

# Análisis Forense con Autopsy

**Alonso Eduardo Caballero Quezada**

Instructor y Consultor en Hacking Ético & Forense Digital

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

Miércoles 27 de Octubre 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 Análisis Forense con Autopsy y Forense Digital. Ha dictado cursos presenciales y virtuales en Ecuador, España, Bolivia y Perú, presentándose también constantemente en exposiciones enfocadas a Análisis Forense con Autopsy, 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



# ¿Qué es el Forense Digital?

Rama de la ciencia forense abarcando la recuperación e investigación de material encontrado en dispositivos digitales, frecuentemente relacionados con crímenes cometidos por computadoras.

El Forense de computadoras es una rama del forense digital, relacionado a la evidencia encontrada en computadoras y medios digitales de almacenamiento.

Su meta es examinar medios digitales de una manera “forense”, con el propósito de identificar, preservar, recuperar, analizar, y presentar hechos sobre la información digital.

El análisis forense es la etapa donde se realiza una investigación profunda, cuyo propósito es identificar objetivamente y documentar los culpables, razones, ruta y consecuencias de un incidente de seguridad, violación de las leyes, etc.

# ¿Cómo se Utiliza?

Debido a la variedad de las fuentes de datos, las técnicas del forense digital pueden ser utilizados para diversos propósitos.

- Investigar crímenes y violaciones a políticas internas
- Reconstruir incidentes de seguridad por computadora
- Resolver problemas operacionales
- Recuperar daños accidentales en los sistemas

Prácticamente toda las organizaciones necesitan tener la capacidad de realizar forense digital.

# Autopsy

Autopsy es la principal plataforma de fuente abierta (open source) para forense digital. Construido por Basis Technology con las funcionalidades fundamentales esperadas de las herramientas forenses comerciales.

Autopsy es rápido, profundo, y eficiente para realizar investigaciones en dispositivos de almacenamiento (discos duros y dispositivos móviles), evolucionando conforme se tienen diversos requerimientos.

Autopsy es una interfaz gráfica para The Sleuth Kit, y otras herramientas del forense digital. Utilizado por fuerzas legales, militares, profesionales corporativos, con el propósito de investigar lo ocurrido en computadoras.

\* <https://www.autopsy.com/>

# Capacidades de Autopsy

- Actividad reciente
- Consulta de hashes
- Identificación por tipo de archivo
- Extracción de archivos
- Analizar imágenes
- Interpretar mensajes de correo electrónico
- Buscar palabras clave
- Detectar inconsistencias en la extensión de archivos
- Detectar archivos interesantes
- Reconstruir archivos
- Detectar encriptación
- Extraer máquinas virtuales
- Entre otras funcionalidades...



# Demostración

Craig Tucker - Autopsy 4.19.1

Case View Tools Window Help


Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Keyword Lists Keyword Search

Listing Images 6998 Results

Table Thumbnail Summary

Page: 1 of 35 Pages: Go to Page: Images: 1-200 Medium Thumbnails Sort Sorted by: 1. Name



\$I8MHF6S.jpg \$IGQWXSI.jpg \$R8MHF6S.jpg \$RGQWXSI.jpg 06a10843-fcc0-4... 0be14e58-0e47-4...

/img\_Craig Tucker Desktop.E01/vol2/\$Recycle.Bin/S-1-5-21-1049150138-4017234595-3791460656-1001/\$RGQWXSI.jpg

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences Video Triage

0% 75% Reset Tags Menu

**CRIME SCENE - DO NOT CROSS**



# Cursos Virtuales Disponibles Video

## Curso Virtual de Análisis Forense con Autopsy

[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

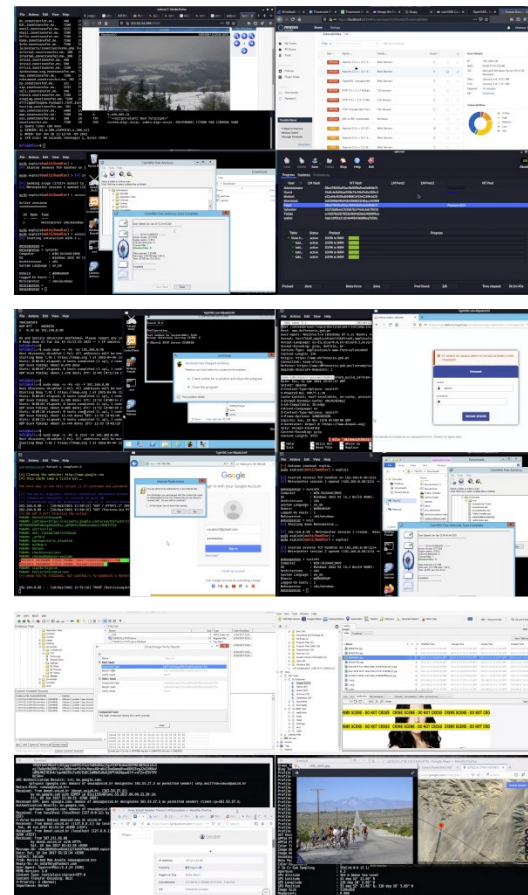
[https://www.reydes.com/d/?q=Curso\\_de\\_OSINT](https://www.reydes.com/d/?q=Curso_de_OSINT)

## Curso Virtual Forense de Redes

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

Y todos los cursos virtuales:

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



# Más Contenidos

## Videos de 70 webinars gratuitos

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

## Diapositivas de los webinars gratuitos

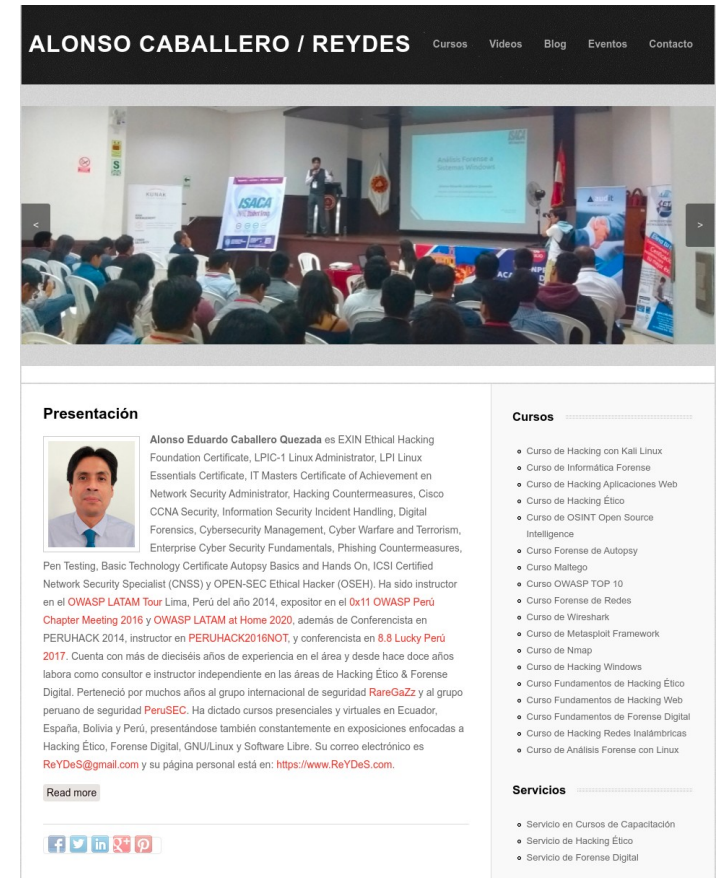
<https://www.reydes.com/d/?q=eventos>

## 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 **Ox11 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 **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, 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](#)



**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 Autopsy
- 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

# Análisis Forense con Autopsy

**Alonso Eduardo Caballero Quezada**

Instructor y Consultor en Hacking Ético & Forense Digital

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

Miércoles 27 de Octubre del 2021