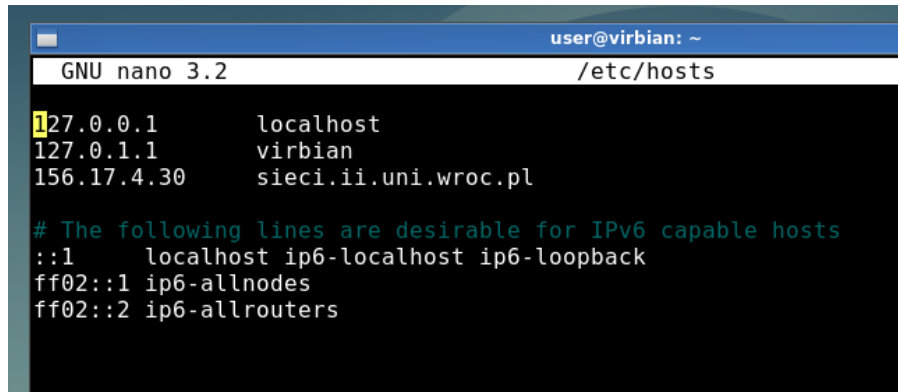


Dawid Dieu
302052

Zadanie do zaprezentowania (2 pkt.)

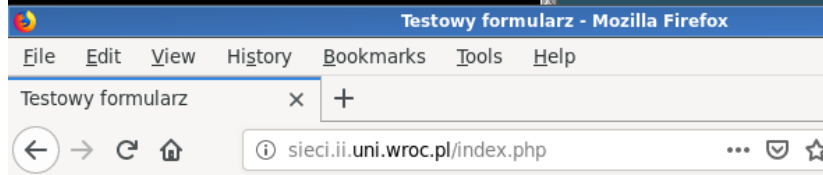
Celem tego zadania jest dodanie nowego wpisu na stronie <http://sieci.ii.uni.wroc.pl/> (<http://sieci.ii.uni.wroc.pl/>). Za pomocą programu `nc`.

- Ponieważ domena sieci.ii.uni.wroc.pl (<http://sieci.ii.uni.wroc.pl/>) nie jest rozpoznawana przez publiczne serwery DNS, dodaj wiersz `156.17.4.30 sieci.ii.uni.wroc.pl` do pliku `/etc/hosts`.



```
user@virbian: ~  
GNU nano 3.2 /etc/hosts  
127.0.0.1    localhost  
127.0.1.1    virbian  
156.17.4.30  sieci.ii.uni.wroc.pl  
  
# The following lines are desirable for IPv6 capable hosts  
::1         localhost ip6-localhost ip6-loopback  
ff02::1     ip6-allnodes  
ff02::2     ip6-allrouters
```

- Wejdź przeglądarką na stronę <http://sieci.ii.uni.wroc.pl/> (<http://sieci.ii.uni.wroc.pl/>) i wykorzystując rozszerzenie przeglądarki Live HTTP Header sprawdź, co dzieje się, kiedy dodajesz jakiś wpis.

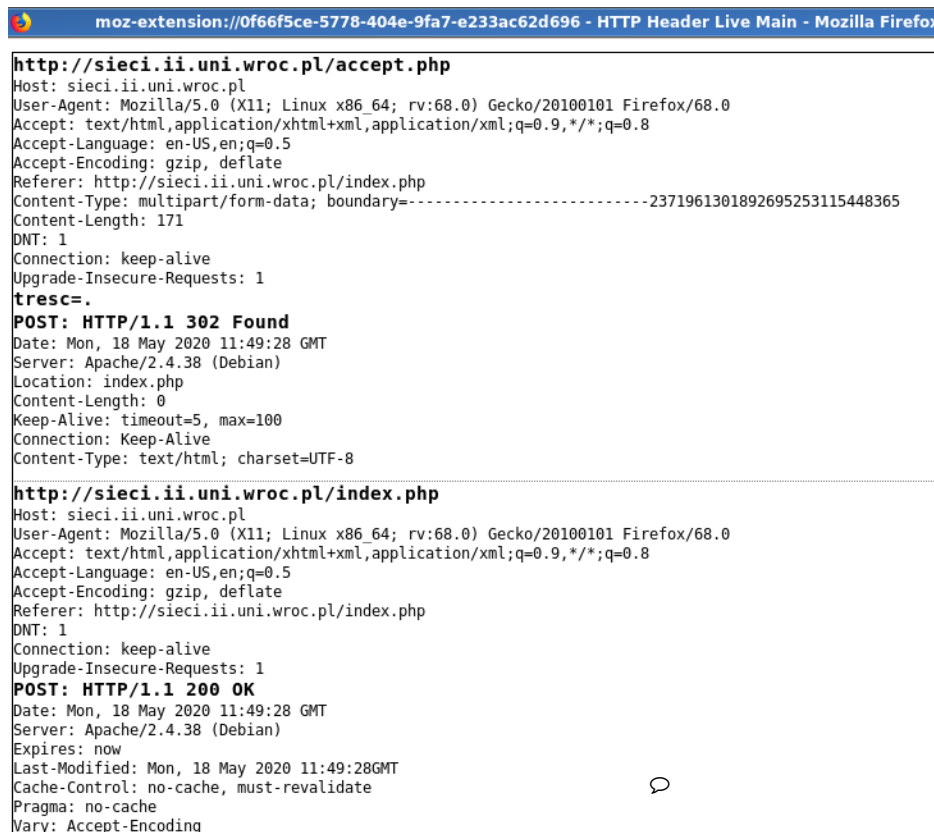


Formularz testowy na podstawie hydeparku Tomasza Wierzbickiego

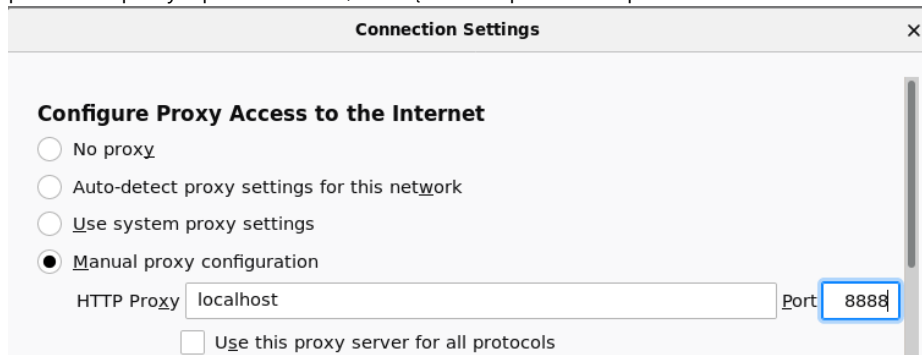
Dodaj uwagę

Wyślij

Wyczyść



- Uruchom program nc w trybie serwera TCP nasłuchującego na porcie 8888 poleceniem
v0\$> nc -l -p 8888 | tee http_request
- Z menu przeglądarki wybierz pozycję *Edit | Preferences*, wyszukaj w opcjach Network settings i w okienku *Connection Settings* wybierz *Manual proxy configuration*. Następnie w polu *HTTP proxy* wpisz **localhost**, a w sąsiednim polu *Port* wpisz 8888.



- Na stronie <http://sieci.ii.uni.wroc.pl/> wpisz jakąś treść w polu „Dodaj uwagę” i kliknij przycisk „Wyślij”. Dlaczego przeglądarka wyświetla w pasku stanu komunikat Waiting for sieci.ii.uni.wroc.pl a odpowiedni wpis nie został

dodany?

```
user@virbian:~$ nc -l -p 8888 | tee http_request
POST http://sieci.ii.uni.wroc.pl/accept.php HTTP/1.1
Host: sieci.ii.uni.wroc.pl
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://sieci.ii.uni.wroc.pl/index.php
Content-Type: multipart/form-data; boundary=-----17561240705817352141291272228
05817352141291272228
Content-Length: 173
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1

-----17561240705817352141291272228
Content-Disposition: form-data; name="tresc"

d
-----17561240705817352141291272228--
```

Formularz testowy na podstawie

Dodaj uwagę

d

Wyślij Wyczyść

Bieżące wpisy

33640: 18-05-2020, 13:49:28

Zmieniliśmy przed chwilą serwer proxy na localhost. Request przez niego nie przechodzi.

- Przerwij działanie programu nc. Co zapisać ten program do pliku **http_request**? Wyłącz ustawienia serwera proxy w przeglądarce.

```
user@virbian:~$ cat http_request
POST http://sieci.ii.uni.wroc.pl/accept.php HTTP/1.1
Host: sieci.ii.uni.wroc.pl
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://sieci.ii.uni.wroc.pl/index.php
Content-Type: multipart/form-data; boundary=-----17561240705817352141291272228
05817352141291272228
Content-Length: 173
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1

-----17561240705817352141291272228
Content-Disposition: form-data; name="tresc"

d
-----17561240705817352141291272228--
user@virbian:~$
```

- Wyślij zapisane zapytanie do serwera WWW poleceniem
`V0$ nc -q 3 sieci.ii.uni.wroc.pl 80 < http_request` i sprawdź przeglądarką, czy odpowiedni komunikat został dodany na stronie WWW

```
user@virbian:~$ nc -q 3 sieci.ii.uni.wroc.pl 80 < http_request
HTTP/1.1 302 Found
Date: Mon, 18 May 2020 12:05:56 GMT
Server: Apache/2.4.38 (Debian)
Location: index.php
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

user@virbian:~$
```

33643: 18-05-2020, 14:05:56

d

- Zmień zawartość pliku **http_request**, wpisując inny komunikat do umieszczenia na stronie. Odpowiednio zmodyfikuj pole **Content-Length**. Ponownie wyślij zapytanie do serwera WWW i upewnij się, że komunikat został dodany na stronie.

```
user@virbian: ~
GNU nano 3.2                                http_request

POST http://sieci.ii.uni.wroc.pl/accept.php HTTP/1.1
Host: sieci.ii.uni.wroc.pl
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://sieci.ii.uni.wroc.pl/index.php
Content-Type: multipart/form-data; boundary=-----
Content-Length: 188
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1

-----17561240705817352141291272228
Content-Disposition: form-data; name="tresc"

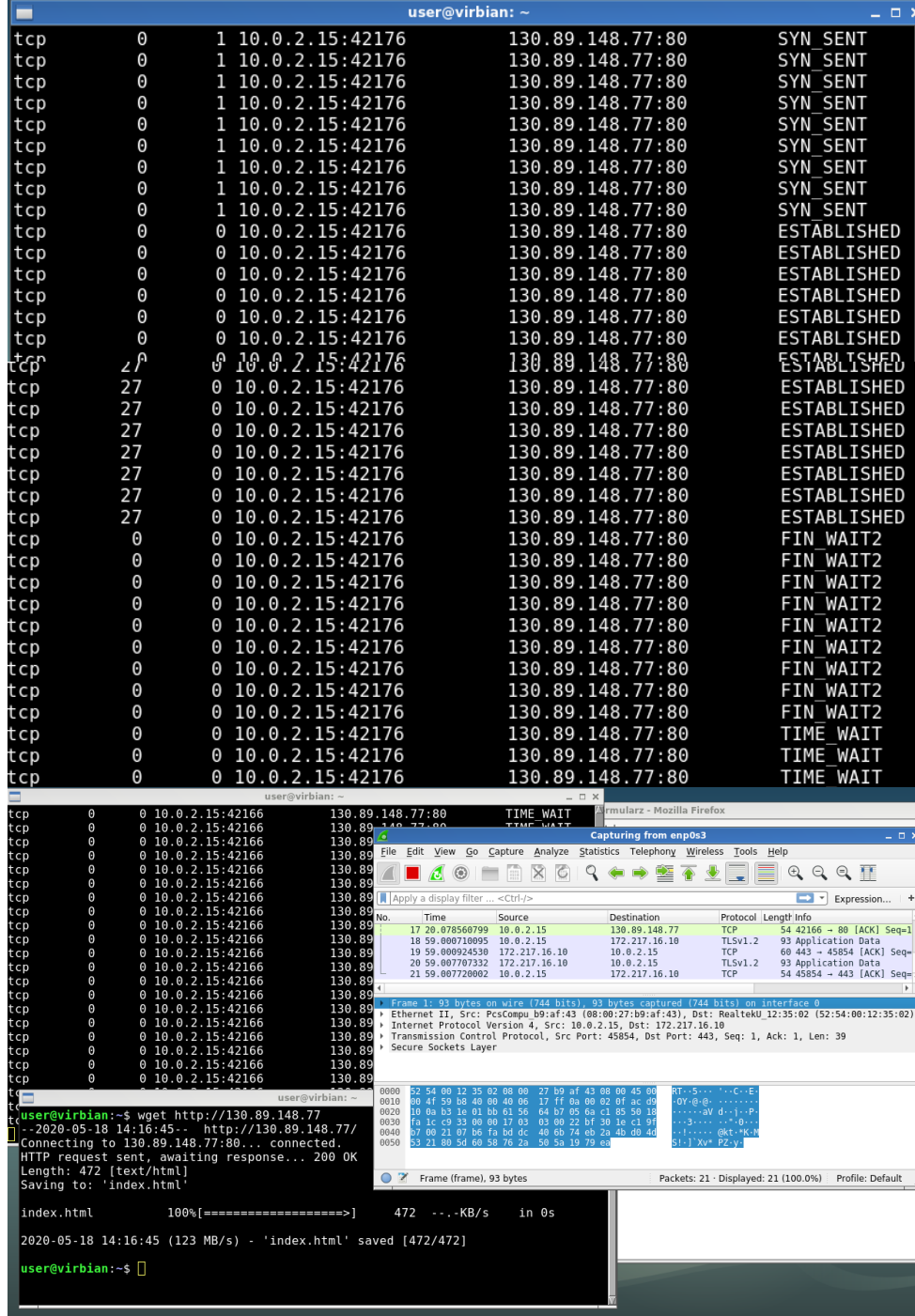
Ostatnie zadanie
-----17561240705817352141291272228--
```

33644: 18-05-2020, 14:08:32
Ostatnie zadanie

Zadanie do zaprezentowania (3 pkt.)

Celem tej części jest przesłanie zmian stanów protokołu TCP i przesyłanych segmentów

- Poleceniem `dig` sprawdź, jakie adresy IP są przypisane do domeny www.debian.org (<http://www.debian.org>). Wybierz jeden z nich; będziemy go nazywać **adres_IP** (130.89.148.77).
- W jednej konsoli uruchom w polecenie
`V0$> (while true; do netstat -tan | grep adres_IP; done) | tee tcp_log`
zaś w drugiej pobierz stronę główną www.debian.org (<http://www.debian.org>). Za pomocą polecenia `V0$> wget http://adres_IP /` (Podaliśmy bezpośrednio adres IP, a nie nazwę domeny, żeby mieć pewność, że będziemy łączyć się z konkretnym adresem IP).
Sprawdź, czy w pliku `tcp_log` zostały zaobserwowane stany TCP gniazda SYN SENT, ESTABLISHED i niektóre ze stanów zamykania połączenia. Jeśli Twoje łącze jest za szybkie i stanów nie udaje się zaobserwować, zmniejsz prędkość pobierania wykorzystując polecenie
`V0$> trickle -d 10 wget http://adres_IP /`



- W Wiresharku obejrzyj pakiety IP i zawarte w nich segmenty TCP związane z wykonaniem powyżej zapytaniem i odpowiedzią HTTP. Jakie gniazda tworzone są do pobierania pliku przez HTTP? Jaki jest port źródłowy a jaki docelowy połączenia? Dla każdego przesyłanego segmentu TCP określ:
 - Jakie z flag SYN / ACK / FIN są włączone dla danego segmentu
 - Które bajty (strumienia danych protokołu HTTP) są przesyłane w segmencie?
 - Które bajty strumienia danych są potwierdzane danym segmentem?
 - Na podstawie diagramu stanów TCP (https://en.wikipedia.org/wiki/File:Tcp_state_diagram.png (https://en.wikipedia.org/wiki/File:Tcp_state_diagram.png)), sprawdź jak zmienia się stan połączenia TCP (po stronie klienta i po stronie serwera) w momencie wystania i odebrania danego segmentu. Które z tych stanów są widoczne w pliku tcp log?

- Ogólny opis wszystkich TCP i HTTP (porty/flagi)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	130.89.148.77	TCP	74	42178 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=74..
2	0.027808484	130.89.148.77	10.0.2.15	TCP	60	80 → 42178 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
3	0.027836228	10.0.2.15	130.89.148.77	TCP	54	42178 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
4	0.027930417	10.0.2.15	130.89.148.77	HTTP	194	GET / HTTP/1.1
5	0.028034290	130.89.148.77	10.0.2.15	TCP	60	80 → 42178 [ACK] Seq=1 Ack=141 Win=65535 Len=0
6	0.055952060	130.89.148.77	10.0.2.15	HTTP	971	HTTP/1.1 200 OK (text/html)
7	0.055969819	10.0.2.15	130.89.148.77	TCP	54	42178 → 80 [ACK] Seq=141 Ack=918 Win=63323 Len=0
8	1.362397079	10.0.2.15	130.89.148.77	TCP	54	42178 → 80 [FIN, ACK] Seq=141 Ack=918 Win=63323 Len=0
9	1.362356084	130.89.148.77	10.0.2.15	TCP	60	80 → 42178 [ACK] Seq=918 Ack=142 Win=65535 Len=0
10	1.389344532	130.89.148.77	10.0.2.15	TCP	60	80 → 42178 [FIN, ACK] Seq=918 Ack=142 Win=65535 Len=0
11	1.389366982	10.0.2.15	130.89.148.77	TCP	54	42178 → 80 [ACK] Seq=142 Ack=919 Win=63323 Len=0
12	1.186.2261372..	fe80::a0b:27ff:feb9..	ff02::12	ICMPv6	70	Router Solicitation from 88:00:27:b9:af:43

- Porty (dokładniej) dla HTTP

4	0.027930417	10.0.2.15	130.89.148.77	HTTP
5	0.028034290	130.89.148.77	10.0.2.15	TCP
6	0.055952060	130.89.148.77	10.0.2.15	HTTP
7	0.055969819	10.0.2.15	130.89.148.77	TCP
8	1.362397079	10.0.2.15	130.89.148.77	TCP
9	1.362536004	130.89.148.77	10.0.2.15	TCP
10	1.389344532	130.89.148.77	10.0.2.15	TCP
11	1.389366982	10.0.2.15	130.89.148.77	TCP
12	1186.2261372...	fe80::a00:27ff:feb9...	ff02::2	ICMPv6

Internet Protocol Version 4, Src: 10.0.2.15, Dst: 130.89.148.77
Transmission Control Protocol, Src Port: 42178, Dst Port: 80, Seq: 1, Ack: 1, Source Port: 42178
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 140]
Sequence number: 1 (relative sequence number)
[Next sequence number: 141 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
0101 = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window size value: 64240
[Calculated window size: 64240]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0x235c [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[SEQ/ACK analysis]
[Timestamps]

- TCPs from server to us:

o No. 2

Ethernet II, Src: RealtekU 12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_b9:af:43 (08:00:27:b9:af:43)
Internet Protocol Version 4, Src: 130.89.148.77, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 80, Dst Port: 42178, Seq: 0, Ack: 1, Len: 0
Source Port: 80
Destination Port: 42178
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
[Next sequence number: 0 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
0110 = Header Length: 24 bytes (6)
Flags: 0x012 (SYN, ACK)
Window size value: 65535
[Calculated window size: 65535]
Checksum: 0x078c [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
Options: (4 bytes), Maximum segment size
[SEQ/ACK analysis]
[Timestamps]

0000	08 00 27 b9 af 43 52 54 00 12 35 02 08 00 45 00	... CRT ..5...E..
0010	00 2c 25 43 00 00 40 06 32 d4 82 59 94 4d 0a 00	..%C...@..2..Y.M..
0020	02 0f 00 50 a4 c2 06 c5 66 01 73 70 e8 8b 60 12	...P...f.sp... ..
0030	ff ff 07 8c 00 00 02 04 05 b4 00 00

o No. 5

Ethernet II, Src: RealtekU 12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_b9:af:43 (08:00:27:b9:af:43)
Internet Protocol Version 4, Src: 130.89.148.77, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 80, Dst Port: 42178, Seq: 1, Ack: 141, Len: 0
Source Port: 80
Destination Port: 42178
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 1 (relative sequence number)
[Next sequence number: 1 (relative sequence number)]
Acknowledgment number: 141 (relative ack number)
0101 = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
Window size value: 65535
[Calculated window size: 65535]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0x1ebd [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[SEQ/ACK analysis]
[Timestamps]

0000	08 00 27 b9 af 43 52 54 00 12 35 02 08 00 45 00	... CRT ..5...E..
0010	00 28 25 44 00 00 40 06 32 d7 82 59 94 4d 0a 00	..(%D...@..2..Y.M..
0020	02 0f 00 50 a4 c2 06 c5 66 02 73 70 e9 17 50 10	...P...f.sp...P..
0030	ff ff 1e bd 00 00 00 00 00 00 00 00

o No. 9

▶ Ethernet II, Src: RealtekU 12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_b9:af:43 (08:00:27:b9:af:43)		
▶ Internet Protocol Version 4, Src: 130.89.148.77, Dst: 10.0.2.15		
▼ Transmission Control Protocol, Src Port: 80, Dst Port: 42178, Seq: 918, Ack: 142, Len: 0		
Source Port: 80		
Destination Port: 42178		
[Stream index: 0]		
[TCP Segment Len: 0]		
Sequence number: 918 (relative sequence number)		
[Next sequence number: 918 (relative sequence number)]		
Acknowledgment number: 142 (relative ack number)		
0101 = Header Length: 20 bytes (5)		
▶ Flags: 0x010 (ACK)		
Window size value: 65535		
[Calculated window size: 65535]		
[Window size scaling factor: -2 (no window scaling used)]		
Checksum: 0x1b27 [unverified]		
[Checksum Status: Unverified]		
Urgent pointer: 0		
▶ [SEQ/ACK analysis]		
▶ [Timestamps]		
0000	08 00 27 b9 af 43 52 54 00 12 35 02 08 00 45 00	..'.CRT..5..E.
0010	00 28 25 46 00 00 40 06 32 d5 82 59 94 4d 0a 00	..(%F..@.2..Y.M..
0020	02 0f 00 50 a4 c2 06 c5 69 97 73 70 e9 18 50 10	...P...1sp..P.
0030	ff ff 1b 27 00 00 00 00 00 00 00 00
Sequence number (tcp.seq), 4 bytes		
Packets: 1		

o No. 10

▶ Ethernet II, Src: RealtekU 12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_b9:af:43 (08:00:27:b9:af:43)		
▶ Internet Protocol Version 4, Src: 130.89.148.77, Dst: 10.0.2.15		
▼ Transmission Control Protocol, Src Port: 80, Dst Port: 42178, Seq: 918, Ack: 142, Len: 0		
Source Port: 80		
Destination Port: 42178		
[Stream index: 0]		
[TCP Segment Len: 0]		
Sequence number: 918 (relative sequence number)		
[Next sequence number: 918 (relative sequence number)]		
Acknowledgment number: 142 (relative ack number)		
0101 = Header Length: 20 bytes (5)		
▶ Flags: 0x011 (FIN, ACK)		
Window size value: 65535		
[Calculated window size: 65535]		
[Window size scaling factor: -2 (no window scaling used)]		
Checksum: 0x1b26 [unverified]		
[Checksum Status: Unverified]		
Urgent pointer: 0		
▶ [Timestamps]		
0000	08 00 27 b9 af 43 52 54 00 12 35 02 08 00 45 00	..'.CRT..5..E.
0010	00 28 25 47 00 00 40 06 32 d4 82 59 94 4d 0a 00	..(%G..@.2..Y.M..
0020	02 0f 00 50 a4 c2 06 c5 69 97 73 70 e9 18 50 11	...P...1sp..P.
0030	ff ff 1b 26 00 00 00 00 00 00 00 00	...&....