

# Capturar Tráfico de Red con Wireshark

**Alonso Eduardo Caballero Quezada**

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

Sitio Web: <https://www.ReYDeS.com> :- e-mail: [ReYDeS@gmail.com](mailto:ReYDeS@gmail.com)

Jueves 3 de Junio del 2021

# Alonso Eduardo Caballero Quezada

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, Cybersecurity Management Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals, Phishing Countermeasures Pen Testing, Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist y OSEH.

Más de 18 años de experiencia como consultor e instructor independiente en las áreas de Hacking Ético y Forense Digital. Ha dictado cursos presenciales y virtuales en Ecuador, España, Bolivia y Perú, presentándose también constantemente en exposiciones enfocadas a Hacking Ético, Forense Digital, GNU/Linux.

# Redes Sociales



<https://www.linkedin.com/in/alonsocaballeroquezada/>



[https://twitter.com/Alonso\\_ReYDeS](https://twitter.com/Alonso_ReYDeS)



<https://www.youtube.com/c/AlonsoCaballero>



<https://www.facebook.com/alonsoreydes/>



<https://www.reydes.com>



[reydes@gmail.com](mailto:reydes@gmail.com)



+51 949 304 030



# Forense de Redes

El Forense de redes es una de las ramas del forense digital, donde los datos a ser analizados están fluyendo en el tráfico de red, desde y hacia los sistemas bajo observación.

El propósito de este tipo de observación es recolectar información, obtener evidencia legalmente, establecer las causas de un evento, analizar el comportamiento de malware, entre otros.

Cuando un incidente se relaciona con un “cable” (inalámbrico), sea este exitoso o no, los artefactos dejados por este ayudan a entender y recrear no únicamente la intención sobre el incidente, sino también conocer las acciones realizadas.

\* [https://forensicswiki.xyz/wiki/index.php?title=Network\\_forensics](https://forensicswiki.xyz/wiki/index.php?title=Network_forensics)

# Captura de Evidencia en Red

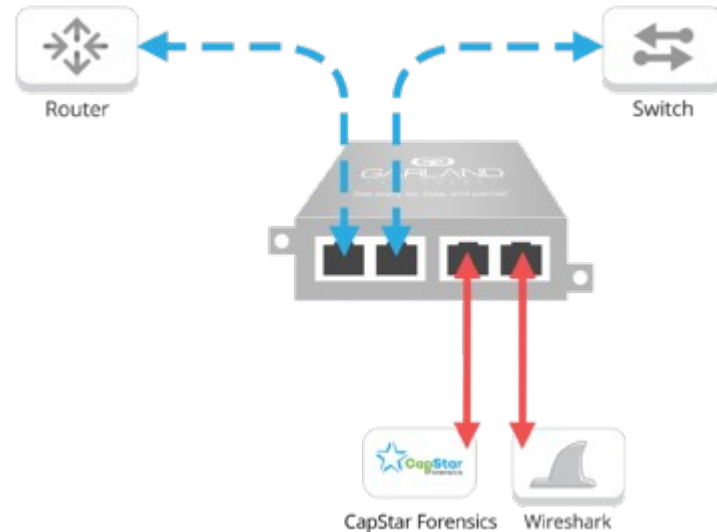
Primero es necesario tener una estrategia para luego planificar la adquisición de la evidencia.

Capturar evidencia requiere por si mismo documentar todos los sistemas accedidos y utilizados, capturar y guardar los flujos de datos, hacia las unidades de almacenamiento, además de recolectar los eventos (logs) desde los servidores, firewalls, etc. Existen algunas prácticas recomendadas para capturar evidencia:

- Crear copias de la evidencia con sus correspondientes hashes
- Nunca trabajar con la evidencia original
- Utilizar herramientas estándares
- Documentar todas las acciones realizadas

# TAP (Derivación) de Red

Proporciona una manera de acceder hacia los datos fluyendo a través de la red. Se utiliza para un tercero vigile el tráfico entre dos puntos de la red. Tiene al menos tres puertos. Puerto A, Puerto B, y Puerto de Vigilancia. Un tap insertado entre A y B pasa todo el tráfico, pero también copia los mismos datos hacia el puerto de vigilancia.



# Wireshark

Es un analizador para paquetes de red. Presenta los datos de paquetes capturados con tanto detalle como sea posible.

Se puede pensar en esta herramienta como en un dispositivo para examinar aquello suscitándose dentro de un cable de red, así como los electrónicos utilizan un voltímetro para examinar aquello suscitándose dentro de un cable electrónico, pero a un nivel más profundo.

En el pasado estas herramientas eran muy caras, propietarias o ambas. Con la llegada de Wireshark todo esto cambió. Pues es libre, de fuente abierta, y uno de los mejores analizadores de paquetes disponibles actualmente.

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

# Wireshark (Cont.)

Capturar datos en vivo de la red es una de las principales características de Wireshark. El motor para captura de Wireshark proporciona lo siguiente:

- Capturar desde diferentes tipos de hardware de red, como Ethernet o 802.11
- Simultáneamente capturar desde múltiples interfaces de red
- Detener la captura basándose en diferentes eventos, como la cantidad de datos capturados, tiempo transcurrido, o el número de paquetes
- Simultáneamente decodificar paquetes mientras son capturados
- Filtrar paquetes, reduciendo la cantidad de datos a ser capturados
- Guardar los paquetes en múltiples archivos, opcionalmente rotándolos a un número fijo de archivos.

\* [https://www.wireshark.org/docs/wsug\\_html\\_chunked/ChapterCapture.html](https://www.wireshark.org/docs/wsug_html_chunked/ChapterCapture.html)



## Curso Virtual Forense de Redes 2021

Domingos 6, 13, 20 y 27 de Junio del 2021. 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 es muy común trabajar en cualquier investigación forense relacionada a un componente de red. El forense de computadoras siempre será un habilidad fundamental y crítica para esta profesión, pues obviar las comunicaciones de red, es similar a ignorar las imágenes proporcionadas por las cámaras de seguridad correspondientes a un crimen cometido. Ya sea se enfrente un incidente relacionado con una intrusión, un caso de robo de datos, uso indebido por parte de los empleados, o se esté involucrado en el descubrimiento pro activo del adversario, la red frecuentemente proporciona una vista incomparable del incidente. Esta evidencia puede proporcionar la prueba necesaria para mostrar intención, descubrir los atacantes han estado activos por meses o más, o incluso puede resultar útil para probar definitivamente la ocurrencia de un delito.



**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, Cybersecurity Management, Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals, Phishing Countermeasures, Pen Testing, Basic Technology Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist (CNSS) y OPEN-SEC Ethical Hacker (OSEH). Ha sido instructor en el OWASP LATAM Tour, expositor en OWASP Perú Chapter Meeting y OWASP

Más Información: [https://www.reydes.com/d/?q=Curso\\_Forense\\_de\\_Red](https://www.reydes.com/d/?q=Curso_Forense_de_Red)

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

🌐 Sitio Web: <https://www.reydes.com>

Alonso Eduardo Caballero Quezada :- Sitio web: <https://www.reydes.com> :- e-mail: [reydes@gmail.com](mailto:reydes@gmail.com)

# Demostraciones

The screenshot shows the Wireshark interface with the following details:

- Packet List:** A table of captured packets with columns for No., Time, Source, Destination, Protocol, and Length. Packet 110 is highlighted.
- Packet Details:** Shows the structure of the selected packet (HTTP GET / HTTP/1.1).
- Packet Bytes:** Shows the raw hex and ASCII data of the selected packet.
- Manage Capture Filters Dialog:** A dialog box is open, showing a list of filters and the selected interface 'enp0s17'. The dialog includes sections for 'Input', 'Output', and 'Options'.

No.	Time	Source	Destination	Protocol	Length	Info
109	35.515711140	192.168.0.96	35.232.111.17	TCP	66	35402 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3396876090...
110	35.515807372	192.168.0.96	35.232.111.17	HTTP	153	GET / HTTP/1.1
111	35.810337518	35.232.111.17	192.168.0.96	TCP	66	80 → 35402 [ACK] Seq=1 Ack=88 Win=64256 Len=0 TSval=247537130...
112	35.810882612	35.232.111.17	192.168.0.96	HTTP	214	HTTP/1.1 204 No Content
113	35.810883140	35.232.111.17	192.168.0.96	TCP	66	80 → 35402 [FIN, ACK] Seq=149 Ack=88 Win=64256 Len=0 TSval=24...
114	35.810961843	192.168.0.96	35.232.111.17	TCP	66	35402 → 80 [ACK] Seq=88 Ack=149 Win=64128 Len=0 TSval=3396876...
115	35.811484215	192.168.0.96	35.232.111.17	TCP	66	35402 → 80 [FIN, ACK] Seq=88 Ack=150 Win=64128 Len=0 TSval=33...
116	36.106469393	35.232.111.17	192.168.0.96	TCP	66	80 → 35402 [ACK] Seq=150 Ack=89 Win=64256 Len=0 TSval=2475371...
117	36.760528184	ARRISGro_9f:c4:8f	Broadcast	0x8999		
118	36.891248506	fe80::f2af:85ff:fea...	ff02::1	ICMPv6		
119	36.902898392	fe80::294:bc6b:8eb5	ff02::16	ICMPv6		
120	36.906619874	fe80::7e79:e744:				
121	37.410421597	fe80::7e79:e744:				
122	37.566910401	fe80::294:bc6b:8				
123	38.760517055	ARRISGro_9f:c4:8				
124	39.739810960	fe80::f2af:85ff:				
125	39.894277046	fe80::f2af:85ff:				
126	39.906464896	fe80::294:bc6b:8				
127	39.910275450	fe80::7e79:e744:				
128	40.037923810	192.168.0.4				

Frame 110: 153 bytes on wire (1224 b)  
Ethernet II, Src: PcsCompu\_9b:b9:e5  
Internet Protocol Version 4, Src: 192.168.0.96, Dst: 35.232.111.17  
Transmission Control Protocol, Src Port: 35402, Dst Port: 80  
Hypertext Transfer Protocol  
GET / HTTP/1.1  
Host: connectivity-check.ubuntu.com  
Accept: /\*  
Connection: close  
[Full request URI: http://connectivity-check.ubuntu.com/]  
[HTTP request 1/1]  
[Response in frame: 112]

0000 f0 af 85 ad 04 8c 08 00 27 9b b9  
0010 00 8b 57 99 40 00 40 0e 8e d2 c0  
0020 6f 11 8a 4a 00 50 ca 68 75 1f 41  
0030 01 f6 54 7f 00 00 01 01 08 0a ca  
0040 29 f6 47 45 54 20 2f 20 48 54 54  
0050 0d 0a 48 6f 73 74 3a 20 63 6f 6e

# Cursos Virtuales Disponibles en Video

## Curso Virtual de Hacking Ético

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

## Curso Virtual de Hacking Aplicaciones Web

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

## Curso Virtual de Informática Forense

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

## Curso Virtual Hacking con Kali Linux

[https://www.reydes.com/d/?q=Curso\\_de\\_Hacking\\_con\\_Kali\\_Linux](https://www.reydes.com/d/?q=Curso_de_Hacking_con_Kali_Linux)

## Curso Virtual OSINT - Open Source Intelligence

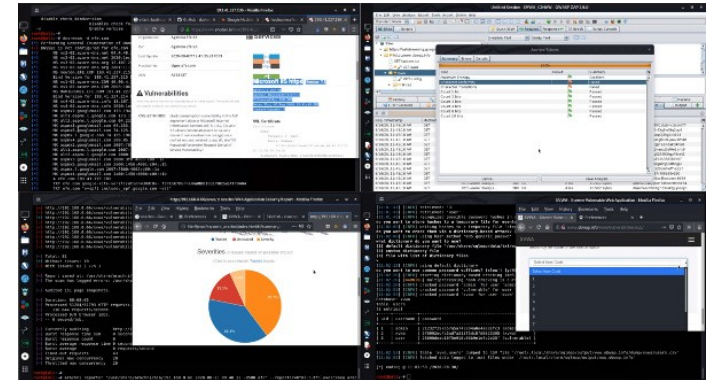
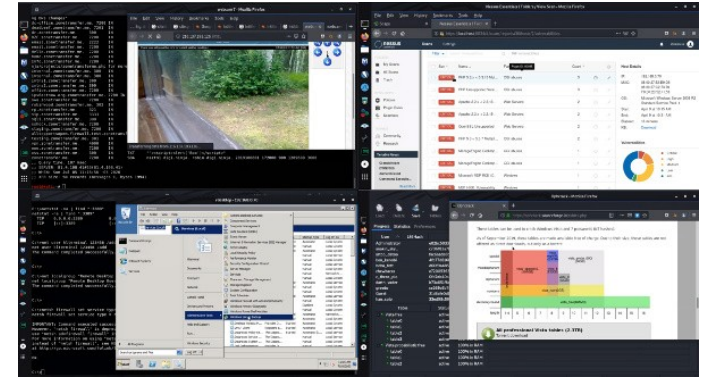
[https://www.reydes.com/d/?q=Curso\\_de\\_OSINT](https://www.reydes.com/d/?q=Curso_de_OSINT)

## Curso Virtual Forense de Redes

[https://www.reydes.com/d/?q=Curso\\_Forense\\_de\\_Red](https://www.reydes.com/d/?q=Curso_Forense_de_Red)

## Y todos los cursos virtuales:

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



# Más Contenidos

## Videos de 66 webinars gratuitos

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

## Diapositivas de los webinars gratuitos

<https://www.reydes.com/d/?q=eventos>


## Artículos y documentos publicados

<https://www.reydes.com/d/?q=documentos>


## Blog sobre temas de mi interés

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

ALONSO CABALLERO / REYDES [Cursos](#) [Videos](#) [Blog](#) [Eventos](#) [Contacto](#)



**Presentación**



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, Cybersecurity Management, Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals, Phishing Countermeasures, Pen Testing, Basic Technology Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist (CNSS) y OPEN-SEC Ethical Hacker (OSEH). Ha sido instructor en el OWASP LATAM Tour Lima, Perú del año 2014, expositor en el 0x11 OWASP Perú Chapter Meeting 2016 y OWASP LATAM at Home 2020, además de Conferencista en PERUHACK 2014, instructor en PERUHACK2016NOT, y conferencista en 8.8 Lucky Perú 2017. Cuenta con más de dieciséis años de experiencia en el área y desde hace doce años labora como consultor e instructor independiente en las áreas de Hacking Ético & Forense Digital. Perteneció por muchos años al grupo internacional de seguridad RareGazzy 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, Forense Digital, GNU/Linux y Software Libre. Su correo electrónico es [ReYDeS@gmail.com](mailto:ReYDeS@gmail.com) y su página personal está en: <https://www.ReYDeS.com>.

[Read more](#)

[f](#) [t](#) [in](#) [x](#) [p](#)

**Cursos**

- Curso de Hacking con Kali Linux
- Curso de Informática Forense
- Curso de Hacking Aplicaciones Web
- Curso de Hacking Ético
- Curso de OSINT Open Source Intelligence
- Curso Forense de Autopsys
- Curso Maltego
- Curso OWASP TOP 10
- Curso Forense de Redes
- Curso de Wireshark
- Curso de Metasploit Framework
- Curso de Nmap
- Curso de Hacking Windows
- Curso Fundamentos de Hacking Ético
- Curso Fundamentos de Hacking Web
- Curso Fundamentos de Forense Digital
- Curso de Hacking Redes Inalámbricas
- Curso de Análisis Forense con Linux

**Servicios**

- Servicio en Cursos de Capacitación
- Servicio de Hacking Ético
- Servicio de Forense Digital

# Capturar Tráfico de Red con Wireshark

**Alonso Eduardo Caballero Quezada**

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

Sitio Web: <https://www.ReYDeS.com> :- e-mail: [ReYDeS@gmail.com](mailto:ReYDeS@gmail.com)

Jueves 3 de Junio del 2021