

## **Trabalho Prático III**

Analise de Trafego de Rede Com Wireshark

**Felipe Longarai Trisotto**

Departamento de Informática e Estatística  
Centro Tecnológico - CTC  
Universidade Federal de Santa Catarina  
INE 5414 - Redes de Computadores I  
Professor: Carlos Becker Westphall  
Nov 20, 2016

## **1 Introdução**

Este relatório expõe a realização do terceiro trabalho prático, solicitado pela matéria de Redes de Computadores I - INE 5414. O objetivo deste trabalho é analisar o tráfego de uma rede para o estabelecimento da conexão, tráfego de dados e finalização da conexão, fazendo uso da ferramenta Wireshark, que registra pacotes que trafegam na rede e suas respectivas informações. Nosso principal interesse nesse trabalho é mostrar os protocolos TCP e HTTP.

## **2 Descrição do funcionamento**

### **2.1 Estabelecimento da conexão**

É possível verificar o estabelecimento da conexão através de pacotes e flags. O cliente, inicialmente, envia uma flag SYN juntamente com pacote TCP com a pretensão de estabelecer uma conexão. Se tudo ocorrer da maneira correta, o servidor responde com um SYN + ACK. Se o cliente receber corretamente, ele envia um ACK para o servidor, estabelecendo a conexão.

### **2.2 Transferência de dados**

O modelo TCP/IP é um conjunto de protocolos que seguem o modelo OSI visto em sala de aula. Obviamente, existem diversos protocolos (HTTP, SMTP, FTP, SNMP, DNS), porém com a ajuda do próprio Wireshark faremos um filtro com aqueles que temos intenção de analisar.

### **2.3 Finalização da conexão**

Quando um dos extremos tiver a iniciativa de finalizar a conexão, será enviado desse um pacote TCP com a flag FIN. Contando que não ocorra erros, o outro irá confirmar o pedido com o ACK e seguidamente irá enviar um FIN; sendo realmente interrompida a ligação quando o primeiro enviar um ACK.

## **3 Desenvolvimento**

A URL escolhida para realizar a análise da conexão foi: <http://www.xboxachievements.com/>, utilizando o filtro “TCP or HTTP” visto que eles são de nosso interesse.

### 3.1 Estabelecimento da conexão

A primeira ação a ser executada e para gerar a conexão com o servidor. Para isso é realizado em três passos:

No.	Time	Source	Destination	Protocol	Length	Info
79	5.712707	xboxachievements.com	192.168.0.20	TCP	1514	[TCP segment of a reassembled PDU]
80	5.712751	192.168.0.20	xboxachievements.com	TCP	54	61769 → http [ACK] Seq=441 Ack=11660 Win=65536 Len=0
82	5.715681	192.168.0.20	xboxachievements.com	TCP	54	61769 → http [ACK] Seq=441 Ack=12090 Win=65024 Len=0
83	5.716069	192.168.0.20	xboxachievements.com	TCP	54	61769 → http [FIN, ACK] Seq=441 Ack=12090 Win=65024 Len=0
84	5.716615	192.168.0.20	xboxachievements.com	TCP	66	61776 → http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
87	5.763807	xboxachievements.com	192.168.0.20	TCP	66	http → 61772 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
88	5.763958	192.168.0.20	xboxachievements.com	TCP	54	61772 → http [ACK] Seq=1 Ack=1 Win=65536 Len=0
89	5.764181	192.168.0.20	ytimg.l.google.com	TCP	66	61777 → https [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
91	5.766334	xboxachievements.com	192.168.0.20	TCP	66	http → 61773 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
92	5.766460	192.168.0.20	xboxachievements.com	TCP	54	61773 → http [ACK] Seq=1 Ack=1 Win=65536 Len=0
94	5.770245	partnerad.l.doublecl	192.168.0.20	TCP	66	http → 61775 [SYN, ACK] Seq=0 Ack=1 Win=42900 Len=0 MSS=1430 SACK_PERM=1 WS=128
95	5.770360	192.168.0.20	partnerad.l.doublecl	TCP	54	61775 → http [ACK] Seq=1 Ack=1 Win=65536 Len=0
96	5.770536	xboxachievements.com	192.168.0.20	TCP	66	http → 61770 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
97	5.770593	192.168.0.20	xboxachievements.com	TCP	54	61770 → http [ACK] Seq=1 Ack=1 Win=65536 Len=0
100	5.774374	xboxachievements.com	192.168.0.20	TCP	66	http → 61771 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
101	5.774533	192.168.0.20	xboxachievements.com	TCP	54	61771 → http [ACK] Seq=1 Ack=1 Win=65536 Len=0
103	5.778639	ytimg.l.google.com	192.168.0.20	TCP	66	https → 61777 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
104	5.778797	192.168.0.20	ytimg.l.google.com	TCP	54	61777 → https [ACK] Seq=1 Ack=1 Win=65536 Len=0
105	5.779224	xboxachievements.com	192.168.0.20	TCP	66	http → 61774 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
106	5.779288	192.168.0.20	xboxachievements.com	TCP	54	61774 → http [ACK] Seq=1 Ack=1 Win=65536 Len=0
109	5.791363	ytimg.l.google.com	192.168.0.20	TCP	60	https → 61777 [ACK] Seq=1 Ack=196 Win=30336 Len=0
110	5.867948	xboxachievements.com	192.168.0.20	TCP	60	http → 61769 [ACK] Seq=12090 Ack=442 Win=6912 Len=0
111	5.880808	xboxachievements.com	192.168.0.20	TCP	66	http → 61776 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
112	5.880968	192.168.0.20	xboxachievements.com	TCP	54	61776 → http [ACK] Seq=1 Ack=1 Win=65536 Len=0

Frame 84: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0  
Ethernet II, Src: e0:ca:94:23:39:f8, Dst: 58:23:8c:61:9d:00  
Internet Protocol Version 4, Src: 192.168.0.20 (192.168.0.20), Dst: xboxachievements.com (69.65.11.56)  
Transmission Control Protocol, Src Port: 61776 (61776), Dst Port: http (80), Seq: 0, Len: 0

0000 58 23 8c 61 9d 00 e0 ca 94 23 39 f8 00 00 45 00 X#.#...#9...E.  
0010 00 34 15 3f 40 00 00 06 d4 4f c0 a8 00 14 45 41 .4?#...0....EA  
0020 0b 38 f1 50 00 50 ca da a9 fb 00 00 00 00 00 02 .8.P.P...  
0030 20 00 d7 63 00 00 02 04 05 b4 01 03 03 08 01 01 ..C.....  
0040 04 02 ..

Primeiro Passo: é feito o pedido inicial com a flag SYN, com um valor aleatório.

Frame 84: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: e0:ca:94:23:39:f8, Dst: 58:23:8c:61:9d:00
Internet Protocol Version 4, Src: 192.168.0.20 (192.168.0.20), Dst: xboxachievements.com (69.65.11.56)
0100 ... = Version: 4
... 0101 = Header Length: 20 bytes
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 52
Identification: 0x153f (5439)
Flags: 0x02 (Don't Fragment)
Fragment offset: 0
Time to live: 128
Protocol: TCP (6) Protocolo usado
Header checksum: 0xd44f (validation disabled)
Source: 192.168.0.20 (192.168.0.20)
Destination: xboxachievements.com (69.65.11.56)
Source GeoIP: Unknown
Destination GeoIP: Unknown
Transmission Control Protocol, Src Port: 61776 (61776), Dst Port: http (80), Seq: 0, Len: 0
Source Port: 61776 (61776)
Destination Port: http (80) Porta usada pela camada TCP/IP
Stream index: 11
TCP Segment Len: 0
Sequence number: 0 (relative sequence number) Valor da Flag SYN
Acknowledgment number: 0
Header Length: 32 bytes
Flags: 0x002 (SYN)
0000 58 23 8c 61 9d 00 e0 ca 94 23 39 f8 00 00 45 00 X#.#...#9...E. 0010 00 34 15 3f 40 00 00 06 d4 4f c0 a8 00 14 45 41 .4?#...0....EA 0020 0b 38 f1 50 00 50 ca da a9 fb 00 00 00 00 00 02 .8.P.P... 0030 20 00 d7 63 00 00 02 04 05 b4 01 03 03 08 01 01 ..C..... 0040 04 02 ..

Segundo Passo: Caso disponível, o servidor confirma o pedido enviando SYN+ACK, cujo valor de ACK é o valor recebido acrescentando uma unidade.

```

> Frame 87: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: 58:23:8c:61:9d:80, Dst: e0:ca:94:23:39:f8
4 Internet Protocol Version 4, Src: xboxachievements.com (69.65.11.56), Dst: 192.168.0.20 (192.168.0.20)
  0100 ... = Version: 4                               Origem do pacote                               Destino do pacote
  ... 0101 = Header Length: 20 bytes
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 52
  Identification: 0x0000 (0)
  > Flags: 0x02 (Don't Fragment)
  Fragment offset: 0
  Time to live: 53
  Protocol: TCP (6) Protocolo usado
  > Header checksum: 0x348f [validation disabled]
  Source: xboxachievements.com (69.65.11.56) Origem do pacote
  Destination: 192.168.0.20 (192.168.0.20) Destino do pacote
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
4 Transmission Control Protocol, Src Port: http (80), Dst Port: 61772 (61772), Seq: 0, Ack: 1, Len: 0
  Source Port: http (80) Porta usada pela camada aplicação TCP/IP
  Destination Port: 61772 (61772)
  [Stream index: 7]
  [TCP Segment Len: 0]
  Sequence number: 0 (relative sequence number) Valor da Flag SYN
  Acknowledgment number: 1 (relative ack number) Valor da Flag ACK
  Header Length: 32 bytes
  > Flags: 0x012 (SYN, ACK)
  Window size value: 5840
  [Calculated window size: 5840]
  > Checksum: 0x7728 [validation disabled]
  Urgent pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted, No-Operation (NOP), Window scale

0000 e0 ca 94 23 39 f8 58 23 8c 61 9d 80 08 00 45 00 ...#9.X# .a....E.
0010 00 34 00 00 40 00 35 06 34 8f 45 41 0b 38 c0 80 ..4..@.5. 4.EA.8..
0020 00 14 00 50 f1 4c 8c cf e8 9b 00 56 68 75 80 12 ...P.L...Vhu...
0030 16 d0 77 28 00 00 02 04 05 b4 01 01 04 02 01 03 ..W{.... .....
0040 03 07

```

Terceiro Passo: Para estabelecer a conexão o cliente retorna um ACK, com SYN com mesmo número de ACK recebido pelo servidor.

```

> Frame 88: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
> Ethernet II, Src: e0:ca:94:23:39:f8, Dst: 58:23:8c:61:9d:80
4 Internet Protocol Version 4, Src: 192.168.0.20 (192.168.0.20), Dst: xboxachievements.com (69.65.11.56)
  0100 ... = Version: 4                               Origem do Pacote                               Destino do Pacote
  ... 0101 = Header Length: 20 bytes
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 40
  Identification: 0x1541 (5441)
  > Flags: 0x02 (Don't Fragment)
  Fragment offset: 0
  Time to live: 128
  Protocol: TCP (6) Protocolo usado
  > Header checksum: 0xd459 [validation disabled]
  Source: 192.168.0.20 (192.168.0.20) Origem do Pacote
  Destination: xboxachievements.com (69.65.11.56) Destino do Pacote
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
4 Transmission Control Protocol, Src Port: 61772 (61772), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0
  Source Port: 61772 (61772)
  Destination Port: http (80) Porta usada pela camada aplicação TCP/IP
  [Stream index: 7]
  [TCP Segment Len: 0]
  Sequence number: 1 (relative sequence number) Valor da Flag SYN
  Acknowledgment number: 1 (relative ack number) Valor da Flag ACK
  Header Length: 20 bytes
  > Flags: 0x010 (ACK)
  Window size value: 256
  [Calculated window size: 65536]
  [Window size scaling factor: 256]
  > Checksum: 0xcdca [validation disabled]
  Urgent pointer: 0

0000 58 23 8c 61 9d 80 e0 ca 94 23 39 f8 08 00 45 00 X#.a....#9...E.
0010 00 28 15 41 40 00 00 06 d4 59 c0 a8 00 14 45 41 .(.@....Y....EA
0020 0b 38 f1 4c 00 50 00 56 68 75 8c cf e8 9c 50 10 .B.L.P.V hu....P.
0030 01 00 cd ca 00 00

```

### 3.2 Transferência de dados

Assim que estabilizada a comunicação entre o navegador, o Firefox, e o servidor da Xbox Achievements. Como ocorre no primeiro pacote HTTP. Dando dois cliques sobre ele e possível verificar esse detalhes. Quando selecionado alguma linha de comando do pacote (dentro do quadro superior), na divisão inferior da página é destacado da informação do conjunto, em hexadecimal.

```

> Frame 58: 494 bytes on wire (3952 bits), 494 bytes captured (3952 bits) on interface 0
> Ethernet II, Src: e8:ca:94:23:39:f8, Dst: 58:23:8c:61:9d:00
> Internet Protocol Version 4, Src: 192.168.0.20 (192.168.0.20), Dst: xboxachievements.com (69.65.11.56)
> Transmission Control Protocol, Src Port: 61769 (61769), Dst Port: http (80), Seq: 1, Ack: 1, Len: 448
Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
  Host: www.xboxachievements.com\r\n
  Connection: keep-alive\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.102 Safari/537.36\r\n
  Referer: https://www.google.com.br/\r\n
  Accept-Encoding: gzip, deflate, sdch\r\n
  Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.6,en;q=0.4\r\n
  \r\n
  [Full request URI: http://www.xboxachievements.com/]
  [HTTP request 1/1]
  [Response in frame: 81]

```

```

0030 01 00 e1 e1 00 00 47 45 54 20 2f 20 48 54 54 56 .....GET / HTTP
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 7e /1.1\r\n
0050 78 62 6f 78 61 63 68 69 65 76 65 6d 65 6e 74 73 xboxachievements
0060 2e 03 0f 0d 0a 45 0f 0e 0e 03 03 74 69 0f 0e www.com
0070 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 61 63 : keep-alive..Ac
0080 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 6c cept: te xt/html,
0090 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d applicat ion/xhtm
00a0 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f l+xml,ap plicatio
00b0 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67 n/xml;q= 0.9,imag
00c0 65 2f 77 65 62 70 2c 2a 2f 2a 3b 71 3d 30 2e 38 e/webp,* /*;q=0.8
00d0 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 ..Upgrad e-Insecu
00e0 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a re-Request: 1..

```

Protocolo

Método

```

Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n Versão do protocolo usado
  Host: www.xboxachievements.com\r\n
  Connection: keep-alive\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.102 Safari/537.36\r\n
  Referer: https://www.google.com.br/\r\n
  Accept-Encoding: gzip, deflate, sdch\r\n
  Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.6,en;q=0.4\r\n
  \r\n
  [Full request URI: http://www.xboxachievements.com/]
  [HTTP request 1/1]
  [Response in frame: 81]

```

Conjunto de informações sobre o pedido, cliente e servidor

É possível verificar a atuação do protocolo TCP, ordenando os pacotes. No Wireshark ao abrir a página com os detalhes do pacote HTTP selecionado, no cabeçalho de origem TCP há a informação do SYN, NEXT SYN e ACK. Quando solicitado o NEXT SYN, o servidor.

```

> Frame 83: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
> Ethernet II, Src: e0:ca:94:23:39:f8, Dst: 58:23:8c:61:9d:80
> Internet Protocol Version 4, Src: 192.168.0.20 (192.168.0.20), Dst: xboxachievements.com (69.65.11.56)
# Transmission Control Protocol, Src Port: 61769 (61769), Dst Port: http (80), Seq: 441, Ack: 12090, Len: 0
    Source Port: 61769 (61769)
    Destination Port: http (80)
    [Stream index: 3]
    [TCP Segment Len: 0]
    Sequence number: 441 (relative sequence number)
    Acknowledgment number: 12090 (relative ack number)
    Header Length: 20 bytes
# Flags: 0x011 (FIN, ACK)
    Window size value: 254
    [Calculated window size: 65024]
    [Window size scaling factor: 256]
# Checksum: 0x9e08 [validation disabled]
    Urgent pointer: 0

```

---

```

0000  58 23 8c 61 9d 80 e0 ca 94 23 39 f8 08 00 45 00  X#.a.....#9...E.
0010  80 20 15 3e 40 00 80 06 d4 5c c0 a8 00 14 45 41  (.>@... \....EA
0020  80 38 f1 49 00 50 14 25 39 8f 57 d4 68 75 50 11  .8.I.P.W 9.W.huP.
0030  00 fe 9e 08 00 00 00 00 00 00 00 00 00 00 00 00  ....

```



Em seguida, o usuário confirma ao servidor o pedido de término e verifica se o servidor irá finalizar também.

```

> Frame 83: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
> Ethernet II, Src: e0:ca:94:23:39:f8, Dst: 58:23:8c:61:9d:80
> Internet Protocol Version 4, Src: 192.168.0.20 (192.168.0.20), Dst: xboxachievements.com (69.65.11.56) Endereço IP do servidor
+ Transmission Control Protocol, Src Port: 61769 (61769), Dst Port: http (80), Seq: 441, Ack: 12090, Len: 0
  Source Port: 61769 (61769)
  Destination Port: http (80)      Endereço IP do cliente
  [Stream index: 3]
  [TCP Segment Len: 0]
  Sequence number: 441      (relative sequence number)
  Acknowledgment number: 12090      (relative ack number)
  Header Length: 20 bytes
  > Flags: 0x011 (FIN, ACK)
  Window size value: 254
  [Calculated window size: 65024]
  [Window size scaling factor: 256]
  > Checksum: 0x9e08 [validation disabled]
  Urgent pointer: 0

0000 58 23 8c 61 9d 80 e0 ca 94 23 39 f8 06 00 45 00 X#.a.... .#9...E.
0010 00 28 15 3e 40 00 00 06 d4 5c c0 a8 00 14 45 41 .(.A@... .Y....EA
0020 0b 38 f1 4c 00 50 00 56 68 75 8c cf e8 9c 50 10 .8.L.P.V hu....P.
0030 01 00 cd ca 00 00 .....

```

```

> Frame 88: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
> Ethernet II, Src: e0:ca:94:23:39:f8, Dst: 58:23:8c:61:9d:80
> Internet Protocol Version 4, Src: 192.168.0.20 (192.168.0.20), Dst: xboxachievements.com (69.65.11.56)
+ Transmission Control Protocol, Src Port: 61772 (61772), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0
  Source Port: 61772 (61772)
  Destination Port: http (80)
  [Stream index: 7]
  [TCP Segment Len: 0]
  Sequence number: 1      (relative sequence number)
  Acknowledgment number: 1      (relative ack number)
  Header Length: 20 bytes
  > Flags: 0x010 (ACK)
  Window size value: 256
  [Calculated window size: 65536]
  [Window size scaling factor: 256]
  > Checksum: 0xcdca [validation disabled]
  Urgent pointer: 0
  > [SEQ/ACK analysis]

0000 58 23 8c 61 9d 80 e0 ca 94 23 39 f8 06 00 45 00 X#.a.... .#9...E.
0010 00 28 15 41 40 00 00 06 d4 59 c0 a8 00 14 45 41 .(.A@... .Y....EA
0020 0b 38 f1 4c 00 50 00 56 68 75 8c cf e8 9c 50 10 .8.L.P.V hu....P.
0030 01 00 cd ca 00 00 .....

```