

CMP-4005 -- Homework 3

Nombre: Mateo Ruiz Davila

Código Banner: 00212195

Answer the following questions.

1) Read the following Wireshark tutorial, and use it to capture traffic from the following scenarios. Use screenshots to show your results.

a) Run 10 traceroute commands against google.com

The image displays two screenshots of a computer screen. The left screenshot shows a Wireshark packet capture of ICMP Echo (ping) requests from 192.168.0.111 to 172.217.173.46. The right screenshot shows a Windows PowerShell window running a traceroute command against google.com, displaying the path and response times for each hop.

Wireshark Packet Capture (Left Screenshot):

No.	Time	Source	Destination	Protocol	Length	Info
122	10.535670	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
123	10.536984	192.168.0.1	192.168.0.111	ICMP	134	Time-to-live exceeded
124	10.537734	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
125	10.538930	192.168.0.1	192.168.0.111	ICMP	134	Time-to-live exceeded
126	10.539609	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
127	10.540712	192.168.0.1	192.168.0.111	ICMP	134	Time-to-live exceeded
165	11.554283	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
315	15.405674	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
316	15.421692	200.63.218.161	192.168.0.111	ICMP	70	Time-to-live exceeded
317	15.424349	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
324	15.436313	200.63.218.161	192.168.0.111	ICMP	70	Time-to-live exceeded
341	16.432134	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
471	20.403307	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
517	24.395614	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
545	28.408597	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
549	28.547277	200.69.177.126	192.168.0.111	ICMP	110	Time-to-live exceeded
550	28.548714	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request

Windows PowerShell Traceroute (Right Screenshot):

```
PS C:\Users\mateo> tracert google.com

Traza a la dirección google.com [172.217.173.46]
sobre un máximo de 30 saltos:

 1  1 ms    1 ms    1 ms  dlinkrouter [192.168.0.1]
 2  *        16 ms   12 ms  161.218.uio.satnet.net [200.63.218.161]
 3  *        *        *    Tiempo de espera agotado para esta solicitud
 4 138 ms   286 ms  494 ms 126.177.uio.satnet.net [200.69.177.126]
 5  51 ms   41 ms   68 ms 142.250.172.196
 6  37 ms   33 ms   33 ms 142.251.51.71
 7  35 ms   36 ms   49 ms 209.85.251.39
 8  810 ms  74 ms    61 ms bog02s12-in-f14.1e100.net [172.217.173.46]

Traza completa.
PS C:\Users\mateo>
```

Wireshark Packet Capture (Bottom Screenshot):

No.	Time	Source	Destination	Protocol	Length	Info
11	1.081388	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
12	1.086543	192.168.0.1	192.168.0.111	ICMP	134	Time-to-live exceeded
13	1.087174	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
14	1.088345	192.168.0.1	192.168.0.111	ICMP	134	Time-to-live exceeded
15	1.088974	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
16	1.090240	192.168.0.1	192.168.0.111	ICMP	134	Time-to-live exceeded
22	2.103764	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
39	6.002926	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
99	10.015188	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
117	14.003776	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
129	18.011497	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
154	22.016141	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
173	26.009386	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
174	26.036527	200.69.177.126	192.168.0.111	ICMP	110	Time-to-live exceeded
175	26.038037	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
176	26.071675	200.69.177.126	192.168.0.111	ICMP	110	Time-to-live exceeded
177	26.073663	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
178	26.101905	200.69.177.126	192.168.0.111	ICMP	110	Time-to-live exceeded
180	27.091842	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
181	27.120624	142.250.172.196	192.168.0.111	ICMP	134	Time-to-live exceeded
182	27.122871	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
183	27.150784	142.250.172.196	192.168.0.111	ICMP	134	Time-to-live exceeded
184	27.152540	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
185	27.180699	142.250.172.196	192.168.0.111	ICMP	134	Time-to-live exceeded
334	33.378769	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
335	33.408660	142.251.51.71	192.168.0.111	ICMP	110	Time-to-live exceeded
336	33.410387	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
338	33.443121	142.251.51.71	192.168.0.111	ICMP	110	Time-to-live exceeded
339	33.445817	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request

Age Group	Percentage
18-24	~12%
25-34	~28%
35-44	~18%
45-54	~15%
55-64	~10%
65-74	~8%
75-84	~5%
85+	~3%

Wireshark packet capture showing ICMP Echo (ping) requests from 192.168.0.111 to 172.217.173.46. The capture shows multiple successful requests and several "Time-to-live exceeded" errors.

No.	Time	Source	Destination	Protocol	Length	Info
7	2.078388	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
8	2.081105	192.168.0.1	192.168.0.111	ICMP	134	Time-to-live exceeded
9	2.082692	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
10	2.083849	192.168.0.1	192.168.0.111	ICMP	134	Time-to-live exceeded
11	2.084780	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
12	2.088108	192.168.0.1	192.168.0.111	ICMP	134	Time-to-live exceeded
20	3.102447	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
69	6.825501	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
290	10.824244	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
291	10.840522	200.63.218.161	192.168.0.111	ICMP	70	Time-to-live exceeded
346	11.838358	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
479	15.816695	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
529	19.824576	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
530	19.843550	200.69.177.217	192.168.0.111	ICMP	70	Time-to-live exceeded
535	20.323776	200.69.177.217	192.168.0.111	ICMP	70	Destination unreachable
543	21.822958	200.69.177.217	192.168.0.111	ICMP	70	Destination unreachable
550	23.323752	200.69.177.217	192.168.0.111	ICMP	70	Destination unreachable
579	25.816962	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
580	25.851984	200.69.177.126	192.168.0.111	ICMP	110	Time-to-live exceeded
581	25.853815	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
582	25.881548	200.69.177.126	192.168.0.111	ICMP	110	Time-to-live exceeded
583	25.883780	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
584	25.911095	200.69.177.126	192.168.0.111	ICMP	110	Time-to-live exceeded
587	26.894543	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
588	26.931301	142.250.172.196	192.168.0.111	ICMP	134	Time-to-live exceeded
589	26.932614	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
590	26.971478	142.250.172.196	192.168.0.111	ICMP	134	Time-to-live exceeded
591	26.972434	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request
595	27.007288	142.250.172.196	192.168.0.111	ICMP	134	Time-to-live exceeded
644	33.153212	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request

Frame 7: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface Wi-Fi, Src: IntelCor_f5:38:c7 (4c:03:4f:f5:38:c7), Dst: 172.217.173.46, Protocol: Internet Protocol Version 4, Src: 192.168.0.111, Dst: 172.217.173.46, Length: 106, Information: Echo (ping) request.

Windows PowerShell terminal showing the output of the `tracert google.com` command. The output shows the path from the local machine to google.com, including hops to dlinkrouter, 161.218.uio.satnet.net, 200.69.177.217, 126.177.uio.satnet.net, 142.250.172.196, 142.251.51.71, 209.85.251.39, and bog02s12-in-f14.1e100.net.

```
PS C:\Users\mateo> tracert google.com

Traza a la dirección google.com [172.217.173.46]
sobre un máximo de 30 saltos:

 1  2 ms    1 ms    3 ms    dlinkrouter [192.168.0.1]
 2  *      *      16 ms   161.218.uio.satnet.net [200.63.218.161]
 3  *      *      19 ms   200.69.177.217
 4  35 ms   27 ms   27 ms   126.177.uio.satnet.net [200.69.177.126]
 5  36 ms   39 ms   35 ms   142.250.172.196
 6  35 ms   35 ms   26 ms   142.251.51.71
 7  32 ms   28 ms   32 ms   209.85.251.39
 8  31 ms   33 ms   33 ms   bog02s12-in-f14.1e100.net [172.217.173.46]

Traza completa.
PS C:\Users\mateo>
```

Wireshark packet capture showing ICMP Echo (ping) requests from 192.168.0.111 to 172.217.173.46. The capture shows multiple successful requests and several "Time-to-live exceeded" errors.

No.	Time	Source	Destination	Protocol	Length	Info
73	1.803562	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
74	1.809338	192.168.0.1	192.168.0.111	ICMP	134	Time-to-live exceeded (TTL=64)
75	1.810002	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
78	1.814588	192.168.0.1	192.168.0.111	ICMP	134	Time-to-live exceeded (TTL=64)
79	1.815228	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
80	1.816613	192.168.0.1	192.168.0.111	ICMP	134	Time-to-live exceeded (TTL=64)
89	2.829085	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
90	2.842666	200.63.218.161	192.168.0.111	ICMP	70	Time-to-live exceeded (TTL=64)
91	2.846160	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
92	2.861151	200.63.218.161	192.168.0.111	ICMP	70	Time-to-live exceeded (TTL=64)
93	2.863633	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
94	2.881773	200.63.218.161	192.168.0.111	ICMP	70	Time-to-live exceeded (TTL=64)
99	3.872360	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
180	7.823845	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
269	11.822471	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
288	15.820165	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
291	15.847359	200.69.177.126	192.168.0.111	ICMP	110	Time-to-live exceeded (TTL=64)
292	15.848944	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
294	15.890156	200.69.177.126	192.168.0.111	ICMP	110	Time-to-live exceeded (TTL=64)
295	15.892284	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
297	15.923084	200.69.177.126	192.168.0.111	ICMP	110	Time-to-live exceeded (TTL=64)
306	16.913488	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
307	16.942039	142.250.172.196	192.168.0.111	ICMP	134	Time-to-live exceeded (TTL=64)
308	16.943996	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
309	16.975231	142.250.172.196	192.168.0.111	ICMP	134	Time-to-live exceeded (TTL=64)
310	16.976658	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
312	17.006032	142.250.172.196	192.168.0.111	ICMP	134	Time-to-live exceeded (TTL=64)
341	23.132785	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
342	23.163566	142.251.51.71	192.168.0.111	ICMP	110	Time-to-live exceeded (TTL=64)
343	23.165968	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0

Frame 73: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface Wi-Fi, Src: IntelCor_f5:38:c7 (4c:03:4f:f5:38:c7), Dst: 172.217.173.46, Protocol: Internet Protocol Version 4, Src: 192.168.0.111, Dst: 172.217.173.46, Length: 106, Information: Echo (ping) request.

Windows PowerShell terminal showing the output of the `tracert google.com` command. The output shows the path from the local machine to google.com, including hops to dlinkrouter, 161.218.uio.satnet.net, 200.63.218.161, 126.177.uio.satnet.net, 142.250.172.196, 142.251.51.71, 209.85.251.39, and bog02s12-in-f14.1e100.net.

```
PS C:\Users\mateo> tracert google.com

Traza a la dirección google.com [172.217.173.46]
sobre un máximo de 30 saltos:

 1  5 ms    4 ms    1 ms    dlinkrouter [192.168.0.1]
 2  13 ms   15 ms   18 ms   161.218.uio.satnet.net [200.63.218.161]
 3  *      *      *      Tiempo de espera agotado para esta solicitud.
 4  27 ms   41 ms   31 ms   126.177.uio.satnet.net [200.69.177.126]
 5  28 ms   31 ms   30 ms   142.250.172.196
 6  30 ms   30 ms   43 ms   142.251.51.71
 7  134 ms  119 ms   30 ms   209.85.251.39
 8  26 ms   32 ms   28 ms   bog02s12-in-f14.1e100.net [172.217.173.46]

Traza completa.
PS C:\Users\mateo>
```

Capturando desde Wi-Fi

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

icmp

No.	Time	Source	Destination	Protocol	Length	Info
390	11.607247	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
391	11.608686	192.168.0.1	192.168.0.111	ICMP	134	Time-to-live exceeded (TTL=0)
392	11.609347	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
393	11.610474	192.168.0.1	192.168.0.111	ICMP	134	Time-to-live exceeded (TTL=0)
394	11.611213	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
395	11.612376	192.168.0.1	192.168.0.111	ICMP	134	Time-to-live exceeded (TTL=0)
407	12.623976	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
408	12.633793	200.63.218.161	192.168.0.111	ICMP	70	Time-to-live exceeded (TTL=0)
409	12.636874	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
410	12.649839	200.63.218.161	192.168.0.111	ICMP	70	Time-to-live exceeded (TTL=0)
411	12.651530	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
412	12.670032	200.63.218.161	192.168.0.111	ICMP	70	Time-to-live exceeded (TTL=0)
418	13.669600	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
559	17.301188	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
697	21.309214	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
895	25.302862	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
898	25.352448	200.69.177.126	192.168.0.111	ICMP	110	Time-to-live exceeded (TTL=0)
899	25.353970	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
900	25.379649	200.69.177.126	192.168.0.111	ICMP	110	Time-to-live exceeded (TTL=0)
901	25.380526	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
905	25.405429	200.69.177.126	192.168.0.111	ICMP	110	Time-to-live exceeded (TTL=0)
959	26.399793	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
965	26.426486	142.250.172.196	192.168.0.111	ICMP	134	Time-to-live exceeded (TTL=0)
966	26.429877	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
967	26.460915	142.250.172.196	192.168.0.111	ICMP	134	Time-to-live exceeded (TTL=0)
968	26.464181	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
970	26.495103	142.250.172.196	192.168.0.111	ICMP	134	Time-to-live exceeded (TTL=0)
1223	32.459814	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
1225	32.495128	142.251.51.71	192.168.0.111	ICMP	110	Time-to-live exceeded (TTL=0)
1226	32.495965	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0

> Frame 390: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on 0
> Ethernet II, Src: IntelCor_f5:38:c7 (4c:03:4f:f5:38:c7), Dst: 192.168.0.111, Protocol: Internet Protocol Version 4, Src: 192.168.0.111, Destination: 172.217.173.46
> Internet Control Message Protocol

Wi-Fi: <live capture in progress> Paquetes: 1441 - Mostrado: 45 (3.1%) Perfil: Default

Windows PowerShell

```
PS C:\Users\mateo> tracert google.com
No se puede resolver el nombre del sistema de destino google.com.
PS C:\Users\mateo> tracert google.com

Traza a la dirección google.com [172.217.173.46]
sobre un máximo de 30 saltos:

  1  1 ms    1 ms    1 ms    dlinkrouter [192.168.0.1]
  2  10 ms   13 ms   18 ms   161.218.uio.satnet.net [200.63.218.161]
  3  *        *        *        Tiempo de espera agotado para esta solicitud.
  4  49 ms   25 ms   25 ms   126.177.uio.satnet.net [200.69.177.126]
  5  26 ms   31 ms   31 ms   142.250.172.196
  6  35 ms   34 ms   32 ms   142.251.51.71
  7  26 ms   33 ms   38 ms   209.85.251.39
  8  28 ms   30 ms   28 ms   bog02s12-in-f14.1e100.net [172.217.173.46]

Traza completa.
PS C:\Users\mateo>
```

Capturando desde Wi-Fi

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

icmp

No.	Time	Source	Destination	Protocol	Length	Info
73	2.312970	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
74	2.314413	192.168.0.1	192.168.0.111	ICMP	134	Time-to-live exceeded (TTL=0)
75	2.315628	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
76	2.316778	192.168.0.1	192.168.0.111	ICMP	134	Time-to-live exceeded (TTL=0)
77	2.317438	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
78	2.318442	192.168.0.1	192.168.0.111	ICMP	134	Time-to-live exceeded (TTL=0)
86	3.325211	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
87	3.337260	200.63.218.161	192.168.0.111	ICMP	70	Time-to-live exceeded (TTL=0)
88	3.338594	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
89	3.353616	200.63.218.161	192.168.0.111	ICMP	70	Time-to-live exceeded (TTL=0)
90	3.355883	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
108	7.085649	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
130	11.090839	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
156	15.078794	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
194	19.095542	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
195	19.124426	200.69.177.126	192.168.0.111	ICMP	110	Time-to-live exceeded (TTL=0)
196	19.125470	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
197	19.158953	200.69.177.126	192.168.0.111	ICMP	110	Time-to-live exceeded (TTL=0)
198	19.160405	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
199	19.194465	200.69.177.126	192.168.0.111	ICMP	110	Time-to-live exceeded (TTL=0)
202	20.183939	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
203	20.213429	142.250.172.196	192.168.0.111	ICMP	134	Time-to-live exceeded (TTL=0)
204	20.214473	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
205	20.241897	142.250.172.196	192.168.0.111	ICMP	134	Time-to-live exceeded (TTL=0)
206	20.243636	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
207	20.272392	142.250.172.196	192.168.0.111	ICMP	134	Time-to-live exceeded (TTL=0)
253	26.918140	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
254	26.949090	142.251.51.71	192.168.0.111	ICMP	110	Time-to-live exceeded (TTL=0)
255	26.951163	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
256	26.980121	142.251.51.71	192.168.0.111	ICMP	110	Time-to-live exceeded (TTL=0)

> Frame 73: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on 0
> Ethernet II, Src: IntelCor_f5:38:c7 (4c:03:4f:f5:38:c7), Dst: 192.168.0.111, Protocol: Internet Protocol Version 4, Src: 192.168.0.111, Destination: 172.217.173.46
> Internet Control Message Protocol

Wi-Fi: <live capture in progress> Paquetes: 531 - Mostrado: 44 (8.3%) Perfil: Default

Windows PowerShell

```
PS C:\Users\mateo> tracert google.com

Traza a la dirección google.com [172.217.173.46]
sobre un máximo de 30 saltos:

  1  1 ms    1 ms    1 ms    dlinkrouter [192.168.0.1]
  2  12 ms   15 ms   *        161.218.uio.satnet.net [200.63.218.161]
  3  *        *        *        Tiempo de espera agotado para esta solicitud.
  4  29 ms   33 ms   34 ms   126.177.uio.satnet.net [200.69.177.126]
  5  29 ms   27 ms   29 ms   142.250.172.196
  6  31 ms   29 ms   32 ms   142.251.51.71
  7  26 ms   31 ms   30 ms   209.85.251.39
  8  37 ms   34 ms   28 ms   bog02s12-in-f14.1e100.net [172.217.173.46]

Traza completa.
PS C:\Users\mateo>
```

Capturando desde Wi-Fi

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

icmp

No.	Time	Source	Destination	Protocol	Length	Info
116	2.041521	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
117	2.043109	192.168.0.1	192.168.0.111	ICMP	134	Time-to-live exceeded (Tl
118	2.043910	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
119	2.044993	192.168.0.1	192.168.0.111	ICMP	134	Time-to-live exceeded (Tl
120	2.045613	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
121	2.046739	192.168.0.1	192.168.0.111	ICMP	134	Time-to-live exceeded (Tl
130	3.067077	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
245	6.694663	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
246	6.717657	200.63.218.161	192.168.0.111	ICMP	70	Time-to-live exceeded (Tl
247	6.721430	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
248	6.733795	200.63.218.161	192.168.0.111	ICMP	70	Time-to-live exceeded (Tl
251	7.744168	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
283	11.708429	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
365	15.694179	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
505	19.698257	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
514	19.726157	200.69.177.126	192.168.0.111	ICMP	110	Time-to-live exceeded (Tl
515	19.726926	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
520	19.759684	200.69.177.126	192.168.0.111	ICMP	110	Time-to-live exceeded (Tl
521	19.761305	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
563	19.789355	200.69.177.126	192.168.0.111	ICMP	110	Time-to-live exceeded (Tl
734	20.769123	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
735	20.802036	142.250.172.196	192.168.0.111	ICMP	134	Time-to-live exceeded (Tl
736	20.802747	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
737	20.836963	142.250.172.196	192.168.0.111	ICMP	134	Time-to-live exceeded (Tl
738	20.838586	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
739	20.867809	142.250.172.196	192.168.0.111	ICMP	134	Time-to-live exceeded (Tl
890	38.020464	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
891	38.052860	142.251.51.71	192.168.0.111	ICMP	110	Time-to-live exceeded (Tl
892	38.054630	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
893	38.084124	142.251.51.71	192.168.0.111	ICMP	110	Time-to-live exceeded (Tl

> Frame 116: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on 0

> Ethernet II, Src: IntelCor_f5:38:c7 (4c:03:4f:f5:38:c7), Dst: 192.168.0.111, ID: 0

> Internet Protocol Version 4, Src: 192.168.0.111, Dst: 172.217.173.46

> Internet Control Message Protocol

Wi-Fi: <live capture in progress>

Paquetes: 1203 · Mostrado: 44 (3.7%)

Perfil: Default

Windows PowerShell

PS C:\Users\mateo> tracert google.com

Traza a la dirección google.com [172.217.173.46] sobre un máximo de 30 saltos:

1	1 ms	1 ms	1 ms	dlinkrouter [192.168.0.1]
2	*	23 ms	12 ms	161.218.uio.satnet.net [200.63.218.161]
3	*	*	*	Tiempo de espera agotado para esta solicitud.
4	28 ms	32 ms	28 ms	126.177.uio.satnet.net [200.69.177.126]
5	33 ms	34 ms	29 ms	142.250.172.196
6	32 ms	30 ms	48 ms	142.251.51.71
7	30 ms	31 ms	41 ms	209.85.251.39
8	29 ms	33 ms	50 ms	bog02s12-in-f14.1e100.net [172.217.173.46]

Traza completa.

PS C:\Users\mateo>

Capturando desde Wi-Fi

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

icmp

No.	Time	Source	Destination	Protocol	Length	Info
23	2.014313	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
24	2.015960	192.168.0.1	192.168.0.111	ICMP	134	Time-to-live exceeded (Tl
25	2.016904	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
26	2.018004	192.168.0.1	192.168.0.111	ICMP	134	Time-to-live exceeded (Tl
27	2.018646	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
28	2.020195	192.168.0.1	192.168.0.111	ICMP	134	Time-to-live exceeded (Tl
33	3.030517	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
52	6.717002	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
75	10.722383	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
126	14.714075	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
159	18.711149	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
262	22.711051	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
338	26.718578	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
339	26.745435	200.69.177.126	192.168.0.111	ICMP	110	Time-to-live exceeded (Tl
340	26.746630	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
341	26.777763	200.69.177.126	192.168.0.111	ICMP	110	Time-to-live exceeded (Tl
342	26.779449	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
343	26.807872	200.69.177.126	192.168.0.111	ICMP	110	Time-to-live exceeded (Tl
349	27.790671	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
351	27.817834	142.250.172.196	192.168.0.111	ICMP	134	Time-to-live exceeded (Tl
352	27.821848	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
353	27.846706	142.250.172.196	192.168.0.111	ICMP	134	Time-to-live exceeded (Tl
354	27.850043	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
355	27.877625	142.250.172.196	192.168.0.111	ICMP	134	Time-to-live exceeded (Tl
375	34.018134	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
376	34.044891	142.251.51.71	192.168.0.111	ICMP	110	Time-to-live exceeded (Tl
377	34.047420	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
378	34.075479	142.251.51.71	192.168.0.111	ICMP	110	Time-to-live exceeded (Tl
379	34.077751	192.168.0.111	172.217.173.46	ICMP	106	Echo (ping) request id=0
380	34.106587	142.251.51.71	192.168.0.111	ICMP	110	Time-to-live exceeded (Tl

> Frame 23: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on 0

> Ethernet II, Src: IntelCor_f5:38:c7 (4c:03:4f:f5:38:c7), Dst: 192.168.0.111, ID: 0

> Internet Protocol Version 4, Src: 192.168.0.111, Dst: 172.217.173.46

> Internet Control Message Protocol

Wi-Fi: <live capture in progress>

Paquetes: 538 · Mostrado: 42 (7.8%)

Perfil: Default

Windows PowerShell

PS C:\Users\mateo> tracert google.com

Traza a la dirección google.com [172.217.173.46] sobre un máximo de 30 saltos:

1	1 ms	1 ms	1 ms	dlinkrouter [192.168.0.1]
2	*	*	*	Tiempo de espera agotado para esta solicitud.
3	*	*	*	Tiempo de espera agotado para esta solicitud.
4	27 ms	31 ms	28 ms	126.177.uio.satnet.net [200.69.177.126]
5	27 ms	25 ms	27 ms	142.250.172.196
6	26 ms	28 ms	28 ms	142.251.51.71
7	31 ms	44 ms	36 ms	209.85.251.39
8	25 ms	25 ms	34 ms	bog02s12-in-f14.1e100.net [172.217.173.46]

Traza completa.

PS C:\Users\mateo>

b) Watch a video from youtube.com. Capture the TCP handshake, and the congestion window.

Wi-Fi

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

tcp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	107.167.110.211	192.168.0.111	TCP	54	443 → 63187 [ACK] Seq=1 Ack=1 Win=41823 Len=0
15	1.590122	162.159.130.234	192.168.0.111	TLSv1.2	157	Application Data
16	1.636355	192.168.0.111	162.159.130.234	TCP	54	62834 → 443 [ACK] Seq=1 Ack=104 Win=256 Len=0
56	5.939804	140.82.112.25	192.168.0.111	TLSv1.2	80	Application Data
57	5.939804	140.82.112.25	192.168.0.111	TCP	80	[TCP Retransmission] 443 → 63090 [PSH, ACK] Seq=1 Ack=1 Win=70 Len=26
58	5.939804	140.82.112.25	192.168.0.111	TCP	80	[TCP Retransmission] 443 → 63090 [PSH, ACK] Seq=1 Ack=1 Win=70 Len=26
59	5.939804	140.82.112.25	192.168.0.111	TCP	80	[TCP Retransmission] 443 → 63090 [PSH, ACK] Seq=1 Ack=1 Win=70 Len=26
60	5.940007	192.168.0.111	140.82.112.25	TCP	66	63090 → 443 [ACK] Seq=1 Ack=27 Win=510 Len=0 SLE=1 SRE=27
61	5.940059	192.168.0.111	140.82.112.25	TCP	66	[TCP Dup ACK 60#1] 63090 → 443 [ACK] Seq=1 Ack=27 Win=510 Len=0 SLE=1 SRE=27
62	5.940081	192.168.0.111	140.82.112.25	TCP	66	[TCP Dup ACK 60#2] 63090 → 443 [ACK] Seq=1 Ack=27 Win=510 Len=0 SLE=1 SRE=27
63	5.940334	192.168.0.111	140.82.112.25	TLSv1.2	84	Application Data
67	6.000719	192.168.0.111	107.167.110.216	TCP	66	63190 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
69	6.025126	140.82.112.25	192.168.0.111	TCP	54	443 → 63090 [ACK] Seq=27 Ack=31 Win=70 Len=0
70	6.088215	107.167.110.216	192.168.0.111	TCP	58	443 → 63190 [SYN, ACK] Seq=0 Ack=1 Win=42340 Len=0 MSS=1460
71	6.088446	192.168.0.111	107.167.110.216	TCP	54	63190 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
72	6.089014	192.168.0.111	107.167.110.216	TLSv1.3	571	Client Hello
74	6.187383	107.167.110.216	192.168.0.111	TCP	54	443 → 63190 [ACK] Seq=1 Ack=518 Win=41823 Len=0
75	6.189016	107.167.110.216	192.168.0.111	TLSv1.3	1514	Server Hello, Change Cipher Spec, Application Data
76	6.189016	107.167.110.216	192.168.0.111	TCP	1514	443 → 63190 [ACK] Seq=1461 Ack=518 Win=41823 Len=1460 [TCP segment of a reassembled PDU]
77	6.189016	107.167.110.216	192.168.0.111	TLSv1.3	272	Application Data, Application Data, Application Data
78	6.189321	192.168.0.111	107.167.110.216	TCP	54	63190 → 443 [ACK] Seq=518 Ack=2921 Win=64240 Len=0
79	6.191293	192.168.0.111	107.167.110.216	TLSv1.3	134	Change Cipher Spec, Application Data
80	6.191303	192.168.0.111	107.167.110.216	TLSv1.3	581	Application Data
81	6.286379	107.167.110.216	192.168.0.111	TCP	54	443 → 63190 [ACK] Seq=3139 Ack=1125 Win=41823 Len=0
90	6.519818	107.167.110.216	192.168.0.111	TLSv1.3	316	Application Data
91	6.560534	192.168.0.111	107.167.110.216	TCP	54	63190 → 443 [ACK] Seq=1125 Ack=3401 Win=63760 Len=0
97	8.780813	192.168.0.111	64.31.17.54	TCP	55	60636 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]
100	7.891418	64.31.17.54	192.168.0.111	TCP	54	443 → 60636 [ACK] Seq=0 Ack=2 Win=501 Len=0
101	7.891488	192.168.0.111	64.31.17.54	TCP	54	[TCP Dup ACK 99#1] [TCP ACKed unseen segment] 60636 → 443 [ACK] Seq=2 Ack=1 Win=513 Len=0
102	7.960314	64.31.17.54	192.168.0.111	TCP	66	[TCP Previous segment not captured] 443 → 60636 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
105	8.267501	192.168.0.111	162.159.137.234	TLSv1.2	115	Application Data
106	8.281589	162.159.137.234	192.168.0.111	TCP	54	443 → 62189 [ACK] Seq=1 Ack=62 Win=8 Len=0
107	8.401543	52.123.129.254	192.168.0.111	TCP	54	443 → 63184 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

> Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF-{6800DC9A-D...} (0.0.0.0) on interface 0
> Ethernet II, Src: D-LinkIn_e9:f9:af (6c:19:8f:e9:f9:af), Dst: IntelCor_f5:38:c7 (4c:03:4f:f5:38:c7)
> Internet Protocol Version 4, Src: 107.167.110.211, Dst: 192.168.0.111
> Transmission Control Protocol, Src Port: 443, Dst Port: 63187, Seq: 1, Ack: 1, Len: 0

wireshark-Wi-Fi616C41.pcapng

Paquetes: 49867 - Mostrado: 288 (0.6%)

Perfil: Default

Wi-Fi

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

tcp

No.	Time	Source	Destination	Protocol	Length	Info
100	7.891418	64.31.17.54	192.168.0.111	TCP	54	443 → 60636 [ACK] Seq=0 Ack=2 Win=501 Len=0
101	7.891488	192.168.0.111	64.31.17.54	TCP	54	[TCP Dup ACK 99#1] [TCP ACKed unseen segment] 60636 → 443 [ACK] Seq=2 Ack=1 Win=513 Len=0
102	7.960314	64.31.17.54	192.168.0.111	TCP	66	[TCP Previous segment not captured] 443 → 60636 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
105	8.267501	192.168.0.111	162.159.137.234	TLSv1.2	115	Application Data
106	8.281589	162.159.137.234	192.168.0.111	TCP	54	443 → 62189 [ACK] Seq=1 Ack=62 Win=8 Len=0
107	8.401543	52.123.129.254	192.168.0.111	TCP	54	443 → 63184 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
108	8.448242	162.159.137.234	192.168.0.111	TLSv1.2	111	Application Data
114	8.497332	192.168.0.111	162.159.137.234	TCP	54	62189 → 443 [ACK] Seq=62 Ack=58 Win=512 Len=0
508	8.783744	13.90.46.132	192.168.0.111	TCP	54	443 → 63183 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1073	10.412547	13.90.46.132	192.168.0.111	TLSv1.2	85	Application Data
1074	10.412710	192.168.0.111	13.90.46.132	TCP	54	62957 → 443 [ACK] Seq=1 Ack=32 Win=1019 Len=0
1075	10.413013	192.168.0.111	13.90.46.132	TLSv1.2	89	Application Data
1515	10.513734	13.90.46.132	192.168.0.111	TLSv1.2	85	Application Data
1516	10.513894	192.168.0.111	13.90.46.132	TCP	54	62957 → 443 [ACK] Seq=36 Ack=63 Win=1019 Len=0
1699	10.807770	204.79.197.222	192.168.0.111	TCP	54	443 → 63186 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1712	11.889491	40.126.212.199	192.168.0.111	TCP	54	443 → 63180 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1717	12.125409	192.168.0.111	52.168.117.169	TCP	66	63191 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1720	12.217128	52.168.117.169	192.168.0.111	TCP	66	443 → 63191 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
1721	12.217348	192.168.0.111	52.168.117.169	TCP	54	63191 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
1722	12.219484	192.168.0.111	52.168.117.169	TLSv1.2	266	Client Hello
1723	12.318196	52.168.117.169	192.168.0.111	TCP	54	443 → 63191 [ACK] Seq=1 Ack=213 Win=525312 Len=0
1724	12.319201	52.168.117.169	192.168.0.111	TCP	1514	443 → 63191 [ACK] Seq=1 Ack=213 Win=525312 Len=1460 [TCP segment of a reassembled PDU]
1725	12.319201	52.168.117.169	192.168.0.111	TCP	1514	443 → 63191 [ACK] Seq=1461 Ack=213 Win=525312 Len=1460 [TCP segment of a reassembled PDU]
1726	12.319201	52.168.117.169	192.168.0.111	TCP	1514	443 → 63191 [ACK] Seq=2921 Ack=213 Win=525312 Len=1460 [TCP segment of a reassembled PDU]
1727	12.319201	52.168.117.169	192.168.0.111	TLSv1.2	76	Server Hello, Certificate, Server Key Exchange, Server Hello Done
1728	12.319564	192.168.0.111	52.168.117.169	TCP	54	63191 → 443 [ACK] Seq=213 Ack=2921 Win=66048 Len=0
1729	12.319751	192.168.0.111	52.168.117.169	TCP	54	63191 → 443 [ACK] Seq=213 Ack=4403 Win=66048 Len=0
1730	12.325315	192.168.0.111	52.168.117.169	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1731	12.425057	52.168.117.169	192.168.0.111	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
1732	12.426559	192.168.0.111	52.168.117.169	TLSv1.2	1024	Application Data
1733	12.426850	192.168.0.111	52.168.117.169	TLSv1.2	1467	Application Data
1734	12.465765	162.159.130.234	192.168.0.111	TLSv1.2	374	Application Data
1735	12.511712	192.168.0.111	162.159.130.234	TCP	54	62834 → 443 [ACK] Seq=1 Ack=424 Win=255 Len=0

> Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF-{6800DC9A-D...} (0.0.0.0) on interface 0
> Ethernet II, Src: D-LinkIn_e9:f9:af (6c:19:8f:e9:f9:af), Dst: IntelCor_f5:38:c7 (4c:03:4f:f5:38:c7)
> Internet Protocol Version 4, Src: 107.167.110.211, Dst: 192.168.0.111
> Transmission Control Protocol, Src Port: 443, Dst Port: 63187, Seq: 1, Ack: 1, Len: 0

wireshark-Wi-Fi616C41.pcapng

Paquetes: 49867 - Mostrado: 288 (0.6%)

Perfil: Default

Wi-Fi

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

tcp

No.	Time	Source	Destination	Protocol	Length	Info
1733	12.426850	192.168.0.111	52.168.117.169	TLSv1.2	1467	Application Data
1734	12.465765	162.159.130.234	192.168.0.111	TLSv1.2	374	Application Data
1735	12.511712	192.168.0.111	162.159.130.234	TCP	54	62834 → 443 [ACK] Seq=1 Ack=424 Win=255 Len=0
1736	12.517677	52.168.117.169	192.168.0.111	TCP	54	443 → 63191 [ACK] Seq=4454 Ack=2754 Win=525568 Len=0
1737	12.522366	52.168.117.169	192.168.0.111	TLSv1.2	507	Application Data
1738	12.528037	192.168.0.111	52.168.117.169	TCP	54	63191 → 443 [FIN, ACK] Seq=2754 Ack=4907 Win=65536 Len=0
1739	12.640351	52.168.117.169	192.168.0.111	TCP	54	443 → 63191 [FIN, ACK] Seq=4907 Ack=2755 Win=525568 Len=0
1740	12.661254	192.168.0.111	172.217.193.188	TLSv1.2	80	Application Data
1741	12.756233	172.217.193.188	192.168.0.111	TCP	54	5228 → 61057 [ACK] Seq=1 Ack=27 Win=265 Len=0
1742	12.756740	172.217.193.188	192.168.0.111	TLSv1.2	80	Application Data
1743	12.809063	192.168.0.111	172.217.193.188	TCP	54	61057 → 5228 [ACK] Seq=27 Ack=27 Win=508 Len=0
1744	12.944982	52.168.117.169	192.168.0.111	TCP	54	[TCP Retransmission] 443 → 63191 [FIN, ACK] Seq=4907 Ack=2755 Win=525568 Len=0
1745	12.945030	192.168.0.111	52.168.117.169	TCP	54	[TCP ZeroWindow] 63191 → 443 [ACK] Seq=2755 Ack=4908 Win=0 Len=0
1750	13.235227	13.107.21.200	192.168.0.111	TCP	54	443 → 63181 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1772	13.972640	13.107.42.254	192.168.0.111	TCP	54	443 → 63185 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1779	14.703536	52.96.29.82	192.168.0.111	TCP	54	443 → 63182 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1875	16.601676	192.168.0.111	34.226.59.12	TCP	54	63174 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1876	16.602075	192.168.0.111	34.226.59.12	TLSv1.2	85	Encrypted Alert
1877	16.602134	192.168.0.111	34.226.59.12	TCP	54	63175 → 443 [RST, ACK] Seq=32 Ack=1 Win=0 Len=0
1878	16.602260	192.168.0.111	34.226.59.12	TLSv1.2	85	Encrypted Alert
1879	16.602306	192.168.0.111	34.226.59.12	TCP	54	63176 → 443 [RST, ACK] Seq=32 Ack=1 Win=0 Len=0
1880	16.602432	192.168.0.111	34.226.59.12	TLSv1.2	85	Encrypted Alert
1881	16.602462	192.168.0.111	34.226.59.12	TCP	54	63177 → 443 [RST, ACK] Seq=32 Ack=1 Win=0 Len=0
1890	16.638165	192.168.0.111	18.207.74.168	TCP	66	63192 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1961	16.742863	18.207.74.168	192.168.0.111	TCP	66	443 → 63192 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1460 SACK_PERM WS=256
1962	16.743165	192.168.0.111	18.207.74.168	TCP	54	63192 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
1972	16.763040	192.168.0.111	18.207.74.168	TLSv1.2	571	Client Hello
2082	16.862924	18.207.74.168	192.168.0.111	TCP	54	443 → 63192 [ACK] Seq=1 Ack=518 Win=28160 Len=0
2086	16.863923	18.207.74.168	192.168.0.111	TLSv1.2	169	Server Hello
2087	16.863923	18.207.74.168	192.168.0.111	TCP	1514	443 → 63192 [ACK] Seq=116 Ack=518 Win=28160 Len=1460 [TCP segment of a reassembled PDU]
2088	16.863923	18.207.74.168	192.168.0.111	TCP	1514	443 → 63192 [ACK] Seq=1576 Ack=518 Win=28160 Len=1460 [TCP segment of a reassembled PDU]
2089	16.863923	18.207.74.168	192.168.0.111	TCP	1514	443 → 63192 [ACK] Seq=3036 Ack=518 Win=28160 Len=1460 [TCP segment of a reassembled PDU]
2090	16.863923	18.207.74.168	192.168.0.111	TLSv1.2	631	Certificate

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{6800DC9A-D...} Ethernet II, Src: D-LinkIn_e9:f9:af (6c:19:8f:e9:f9:af), Dst: IntelCor_f5:38:c7 (4c:03:4f:f5:38:c7)

Internet Protocol Version 4, Src: 107.167.110.211, Dst: 192.168.0.111

Transmission Control Protocol, Src Port: 443, Dst Port: 63187, Seq: 1, Ack: 1, Len: 0

0000 4c 03 4f f5 38 c7 6c 19 8f e9 f9 af 00 00 45 00 L 0 8 1 ... E

0010 00 28 9e 03 40 00 38 06 09 3b 6b a7 6e d3 c0 a8 (- 8 . ; k n ...

0020 00 6f 01 bb f6 d3 1a 6f c3 ae 9f 3b c1 1b 50 10 o ... o ... ; . P ...

0030 a3 5f 39 df 00 00 _ 9 ...

Paquetes: 49867 - Mostrado: 288 (0.6%) Perfil: Default

Wi-Fi

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

tcp

No.	Time	Source	Destination	Protocol	Length	Info
16330	21.692733	192.168.0.111	20.94.21.149	TCP	55	62841 → 443 [ACK] Seq=1 Ack=1 Win=256 Len=1 [TCP segment of a reassembled PDU]
17251	21.827686	20.94.21.149	192.168.0.111	TCP	66	443 → 62841 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
18261	22.017933	192.168.0.111	162.159.137.234	TLSv1.2	115	Application Data
18388	22.048464	162.159.137.234	192.168.0.111	TCP	54	443 → 62189 [ACK] Seq=58 Ack=123 Win=8 Len=0
18405	22.202652	162.159.137.234	192.168.0.111	TLSv1.2	111	Application Data
18408	22.247942	192.168.0.111	162.159.137.234	TCP	54	62189 → 443 [ACK] Seq=123 Ack=115 Win=514 Len=0
23201	28.067311	192.168.0.111	64.31.17.54	TCP	55	[TCP Keep-Alive] 60636 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1
23202	28.116733	64.31.17.54	192.168.0.111	TCP	54	[TCP Keep-Alive] 443 → 60636 [ACK] Seq=0 Ack=2 Win=501 Len=0
23203	28.116791	192.168.0.111	64.31.17.54	TCP	54	[TCP Keep-Alive ACK] 60636 → 443 [ACK] Seq=2 Ack=1 Win=513 Len=0
23205	28.150742	64.31.17.54	192.168.0.111	TCP	66	[TCP Dup ACK 160#1] 443 → 60636 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
23207	28.707193	192.168.0.111	107.167.110.211	TCP	54	63187 → 443 [FIN, ACK] Seq=1 Ack=26 Win=63646 Len=0
23208	28.707296	107.167.110.211	192.168.0.111	TCP	54	63187 → 443 [RST, ACK] Seq=2 Ack=26 Win=0 Len=0
23212	28.800870	107.167.110.211	192.168.0.111	TCP	54	443 → 63187 [ACK] Seq=26 Ack=2 Win=41823 Len=0
25469	30.430910	192.168.0.111	107.167.110.211	TCP	66	63193 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
25470	30.515008	192.168.0.111	107.167.110.211	TCP	66	63194 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
25471	30.517150	107.167.110.211	192.168.0.111	TCP	66	443 → 63193 [SYN, ACK] Seq=0 Ack=1 Win=42340 Len=0 MSS=1460 SACK_PERM WS=512
25472	30.517350	192.168.0.111	107.167.110.211	TCP	54	63193 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
25473	30.517943	192.168.0.111	107.167.110.211	TLSv1.3	571	Client Hello
25474	30.606463	107.167.110.211	192.168.0.111	TCP	66	443 → 63194 [SYN, ACK] Seq=0 Ack=1 Win=42340 Len=0 MSS=1460 SACK_PERM WS=512
25475	30.606668	192.168.0.111	107.167.110.211	TCP	54	63194 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
25476	30.607286	192.168.0.111	107.167.110.211	TLSv1.3	571	Client Hello
25477	30.611448	107.167.110.211	192.168.0.111	TCP	54	443 → 63193 [ACK] Seq=1 Ack=518 Win=42496 Len=0
25478	30.612990	107.167.110.211	192.168.0.111	TCP	54	[TCP Dup ACK 25477#1] 443 → 63193 [ACK] Seq=1 Ack=518 Win=42496 Len=0
25479	30.612990	107.167.110.211	192.168.0.111	TLSv1.3	1514	Server Hello, Change Cipher Spec, Application Data
25480	30.612990	107.167.110.211	192.168.0.111	TCP	1514	443 → 63193 [PSH, ACK] Seq=1461 Ack=518 Win=42496 Len=1460 [TCP segment of a reassembled PDU]
25481	30.612990	107.167.110.211	192.168.0.111	TLSv1.3	271	Application Data, Application Data
25482	30.613190	192.168.0.111	107.167.110.211	TCP	54	63193 → 443 [ACK] Seq=518 Ack=2921 Win=65536 Len=0
25483	30.613704	192.168.0.111	107.167.110.211	TLSv1.3	134	Change Cipher Spec, Application Data
25484	30.613803	192.168.0.111	107.167.110.211	TLSv1.3	490	Application Data
25485	30.703034	107.167.110.211	192.168.0.111	TCP	54	443 → 63194 [ACK] Seq=1 Ack=518 Win=42496 Len=0
25486	30.703034	107.167.110.211	192.168.0.111	TCP	54	443 → 63193 [ACK] Seq=3138 Ack=1034 Win=42496 Len=0
25487	30.703502	107.167.110.211	192.168.0.111	TLSv1.3	1514	Server Hello, Change Cipher Spec, Application Data
25488	30.703502	107.167.110.211	192.168.0.111	TCP	1514	443 → 63194 [PSH, ACK] Seq=1461 Ack=518 Win=42496 Len=1460 [TCP segment of a reassembled PDU]

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{6800DC9A-D...} Ethernet II, Src: D-LinkIn_e9:f9:af (6c:19:8f:e9:f9:af), Dst: IntelCor_f5:38:c7 (4c:03:4f:f5:38:c7)

Internet Protocol Version 4, Src: 107.167.110.211, Dst: 192.168.0.111

Transmission Control Protocol, Src Port: 443, Dst Port: 63187, Seq: 1, Ack: 1, Len: 0

0000 4c 03 4f f5 38 c7 6c 19 8f e9 f9 af 00 00 45 00 L 0 8 1 ... E

0010 00 28 9e 03 40 00 38 06 09 3b 6b a7 6e d3 c0 a8 (- 8 . ; k n ...

0020 00 6f 01 bb f6 d3 1a 6f c3 ae 9f 3b c1 1b 50 10 o ... o ... ; . P ...

0030 a3 5f 39 df 00 00 _ 9 ...

Paquetes: 49867 - Mostrado: 288 (0.6%) Perfil: Default

2) Use Dijkstra's to get the routing tables for nodes A, B and E.

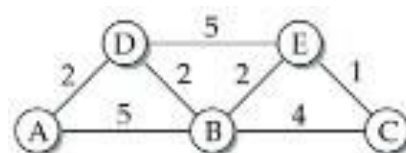


Tabla de enrutamiento para el nodo A:

Destino	Siguiente salto	Distancia
A	Null	0
B	D	4
C	B	8
D	A	2
E	D	7

Tabla de enrutamiento para el nodo B:

Destino	Siguiente salto	Distancia
A	D	4
B	Null	0
C	B	4
D	B	2
E	C	5

Tabla de enrutamiento para el nodo E:

Destino	Siguiente salto	Distancia
A	D	7
B	C	5
C	E	1
D	E	5
E	Null	0

Código utilizado:

```
import sys

def dijkstra(graph, start_node):
    distances = {node: float('inf') for node in graph}
    distances[start_node] = 0

    next_hops = {node: None for node in graph}

    visited = set()

    while len(visited) < len(graph):
        current_node = min(
            (node for node in graph if node not in visited),
            key=lambda node: distances[node]
        )
        visited.add(current_node)

        for neighbor, weight in graph[current_node].items():
            distance = distances[current_node] + weight
            if distance < distances[neighbor]:
                distances[neighbor] = distance
                next_hops[neighbor] = current_node

    return distances, next_hops

graph = {
    'A': {'B': 5, 'D': 2},
    'B': {'A': 5, 'D': 2, 'C': 4, 'E': 4 },
    'C': {'B': 4, 'E': 1},
    'D': {'A': 2, 'B': 2, 'E': 5},
    'E': {'C': 1, 'D': 5}
}
```


- 3) Suppose a host wants to establish the reliability of a link by sending packets and measuring the percentage that are received; routers, for example, do this. Explain the difficulty of doing this over a TCP connection.

Intentar establecer la confiabilidad de una conexión red mediante el envío de paquetes puede ser un tanto complicada en una conexión TCP en comparación a otras conexiones. Esto se debe a que el mecanismo de control de flujo y control de congestión implementado en el protocolo TCP, puesto que el TCP utiliza algoritmos que garantizan una entrega confiable de datos. En este caso el TCP tiene mecanismos de retransmisiones automáticas, el cual, cuando detecta una pérdida de paquetes en la conexión TCP, el protocolo lo volverá a retransmitir de forma automática, ocasionando que los paquetes perdidos puedan llegar a su destino tarde, de igual manera también tenemos el control de congestión, mecanismo que usa algoritmos para regular el flujo de datos para evitar una posible congestión en la red ocasionando que la velocidad de envío de paquetes varíe dinámicamente. Estos mecanismos aumentan la complejidad al momento de medir la confiabilidad, por lo que la dificultad también es alta.

- 4) Consider a simple congestion control algorithm that uses linear increase and multiplicative decrease (no slow start). Assume the congestion window size is in units of packets rather than bytes, and it is one packet initially.
- a) Give a detailed sketch of this algorithm.
 - b) Assume the delay is latency only, and that when a group of packets is sent, only a single ACK is returned.
 - c) Plot the congestion window as a function of RTT for the situation in which the following packets are lost: 9, 25, 30, 38 and 50. For simplicity, assume a perfect timeout mechanism that detects a lost packet exactly 1 RTT after it is transmitted.

Suponiendo que el tamaño del remitente es de 1 paquete, este envía una ventana completa en un lote. Eso significa que por cada ACK de una ventana que el remitente recibe, aumenta su ventana efectiva en uno. Sin embargo, esta se reduce a la mitad del número de paquetes cuando pasa el timeout. Si tomamos en cuenta la situación en la que se nos indica la existencia de paquetes perdidos, el tamaño de la ventana inicialmente es 1 y cuando se obtiene el primer ACK este crece a 2. Cuando inicia el segundo RTT enviamos paquetes 2 y 3, y cuando estos obtienen sus ACK la ventana incrementa a 3 y enviamos los paquetes 4, 5 y 6, que, con su llegada el tamaño de la ventana pasa a ser 4. Prosiguiendo, cuando llegamos al cuarto RTT, se envían los paquetes 7, 8, 9, 10, donde el paquete 9 se pierde, por tanto, después del timeout el tamaño de la ventana se reduce a 2. Finalmente, la ventana de congestión aumenta hasta perder al paquete 25, reduciendo su tamaño a la mitad el cual vendría a hacer el valor de 3 cuando acaba el noveno RTT.

