTP/1.1 200 0K (TeXT/hTml) 414 66.2864110.192.168.123.103 213.180.141.140 HTTP 109 GET / cdf/client.is HTTP/1.1	E
420 66.3408530 213.180.141.140 192.168.123.103 НТТР 610 НТТР/1.1 200 ок (text/javascript)	
436 69.1592840 192.168.123.103 213.180.141.140 HTTP 566 POST /_cdf/render HTTP/1.1 (application/x-www-form-urlenc	10
440 09.2144320 213.180.141.140 192.108.123.103 HTTP 538 HTP/1.1 200 0K (text/filmi) 558 69.4804690 213.180.141.140 192.168.123.103 HTTP 538 [TCP Retransmission] HTTP/1.1 200 0K (text/html)	
1293 185.062849192.168.123.103 213.180.141.140 HTTP 1115 GET / HTTP/1.1	
137/ 185 211272 213 180 1/1 1/0 102 168 123 103 HTTE /73 HTTE/1 1 200 0K (tevt/html)	1
E ANCENNEE TTOLOGENT VETSTON 4, STEL ADJANGULALIAN (ALLADOUALIAND), DSC. IJELIOULALIAN (AJELIOULALIAN)	
■ Transmission Control Protocol, Src Port: http (80), Dst Port: 50013 (50013), Seq: 35041, Ack: 1062, Len: 406	
Destination port: 50013 (50013) [Stream index: 10]	
Sequence number: 35041 (relative sequence number)	II
[Next sequence number: 35447 (relative sequence number)]	
Header Tenath: 20 bytes	
⊕ Flags: 0x018 (PSH, ACK)	
Window size value: 33	-
Carculated window size: 100501	•
0020 7b 67 00 50 c2 5d 8c 92 2b 19 03 3c 5a ac 50 18 fd P ] + c7 P	In state
0030 00 21 4f 49 00 00 f6 3d d6 19 7c 7b ef 5b ea 26	1
Frame (460 bytes) Reassembled TCP (35446 bytes) Uncompressed entity body (227890 bytes)	
Irransmission Control Protocol (tcp), 20 bytes   Packets: 4336 Displayed: 16 Marked: 0   Profile: Default	
Capturing from Realtek PCIe FE Family Controller: \Device\NPF_(CE90751F-1E78-4708-8548-DD99E8AF1AA9) [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)]	×
<u>File Edit View Go Capture Analyze Statistics Telephony Iools Internals H</u> elp	
■         ●	
■         ●	
Image: Source       Destination       Protocol       Length       Image: Source       Protocol       Length       Image: Source       Protocol       Length       Image: Source       I	-
Image: Source       Destination       Protocol       Length       Image: Source       Destination         325       65.7/1337/40       192.168.123.103       213.180.141.140       Protocol       Length       Info         412       66. 2662/10.213.180.141.140       192.168.123.103       213.180.141.140       HTTP       113.66.7       HTTP/1.1         412       66. 2662/10.213.180.141.140       HTTP       109.9 GeT       /cdf/client_js       HTTP/1.1         414       66. 2662/10.123.180.141.140       HTTP       109.9 GeT       /cdf/client_js       HTTP/1.1         414       66. 2804110.192.168.123.103       213.180.141.140       HTTP       109.9 GeT       /cdf/client_js       HTTP/1.1	× E
Image: Source       Destination       Protocol       Length       Image: Source       Destination         No.       Time       Source       Destination       Protocol       Length       Info         325       65.7133740       192.168.123.103       213.180.141.140       HTTP       1115       GET       / HTTP/1.1         412       66.2662710       213.180.141.140       HTTP       1109       GET       / Col (text/html)         414       66.2662710       213.180.141.140       HTTP       1099       GET       / Col (text/html)         414       66.3408530       213.180.141.140       192.168.123.103       HTTP       610       HTTP/1.1       200       ock       (text/javascript)         420       66.3408530       213.180.141.140       192.168.123.103       HTTP       610       HTTP/1.1       200 oK       (text/javascript)         436       69.1592840       192.168.123.103       HTTP       610       HTTP/1.1       (application/x-www-form-urlend)	×
Image: Solution of the system of the syst	Ē
Image: Solution of the second seco	
Image: Solution of the second seco	
Image: Solution of the second seco	
Image: Solution of the second seco	
Image: Source	
Image: Solution of the second seco	
Image: Solution of the second seco	
Image: Solution of the second seco	
Image: Solution of the second seco	
Image: Solution of the second seco	
Image: Solution of the second seco	
Image: Solution of the second seco	
Image: Solution of the second seco	

Co daje niezamykanie połączeń (czyli http w trybie keep-alive)? Jakie są możliwe problemy?

#### VI. IP



Nagłówek IPv4 - tą część wykonujemy z włączonym łapaniem pakietów

## Przeanalizuj zawartość nagłówka IP

Eile Edit View Go Capture Analyze Statistics Telephony Iools Internals Help	
Filter: http   Expression Clear Apply Save	
No Time Source Dertination Drotocol Length Info	÷
Frame 5: 123 bytes on wire (984 bits), 123 bytes captured (984 bits) on interface 0	
B Ethernet 11, SrC: Wistroni_colls:cs (r0:de:r1:colls:cs), DsC: Amnt_oc:ra:dc (00:30:18:02:ra:dc) ■ Internet Protocol Version 4, Src: 192.168.123.103 (192.168.123.103), Dst: 213.180.142.191 (213.180.142.191)	
Version: 4 Header length: 20 bytes	
B Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))     Total Length: 109	
Identification: 0x4035 (16437)	
Fragment offset: 0	
Protocol: TCP (6)	
Header checksum: 0x0000 [incorrect, should be 0x19d2 (may be caused by "IP checksum off[oad"?)] Source: 192.168.123.103 (192.168.123.103)	
Destination: 213.180.142.191 (213.180.142.191) [Source GeoIP: Unknown]	
[Destination GeoIP: Unknown] Transmission Control Protocol, Src Port: 50203 (50203), Dst Port: http://800. Seg: 1426. Ack: 1, Len: 69	
Hypertext fransfer Protocol     Line-based text data: application/x-www-form-urlencoded	
0000 00 50 18 62 fa dc f0 de f1 c6 15 c3 08 00 45 00 .P.b	
0010 00 6d 40 35 40 00 80 06 00 00 c0 a8 7b 67 d5 b4	•
Frame (123 bytes) Reassembled TCP (1494 bytes)	
Internet Protocol Version 4 (ip), 20 bytes     Packets: 586 Displayed: 177 Marked: 0     Profile: Default	
Wybierz pakiet zawierający odpowiedź http	
5 0.01752200 192.168.123.103 213.180.142.191 HTTP 123 POST /0/? HTTP/1.1 (application/x-www-form-u	rlencoded
9 0.05956000 213.180.142.191 192.168.123.103 HTTP 115 HTTP/1.1 200 OK (text/html) 13 0.78371000 fe80::f850:ac2b:20cff02::c SSDP 208 M-SEARCH * HTTP/1.1	
17 1.84691800 192.168.123.103 213.180.141.140 HTTP 1115 GET / HTTP/1.1	ne.templa
79 2.01549100 213.180.141.142 192.168.123.103 HTTP 343 HTTP/1.1 304 Not Modified	gereempra
96 2.10658300 192.108.123.103 213.180.141.148 HTTP 11/0 GET /S.CSF/405K0TeS/S.CSS HTTP/1.1 101 2.13907500 213.180.141.148 192.168.123.103 HTTP 343 HTTP/1.1 304 Not Modified	
102 2.14345600 192.168.123.103 213.180.141.142 HTTP 550 GET /images/pulscms/MDg7MDA_/78b9324830ba025e 103 2.14486300 192.168.123.103 213.180.141.145 HTTP 536 GET / m/55fade2068e7503eae8d7ddf5eb6bd09.0.29	2991d9974 .aif HTTP
104 2.14841800 213.180.141.140 192.168.123.103 HTTP 435 HTTP/1.1 200 OK (text/html)	
105 2.107 304 00 122.108.123.1 259.259.259.250 350F 350 KOTAPT HTTP/.11 106 2.17232500 213.180.141.142 192.168.123.103 HTTP 301 HTTP/1.1 304 Not Modified	
> Jakie jest TTL ?	
Jakie jest TTL?      Capturing from Realtek PCIe FE Family Controller: \Device\NPF (CE90751F-1E78-4708-8548-DD99E8AF1AA9) [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)]	• ×
Jakie jest TTL?     Capturing from Realtek PCIe FE Family Controller: \Device\NPF_(CE90751F-1E7B-470B-8548-DD99E8AF1AA9) [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)]     Eile Edit View Go Capture Analyze Statistics Telephony Tools Internals Help	
➤ Jakie jest TTL? I Capturing from Realtek PCle FE Family Controller: \Device\NPF_(CE90751F-1E7B-4708-8548-DD99E8AF1AA9) [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)] Eile Edit View Go Capture Analyze Statistics Telephony Iools Internals Help I See See See See See See See See See Se	• ×
► Jakie jest TTL? I Capturing from Realtek PCIe FE Family Controller: \Device\NPF_(CE90751F-1E78-4708-8548-DD99E8AF1AA9) [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)] File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help I I I I I I I I I I I I I I I I I I I	• X
<ul> <li>➢ Jakie jest TTL?</li> <li>☑ Capturing from Realtek PCIe FE Family Controller: \Device\NPF_(CE90751F-1E78-4708-8548-DD99E8AF1AA9) [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)]</li> <li>□ Edit View Go Capture Analyze Statistics Telephony Iools Internals Help</li> <li>□ Edit View Go Capture Analyze Statistics Telephony Iools Internals Help</li> <li>□ Edit View Go Capture Analyze Statistics Telephony Iools Internals Help</li> <li>□ Edit View Go Capture Analyze Statistics Telephony Iools Internals Help</li> <li>□ Edit View Go Capture Analyze Statistics Telephony Iools Internals Help</li> <li>□ Edit View Go Capture Analyze Statistics Telephony Iools Internals Help</li> <li>□ Edit View Go Capture Analyze Statistics Telephony Iools Internals Help</li> <li>□ Edit View Go Capture Analyze Statistics Telephony Iools Internals Help</li> <li>□ Edit View Go Capture Analyze Statistics Telephony Iools Internals Help</li> <li>□ Edit View Go Capture Analyze Statistics Telephony Iools Internals Help</li> <li>□ Edit View Go Capture Analyze Statistics Telephony Iools Internals Help</li> <li>□ Edit View Go Capture Analyze Statistics Telephony Iools Internals Help</li> <li>□ Edit View Go Capture Analyze Statistics Telephony Iools Internals Help</li> <li>□ Edit View Go Capture Analyze Statistics Telephony Iools Internals Help</li> <li>□ Edit View Go Capture Analyze Statistics Telephony Iools Internals Help</li> <li>□ Edit View Go Capture Analyze Statistics Telephony Iools Internals Help</li> <li>□ Edit View Go Capture Analyze Statistics Telephony Iools Internals Help</li> <li>□ Edit View Go Capture Analyze Statistics Telephony Iools Ioon</li> <li>□ Edit View Go Capture Analyze Statistics Telephony Iools Ioon</li> <li>□ Edit View Go Capture Analyze Statistics Telephony Ioon</li> <li>□ Edit View Go Capture Analyze Statistics Telephony Ioon</li> <li>□ Edit View Go Capture Analyze Statistics Telephony Ioon</li> <li>□ Edit View</li></ul>	• ×
► Jakie jest TTL? Capturing from Realtek PCle FE Family Controller: \Device\NPF_CCE90751F-1E78-4708-8548-DD99E8AF1AA9) [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)] Eile Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Iool Iools Internals Help File Edit View Go Capture Analyze Statistics Iool Iools	• X
> Jakie jest TTL?         I Capturing from Realtek PCle FE Family Controller: \Device\NPF_CCE90751F-1E7B-4708-8548-DD99E8AF1AA9) [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8]]         File Edit Yiew Go Capture Analyze Statistics Telephony Iools Internals Help         I G G G Gapture Analyze Statistics Telephony Iools Internals Help         I G G G Gapture Analyze Statistics Telephony Iools Internals Help         I G G G Gapture Analyze Statistics Telephony Iools Internals Help         I G G G Gapture Analyze Statistics Telephony Iools Internals Help         I G G G Gapture Analyze Statistics Telephony Iools Internals Help         I G G G G Gapture Analyze Statistics Telephony Iools Internals Help         I G G G G Gapture Analyze Statistics Telephony Iools Internals Help         I G G C G G G G G Gapture Analyze Statistics Telephony Iools Internals Help         I G G C G G G G G G G G G G G G G G G G	• ×
▶       Jakie jest TTL?         I Capturing from Realtek PCIe FE Family Controller: \Device\NPF_(CE90751F-1E78-4708-8548-DD99E8AF1AA9)       [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)]         File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help         I Edit View Go Capture Analyze Statistics Telephony Iools Internals Help         I Edit View Go Capture Analyze Statistics Telephony Iools Internals Help         I Edit View Go Capture Analyze Statistics Telephony Iools Internals Help         I Edit View Go Capture Analyze Statistics Telephony Iools Internals Help         I Edit View Go Capture Analyze Statistics Telephony Iools Internals Help         I Edit View Go Capture Analyze Statistics Telephony Iools Internals Help         I Edit View Go Capture Analyze Statistics Telephony Iools Internals Help         I Edit View Go Capture Analyze Statistics Telephony Iools Internals Help         I Edit View Go Capture Analyze Statistics Telephony Iools Internals Help         I Edit View Go Capture Analyze Statistics Telephony Iools Internals Help         I Edit View Go Capture Analyze Statistics Telephony Iools Internals Help         I Edit View Go Capture Analyze Statistics Telephony Iools Internals Help         I Edit View Go Capture Analyze Statistics Telephony Iools Internals Help         I Edit View Go Capture Analyze Statistics Telephony Iools Internals Help         I Edit View Go Capture Analyze Statistics Telephony Iools Internals Help         I Edit View Go Capture Analyze	
<ul> <li>➢ Jakie jest TTL?</li> <li>☑ Capturing from Realtek PCIe FE Family Controller: \Device\NPF_(CE90751F-1E78-4708-8548-DD99E8AF1AA9) [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)]</li> <li>☑ Edit View Go Capture Analyze Statistics Telephony Iools Internals Help</li> <li>☑ I I I I I I I I I I I I I I I I I I I</li></ul>	• X
► Jakie jest TTL? Capturing from Realtek PCLe FE Family Controller: \Device\NPF_CE90751F-1E78-4708-8548-DD99E8AF1AA9) [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)] File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help Filter: http Expression Clear Apply Save No. Time Source Destination Protocol Length Info 105 2.16756400 192.166.123.1 239.255.255.250 SD0P 369 NOTTEY * HTTP/1.1 106 2.17232500 213.180.141.142 192.168.123.103 HTTP 301 HTTP/1.1 304 Not Modified 108 2.17440000 213.180.141.145 [213.180.141.145 (213.180.141.145), Dst: 192.168.123.103 (192.168.123.103) Version: 4 Header length: 20 bytes B Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00; Not-ECT (Not ECN-Capable Transport))	
► Jakie jest TTL? Capturing from Realtek PCIe FE Family Controller: \Device\NPF_CCE90751F-1E78-4708-8548-DD99E8AF1AA9) [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8]] File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File: http Expression Clear Apply Save No. Time Source Destination Protocol Length Info 104 2.14841800 213.180.141.140 Postocol Length Info 104 2.14841800 213.180.141.142 192.168.123.103 HTTP 309 HTTP/1.1 200 C (Ext/ntml) 105 2.16756400 192.166.123.1 29.255.255.250 29.09 NOTIFY * HTTP/1.1 106 2.17232500 213.180.141.142 192.168.123.103 HTTP 309 HTTP/1.1 304 Not Modified 108 2.17440000 213.180.141.145 192.168.123.103 HTTP 309 HTTP/1.1 304 Not Modified Version: 4 Header length: 20 bytes B Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)) Total Length: 295 Identification: 0x892f (35119)	
➤ Jakie jest TTL? Capturing from Realtek PCLe FE Family Controller: \Device\NPF_(CE90751F-1E78-4708-8548-DD99E8AF1AA9) [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)] File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help Filter: http Expression Clear Apply Save No. Time Source 104 2.14841800 213.180.141.140 Period Internals Help Expression Clear Apply Save No. Time Source 104 2.14841800 213.180.141.140 Period Internals Help Filter: http Period Internals Help Period Internals Help Filter: http Period Internals Help Period Internals Period Internals Help <p< td=""><td></td></p<>	
Jakie jest TTL? Capturing from Realtek PCie FE Family Controller: \Device\NPF_(CE90751F-1E78-4708-8548-DD99E8AF1AA9) [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)] File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help File Market Back PCI FE Family Controller: View Go Capture Analyze Statistics Telephony Tools Internals Help File: http File: http File: Expression Clear Apply Save No. Time Source Source Destination Protocol Length Info 104 2.14841800 213.180.141.140 192.16756400 192.168.123.1 2 239.255.255.255 SSDP 369 NoTTPY * HTTP/1.1 106 2.17232500 213.180.141.142 192.168.123.103 HTTP 301 HTTP/1.1 304 Not Modified 108 2.17440000 213.180.141.145 192.168.123.103 HTTP 301 HTTP/1.1 304 Not Modified Version: 4 Header length: 20 bytes B Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)) Total Length: 20 bytes B Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)) Total Length: 20 for 10 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)) Total Length: 20 for 10 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)) Total Length: 20 for 10 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)) Total Length: 20 for 10 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)) Total Length: 20 for 10 (DSCP 0x00: DEfa	
<pre>&gt; Jakie jest TTL? Capturing from Realtek PCIe FE Family Controller: \Device\NPF_[CE90751F-1E78-4708-8548-DD99E8AF1AA9] [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8]) File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help Filter http No. Time Source Destination Protocol Length Info HIIP + 459 HIIP/1.1 200 OK (TEXT/ITEII)) 105 2.16756400 192.168.123.1 239.255.255.250 SSDP 369 NOTIFY * HTTP/1.1 106 2.17232500 213.180.141.142 192.168.123.103 HTTP 301 HTTP/1.1 304 Not Modified 108 2.17440000 213.180.141.145 192.168.123.103 HTTP 309 HTTP/1.1 304 Not Modified 108 2.17440000 213.180.141.145 (213.180.141.145), Dst: 192.168.123.103 (192.168.123.103) Version: 4 Header length: 20 bytes B Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)) Total Length: 295 Identification: 0x892f (35119) B Flags: 0x02 (Don't Fragment) Ergent ffert: 0 From tool ive: 56 Protocol: TCP (6) B Header Checksum: 0x194c [correct]</pre>	
➤ Jakie jest TTL? Capturing from Realtek PCIe FE Family Controller. 'Device\NPF_(CE90751F-1E78-4708-8548-DD99E8AF1AA9) [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)] File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help Fotocol Internet Protocol View Iool Internet Protocol View Iool Internet Protocol View Stole Analyze Ioon Ioon Ioon Ioon Ioon Ioon Ioon Ioo	
<ul> <li>➢ Jakie jest TTL?</li> <li>☑ Capturing from Realtek PCIe FE Family Controller: \Device\NPF_ICE00751F-1E78-4708-8548-DD99E8AF1AA9 [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)]</li> <li>☑ I i i i i i i i i i i i i i i i i i i</li></ul>	
<pre>&gt; Jakie jest TTL? Copturing from Reatek PCIe FE Family Controller: Device\NPF_(CE90751F-1E78-4708-8548-DD99E8AF1AA9) [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)] File Edit View So Capture Analyze Statistics Telephony Iools Internals Help File Edit View So Capture Analyze Statistics Telephony Iools Internals Help File Edit View So Capture Analyze Statistics Telephony Iools Internals Help File Edit View So Capture Analyze Statistics Telephony Iools Internals Help File Edit View So Capture Analyze Statistics Telephony Iools Internals Help File Edit View So Capture Analyze Statistics Telephony Iools Internals Help File Edit View So Capture Analyze Statistics Telephony Iools Internals Help File Edit View So Capture Analyze Statistics Telephony Iools Internals Help File Edit View So Capture Analyze Statistics Telephony Iools Internals Help File Edit View So Capture Analyze Statistics Telephony Iools Internals Help File Edit View So Capture Analyze Statistics Telephony Iools Internals Help File Edit View So Capture Analyze Statistics Telephony Iools Internals Help File Edit View So Capture Analyze Statistics Telephony Iools Internals Help File Edit View So Capture Analyze Statistics Telephony Iools Internals Help File Edit View So Capture Analyze Statistics Telephony Iools Internals Help File Edit View So Capture Analyze Statistics Telephony Iools Internals Help File Edit View So Capture Analyze Statistics Telephony Iools Internals Help File Edit View So Capture Analyze Statistics Telephony Iools Internals Help Hilp Hilp Hilp Hilp Hilp Hilp Hilp Hi</pre>	
<pre>&gt; Jakie jest TTL? Copturing from Realtek PCIe FE Family Controller: NewiceNNPF_CCE90751F-1E78-4708-8548-DD99E8AF1AA9 [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8]] File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help File Edit View Go Capture Analyze Statistics Telephony Telephony</pre>	
<pre>&gt; Jakie jest TTL? Capturing from Realtek PCLF FF Tamily Controller: (Device\NPF_CE90751F-1E78-4708-8548-DD99E8AF1AA9) [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8]) File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help File Edit View Go Capture Analyze Statistics Internals Help File Internet Protocol View Idea Internals Interna</pre>	
<pre>&gt; Jakie jest TTL? Capturing from Realtek PCIe FE Family Controller: Device\NPF_(CE90731F-1E78-4708-8548-DD99E8AF1AA9) [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8]) File fait View So Sapture Analyze Statistics Telephony Tools Internals Help File fait View So Sapture Analyze Statistics Telephony Tools Internals Help File fait View So Sapture Analyze Statistics Telephony Tools Internals Help File fait View So Sapture Analyze Statistics Telephony Tools Internals Help File fait View So Sapture Analyze Statistics Telephony Tools Internals Help File fait View So Sapture Analyze Statistics Telephony Tools Internals Help File fait View So Sapture Analyze Statistics Telephony Could Part Analyze Save No. Time Source Destination Foreign Internals Help File fait View So View So Sapture Analyze Statistics Telephony Could Part Analyze Save No. Time Source Could Part Internation Protocol Length Info 105 2.17440000 213.180.141.145 192.168.123.103 HTTP 301 HTTP/1.1 304 Not Modiffied 108 2.17440000 213.180.141.145 192.168.123.103 HTTP 309 HTTP/1.1 304 Not Modiffied 108 2.17440000 213.180.141.145 (213.180.141.145 (213.180.141.145), Dst: 192.168.123.103 (192.168.123.103) Version: 4 Header length: 20 bytes B Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)) Total Length: 20 Syste 10 File Total Control Protocol, Sec Port: http (80), Dst Port: 50209 (50209), Seq: 1, Ack: 483, Len: 255 B Hyperex Transfer Protocol Coll 0 12 7 89 Zf 40 00 00 06 19 4c d5 b4 8d 91 c0 a8</pre>	

# > W jakim celu wprowadzono pole Protocol?

		5		-				
🔼 Ca	pturing from	Realtek PCIe FE Family Co	ntroller: \Device\NPF_(	E90751F-1E7B-470E	-8548-DD99E8AF1AA9	} [Wireshark 1.8.4 (SVN Rev 46250 from	n /trunk-1.8)]	
Eile	Edit View	Go Capture Analyze	Statistics Telephon		Help			
m								
					] = विवय			
Filter	http			- Expre	ssion Clear Apply	Save		
No	Time	Course	Dectiontion	Deat	acal Lonath Info			
110.	104 2.1484	1800 213.180.141.	140 192.108.	123.103 HI	P 435 H11P/	1.1 200 OK (TEXT/NTMI)		<u> </u>
	LO5 2.1675	6400 192.168.123.	1 239.255.	255.250 SSI	OP 369 NOTIF	Y * HTTP/1.1		
	LOG 2.1723	2500 213.180.141.	142 192.168.	L23.103 HTT	P 301 HTTP/	1.1 304 Not Modified		
1	LO8 2.1744	0000 213.180.141.	145 192.168.	123.103 HTT	P 309 HTTP/	1.1 304 Not Modified		-
< 📃					m			
æ	Version: Header le Different Total Len Identific Flags: Ox Fragment	4 ngth: 20 bytes iated Services Fi gth: 295 ation: 0x892f (35 02 (Don't Fragmen offset: 0	eld: 0x00 (DSCP 119) 1t)	0x00: Default	; ECN: 0x00: No	t-ECT (Not ECN-Capable Tran:	;port))	
1	Protocol:	TCP (6)						
	Woader ch	ecksum: 0:194c [c	orrect]					
	Source: 2	13.180.141.145 (2	13.180.141.145)					
	Destinati	on: 192.168.123.1	.03 (192.168.123	.103)				E.
	[source G	eoIP: Unknown]	20 <b>.</b>					
10.000	LDestinat	10n Geoip: Unknow	/nj J. Sne Bonti ht	to (00) Det 1	ant - 50200 (502	00) 5001 1 4561 182 1001	255	
	ansmissic	n control Protoco	of, Src Port: ht	Cp (80), DST P	ort: 50209 (502	09), Seq: I, ACK: 483, Len:	200	
(a m)	percext	Tansfel Prococor						
0010	01 27 8	9 2f 40 00 38 00	19 4c d5 b4 8d	91 c0 a8 .	./@.8 <mark>.</mark> .L			
0020	00 0e 4	0 1b 00 00 48 54	54 50 2f 31 2e	31 20 33	a HT TP/1.1 3			
0040	30 34 2	0 4e 6f 74 20 4d	6f 64 69 66 69	65 64 0d 04	Not M odified.			
0050	0a 44 6	1 74 65 3a 20 53	61 74 2c 20 30	38 20 44 .D	ate: 5 at, 08 D			*
0 2	Protocol (ip	proto), 1 byte	Packets: 523	B Displayed: 740 Mar	ced: 0	Profile: Default		

# ➢ Co sugeruje obecność pola "Fragment Offset"?

Capturing from Realtek PCIe FE Family Controller: \Device\NPF_[CE90751F-1E7B-470B-8548-DD99E8AF1AA9] [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)]
Eile Edit Yiew Go Capture Analyze Statistics Telephony Iools Internals Help
≝≝≝≝≝≡≣≭≈≓⊟∣҈⇔⇒⇒∓⊈∣≣⊡∣QQQ⊡∣₩⊠⊠®%;⊠
Filter: http
No.         Time         Source         Destination         Protocol Length         Info           104         2.1484L800         115.180.141.140         192.108.123.10         H11P         435 H11P/1.1         200 0K (Text/ntm1)           105         2.16756400         192.168.123.1         239.255.255.250         SSDP         369 NOTEY * HTTP/1.1           106         2.17232500         213.180.141.142         192.168.123.103         HTTP         301 HTTP/1.1         304 Not Modified           108         2.17440000         213.180.141.145         192.168.123.103         HTTP         309 HTTP/1.1         304 Not Modified
<pre>Internet Protocol Version 4, Src: 213.180.141.145 (213.180.141.145), Dst: 192.168.123.103 (192.168.123.103) Version: 4 Header length: 20 bytes B Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)) Total Length: 295 Identification: 0x892f (35119) P Flags. 0x02 (Don t Fragment) Fragment offset: 0 Time to live: 56 Protocol: fCP (6) B Header checksum: 0x194c [correct] Source: 213.180.141.145 (213.180.141.145) Destination: 192.168.123.103 (192.168.123.103) [Source GeoIP: Unknown]</pre>
[Destination GeoIP: Unknown] Transmission Control Protocol, Src Port: http (80), Dst Port: 50209 (50209), Seq: 1, Ack: 483, Len: 255 Hypertext Transfer Protocol
0010 01 27 89 2f 40 00 38 06 19 4c d5 b4 8d 91 c0 a8'./& 8L 0020 7b 67 00 50 c4 21 f7 1e 5b 5b da 10 c8 d5 50 18 {g.p.l. [[P. 0030 00 00 e4 01 b0 00 48 54 54 54 02 f 31 2 2 31 20 33 (HT TP/1.1 3 0040 30 34 20 4e 6f 74 20 4d 6f 64 69 66 69 65 64 0d 04 Not M odified. 0050 0a 44 61 74 65 3a 20 35 161 74 2c 20 38 20 44 Date: 5 at, 08 D 0050 65 62 20 27 20 21 27 20 31 28 29 20 39 24 22 cor 2012 18:00.42 0050 0a 46 17 40 55 ac 00 18 20 38 20 40 04 Date: 5 at, 08 D
Tragment onset (15 bits) (ip.mag_onset), 2 B Patkets: 5551 Displayed: 7.30 Markets: 0 Profile: Default