Security and Computer System

Informatics Course

Lodz University(2016/2017)

WireShark

Iván Sevillano García

26 de octubre de 2016

1. Wiresharck: Network Monitoring Tool

Wireshark is a powerfull tool which can show information about the network traffic, which means to see all packages that goes througth your computer. Using this tool you can see some risky information from the users of the network, or detecting an attack to a server. Let's see an example:

- The scenario will be as it follows. My computer is sharing internet and it has my phone conected. We are going to start sniffing the net traffic(wlan0) and see what my phone is doing...

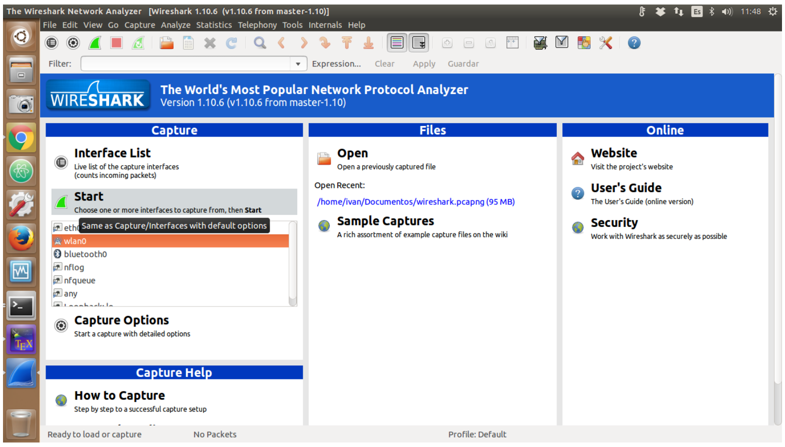
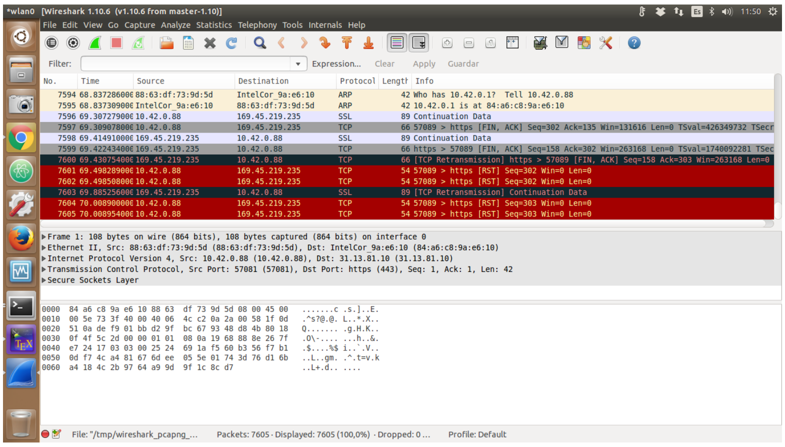

The Wireshark Network Analyzer [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
11:48
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression...
Clear
Apply
Guardar
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Version 1.10.6 (v1.10.6 from master-1.10)
Capture
Interface List
Live list of the capture interfaces (counts incoming packets)
Start
Choose one or more interfaces to capture from, then Start
eth0
Same as Capture/Interfaces with default options
wlan0
bluetooth0
nflog
nfqueue
any
Capture Options
Start a capture with detailed options
Capture Help
How to Capture
Step by step to a successful capture setup
Files
Open
Open a previously captured file
Open Recent:
/home/ivan/Documentos/wireshark.pcapng (95 MB)
Sample Captures
A rich assortment of example capture files on the wiki
Online
Website
Visit the project's website
User's Guide
The User's Guide (online version)
Security
Work with Wireshark as securely as possible
Ready to load or capture
No Packets
Profile: Default

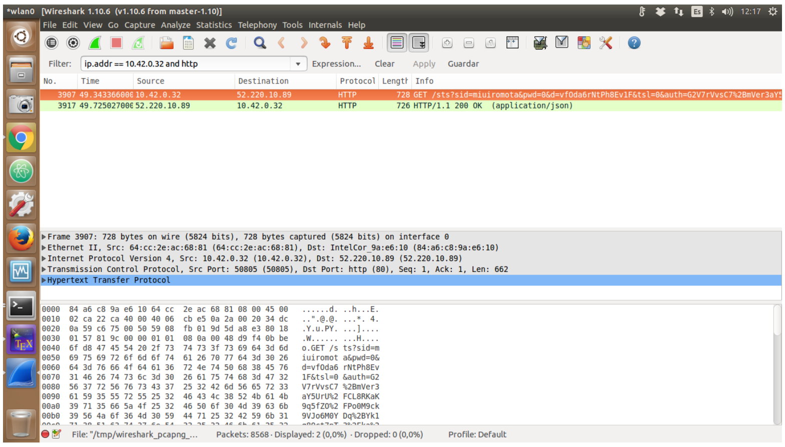
Figura 1.1:


*wlan0 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
11:50
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression...
Clear
Apply
Guardar

```
No.   Time              Source            Destination       Protocol Lengtł Info
 7594 68.837286000 88:63:df:73:9d:5d   IntelCor_9a:e6:10   ARP       42 Who has 10.42.0.1?  Tell 10.42.0.88
 7595 68.837309000 IntelCor_9a:e6:10   88:63:df:73:9d:5d   ARP       42 10.42.0.1 is at 84:a6:c8:9a:e6:10
 7596 69.307279000 10.42.0.88          169.45.219.235      SSL       89 Continuation Data
 7597 69.309078000 10.42.0.88          169.45.219.235      TCP       66 57089 > https [FIN, ACK] Seq=302 Ack=135 Win=131616 Len=0 TSval=426349732 TSecr
 7598 69.414910000 169.45.219.235      10.42.0.88          SSL       89 Continuation Data
 7599 69.422434000 169.45.219.235      10.42.0.88          TCP       66 https > 57089 [FIN, ACK] Seq=158 Ack=302 Win=263168 Len=0 TSval=1740092281 TSec
 7600 69.430754000 169.45.219.235      10.42.0.88          TCP       66 [TCP Retransmission] https > 57089 [FIN, ACK] Seq=158 Ack=303 Win=263168 Len=0
 7601 69.498289000 10.42.0.88          169.45.219.235      TCP       54 57089 > https [RST] Seq=302 Win=0 Len=0
 7602 69.498508000 10.42.0.88          169.45.219.235      TCP       54 57089 > https [RST] Seq=302 Win=0 Len=0
 7603 69.885256000 169.45.219.235      10.42.0.88          SSL       89 [TCP Retransmission] Continuation Data
 7604 70.008900000 10.42.0.88          169.45.219.235      TCP       54 57089 > https [RST] Seq=303 Win=0 Len=0
 7605 70.008954000 10.42.0.88          169.45.219.235      TCP       54 57089 > https [RST] Seq=303 Win=0 Len=0

▶Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface 0
▶Ethernet II, Src: 88:63:df:73:9d:5d (88:63:df:73:9d:5d), Dst: IntelCor_9a:e6:10 (84:a6:c8:9a:e6:10)
▶Internet Protocol Version 4, Src: 10.42.0.88 (10.42.0.88), Dst: 31.13.81.10 (31.13.81.10)
▶Transmission Control Protocol, Src Port: 57081 (57081), Dst Port: https (443), Seq: 1, Ack: 1, Len: 42
▶Secure Sockets Layer

0000  84 a6 c8 9a e6 10 88 63  df 73 9d 5d 08 00 45 00   .......c .s.]..E.
0010  00 5e 73 3f 40 00 40 06  4c c2 0a 2a 00 58 1f 0d   .^s?@.@. L..*.X..
0020  51 0a de f9 01 bb d2 9f  bc 67 93 48 d8 4b 80 18   Q....... .g.H.K..
0030  0f 4f 5c 2d 00 00 01 01  08 0a 19 68 88 8e 26 7f   .O\-.... ...h..&.
0040  e7 24 17 03 03 00 25 24  69 1a f5 60 b3 56 f7 b1   .$....%$ i..`.V..
0050  0d f7 4c a4 81 67 6d ee  05 5e 01 74 3d 76 d1 6b   ..L..gm. .^.t=v.k
0060  a4 18 4c 2b 97 64 a9 9d  9f 1c 8c d7               ..L+.d.. ....

File: "/tmp/wireshark_pcapng_...   Packets: 7605 · Displayed: 7605 (100,0%) · Dropped: 0 ...   Profile: Default
```

Figura 1.2:

- Now we will see which information could we take. Our network gives directions from 10.42.0.0/24, so we will look for this ips. With a simple nmap scanning, we notice there are three ips connected, one of them is the router(my computer), one of them should be my phone and the other one must be one of my friends phone. We are not going to look for what he is doing, so pay attention to my phone(.32 ip). Also, we want to know what is this phone looking, for example, on internet(http packages):


*wlan0 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
12:17
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Guardar

Filter: ip.addr == 10.42.0.32 and http

```
No.   Time        Source         Destination    Protocol Lengtł Info
 3907 49.34336600( 10.42.0.32    52.220.10.89   HTTP      728 GET /sts?sid=miuiromota&pwd=0&d=vfOda6rNtPh8Ev1F&tsl=0&auth=G2V7rVvsC7%2BmVer3aY5
 3917 49.72502700( 52.220.10.89  10.42.0.32     HTTP      726 HTTP/1.1 200 OK  (application/json)
```

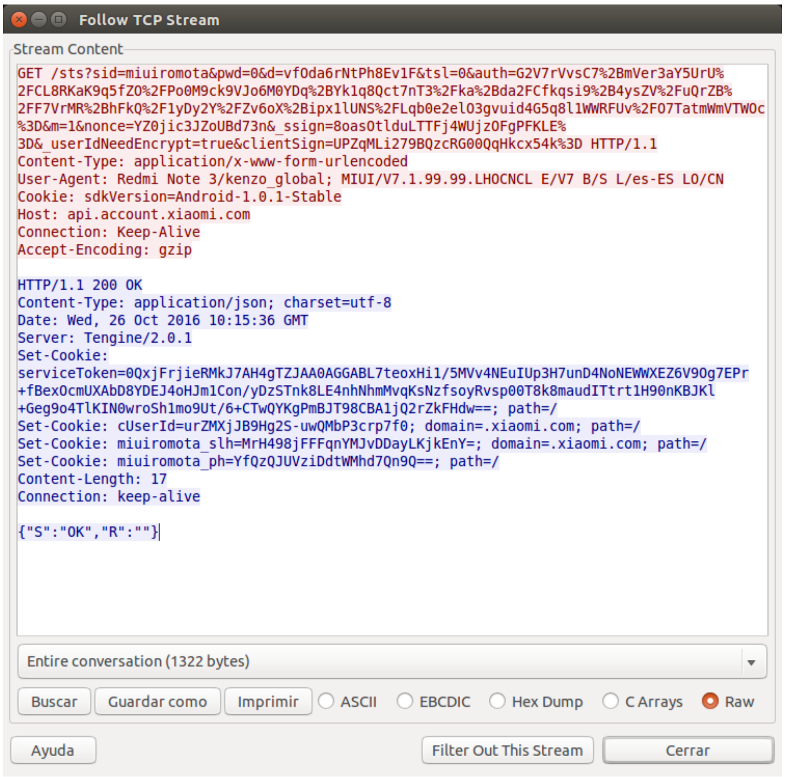
```
▶Frame 3907: 728 bytes on wire (5824 bits), 728 bytes captured (5824 bits) on interface 0
▶Ethernet II, Src: 64:cc:2e:ac:68:81 (64:cc:2e:ac:68:81), Dst: IntelCor_9a:e6:10 (84:a6:c8:9a:e6:10)
▶Internet Protocol Version 4, Src: 10.42.0.32 (10.42.0.32), Dst: 52.220.10.89 (52.220.10.89)
▶Transmission Control Protocol, Src Port: 50805 (50805), Dst Port: http (80), Seq: 1, Ack: 1, Len: 662
▶Hypertext Transfer Protocol
```

```
0000  84 a6 c8 9a e6 10 64 cc  2e ac 68 81 08 00 45 00   ......d. ..h...E.
0010  02 ca 22 ca 40 00 40 06  cb e5 0a 2a 00 20 34 dc   ..".@.@. ...*. 4.
0020  0a 59 c6 75 00 50 59 08  fb 01 9d 5d a8 e3 80 18   .Y.u.PY. ...]....
0030  01 57 81 9c 00 00 01 01  08 0a 00 48 d9 f4 0b be   .W...... ...H....
0040  6f d8 47 45 54 20 2f 73  74 73 3f 73 69 64 3d 6d   o.GET /s ts?sid=m
0050  69 75 69 72 6f 6d 6f 74  61 26 70 77 64 3d 30 26   iuiromot a&pwd=0&
0060  64 3d 76 66 4f 64 61 36  72 4e 74 50 68 38 45 76   d=vfOda6 rNtPh8Ev
0070  31 46 26 74 73 6c 3d 30  26 61 75 74 68 3d 47 32   1F&tsl=0 &auth=G2
0080  56 37 72 56 76 73 43 37  25 32 42 6d 56 65 72 33   V7rVvsC7 %2BmVer3
0090  61 59 35 55 72 55 25 32  46 43 4c 38 52 4b 61 4b   aY5UrU%2 FCL8RKaK
00a0  39 71 35 66 5a 4f 25 32  46 50 6f 30 4d 39 63 6b   9q5fZO%2 FPo0M9ck
00b0  39 56 4a 6f 36 4d 30 59  44 71 25 32 42 59 6b 31   9VJo6M0Y Dq%2BYk1
```

File: "/tmp/wireshark_pcapng_... Packets: 8568 · Displayed: 2 (0,0%) · Dropped: 0 (0,0%) Profile: Default

Figura 1.3:

- If we follow the TCP Stream of the http package with the "GET"method, that is what we see:



```
GET /sts?sid=miuiromota&pwd=0&d=vfOda6rNtPh8Ev1F&tsl=0&auth=G2V7rVvsC7%2BmVer3aY5UrU%
2FCL8RKaK9q5fZO%2FPo0M9ck9VJo6M0YDq%2BYk1q8Qct7nT3%2Fka%2Bda2FCfkqsi9%2B4ysZV%2FuQrZB%
2FF7VrMR%2BhFkQ%2F1yDy2Y%2FZv6oX%2Bipx1lUNS%2FLqb0e2elO3gvuid4G5q8l1WWRFUv%2FO7TatmWmVTWOc
%3D&m=1&nonce=YZ0jic3JZoUBd73n&_ssign=8oasOtlduLTTFj4WUjzOFgPFKLE%
3D&_userIdNeedEncrypt=true&clientSign=UPZqMLi279BQzcRG00QqHkcx54k%3D HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Redmi Note 3/kenzo_global; MIUI/V7.1.99.99.LHOCNCL E/V7 B/S L/es-ES LO/CN
Cookie: sdkVersion=Android-1.0.1-Stable
Host: api.account.xiaomi.com
Connection: Keep-Alive
Accept-Encoding: gzip

HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
Date: Wed, 26 Oct 2016 10:15:36 GMT
Server: Tengine/2.0.1
Set-Cookie:
serviceToken=0QxjFrjieRMkJ7AH4gTZJAA0AGGABL7teoxHi1/5MVv4NEuIUp3H7unD4NoNEWWXEZ6V9Og7EPr
+fBexOcmUXAbD8YDEJ4oHJm1Con/yDzSTnk8LE4nhNhmMvqKsNzfsoyRvsp00T8k8maudITtrt1H90nKBJKl
+Geg9o4TlKIN0wroSh1mo9Ut/6+CTwQYKgPmBJT98CBA1jQ2rZkFHdw==; path=/
Set-Cookie: cUserId=urZMXjJB9Hg2S-uwQMbP3crp7f0; domain=.xiaomi.com; path=/
Set-Cookie: miuiromota_slh=MrH498jFFFqnYMJvDDayLKjkEnY=; domain=.xiaomi.com; path=/
Set-Cookie: miuiromota_ph=YfQzQJUVziDdtWMhd7Qn9Q==; path=/
Content-Length: 17
Connection: keep-alive

{"S":"OK","R":""}
```

Figura 1.4:

- We can see information of not only the Web page the user has visited, we can also see the user hardware.

That is just like the "Hello World"for Wiresharsk.