Webinar Gratuito

Rastrear Personas utilizando OSINT

Alonso Eduardo Caballero Quezada

:|: Hacking :|: Forense :|: Linux :|: OSINT :|: Ciberseguridad :|:

Sitio Web: www.ReYDeS.com -:- Correo: ReYDeS@gmail.com

Jueves 4 Junio 2026

Alonso Eduardo Caballero Quezada

Cuento con más de diecinueve años de experiencia en el área y desde hace quince años me especializo en la áreas de Hacking, Forense, OSINT, Ciberseguridad y temas relacionados.

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

https://x.com/Alonso_ReYDeS

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

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

https://www.instagram.com/alonso_reydes/

reydes@gmail.com

www.reydes.com

https://wa.me/51949304030

https://t.me/ReYDeS

Anatomía de una “Huella Digital”

OSINT (Open Source Intelligence) es el proceso de recolectar, analizar, y tomar decisiones con datos públicamente disponibles y siendo estos legales.

Huella Activa vs. Pasiva

- Activa: Aquello lo cual se publica conscientemente; posts, estados, imágenes, fotos, comentarios, etc.

- Pasiva: Aquello lo cual se deja sin ser consciente de ello; metadatos, registros en servidores, conexiones entre cuentas, etc.

El problema no es publicar una foto, sino como varios datos “aislados” pueden revelar algo.

OPSEC en Investigaciones

La Regla de Oro: "Si observas hacia el abismo, el abismo también te observa".

Riesgos del investigador

- Alertar a quien se está investigando; al visitar su perfil en LinkedIn u otra red social, o visualizar su historia de Instagram sin protegerse
- Contaminar la investigación
- Dejar la dirección IP propia, o algunos datos expuestos

No se deben utilizar cuentas personales ni tampoco directamente nuestra red.

De un Nombre de Usuario a su Ubicación

Se sugiere seguir las siguientes etapas:

- Etapa 1: Pivoteo del Alias: “Clonar” la presencia digital en base a un simple nickname o sobrenombre
- Etapa 2: Reconocimiento Facial: Rastrear o hacer un seguimiento de perfiles ocultos o no vinculados con imágenes
- Etapa 3: Extracción Física: Intentar localizar geográficamente al objetivo utilizando archivos

Rastrear el Nickname

La meta es encontrar en cuales plataformas está registrado el objetivo, utilizando su alias, sobrenombre, “nombre”, o nickname común.

Se pueden utilizar herramientas como:

- WhatsMyName
- Sherlock

Existe consecuentemente un peligro en la reutilización de nombres de usuario

Busqueda Reversa y Reconocimiento Facial

La meta es encontrar fotos del objetivo en páginas donde no utiliza su nombre real (foros, prensa, redes sociales, (cuentas secundarias), etc).

Se pueden utilizar herramientas como:

- FaceCheck.id
- PimEyes

Se percibe una potencia de las bases de datos para reconocimiento facial frente a al tradicional “Google Imágenes”

Lo Expuesto por las Fotos

La meta es extraer la información “invisible” (Metadatos EXIF) desde un archivo, con el propósito de obtener coordenadas geográficas, y diversa información relevante.

Se pueden utilizar herramientas como:

- Jimpl
- ExifMeta

Es el riesgo de enviar fotos a través de medios o canales los cuales no limpian metadatos.

¿Cómo Protegerse de estas Técnicas?

Higiene Digital Básica

- Utilizar alias, sobrenombres, o nicknames distintos para entornos profesionales, personales, y de diversión
- Desactivar el GPS de la cámara (en general) en el teléfono móvil
- Solicitar la eliminación de fotos en buscadores para reconocimiento facial

No únicamente es conocer como atacar o investigar, es importante saber como protegerse conocimiento cuan fácil puede ser conseguir estos datos.

Poder de la Información Pública

OSINT no necesariamente requiere software gubernamental o muy complejo, fundamentalmente requiere metodología y curiosidad.

La automatización y la Inteligencia Artificial están acelerando los tiempos para realizar investigaciones.

Se deben de utilizar estas competencias de manera ética y profesional (Ciberseguridad, Auditoría, Cumplimiento, etc).

Es muy importante capacitarse formalmente en OSINT y temas relacionados.

Curso OSINT - Open Source Intelligence

Alonso Eduardo Caballero Quezada (ReYDeS)

Curso OSINT - Open Source Intelligence 2026

5 Sesiones | 14 Horas | En vivo, Virtual, o Personalizado

Alonso Eduardo Caballero Quezada

Tengo más de veintidós años de experiencia, y desde hace dieciocho años realizo capacitaciones y consultorías en Hacking, Forense, OSINT, CiberSeguridad, y GNU/Linux

Redes Sociales

LinkedIn
X (Twitter)
YouTube
Facebook
Sitio Web
e-mail
WhatsApp

Presentación

En la actualidad se almacenan inconmensurables cantidades de información personal y datos potencialmente incriminatorios, en sitios web, aplicaciones, y plataformas de redes sociales. Estas son accedidas y actualizadas diariamente por las personas o empresas mediante diversos tipos de dispositivos. Estos datos pueden convertirse en evidencia digital, la cual puede ser utilizada por ciudadanos, gobiernos, y empresas; de tal manera puedan resolver problemas financieros, laborales y penales; con la ayuda de un profesional quien pueda capturar o recopilar toda esta información. Muchas personas creen únicamente utilizando su motor de búsqueda favorito es suficiente para encontrar datos. Este curso enseña maneras legítimas y efectivas para encontrar, obtener, y analizar datos desde Internet, mediante la utilización de métodos y herramientas, tanto manuales como automáticos.

Objetivos

Este curso enseña a los participantes a realizar recopilación o captura de inteligencia desde fuentes abiertas u Open Source Intelligence, OSINT por sus siglas en inglés. Se expondrán directamente las principales áreas implicadas en el tema. Se aprenderán conocimientos, técnicas, y herramientas utilizadas por las fuerzas legales, investigadores privados, ciberatacantes, además los defensores también utilizan OSINT para examinar la gran cantidad de información en Internet, analizar los resultados, y basarse en elementos de datos interesantes para encontrar otras áreas de investigación. El objetivo es proporcionar conocimientos sobre OSINT para los participantes tenga éxito en sus campos de especialización, ya sean defensores cibernéticos, analistas de inteligencia sobre amenazas, personal de las fuerzas legales, o simplemente curiosos sobre OSINT.

www.ReYDeS.com -:- ReYDeS@gmail.com

Alonso Eduardo Caballero Quezada (ReYDeS)

Curso OSINT - Open Source Intelligence 2026

Temario

Open Source Intelligence
Evolución de OSINT
Categorías de Información de Fuente Abierta
Anotaciones importantes sobre OSINT
Tipos de OSINT
Partes Interesadas en Información OSINT
Tipos de Captura de Información
Recolección Pasiva, Semipasiva y Activa
Retos de la Inteligencia de Fuente Abierta
Restricciones Legales y Éticas
Inteligencia de Medios Sociales
Cuentas "marionetas"
Acceso Común hacia OSINT
Búsqueda Específicas en Redes Sociales
Operaciones del Navegador
Navegadores Web en Linea de Comandos
Características de los Navegadores.
Añadidos para un Navegador y Marcadores.
Amenazas Poseídas por los Navegadores.
Inteligencia Artificial
Búsqueda de Personas, Empresas y Compañías
Búsqueda de Nombres de Usuarios y Correos Electrónicos
Búsqueda de Medios Sociales
Información de Tecnologías y Búsqueda Inversa de Imágenes
Búsqueda Avanzadas utilizando Google, Bing y Yandex
Herramientas y Técnicas OSINT
The Harvester
Shodan y Censys
Recon-NG
Maltego Graph
Metadatos
ExifTool
MetafooFil
Sherlock
Photon
Hunter
Anonimato en Línea
¿Porqué es Necesario ser Anónimo?
Maneras de ser Anónimo
Proxy, VPN, y Redes de Anonimato
Clearweb, Darkweb, y DeepWeb
¿Porqué utilizar la DeepWeb?
Servicios en la Red Obscura
Proyecto Tor

Beneficios

- Acceso al aula virtual por 60 días
- Acceso a las sesiones en vivo
- Video de las cinco (5) sesiones
- Acceso libre a las sesiones en vivo de los siguientes cursos a dictarse
- Material utilizado durante el desarrollo del curso
- Dos (2) horas de asesoría personalizada en vivo por videoconferencia
- Libro "Fundamentos de Hacking Ético" escrito por el instructor
- Certificado digital de participación
- Certificado digital de aprobación por una duración total de 24 horas

Inversión

Perú: S/. 450 Soles

- Depósito o transferencia interbancaria a Scotiabank
- Pago mediante YAPE o PLIN

Otros países: $ 140 Dólares

- Pago mediante PayPal

Escriba un mensaje al WhatsApp https://wa.me/51949304030 para proporcionarle los datos pertinentes.

Información

Para obtener más información sobre este curso tiene a su disposición los siguientes mecanismos de contacto.

WhatsApp: https://wa.me/51949304030

Correo electrónico: reydes@gmail.com

www.ReYDeS.com -:- ReYDeS@gmail.com

Sitio Web:

www.reydes.com

Correo:

reydes@gmail.com

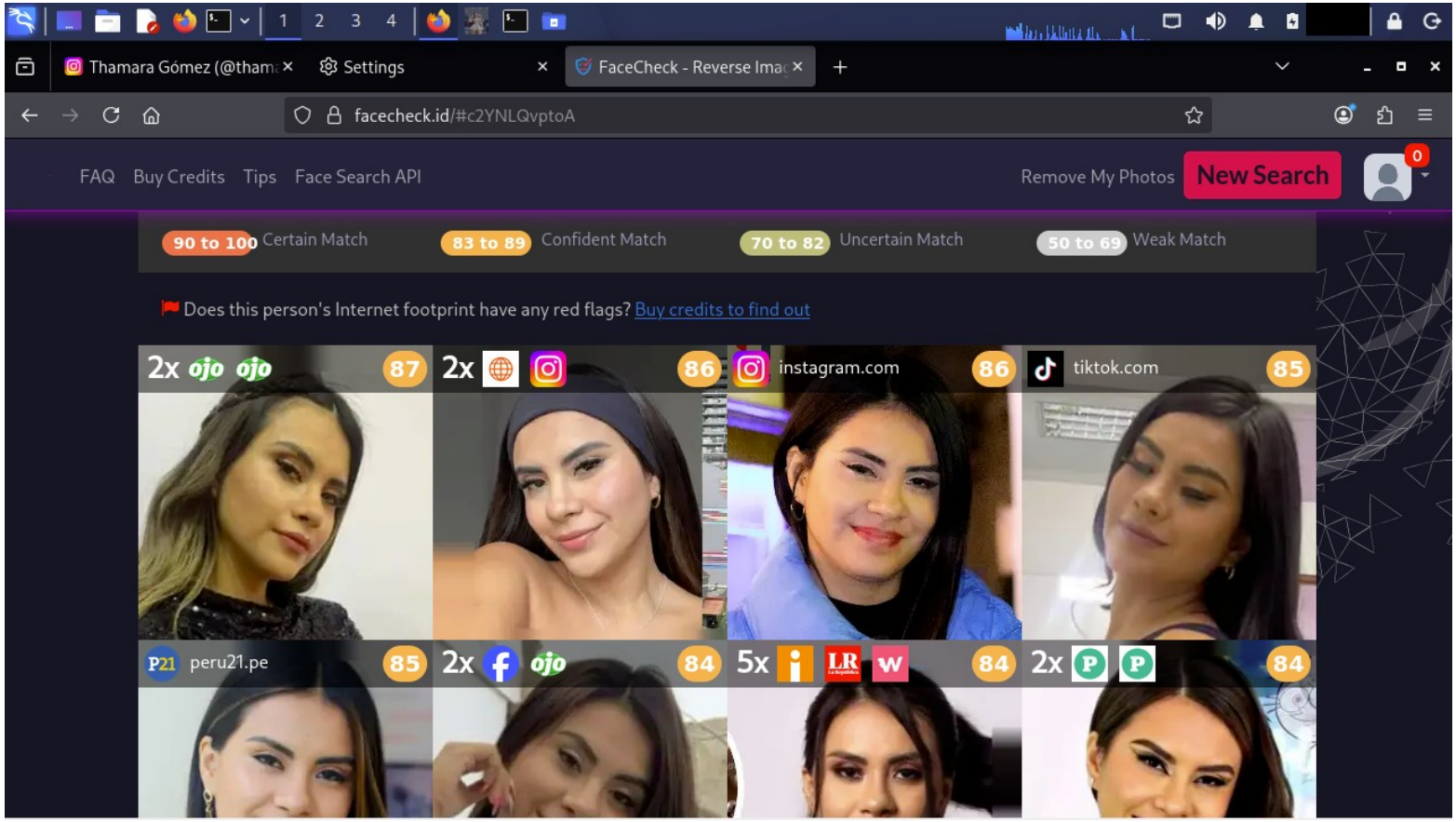
WhatsApp:

https://wa.me/51949304030

Más Información:

https://www.reydes.com/e/Curso_de_OSINT

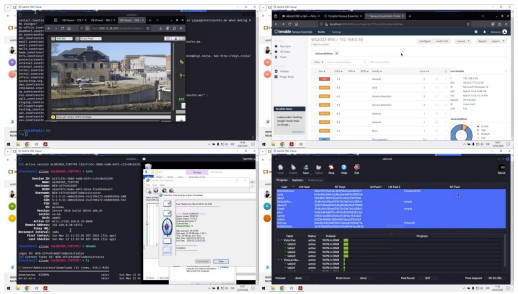
Prácticas

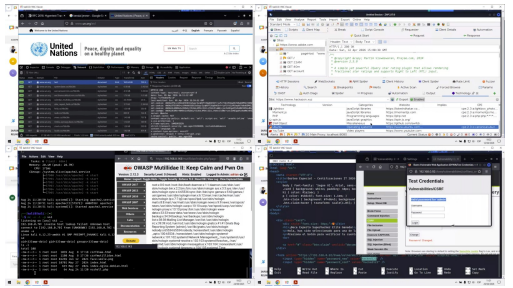


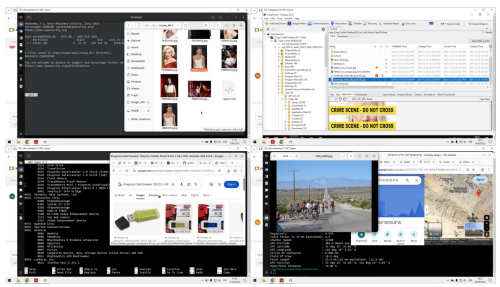
Alonso Eduardo Caballero Quezada :|: Sitio web: www.reydes.com :|: Correo: reydes@gmail.com

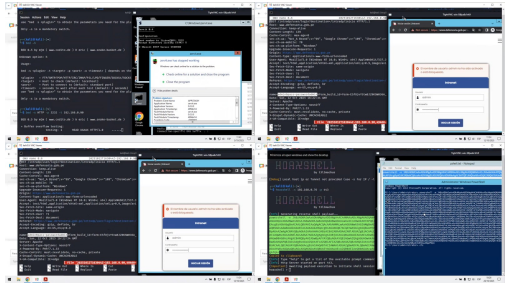
Cursos (Aula Virtual)

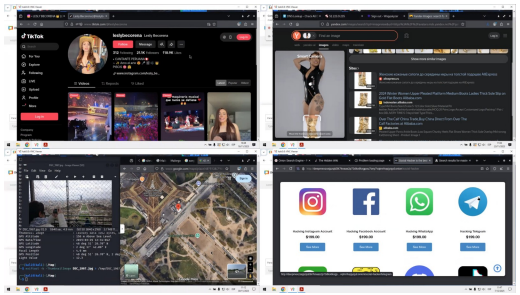
- Curso Hacking Ético
- Curso Hacking Aplicaciones Web
- Curso Informática Forense
- Curso Hacking con Kali Linux
- Curso OSINT - Open Source Intelligence
- Curso Forense de Redes
- Curso CiberSeguridad
- Curso Ciberseguridad Windows y Linux
- Curso OWASP Top 10
- Curso Análisis de Malware
- Curso Hacking OT
- Curso Maltego Graph CE
- Y más...

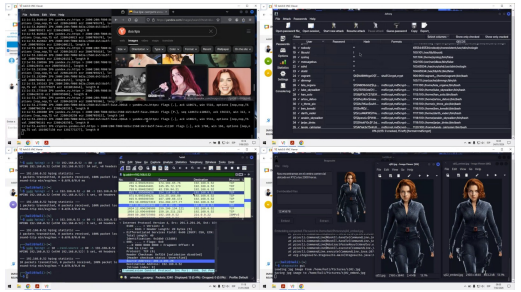












Alonso Eduardo Caballero Quezada :|: Sitio web: www.reydes.com :|: Correo: reydes@gmail.com

Webinar Gratuito

Rastrear Personas utilizando OSINT

Alonso Eduardo Caballero Quezada

:|: Hacking :|: Forense :|: Linux :|: OSINT :|: Ciberseguridad :|:

Sitio Web: www.ReYDeS.com -:- Correo: ReYDeS@gmail.com

Jueves 4 Junio 2026