Quick and dirty Wireshark tutorial

Karthik R and Pramod S

Wireshark has become a very useful tool for many infosec pros. This hands-on Wireshark tutorial will acquaint you with the network sniffer's capabilities.

Read the second part of this tutorial here.

Wireshark (earlier known as Ethereal) is one of the most popular open source network sniffer and packet/protocol analyzer solutions. It is used for troubleshooting, analysis, software and communications protocol development, as well as educational purposes. Wireshark has gained popularity because of its following features:

Related reading

5 penetration testing tools to secure your network

Penetration testing tool usage best practices

An ethical hacker career : Tips to gear up for this option

Vulnerability assessment and management tricks of the trade

1. Live capture, which allows sniffing data from a live network in real time.
2. Support for offline protocol analysis.
3. Enriched user interface (UI).
4. Supports almost all network, transport and application protocols.
5. Active development by enthusiasts across the globe.
6. Compatibility with other products. Supports standard .pcap format which makes it compatible for use with other such tools.

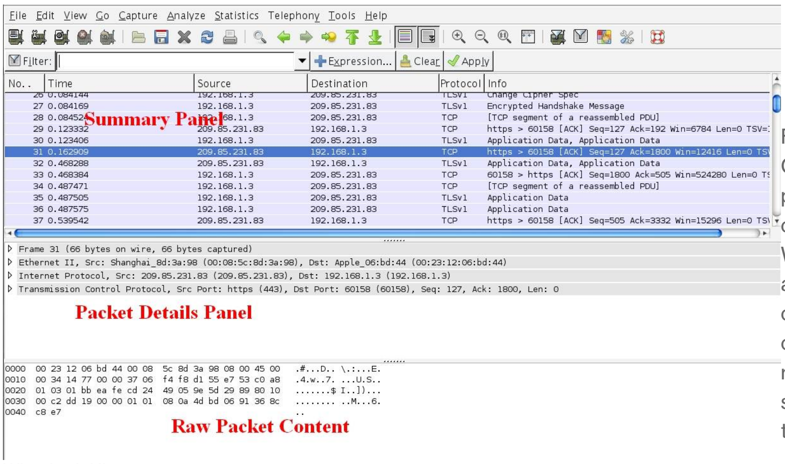
Wireshark is available as a free download for UNIX/Linux, Macintosh and Microsoft Windows operating systems. Once you have downloaded the tool, it's time to move on to the first step of our Wireshark tutorial.

Wireshark tutorial step 1: Install (Simple)

The analyzer's UI is very simple, and there shouldn't be any installation issues. Once installed, you can open Wireshark like other software installed on your computer from the **Start** menu (for Windows users), or in a similar manner for those who use Mac/Linux/Unix systems.

Wireshark tutorial step 2: Preps (Slight modifications required)

Set your browser to load a blank Web page so that unnecessary packets don't get captured. Once you are done with this, open Wireshark to get the UI shown in the screenshot; to capture packets, the capturing interface needs to be set up. Hence, go to the Menu bar and click **Capture -> Interfaces**.



```
No. .  Time      Source         Destination    Protocol Info
   26 0.084144  192.168.1.3    209.85.231.83  TLSv1    Change Cipher Spec
   27 0.084169  192.168.1.3    209.85.231.83  TLSv1    Encrypted Handshake Message
   28 0.08452   192.168.1.3    209.85.231.83  TCP      [TCP segment of a reassembled PDU]
   29 0.123332  209.85.231.83  192.168.1.3    TCP      https > 60158 [ACK] Seq=127 Ack=192 Win=6784 Len=0 TSV=
   30 0.123406  192.168.1.3    209.85.231.83  TLSv1    Application Data, Application Data
   31 0.162909  209.85.231.83  192.168.1.3    TCP      https > 60158 [ACK] Seq=127 Ack=1800 Win=12416 Len=0 TS
   32 0.468288  209.85.231.83  192.168.1.3    TLSv1    Application Data, Application Data
   33 0.468384  192.168.1.3    209.85.231.83  TCP      60158 > https [ACK] Seq=1800 Ack=505 Win=524280 Len=0 T
   34 0.487471  192.168.1.3    209.85.231.83  TCP      [TCP segment of a reassembled PDU]
   35 0.487505  192.168.1.3    209.85.231.83  TLSv1    Application Data
   36 0.487575  192.168.1.3    209.85.231.83  TLSv1    Application Data
   37 0.539542  209.85.231.83  192.168.1.3    TCP      https > 60158 [ACK] Seq=505 Ack=3332 Win=15296 Len=0 TS

▷ Frame 31 (66 bytes on wire, 66 bytes captured)
▷ Ethernet II, Src: Shanghai_8d:3a:98 (00:08:5c:8d:3a:98), Dst: Apple_06:bd:44 (00:23:12:06:bd:44)
▷ Internet Protocol, Src: 209.85.231.83 (209.85.231.83), Dst: 192.168.1.3 (192.168.1.3)
▷ Transmission Control Protocol, Src Port: https (443), Dst Port: 60158 (60158), Seq: 127, Ack: 1800, Len: 0

0000  00 23 12 06 bd 44 00 08  5c 8d 3a 98 08 00 45 00   .#...D.. \.:...E.
0010  00 34 14 77 00 00 37 06  f4 f8 d1 55 e7 53 c0 a8   .4.w..7. ...U.S..
0020  01 03 01 bb ea fe cd 24  49 05 9e 5d 29 89 80 10   .......$ I..])...
0030  00 c2 dd 19 00 00 01 01  08 0a 4d bd 06 91 36 8c   ........ ..M...6.
0040  c8 e7                                              ..
```

Wireshark UI

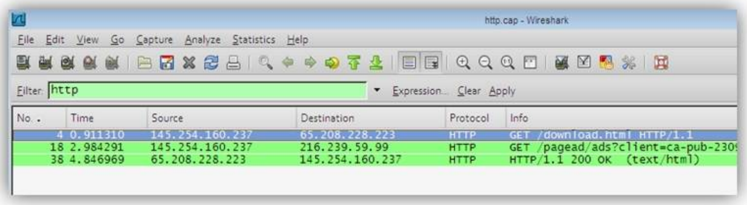
From here, choose the device that has an active IP address. Click on **Start** so that Wireshark is ready to capture any packets sent through the interface. In the Web browser, open http://www.httprecipes.com and hit **Go**. You will see Wireshark capturing all packets between your computer and the server. Captured communication can be analyzed in case of need for particular data. Since all packet types are captured and we are interested in examining HTTP requests as part of this Wireshark tutorial, HTTP packets should be filtered out from the rest. This can be achieved in two ways:

a) In the **Filter** bar, enter the type of packets to be filtered out.

Or,

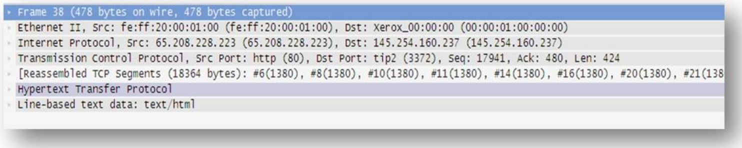
b) Use the **Expressions** button to choose **HTTP** option.

Wireshark tutorial step 3: HTTP analysis (Time to dive in)



```
Filter: http

No. .  Time      Source           Destination      Protocol  Info
    4 0.911310  145.254.160.237  65.208.228.223   HTTP      GET /download.html HTTP/1.1
   18 2.984291  145.254.160.237  216.239.59.99    HTTP      GET /pagead/ads?client=ca-pub-230
   38 4.846969  65.208.228.223   145.254.160.237  HTTP      HTTP/1.1 200 OK  (text/html)
```



```
▸ Frame 38 (478 bytes on wire, 478 bytes captured)
▸ Ethernet II, Src: fe:ff:20:00:01:00 (fe:ff:20:00:01:00), Dst: Xerox_00:00:00 (00:00:01:00:00:00)
▸ Internet Protocol, Src: 65.208.228.223 (65.208.228.223), Dst: 145.254.160.237 (145.254.160.237)
▸ Transmission Control Protocol, Src Port: http (80), Dst Port: tip2 (3372), Seq: 17941, Ack: 480, Len: 424
▸ [Reassembled TCP Segments (18364 bytes): #6(1380), #8(1380), #10(1380), #11(1380), #14(1380), #16(1380), #20(1380), #21(138
▸ Hypertext Transfer Protocol
▸ Line-based text data: text/html
```

The screenshot given above shows HTTP capture filtered from the other captures. Now, let's look at another screenshot to help you analyze the HTTP packets as part of our Wireshark tutorial.

We have different sections to examine, as seen above. Wireshark segregates the relevant data following the transmission control protocol (TCP) stack principle for better understanding. Let's understand the information that can be collected within these fields.

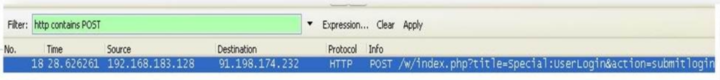
- **Frame:** This tells users the frame number, time related information regarding the packet, frame length, protocols within the frame, and the coloring rule.
- **Ethernet II:** Indicates the packet's source and destination.
- **Internet Protocol:** Contains the source and destination information along with version, header details, and lifetime. You will find source and destination IP addresses here.
- **TCP:** Captures information about source and destination ports involved in the communication, next sequence number to look out for, and different flags (along with their values).
- **HTTP:** Contains information on the HTTP version, server info, timeout value, connection status, content type, and character set used in the communication.
- **Line-based text data:** This contains HTML source code (since we are analyzing the HTTP protocol).

Wireshark tutorial step 4: Grab passwords (Shades of grey?)

This section of our Wireshark tutorial graduates you to the intermediate user level. Here, we will deal with how to capture a username and password from transferred packets. In case you are wondering whether we are drifting to the dark side of things, that isn't the case. This Wireshark tutorial is only for educational purposes.

If the username and password are not in clear text format, you might have to use few descriptors to get a readable username and password. The following part of our Wireshark tutorial presents a clear text form of packing data. Hence, there is no need of decryption tools. You can use this technique for FTP, HTTP, and other protocols, since they are in clear-text form.

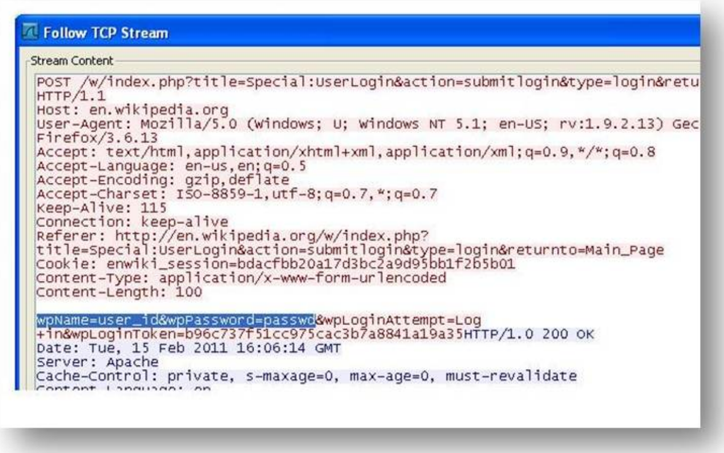
- Open any Website that supports the user name and login form; enter the credentials.
- Ensure that Wireshark's Capture mode is active and click on the **Log In** button.
- Stop the capture of packets and search for a packet with POST method which has the following filter query: HTTP contains POST in the **Filter** bar.



Filter: http contains POST

```
No.   Time       Source           Destination     Protocol  Info
   18 28.626261  192.168.183.128  91.198.174.232  HTTP      POST /w/index.php?title=Special:UserLogin&action=submitlogin
```

- Right click on the packet and choose the option à **Follow TCP/IP stream**
- The following screenshot tells you where the details are stored.



```
POST /w/index.php?title=Special:UserLogin&action=submitlogin&type=login&retu
HTTP/1.1
Host: en.wikipedia.org
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.13) Gec
Firefox/3.6.13
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Referer: http://en.wikipedia.org/w/index.php?
title=Special:UserLogin&action=submitlogin&type=login&returnto=Main_Page
Cookie: enwiki_session=bdacfbb20a17d3bc2a9d95bb1f2b5b01
Content-Type: application/x-www-form-urlencoded
Content-Length: 100

wpName=user_id&wpPassword=passwd&wpLoginAttempt=Log
+in&wpLoginToken=b96c737f51cc975cac3b7a8841a19a35HTTP/1.0 200 OK
Date: Tue, 15 Feb 2011 16:06:14 GMT
Server: Apache
Cache-Control: private, s-maxage=0, max-age=0, must-revalidate
```

We hope that this Wireshark tutorial helps you understand the tool in a better way. Keep experimenting with Wireshark, since results will never be the same. A new result will lead you to explore new possibilities. Wireshark is a great tool with more capabilities than described here. So keep exploring to expand your knowledge.

Read the second part of this tutorial here.

About the authors: Karthik R and Pramod S are members of the NULL community (www.null.co.in). Fueled by their interest in Ethical Hacking and Information security, the duo founded a startup named Raining Brains Security Solutions, focusing mainly on security issues in the cyber world. Karthik and Pramod completed their training for EC-council CEH in December 2010, and are at present pursuing their third year of B.Tech in Information Technology, from National Institute of Technology, Surathkal. Karthik and Pramod can be contacted on kr2910@yahoo.com and pramods.nitk@gmail.com respectively.

This was last published in February 2011

Read more on Hackers and cybercrime prevention

Security Think Tank: Data integrity breaches – the challenge facing banks

Data breaches affect all parts of business, Verizon report shows

Security Think Tank: Under-the-radar data integrity attacks expected to rise

NHS websites defaced by Tunisian Islamist hacktivists

Load More

Start the conversation

☑ Send me notifications when other members comment.

Add My Comment

SearchCIO

Dunkin' pins growth on digital tech

unkin' celebrates progress on digital initiatives, but using digital tech to deliver customer value is no slam dunk, says ...

nformation technology adoption: CIO Ted Ross discusses LA's strategy

Ted Ross, Los Angeles CIO, discusses enterprise technology refresh against the backdrop of developments such as Windows Server ...

About Us Contact Us Privacy Policy Our Use of Cookies Advertisers Business Partners Media Kit Corporate Site

Contributors Reprints Archive Site Map Answers E-Products Events In Depth

Guides Opinions Quizzes Photo Stories Tips Tutorials Videos