

# Wireshark

Alonso Eduardo Caballero Quezada

Instructor y Consultor en Hacking Ético, Informática Forense & GNU/Linux

Sitio Web: <http://www.ReYDeS.com>

e-mail: [ReYDeS@gmail.com](mailto:ReYDeS@gmail.com)

# Presentación

Alonso Eduardo Caballero Quezada es EXIN Ethical Hacking Foundation Certificate, LPIC-1 Linux Administrator Certified, LPI Linux Essentials Certificate, IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics y Cybersecurity Management.

Ha sido Instructor en el OWASP LATAM Tour Lima Perú y expositor en el 0x11 OWASP Perú Chapter Meeting, además de Conferencista e Instructor en PERUHACK. Cuenta con más de catorce años de experiencia y desde hace diez años labora como Consultor e Instructor Independiente en las áreas de Hacking Ético e Informática Forense. Perteneció por muchos años al grupo internacional de Seguridad RareGaZz y al Grupo Peruano PeruSEC. Ha dictado cursos presenciales y virtuales en Ecuador, España, Bolivia y Perú, presentándose también constantemente en exposiciones enfocadas a Hacking Ético, Informática Forense, GNU/Linux.



@Alonso\_ReYDeS 

[www.facebook.com/alonsoreydes](http://www.facebook.com/alonsoreydes) 

[pe.linkedin.com/in/alonsocaballeroquezada/](http://pe.linkedin.com/in/alonsocaballeroquezada/) 

Wireshark es un analizador para paquetes de red. Un analizador para paquetes red intentará capturar los paquetes de la red, e intentará mostrar los datos del paquete tan detalladamente como sea posible.

Se podría pensar en un analizador para paquetes de red como un dispositivo de medición utilizado para examinar aquello suscitándose dentro del cable de red, así como un voltímetro es utilizado por un electrónico para examinar aquello suscitándose dentro de un cable eléctrico (pero a nivel superior, de hecho).

En el pasado, tales herramientas eran ya sea muy costosas, propietarias, o ambas cosas. Sin embargo, con el advenimiento de Wireshark, todo esto cambió.

Wireshark es quizá uno de los mejores analizadores para paquetes disponibles actualmente.

\* <https://www.wireshark.org>

# Wireshark (Cont.)

Wireshark es utilizado por diferentes personas:

- Administradores de red lo utilizan para solucionar problemas de red.
- Ingenieros de seguridad en redes lo utilizan para examinar problemas de seguridad.
- Desarrolladores lo utilizan para depurar implementaciones de protocolos.
- Las personas lo utilizan para aprender sobre lo interno de los protocolos de red.

Wireshark no proporciona lo siguiente:

- Wireshark no es un sistema para la detección de intrusiones. Podría no advertir cuando alguien haga cosas extrañas en la red, Wireshark podría ayudar a averiguar aquello lo cual realmente está ocurriendo.
- Wireshark no manipulará cosas en la red, podría únicamente “medir” cosas desde este. Wireshark no envía paquetes sobre la red o hace otras cosas activas. (excepto para resoluciones de nombres).

# Características de Wireshark

Las siguientes son algunas de las diversas características proporcionadas por Wireshark:

- Disponible para Windows y GNU/Linux.
- Captura en vivo de paquetes desde una interfaz de red.
- Abrir archivos conteniendo datos de paquetes capturados con tcpdump/WinDump, Wireshark, y otros programas para la captura de paquetes.
- Importar paquetes desde archivos de texto conteniendo volcados hexadecimales de paquetes de datos.
- Mostrar paquetes con una información muy detallada del protocolo.
- Guardar paquetes de datos capturados.
- Exportar algunos o todos los paquetes en diferentes formatos para la captura de archivos.
- Filtrar paquetes sobre diversos criterios.
- Busca paquetes sobre diversos criterios.
- Colorear la visualización de paquetes basado en filtros.
- Crear diversas estadísticas.
- Y mucho mas.

# Curso Virtual de Hacking Ético

## Curso Virtual de Hacking Ético 2017

Domingos 8, 15, 22 y 29 de Octubre del 2017. De 9:00 am a 12:15 pm (UTC -05:00)

Este curso virtual ha sido dictado a participantes residentes en los siguientes países:



### Presentación:

En la actualidad se requieren profesionales quienes sean responsables de encontrar y entender las vulnerabilidades en las organizaciones, además de trabajar diligentemente para mitigarlas antes de ser aprovechadas por los atacantes maliciosos. Este curso abarca las herramientas, técnicas y metodologías para realizar adecuadamente proyectos de hacking ético o pruebas de penetración de principio a fin. Todas las organizaciones necesitan personal experimentado quienes puedan encontrar vulnerabilidades, y este curso proporciona los conocimientos ideales.

### Objetivos:

Este curso enseña a los participantes a realizar un reconocimiento detallado, aprendiendo sobre la infraestructura del objetivo mediante búsquedas en blogs, motores de búsqueda, redes sociales y otros sitios de Internet. Se escanean las redes objetivo utilizando las mejores herramientas disponibles, proporcionando las opciones y configuraciones óptimas para realizar los escaneos. Luego se exploran diversos métodos de explotación para ganar acceso hacia los sistemas objetivo y medir el riesgo real para la organización. Después se realizan acciones de post-explotación. Todo realizado en un laboratorio de pruebas controlado donde se desarrollan los ataques.



Alonso Eduardo Caballero Quezada es EXIN Ethical Hacking Foundation Certificate, LPIC-1 Linux Administrator, LPI Linux Essentials Certificate, IT Masters Certificate of Achievement en Network Security Administrator,

Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics y Cybersecurity Management. Ha sido Instructor en el OWASP LATAM Tour Lima, Perú y Conferencista en PERUHACK. Cuenta con más de trece años de experiencia en el área y desde hace nueve años labora como Consultor e Instructor Independiente en las áreas de Hacking Ético & Informática Forense. Perteneció por muchos años al grupo internacional de Seguridad RareGaZz y al Grupo Peruano de Seguridad PeruSEC. Ha dictado cursos presenciales y virtuales en Ecuador, España, Bolivia y Perú, presentándose también constantemente en exposiciones enfocadas a Hacking Ético, Informática Forense, GNU/Linux y Software Libre. Su correo electrónico es ReYDeS@gmail.com y su página personal está en: <http://www.ReYDeS.com>.

Más Información: [http://www.reydes.com/d/?q=Curso\\_de\\_Hacking\\_Etico](http://www.reydes.com/d/?q=Curso_de_Hacking_Etico)

E-mail: [caballero.alonso@gmail.com](mailto:caballero.alonso@gmail.com) / Sitio Web: <http://www.reydes.com>

# Demostraciones

Applications ▾ Places ▾ Wireshark ▾ 1

\*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

| No. | Time         | Source         | Destination    | Protocol | Length | Info   |
|-----|--------------|----------------|----------------|----------|--------|--|
| 46  | 8.975412442  | 72.21.91.29    | 192.168.0.46   | OCSP     | 854    | Response   |
| 47  | 8.975432916  | 192.168.0.46   | 72.21.91.29    | TCP      | 66     | 39530 → 80 [ACK] Seq=430 Ack=789 Win=30848 Len=0 TSval=429493833   |
| 48  | 8.978170074  | 192.168.0.46   | 72.21.91.29    | OCSP     | 495    | Request  |
| 49  | 9.119828634  | 72.21.91.29    | 192.168.0.46   | OCSP     | 854    | Response   |
| 50  | 9.160802936  | 192.168.0.46   | 72.21.91.29    | TCP      | 66     | 39530 → 80 [ACK] Seq=859 Ack=1577 Win=32384 Len=0 TSval=429493838  |
| 51  | 9.215410796  | 192.168.0.46   | 52.88.1.68     | TLSv1.2  | 432    | Application Data   |
| 52  | 9.384288124  | 52.88.1.68     | 192.168.0.46   | TLSv1.2  | 1200   | Application Data   |
| 53  | 9.384382422  | 192.168.0.46   | 52.88.1.68     | TCP      | 66     | 43484 → 443 [ACK] Seq=693 Ack=4903 Win=40832 Len=0 TSval=429493844 |
| 54  | 10.930294616 | 192.168.0.46   | 190.113.220.54 | DNS      | 74     | Standard query response 0x6f0c A www.google.com                    |
| 55  | 10.930346358 | 192.168.0.46   | 190.113.220.54 | DNS      | 74     | Standard query response 0x783f AAAA www.google.com                 |
| 56  | 10.940440808 | 190.113.220.54 | 192.168.0.46   | TCP      | 60     | Standard query response 0x6f0c A www.google.com A 172.217.8.68 NS  |
| 57  | 10.940494927 | 190.113.220.54 | 192.168.0.46   | TCP      | 60     | Standard query response 0x783f AAAA www.google.com AAAA 2607:f8b0  |
| 58  | 10.940691783 | 192.168.0.46   | 172.217.8.68   | TCP      | 60     | Standard query response 0x783f AAAA www.google.com AAAA 2607:f8b0  |
| 59  | 11.023244203 | 172.217.8.68   | 192.168.0.46   | TCP      | 60     | Standard query response 0x783f AAAA www.google.com AAAA 2607:f8b0  |
| 60  | 11.023338941 | 192.168.0.46   | 172.217.8.68   | TCP      | 60     | Standard query response 0x783f AAAA www.google.com AAAA 2607:f8b0  |
| 61  | 11.023789238 | 192.168.0.46   | 172.217.8.68   | TCP      | 60     | Standard query response 0x783f AAAA www.google.com AAAA 2607:f8b0  |

Frame 54: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0

Ethernet II, Src: 08:00:27:37:8c:6f, Dst: f4:5f:d4:be:89:23

Internet Protocol Version 4, Src: 192.168.0.46, Dst: 190.113.220.54

User Datagram Protocol, Src Port: 39448, Dst Port: 53

Domain Name System (query)

[Response In: 56]

Transaction ID: 0x6f0c

Flags: 0x0100 Standard query response

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

```
0000 f4 5f d4 be 89 23 08 00 27 37 8c 6f 08 00 45 00  . . . . #
0010 00 3c 69 89 40 00 40 11 75 a9 c0 a8 00 2e be 71  .<1.@.
0020 dc 36 9a 18 00 35 00 28 5b b8 6f 0c 01 00 00 01  .6...5
0030 00 00 00 00 00 00 03 77 77 77 06 67 6f 6f 67 6c  . . . . .
0040 65 03 63 6f 6d 00 00 01 00 01                    e.com.
```

wireshark\_eth0\_20170929182130\_pp0YwO

pkts: 564 · Displayed: 564 (100.0%) Profile: Default

# Cursos Virtuales Disponibles en Video

Curso Virtual de Hacking Ético

[http://www.reydes.com/d/?q=Curso\\_de\\_Hacking\\_Etico](http://www.reydes.com/d/?q=Curso_de_Hacking_Etico)

Curso Virtual de Hacking Aplicaciones Web

[http://www.reydes.com/d/?q=Curso\\_de\\_Hacking\\_Aplicaciones\\_Web](http://www.reydes.com/d/?q=Curso_de_Hacking_Aplicaciones_Web)

Curso Virtual de Informática Forense

[http://www.reydes.com/d/?q=Curso\\_de\\_Informatica\\_Forense](http://www.reydes.com/d/?q=Curso_de_Informatica_Forense)

Curso Virtual Fundamentos de Hacking Ético

[http://www.reydes.com/d/?q=Curso\\_Fundamentos\\_de\\_Hacking\\_Etico](http://www.reydes.com/d/?q=Curso_Fundamentos_de_Hacking_Etico)

Curso Virtual Fundamentos de Hacking Web

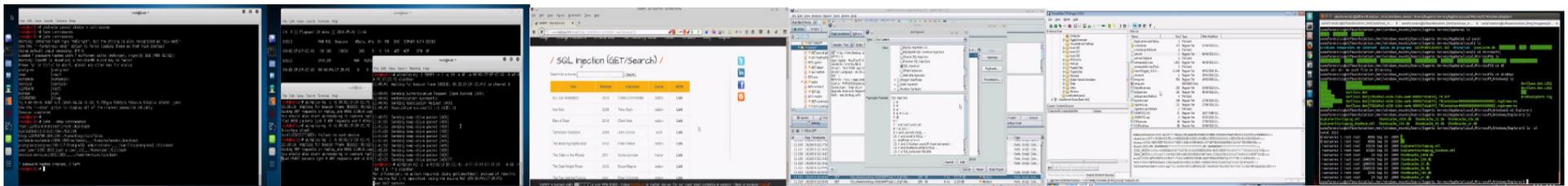
[http://www.reydes.com/d/?q=Curso\\_Fundamentos\\_de\\_Hacking\\_Web](http://www.reydes.com/d/?q=Curso_Fundamentos_de_Hacking_Web)

Curso Virtual Fundamentos de Forense Digital

[http://www.reydes.com/d/?q=Curso\\_Fundamentos\\_de\\_Forense\\_Digital](http://www.reydes.com/d/?q=Curso_Fundamentos_de_Forense_Digital)

**Y todos los cursos virtuales:**

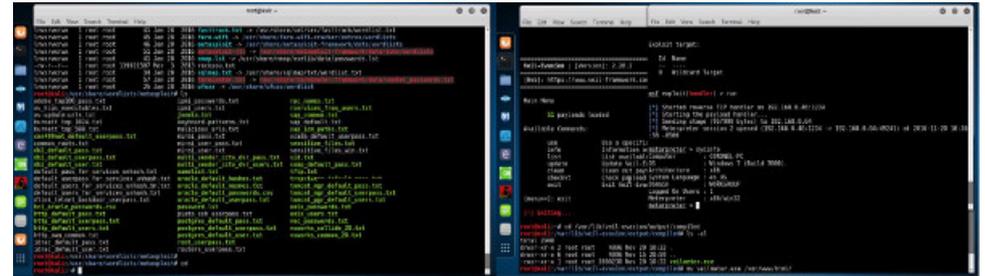
<http://www.reydes.com/d/?q=cursos>



# Más Contenidos

Videos de 36 Webinars Gratuitos

<http://www.reydes.com/d/?q=videos>



Diapositivas utilizadas en los Webinars Gratuitos.

<http://www.reydes.com/d/?q=node/3>

Artículos y documentos publicados

<http://www.reydes.com/d/?q=node/2>

Mi Blog sobre temas de mi interés.

<http://www.reydes.com/d/?q=blog/1>

**Alonso Caballero Quezada / ReYDeS** Cursos Videos Blog Eventos Contacto

Servicio Independiente de Hacking Ético

**Presentación**

**Cursos**

- Curso de Informática Forense
- Curso de Hacking Windows
- Curso OWASP TOP 10
- Curso de Hacking Linux
- Curso de Hacking Aplicaciones Web
- Curso de Hacking Ético
- Curso de Hacking con Kali Linux 2.0
- Curso Forense de Autopsy 4
- Curso de Metasploit Framework
- Curso de Nmap
- Curso Forense de Windows XP

Alonso Eduardo Caballero Quezada es EXIN Ethical Hacking Foundation Certificate, LPI Linux Essentials Certificate, Brainbench Certified Network Security (Master), Computer Forensics (U.S.) & Linux Administration (General), IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident

# Wireshark

Alonso Eduardo Caballero Quezada

Instructor y Consultor en Hacking Ético, Informática Forense & GNU/Linux

Sitio Web: <http://www.ReYDeS.com>

e-mail: [ReYDeS@gmail.com](mailto:ReYDeS@gmail.com)