

TP 4 - Étude des protocoles UDP et TCP

Étude du protocole UDP

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.1	192.168.1.2	DNS	Standard query

A www.google.fr

Frame 1 (73 bytes on wire, 73 bytes captured)
Ethernet II, Src: BbnInter_bf:bf:bb (02:04:06:bf:bf:bb), Dst: BbnInter_e3:c4:48 (02:04:06:e3:c4:48)
...
Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.2 (192.168.1.2)
Version: 4
Header length: 20 bytes
...
Total Length: 59
...
Time to live: 64
Protocol: UDP (0x11)
Header checksum: 0xb75e [correct]
[Good: True]
[Bad : False]
Source: 192.168.1.1 (192.168.1.1)
Destination: 192.168.1.2 (192.168.1.2)
User Datagram Protocol, Src Port: shilp (2049), Dst Port: domain (53)
Source port: shilp (2049)
Destination port: domain (53)
Length: 39
Checksum: 0x7028 [correct]
[Good Checksum: True]
[Bad Checksum: False]
Domain Name System (query)
Transaction ID: 0xdd46
Flags: 0x0100 (Standard query)
...
Questions: 1
...
Queries
www.google.fr: type A, class IN
Name: www.google.fr
Type: A (Host address)
Class: IN (0x0001)

Les champs différents sont les suivants :

- les adresses MAC

Chaque machine étant supposée avoir une unique adresse MAC, il n'est pas étonnant de les voir diverger.

- le nom associé au port source

Le numéro de port est cependant le même. On peut expliquer cela par le fait que 2049 est un port traditionnellement associé à UDP.

- le checksum de la partie UDP

La somme de contrôle (checksum) permet de s'assurer de l'intégrité du paquet reçu. Elle est calculée sur l'ensemble de l'en-tête UDP et des données, mais aussi sur un pseudo en-tête

- transaction ID de la partie DNS

L'ID de transaction est créé par l'expéditeur du message (dans notre cas, m1) et est copié par le récepteur (ici, m2) dans son message de réponse.

- le temps de la requête (Time)

Les autres champs sont identiques.

Étude du protocole TCP

Question 1

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.1	192.168.1.2	TCP	apocd > http [SYN, Seq=0 Win=5840]
2	0.000343	192.168.1.2	192.168.1.1	TCP	http > apocd [SYN, ACK] Seq=0 Ack=1 Win=5792
3	0.000287	192.168.1.1	192.168.1.2	TCP	apocd > http [ACK] Seq=1 Ack=1 Win=5840
4	0.020884	192.168.1.1	192.168.1.2	HTTP	GET / HTTP/1.0
5	0.020911	192.168.1.2	192.168.1.1	TCP	apocd > 4083 [ACK] Seq=1 Ack=216 Win=6864
6	0.068318	192.168.1.2	192.168.1.1	HTTP	HTTP/1.1 200 OK (text/html)
7	0.068594	192.168.1.1	192.168.1.2	TCP	apocd > http [ACK] Seq=216 Ack=297 Win=6912
8	0.069314	192.168.1.2	192.168.1.1	TCP	http > apocd [FIN, ACK] Seq=297 Ack=216 Win=6864
9	0.113180	192.168.1.1	192.168.1.2	TCP	apocd > http [ACK] Seq=216 Ack=298 Win=6912
10	0.113182	192.168.1.1	192.168.1.2	TCP	apocd > http [FIN, ACK] Seq=216 Ack=298 Win=6912
11	0.113213	192.168.1.2	192.168.1.1	TCP	http > apocd [ACK] Seq=298 Ack=217 Win=6864

- l'ordre des trames ainsi que les numéros des sequences et des accusés de réception sont exactement les mêmes que dans la feuille de TP. La seule différence que l'on observe est une différence dans le nom de machine : on a apocd au lieu de m1.

- les trois premières trames correspondent à l'ouverture d'une connexion *TCP* entre les machine *m1* et *m2*. La machine *m1* est le client et la machine *m2* est le serveur. la première trame signifie que le client demande au serveur d'ouvrir une connexion en envoyant l'indicateur *SYN*. Le serveur (*m2*) alloue un socket et l'associe au socket client (*m1*). Ensuite, le serveur répond à la demande de connexion *SYN* en envoyant un accusé de réception *ACK* ($ACK = seqInitial + 1 = 0 + 1 = 1$) avec sa propre requête de synchronisation (*SYN*). Puis le client reçoit le message du serveur et répond par un accusé de réception. À partir de là, la connexion *TCP* est complètement établie entre le client et serveur.

Question 2

En comparant notre capture d'écran avec la capture d'écran de la feuille de TP, on voit que les champs différents sont le numéro du port, le nom de la machine et le checksum (la somme de contrôle). Tous les autres champs sont identiques.

Dans la feuille de TP, le port utilisé est 2657 et le nom de machine est *m1*, mais dans notre capture on voit que le port utilisé est 3809 et le nom de la machine est *apocd*. Dans la liste des ports *TCP* de l'organisation IANA, on trouve que le port 3809 correspond à *Java Desktop System Configuration Agent* qui a comme nom de service *apocd*.

Fiabilité des connexions TCP

Connexion TCP client-serveur

Capture des trames

...					
No.	Time	Source	Destination	Protocol	Info
3	0.000696	192.168.1.1	192.168.1.2	TCP	apocd > http
[SYN] Seq=0 Win=5840					
4	0.000778	192.168.1.2	192.168.1.1	TCP	http > apocd
[SYN, ACK] Seq=0 Ack=1 Win=5792					
5	0.001649	192.168.1.1	192.168.1.2	TCP	apocd > http
[ACK] Seq=1 Ack=1 Win=5840					
6	0.023627	192.168.1.1	192.168.1.2	HTTP	GET / HTTP/1.0
7	0.023693	192.168.1.2	192.168.1.1	TCP	http > apocd
[ACK] Seq=1 Ack=216 Win=6864					
8	7.160482	192.168.1.2	192.168.1.1	TCP	http > apocd
[FIN, ACK] Seq=1 Ack=216 Win=6864					
9	7.173982	192.168.1.1	192.168.1.2	TCP	apocd > http
[ACK] Seq=216 Ack=2 Win=5840					
10	10.181036	192.168.1.1	192.168.1.2	TCP	apocd > http
[FIN, ACK] Seq=216 Ack=2 Win=5840					
11	10.181102	192.168.1.2	192.168.1.1	TCP	http > apocd
[ACK] Seq=2 Ack=217 Win=6864					
...					

Avant de forcer la terminaison du processus *netcat*, on voit dans le terminal que *m1* envoie une requête HTTP à *m2* et attend donc une réponse de la part de *m2*. Cependant, *netcat* est un utilitaire permettant d'ouvrir des connexions réseau, donc *m1* ne recevra pas de réponse. Après avoir forcé l'arrêt du processus *netcat*, on voit que *m2* signale la fin de la connexion en envoyant l'indicateur *FIN* et un accusé de réception. Par la suite, *m1* réponds qu'il a bien reçu la demande de fin de la connexion et renvoie à *http* l'indicateur *Fin* + *Ack*. Ensuite *http*

envoie un accusé de réception. À partir de là, on peut déduire que la connexion est terminée. La ligne 8 nous montre donc que netcat a bien la "*politesse*" d'envoyer un datagramme de fin de connexion TCP.

Fiabilité d'une connexion TCP

Dans l'onglet *Anomalies de marionnet*, on choisit la ligne correspondante au câble croisé (c1) et on modélise les dysfonctionnements suivants :

- to m1 = 20 % & to m2 = 20 %

```
ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=19.7 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=0.890 ms
64 bytes from 192.168.1.1: icmp_seq=6 ttl=64 time=0.762 ms
64 bytes from 192.168.1.1: icmp_seq=10 ttl=64 time=0.923 ms
64 bytes from 192.168.1.1: icmp_seq=13 ttl=64 time=0.761 ms
64 bytes from 192.168.1.1: icmp_seq=14 ttl=64 time=2.47 ms
64 bytes from 192.168.1.1: icmp_seq=16 ttl=64 time=0.885 ms
64 bytes from 192.168.1.1: icmp_seq=17 ttl=64 time=0.869 ms
64 bytes from 192.168.1.1: icmp_seq=20 ttl=64 time=0.795 ms
64 bytes from 192.168.1.1: icmp_seq=22 ttl=64 time=0.789 ms
64 bytes from 192.168.1.1: icmp_seq=23 ttl=64 time=0.703 ms
64 bytes from 192.168.1.1: icmp_seq=25 ttl=64 time=1.18 ms
64 bytes from 192.168.1.1: icmp_seq=27 ttl=64 time=0.875 ms
64 bytes from 192.168.1.1: icmp_seq=28 ttl=64 time=0.645 ms
64 bytes from 192.168.1.1: icmp_seq=29 ttl=64 time=1.21 ms
64 bytes from 192.168.1.1: icmp_seq=30 ttl=64 time=0.624 ms
64 bytes from 192.168.1.1: icmp_seq=31 ttl=64 time=1.16 ms
64 bytes from 192.168.1.1: icmp_seq=34 ttl=64 time=0.792 ms
64 bytes from 192.168.1.1: icmp_seq=35 ttl=64 time=1.15 ms
64 bytes from 192.168.1.1: icmp_seq=37 ttl=64 time=0.776 ms
64 bytes from 192.168.1.1: icmp_seq=38 ttl=64 time=0.886 ms
64 bytes from 192.168.1.1: icmp_seq=39 ttl=64 time=1.10 ms
64 bytes from 192.168.1.1: icmp_seq=40 ttl=64 time=0.972 ms

--- 192.168.1.1 ping statistics ---
40 packets transmitted, 23 received, 42% packet loss, time 39386ms
rtt min/avg/max/mdev = 0.624/1.782/19.738/3.845 ms
```

On remarque que l'on a perdu entre autres les deux premiers paquets et que le nombre maximum de paquets successifs perdus ne dépasse pas 3.

- to m1 = 40 % & to m2 = 40 %

```

ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=3.08 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=0.797 ms
64 bytes from 192.168.1.1: icmp_seq=8 ttl=64 time=0.826 ms
64 bytes from 192.168.1.1: icmp_seq=12 ttl=64 time=0.942 ms
64 bytes from 192.168.1.1: icmp_seq=14 ttl=64 time=1.05 ms
64 bytes from 192.168.1.1: icmp_seq=17 ttl=64 time=0.949 ms
64 bytes from 192.168.1.1: icmp_seq=18 ttl=64 time=1.15 ms
64 bytes from 192.168.1.1: icmp_seq=22 ttl=64 time=0.925 ms
64 bytes from 192.168.1.1: icmp_seq=23 ttl=64 time=0.868 ms
64 bytes from 192.168.1.1: icmp_seq=26 ttl=64 time=0.867 ms
64 bytes from 192.168.1.1: icmp_seq=33 ttl=64 time=0.736 ms
64 bytes from 192.168.1.1: icmp_seq=35 ttl=64 time=1.08 ms
64 bytes from 192.168.1.1: icmp_seq=36 ttl=64 time=1.06 ms
64 bytes from 192.168.1.1: icmp_seq=39 ttl=64 time=0.987 ms
64 bytes from 192.168.1.1: icmp_seq=40 ttl=64 time=0.507 ms

--- 192.168.1.1 ping statistics ---
40 packets transmitted, 15 received, 62% packet loss, time 39416ms
rtt min/avg/max/mdev = 0.507/1.056/3.088/0.565 ms

```

Sur les 40 paquets transmis, on remarque que, le plus grand écart entre les paquets successifs perdus est 6 (entre 26 et 33).

- to m1 = 60 % & to m2 = 60 %

```

ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
From 192.168.1.2 icmp_seq=11 Destination Host Unreachable
From 192.168.1.2 icmp_seq=12 Destination Host Unreachable
From 192.168.1.2 icmp_seq=13 Destination Host Unreachable
64 bytes from 192.168.1.1: icmp_seq=16 ttl=64 time=1.00 ms
64 bytes from 192.168.1.1: icmp_seq=21 ttl=64 time=0.888 ms
64 bytes from 192.168.1.1: icmp_seq=22 ttl=64 time=0.687 ms
64 bytes from 192.168.1.1: icmp_seq=30 ttl=64 time=0.923 ms
64 bytes from 192.168.1.1: icmp_seq=33 ttl=64 time=1.01 ms
64 bytes from 192.168.1.1: icmp_seq=34 ttl=64 time=1.08 ms
64 bytes from 192.168.1.1: icmp_seq=37 ttl=64 time=1.13 ms
64 bytes from 192.168.1.1: icmp_seq=42 ttl=64 time=1.26 ms
c64 bytes from 192.168.1.1: icmp_seq=43 ttl=64 time=1.02 ms

--- 192.168.1.1 ping statistics ---
43 packets transmitted, 9 received, +3 errors, 79% packet loss, time 42446ms
rtt min/avg/max/mdev = 0.687/1.004/1.262/0.154 ms, pipe 3

```

On remarque qu'il a été difficile d'atteindre m1 à cause d'une trop grande perte de paquets et que le premier paquet arrivé sur la machine m1 est le paquet numéro 16.

- to m1 = 80 % & to m2 = 80 %

```
ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
From 192.168.1.2 icmp_seq=9 Destination Host Unreachable
From 192.168.1.2 icmp_seq=10 Destination Host Unreachable
From 192.168.1.2 icmp_seq=11 Destination Host Unreachable
From 192.168.1.2 icmp_seq=52 Destination Host Unreachable
From 192.168.1.2 icmp_seq=53 Destination Host Unreachable
From 192.168.1.2 icmp_seq=54 Destination Host Unreachable
From 192.168.1.2 icmp_seq=55 Destination Host Unreachable
From 192.168.1.2 icmp_seq=56 Destination Host Unreachable
From 192.168.1.2 icmp_seq=57 Destination Host Unreachable
From 192.168.1.2 icmp_seq=58 Destination Host Unreachable
From 192.168.1.2 icmp_seq=59 Destination Host Unreachable
From 192.168.1.2 icmp_seq=60 Destination Host Unreachable
From 192.168.1.2 icmp_seq=61 Destination Host Unreachable
From 192.168.1.2 icmp_seq=62 Destination Host Unreachable
From 192.168.1.2 icmp_seq=63 Destination Host Unreachable
From 192.168.1.2 icmp_seq=64 Destination Host Unreachable
From 192.168.1.2 icmp_seq=65 Destination Host Unreachable
From 192.168.1.2 icmp_seq=66 Destination Host Unreachable
From 192.168.1.2 icmp_seq=67 Destination Host Unreachable
From 192.168.1.2 icmp_seq=68 Destination Host Unreachable
From 192.168.1.2 icmp_seq=69 Destination Host Unreachable

--- 192.168.1.1 ping statistics ---
70 packets transmitted, 0 received, +21 errors, 100% packet loss, time 69734ms
, pipe 4
```

On voit que avec 80 % de dysfonctionnements, on n'arrive plus à communiquer avec m1. Le taux de perte des paquets est de 100 %.

Annexe

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.1	192.168.1.2	TCP	apocd > http

[SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=134589 TSER=0 WS=1

Frame 1 (74 bytes on wire, 74 bytes captured)

Ethernet II, Src: BbnInter_9d:e2:92 (02:04:06:9d:e2:92), Dst: BbnInter_91:d5:bb (02:04:06:91:d5:bb)

Internet Protocol, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.2 (192.168.1.2)

Transmission Control Protocol, Src Port: apocd (3809), Dst Port: http (80), Seq: 0, Len: 0

Source port: apocd (3809)

Destination port: http (80)

Sequence number: 0 (relative sequence number)

Header length: 40 bytes

Flags: 0x02 (SYN)

Window size: 5840

Checksum: 0xfa74 [correct]

Options: (20 bytes)

No.	Time	Source	Destination	Protocol	Info
2	0.000250	192.168.1.2	192.168.1.1	TCP	http > apocd

[SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 TSV=134349 TSER=134589 WS=1

Frame 2 (74 bytes on wire, 74 bytes captured)

Ethernet II, Src: BbnInter_91:d5:bb (02:04:06:91:d5:bb), Dst: BbnInter_9d:e2:92 (02:04:06:9d:e2:92)

Internet Protocol, Src: 192.168.1.2 (192.168.1.2), Dst: 192.168.1.1 (192.168.1.1)

Transmission Control Protocol, Src Port: http (80), Dst Port: apocd (3809), Seq: 0, Ack: 1, Len: 0

Source port: http (80)

Destination port: apocd (3809)

Sequence number: 0 (relative sequence number)

Acknowledgement number: 1 (relative ack number)

Header length: 40 bytes

Flags: 0x12 (SYN, ACK)

Window size: 5792

Checksum: 0x053b [correct]

Options: (20 bytes)

[SEQ/ACK analysis]

No.	Time	Source	Destination	Protocol	Info
3	0.000490	192.168.1.1	192.168.1.2	TCP	apocd > http

[ACK] Seq=1 Ack=1 Win=5840 Len=0 TSV=134589 TSER=134349

Frame 3 (66 bytes on wire, 66 bytes captured)

Ethernet II, Src: BbnInter_9d:e2:92 (02:04:06:9d:e2:92), Dst: BbnInter_91:d5:bb (02:04:06:91:d5:bb)

Internet Protocol, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.2 (192.168.1.2)

Transmission Control Protocol, Src Port: apocd (3809), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0

Source port: apocd (3809)

Destination port: http (80)

Sequence number: 1 (relative sequence number)

Acknowledgement number: 1 (relative ack number)

Header length: 32 bytes

Flags: 0x10 (ACK)
Window size: 5840 (scaled)
Checksum: 0x3f39 [correct]
Options: (12 bytes)
[SEQ/ACK analysis]

No.	Time	Source	Destination	Protocol	Info
4	0.021738	192.168.1.1	192.168.1.2	HTTP	GET / HTTP/1.0

Frame 4 (281 bytes on wire, 281 bytes captured)

Ethernet II, Src: BbnInter_9d:e2:92 (02:04:06:9d:e2:92), Dst: BbnInter_91:d5:bb (02:04:06:91:d5:bb)

Internet Protocol, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.2 (192.168.1.2)

Transmission Control Protocol, Src Port: apocd (3809), Dst Port: http (80), Seq: 1, Ack: 1, Len: 215

Source port: apocd (3809)
Destination port: http (80)
Sequence number: 1 (relative sequence number)
[Next sequence number: 216 (relative sequence number)]
Acknowledgement number: 1 (relative ack number)
Header length: 32 bytes
Flags: 0x18 (PSH, ACK)
Window size: 5840 (scaled)
Checksum: 0xf915 [correct]
Options: (12 bytes)

Hypertext Transfer Protocol

No.	Time	Source	Destination	Protocol	Info
5	0.021816	192.168.1.2	192.168.1.1	TCP	http > apocd

[ACK] Seq=1 Ack=216 Win=6864 Len=0 TSV=134351 TSER=134591

Frame 5 (66 bytes on wire, 66 bytes captured)

Ethernet II, Src: BbnInter_91:d5:bb (02:04:06:91:d5:bb), Dst: BbnInter_9d:e2:92 (02:04:06:9d:e2:92)

Internet Protocol, Src: 192.168.1.2 (192.168.1.2), Dst: 192.168.1.1 (192.168.1.1)

Transmission Control Protocol, Src Port: http (80), Dst Port: apocd (3809), Seq: 1, Ack: 216, Len: 0

Source port: http (80)
Destination port: apocd (3809)
Sequence number: 1 (relative sequence number)
Acknowledgement number: 216 (relative ack number)
Header length: 32 bytes
Flags: 0x10 (ACK)
Window size: 6864 (scaled)
Checksum: 0x3c5e [correct]
Options: (12 bytes)
[SEQ/ACK analysis]

No.	Time	Source	Destination	Protocol	Info
6	0.029557	192.168.1.2	192.168.1.1	HTTP	HTTP/1.1 200

OK (text/html)

Frame 6 (362 bytes on wire, 362 bytes captured)

Ethernet II, Src: BbnInter_91:d5:bb (02:04:06:91:d5:bb), Dst: BbnInter_9d:e2:92 (02:04:06:9d:e2:92)

Internet Protocol, Src: 192.168.1.2 (192.168.1.2), Dst: 192.168.1.1 (192.168.1.1)

Transmission Control Protocol, Src Port: http (80), Dst Port: apocd (3809), Seq: 1, Ack: 216, Len: 296

Source port: http (80)
Destination port: apocd (3809)
Sequence number: 1 (relative sequence number)
[Next sequence number: 297 (relative sequence number)]
Acknowledgement number: 216 (relative ack number)
Header length: 32 bytes
Flags: 0x18 (PSH, ACK)
Window size: 6864 (scaled)
Checksum: 0x1f09 [correct]
Options: (12 bytes)

Hypertext Transfer Protocol

Line-based text data: text/html

No.	Time	Source	Destination	Protocol	Info
7	0.030102	192.168.1.1	192.168.1.2	TCP	apocd > http

[ACK] Seq=216 Ack=297 Win=6912 Len=0 TSV=134591 TSER=134351

Frame 7 (66 bytes on wire, 66 bytes captured)

Ethernet II, Src: BbnInter_9d:e2:92 (02:04:06:9d:e2:92), Dst: BbnInter_91:d5:bb (02:04:06:91:d5:bb)

Internet Protocol, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.2 (192.168.1.2)

Transmission Control Protocol, Src Port: apocd (3809), Dst Port: http (80), Seq: 216, Ack: 297, Len: 0

Source port: apocd (3809)
Destination port: http (80)
Sequence number: 216 (relative sequence number)
Acknowledgement number: 297 (relative ack number)
Header length: 32 bytes
Flags: 0x10 (ACK)
Window size: 6912 (scaled)
Checksum: 0x3b1e [correct]
Options: (12 bytes)
[SEQ/ACK analysis]

No.	Time	Source	Destination	Protocol	Info
8	0.030877	192.168.1.2	192.168.1.1	TCP	http > apocd

[FIN, ACK] Seq=297 Ack=216 Win=6864 Len=0 TSV=134351 TSER=134591

Frame 8 (66 bytes on wire, 66 bytes captured)

Ethernet II, Src: BbnInter_91:d5:bb (02:04:06:91:d5:bb), Dst: BbnInter_9d:e2:92 (02:04:06:9d:e2:92)

Internet Protocol, Src: 192.168.1.2 (192.168.1.2), Dst: 192.168.1.1 (192.168.1.1)

Transmission Control Protocol, Src Port: http (80), Dst Port: apocd (3809), Seq: 297, Ack: 216, Len: 0

Source port: http (80)
Destination port: apocd (3809)
Sequence number: 297 (relative sequence number)
Acknowledgement number: 216 (relative ack number)
Header length: 32 bytes
Flags: 0x11 (FIN, ACK)
Window size: 6864 (scaled)
Checksum: 0x3b35 [correct]
Options: (12 bytes)

[SEQ/ACK analysis]

No.	Time	Source	Destination	Protocol	Info
9	0.071322	192.168.1.1	192.168.1.2	TCP	apocd > http

[ACK] Seq=216 Ack=298 Win=6912 Len=0 TSV=134595 TSER=134351

Frame 9 (66 bytes on wire, 66 bytes captured)

Ethernet II, Src: BbnInter_9d:e2:92 (02:04:06:9d:e2:92), Dst: BbnInter_91:d5:bb (02:04:06:91:d5:bb)

Internet Protocol, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.2 (192.168.1.2)

Transmission Control Protocol, Src Port: apocd (3809), Dst Port: http (80), Seq: 216, Ack: 298, Len: 0

Source port: apocd (3809)

Destination port: http (80)

Sequence number: 216 (relative sequence number)

Acknowledgement number: 298 (relative ack number)

Header length: 32 bytes

Flags: 0x10 (ACK)

Window size: 6912 (scaled)

Checksum: 0x3b19 [correct]

Options: (12 bytes)

[SEQ/ACK analysis]

No.	Time	Source	Destination	Protocol	Info
10	0.095600	192.168.1.1	192.168.1.2	TCP	apocd > http

[FIN, ACK] Seq=216 Ack=298 Win=6912 Len=0 TSV=134598 TSER=134351

Frame 10 (66 bytes on wire, 66 bytes captured)

Ethernet II, Src: BbnInter_9d:e2:92 (02:04:06:9d:e2:92), Dst: BbnInter_91:d5:bb (02:04:06:91:d5:bb)

Internet Protocol, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.2 (192.168.1.2)

Transmission Control Protocol, Src Port: apocd (3809), Dst Port: http (80), Seq: 216, Ack: 298, Len: 0

Source port: apocd (3809)

Destination port: http (80)

Sequence number: 216 (relative sequence number)

Acknowledgement number: 298 (relative ack number)

Header length: 32 bytes

Flags: 0x11 (FIN, ACK)

Window size: 6912 (scaled)

Checksum: 0x3b15 [correct]

Options: (12 bytes)

No.	Time	Source	Destination	Protocol	Info
11	0.095640	192.168.1.2	192.168.1.1	TCP	http > apocd

[ACK] Seq=298 Ack=217 Win=6864 Len=0 TSV=134358 TSER=134598

Frame 11 (66 bytes on wire, 66 bytes captured)

Ethernet II, Src: BbnInter_91:d5:bb (02:04:06:91:d5:bb), Dst: BbnInter_9d:e2:92 (02:04:06:9d:e2:92)

Internet Protocol, Src: 192.168.1.2 (192.168.1.2), Dst: 192.168.1.1 (192.168.1.1)

Transmission Control Protocol, Src Port: http (80), Dst Port: apocd (3809), Seq: 298, Ack: 217, Len: 0

Source port: http (80)

Destination port: apocd (3809)

Sequence number: 298 (relative sequence number)

Acknowledgement number: 217 (relative ack number)
Header length: 32 bytes
Flags: 0x10 (ACK)
Window size: 6864 (scaled)
Checksum: 0x3b26 [correct]
Options: (12 bytes)
[SEQ/ACK analysis]