

curso “Experto en Ciberseguridad de Redes y Sistemas”

TEMAS

1. Fingerprinting
2. Footprinting
3. IDSs - Snort
4. Nessus
5. Firewalls
6. SGSI
7. Antiphishing
8. MITRE
9. Red Team y Blue Team
10. Introducción a OSINT



TEMA 10 Introducción a OSINT

10.1. OSINT Introducción

Introducción y contexto (enfoque didáctico)

El desarrollo de todo el tema 10 se basa en nuestro artículo “**OSINT en detalle (Parte 1)**” que, como siempre podéis descargarlo de nuestra Web: www.darFe.es, en el menú “Descargas” → “Artículos”, o a través del siguiente enlace:

https://darfe.es/wp-content/uploads/2026/01/OSINT_parte-1.pdf



En este tema comenzamos con **OSINT (Open Source Intelligence)**. El objetivo principal es que el alumno comprenda desde la base **qué es OSINT, para qué sirve y por qué es una disciplina clave en la ciberseguridad moderna**, antes de empezar a usar herramientas.

OSINT no consiste en "hackear" ni en realizar actividades intrusivas. Se basa exclusivamente en la **recopilación, análisis y correlación de información disponible públicamente**, pero aplicada con mentalidad analítica y objetivos claros.

Este primer video es **100 % teórico**, pero absolutamente necesario para evitar errores conceptuales, legales y éticos en los siguientes capítulos.

Su evolución

No existe una única persona a la que se le atribuya la invención de OSINT (Inteligencia de Fuentes Abiertas) de manera aislada, ya que es una disciplina que ha evolucionado desde el siglo XIX. No obstante, se destacan tres figuras y organismos clave como sus principales precursores y pioneros:

a. **Sherman Kent:** El "Padre" del Análisis de Inteligencia

Aunque a menudo se le cita como el padre del análisis de inteligencia moderno, Sherman Kent sentó las bases metodológicas que utiliza el OSINT actual. Defendió el uso de métodos académicos, el rigor científico y el análisis de información pública y publicada para la seguridad nacional.

Su libro **Strategic Intelligence for American World Policy** (1949) es considerado la piedra angular para estructurar cómo se procesa la información en las agencias de inteligencia.

b. **Robert David Steele:** El impulsor moderno

En la era contemporánea, Robert David Steele (*ex oficial de la CIA*) es ampliamente reconocido como uno de los mayores promotores del concepto moderno de OSINT. Fue pionero en abogar por una comunidad de inteligencia basada en la transparencia y el código abierto, fundando eventos y organizaciones para profesionalizar esta disciplina fuera de los canales clasificados tradicionales.

c. **Hitos institucionales** (Los precursores organizativos)

Antes de que existiera el término como tal, ya se practicaba de forma institucional:

Foreign Broadcast Monitoring Service (FBMS): Creado en 1941 en EE. UU., fue el primer organismo responsable de monitorizar y traducir transmisiones extranjeras (radio y prensa) para obtener inteligencia, marcando el inicio formal de estas prácticas.

Justin Nordine: En el ámbito tecnológico actual, es el creador del **OSINT Framework**, la herramienta de referencia que organiza y categoriza los recursos digitales de fuentes abiertas para investigadores modernos.

¿Qué es OSINT?

OSINT (Open Source Intelligence) disciplina que se encarga de:

- Identificar
- Recopilar
- Analizar
- Correlacionar
- Documentar

información procedente de **fuentes abiertas**,
accesibles legalmente sin autorización especial.

Definición formal

Según el **NATO OSINT Handbook**:

<https://github.com/lawsecnet/OPSEC/blob/master/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf>

OSINT es la inteligencia producida a partir de información disponible públicamente, recolectada, explotada y difundida de forma adecuada para satisfacer una necesidad específica de inteligencia.

EL PROCESO OSINT (*Figure 7 - The OSINT Process, página 15 de NATO OSINT Handbook*)

- **Descubrimiento:** saber quién sabe.
- **Discriminación:** saber qué es qué.
- **Destilación:** saber qué es lo más importante.
- **Difusión:** saber quién es quién.

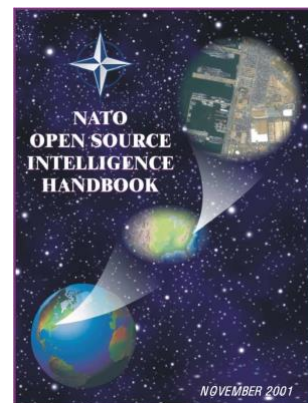
El comandante es el responsable último de establecer los EEI.

EEI: elementos esenciales de información

Los EEI son interrogantes específicos y directos sobre el enemigo, el terreno, el clima o las propias capacidades que, de ser respondidos, reducirían significativamente la incertidumbre.

Tabla 4: Tipos de recopilación de inteligencia (*página 17*).

Impulsado por analistas: basado en el conocimiento del cliente y los problemas.



Impulsado por eventos: en respuesta a eventos relevantes urgentes.

WEB SITE EVALUATION CHECKLIST

Each Internet Website of potential intelligence value must be evaluated as to its suitability for intelligence exploitation before it is cited in OSINT reports or used as collateral information in classified reporting. The essential questions remain: who, what, where, when and why?

1. WHO? Examine the URL first. In the page scan for names, and "about" links.

What type of domain is it? (.com / .org / .edu / .gov / .mil / country code) – Is this appropriate for the material presented?
Might it be a personal page? (use of ~ in URL often suggests this)

Who wrote it? **Look for e-mail contact.**
Credentials? **Search on author's name.**
Check source code as webpage's author is often embedded in the code.

Who is the owner of the host server? **Use WHOIS and DNS LOOKUP tools at www.samspace.org to determine the registered owner of the website and evaluate this information. Does this match earlier information gathered?**

What do others say? **Search to see if others cite the author or the web-site.**
Who links to it? **In Google or AltaVista, enter the search string (link:webaddress) to find who links to the site. Evaluate the community of interests.**

Opinions of it? What do others think of this website?
Found in any reliable directories? **Determine if the website is contained within reliable web directories or web portals for the topic.**

2. WHAT?

Is the material presented authentic, with sources and dates?
Is data unaltered from its original source?
Note: Little value can be attached to information that is either undated or unsourced.

3. WHERE?

Where does the information originate? **Use www.samspace.org to conduct a TRACEROUTE search. TRACEROUTE will determine the path between your computer and the server hosting the information.**
Is the server located where the author purports to reside? Why or why not?

4. WHEN?

How current is the information provided? **Look for a last updated statement or dates on references.**
How often is the information maintained? Should it contain more recent information?

5. WHY?

What's the page's aim, intent?
Why was it created?
Who sponsor's the page? **Look for an "About us" entry.**

Source: Developed from material created by Joe Barker and maintained on server: www.lib.berkelev.edu.

Programado: actividades periódicas para documentar y actualizar el estado del objetivo.

Si bien la variedad de fuentes abiertas disponibles es abrumadora, la capacidad de centrar rápidamente la recopilación en un tema emergente de interés para la inteligencia es la **capacidad clave** (página 19).

SECCIÓN D. BÚSQUEDA ANÓNIMA EN INTERNET

Aunque gran parte del ciclo OSINT puede llevarse a cabo de forma abierta, un programa OSINT sólido debe incluir la capacidad de trabajar de forma anónima en Internet. A pesar de que toda la información de la web está disponible gratuitamente para cualquier persona con un ordenador y conexión a Internet, existirían riesgos de seguridad al buscarla (página 27). *El documento dedica varias páginas a este tema.*

APPENDIX A: GENERAL REFERENCE LINK TABLE

HUMINT (Human Intelligence) inteligencia de fuentes humanas
SIGINT (Signals Intelligence) inteligencia de señales interceptadas
IMINT (Imagery Intelligence) Inteligencia de imágenes
MASINT (Measurement and Signature Intelligence) inteligencia de mediciones y firmas

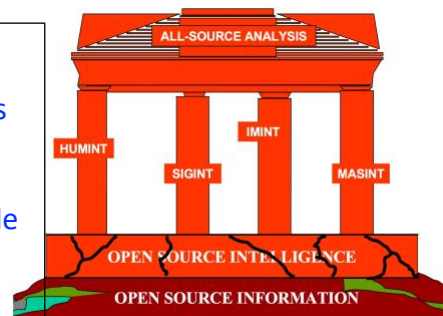


Figure 17 - Open Source - All-Source relationship

APPENDIX A: GENERAL REFERENCE LINK TABLE
APPENDIX B: TRAINING LINK TABLE
APPENDIX C: CATEGORIES OF MISPERCEPTION AND BIAS
 (percepciones erróneas y sesgos)
APPENDIX D. LIST OF ABBREVIATIONS

Este tema lo desarrollamos en detalle en el video 182 **(Obligatorio)**.

🌐 OSINT Introducción - Charla 182 - Aprendiendo Ciberseguridad paso a paso
<https://youtu.be/lhHLxiv68BA>



10.2. OSINT Metodología profesional

En este tema se explica **cómo se trabaja OSINT de forma profesional**, independientemente de las herramientas. La mayoría de errores en OSINT no son técnicos, sino **metodológicos**. Este capítulo es clave para que el alumno piense como analista y no como simple recolector de datos.

El ciclo OSINT

La metodología OSINT se basa en un ciclo continuo:

- 1) **Definición del objetivo**
- 2) **Recolección de información**
- 3) **Procesamiento y normalización**
- 4) **Análisis y correlación**
- 5) **Validación**
- 6) **Documentación y reporte**

Este ciclo está alineado con modelos de inteligencia usados en:

- NIST
- NATO

- Fuerzas y cuerpos de seguridad

1). Definición del objetivo

Nunca se empieza OSINT sin objetivo.

Ejemplos de objetivos

- Analizar la huella digital de una empresa
- Identificar exposición pública de empleados
- Localizar activos publicados accidentalmente

Errores comunes

- Objetivos demasiado amplios
- Falta de límites legales

2) Recolección de información

La **recolección de información** es la fase en la que el analista OSINT obtiene datos a partir de fuentes abiertas. Aunque suele percibirse como la parte “más fácil”, en realidad es **una de las más críticas**, ya que una mala recolección conduce inevitablemente a **malos análisis y conclusiones erróneas**.

a. Principio clave: *cantidad no es calidad*

Uno de los errores más comunes en OSINT es pensar que **cuantos más datos se recopilen, mejor será el resultado**. Esto es falso.

En OSINT:

- Un gran volumen de datos **sin filtrar** genera ruido
- El ruido oculta la información realmente relevante
- El analista pierde tiempo y contexto

👉 Un buen analista OSINT **no busca todo**, busca **lo que responde al objetivo definido**.

Ejemplo

Si el objetivo es analizar la exposición digital de una empresa:

- No es útil recopilar miles de resultados irrelevantes
- Sí es útil identificar:
 - Documentos públicos
 - Correos corporativos
 - Tecnologías visibles
 - Infraestructura accesible

Este principio está alineado con buenas prácticas de inteligencia recogidas en marcos como **NIST** y **OTAN**, donde la recolección siempre está guiada por un objetivo claro.

b. Fuentes primarias

Las **fuentes primarias** son aquellas que proporcionan información **directamente desde el origen**, sin intermediarios ni reinterpretaciones.

Ejemplos de fuentes primarias

- Página web oficial de una empresa
- Documentos publicados por la propia organización
- Perfiles oficiales en redes sociales
- Registros DNS y WHOIS
- Repositorios de código públicos (GitHub, GitLab)

Características

- Mayor fiabilidad inicial
- Menor riesgo de distorsión
- Pueden contener errores humanos importantes

Ejemplo OSINT

Un documento PDF publicado por una empresa es una fuente primaria. Su contenido visible y su metadata proceden directamente del origen.

c. Fuentes secundarias

Las **fuentes secundarias** son aquellas que **recopilan, replican o reinterpretan información procedente de fuentes primarias**.

Ejemplos de fuentes secundarias

- Buscadores (Google, Bing)
- Plataformas de análisis (Shodan, censys)
- Foros públicos
- Noticias
- Bases de datos recopiladas por terceros

Características

- Útiles para ampliar contexto
- Pueden contener errores o datos desactualizados
- Nunca deben tomarse como verdad absoluta

Ejemplo OSINT

Un motor de búsqueda puede mostrar documentos antiguos que ya no están publicados oficialmente, pero siguen siendo relevantes desde el punto de vista de la exposición.

Te proponemos que completes la lectura de este tema desde nuestro artículo “**OSINT en detalle (Parte 1)**”.

Este tema lo desarrollamos en detalle en el video 183 (**Obligatorio**).

🌐 OSINT Metodología profesional - Charla 183 - Aprendiendo Ciberseguridad paso a paso
<https://youtu.be/pMEUgi7fua0>



10.3. OSINT Preparación de Kali

Por qué Kali es adecuado para OSINT

Kali aporta varias ventajas clave para OSINT:

- Amplio **repositorio de herramientas OSINT** ya integradas
- Entorno Linux ideal para:
 - Automatización
 - Scripting
 - Procesamiento de datos
- Separación clara entre:
 - Entorno personal
 - Entorno de análisis
- Comunidad activa y documentación abundante

Además, Kali permite **combinar OSINT con otras disciplinas**, como:

- Threat Intelligence
- Forense
- Pentesting
- Blue Team

Esto es fundamental en un ciclo como el tuyo, donde OSINT **no es una isla**, sino parte de un todo.

En versiones antiguas de Kali Linux, las herramientas OSINT se encontraban claramente agrupadas dentro de la categoría “**Information Gathering**”, con subcategorías específicas como *Domain Information*, *Web Crawlers* o *People OSINT*.

🌀 **Esto ya no es así en las versiones actuales de Kali Linux.**

Hoy, Kali adopta un enfoque mucho más **minimalista y modular**, donde:

- Muchas herramientas OSINT **ya no vienen preinstaladas**

- Varias han sido **retiradas del menú gráfico**
- Otras quedan disponibles **solo vía repositorios o instalación manual**

Esto no es un problema, sino una ventaja:

👉 Nos permite **construir un entorno OSINT profesional, controlado y actualizado**, exactamente como se hace en escenarios reales.

¿Dónde está OSINT hoy en Kali?

En Kali moderno:

- **No existe una categoría OSINT dedicada**
- Las herramientas OSINT están:
 - Repartidas entre categorías genéricas
 - O directamente **no instaladas**

El enfoque correcto hoy no es “buscar la categoría”, sino:

Preparar Kali como una plataforma OSINT a medida

Lista para trabajar desde este video 184 en adelante.

Nuevo enfoque: Kali como base OSINT

Desde el video 01 venimos usando Kali como:

- Sistema base
- Entorno controlado
- Laboratorio de prácticas

A partir de este tema, Kali pasa a ser:

Una plataforma OSINT modular, que iremos ampliando progresivamente.

Esto replica el flujo real de un analista:

1. Sistema limpio
2. Instalación consciente de herramientas
3. Control de versiones
4. Preparación previa antes de investigar

Te proponemos que completes la lectura de este tema desde nuestro artículo **“OSINT en detalle (Parte 1)”**.

Este tema lo desarrollamos en detalle en el video 184 **(Obligatorio)**.

🌐 OSINT Preparación de Kali - Charla 184 - Aprendiendo Ciberseguridad paso a paso



<https://youtu.be/J3wAGLFAF5Q>

10.4. OSINT sobre dominios

En este tema entramos de lleno en el **OSINT técnico pasivo aplicado a dominios**, una de las fases más importantes de cualquier investigación OSINT y también de cualquier auditoría de seguridad o ejercicio de pentesting.

El objetivo no es "sacar información" sin más, sino **entender qué información expone un dominio, por qué está expuesta y qué riesgos reales implica**. Todo lo que se hace en este vídeo es **100 % pasivo**, sin interacción directa con el objetivo.

Información que expone un dominio

Un dominio en Internet es mucho más que un nombre.

Es un **punto de agregación de información técnica, organizativa y humana**.

Tipos de información expuesta

A través de OSINT pasivo, un dominio puede revelar:

- Identidad de la organización
- Proveedores tecnológicos
- Correos electrónicos corporativos
- Estructura interna de nombres
- Infraestructura asociada
- Tecnologías utilizadas

Esta información suele estar expuesta por:

- Mala configuración
- Falta de concienciación
- Necesidades operativas legítimas

Riesgo asociado a la información de dominio

El riesgo no está en un dato aislado, sino en la **correlación de varios datos**.

Ejemplo realista:

- Dominio → correos
- Correos → nombres reales
- Nombres → redes sociales

Esto habilita ataques de **phishing dirigido**.

WHOIS: análisis detallado

Qué es WHOIS

WHOIS es un protocolo que permite consultar bases de datos públicas de registro de dominios.

Proporciona información administrativa y técnica sobre:

- Propietario del dominio
- Registrador
- Fechas clave
- Contactos técnicos (cuando no están protegidos)

Ejecución del comando

whois ejemplo.com

Ejemplo: **whois google.com**

Ejemplo: **whois google.com**

Ejemplo: **whois google.com**

Interpretación profesional del resultado

Campos relevantes:

- Registrar
- Creation Date / Expiry Date
- Name Servers
- Email (si no hay privacidad)

Buenas prácticas:

- Analizar coherencia temporal
- Revisar cambios históricos

Limitaciones de WHOIS

- Protección de privacidad (GDPR)
- Información incompleta
- Datos obsoletos

Por eso WHOIS **nunca se usa de forma aislada.**

DNS y enumeración pasiva

Qué es DNS en OSINT

DNS actúa como un **mapa público de infraestructura.**

Permite identificar:

- Servidores

- Proveedores
- Subdominios

Comandos básicos

dig ejemplo.com A

dig ejemplo.com MX

dig ejemplo.com NS

Ejemplo: **dig darfe.es A**

Ejemplo: **dig darfe.es MX**

Ejemplo: **dig darfe.es NS**

Analizar en detalle cada respuesta

Cada registro aporta contexto distinto.

Interpretación de registros

- MX → servicios de correo
- NS → proveedores DNS
- TXT → SPF, DKIM

Te proponemos que completes la lectura de este tema desde nuestro artículo “**OSINT en detalle (Parte 1)**”.

Este tema lo desarrollamos en detalle en el video 185 (**Obligatorio**).

 OSINT sobre dominios - Charla 185 - Aprendiendo Ciberseguridad paso a paso
<https://youtu.be/xH0xhzUTj4k>



10.5. OSINT Google Dorks y buscadores avanzados

En este tema abordamos uno de los pilares del OSINT moderno: **Google Dorks**, también conocido como **Google Hacking**. No se trata de "trucos de búsqueda", sino del uso avanzado de operadores para **explotar la forma en la que los motores de búsqueda indexan información pública**.

Dorks en inglés puede significar "tonto" o "nerd", pero también se refiere a una persona obsesionada con algo. Se emplea para describir el uso de **consultas específicas y operadores avanzados** en Google.

Google Dorks permite descubrir información que **no debería ser fácilmente accesible**, pero que es indexada por errores de configuración, malas prácticas o desconocimiento.

El objetivo no es memorizar operadores, sino **entender qué tipo de errores humanos y técnicos permiten que esta información sea indexada.**

¿Qué podemos encontrar con Google Dorks?

- Credenciales de usuarios y contraseñas.
- Contenido multimedia: fotos, imágenes y vídeos.
- URLs de diferentes dominios.
- Documentación de interés: DNIs, NIFs, identificadores, teléfonos, direcciones, códigos.
- Información bancaria: números de cuenta o tarjetas.
- Correos electrónicos.
- Datos de Acceso, autenticación.
- Rutas, itinerarios, hábitos, costumbres, amistades, familia.
- Etc.

Su uso es perfectamente legal, siempre y cuando mantengas la metodología que venimos presentando desde el primer video de OSINT.

Cómo funciona la indexación

Qué indexa Google realmente

Google no indexa "páginas", indexa **contenido accesible públicamente.**

Indexa:

- HTML
- PDFs
- DOCX, XLSX
- Directorios
- Metadatos

Si algo aparece en Google, es porque el servidor lo permite.

Robots.txt y falsas creencias

robots.txt no protege información, solo indica a los bots qué no deberían indexar.

Ejemplo:

User-agent: *

Disallow: /backup/

Esto revela indirectamente que existe un directorio /backup/.

Operadores avanzados (Google Dorks)

Qué es unGoogle Dork

Un Google Dork es una **consulta avanzada** que combina operadores para filtrar resultados muy específicos.

No explota vulnerabilidades técnicas, explota **exposición de información pública**.

Marco ético y legal

Buenas prácticas:

- No descargar información sensible
- No autenticarte
- No interactuar
- Documentar sin explotar

Operadores básicos (uso real)

site: Limita resultados a un dominio, o subdominio

Muestra qué páginas están indexadas en Google

(por ejemplo: site:books.google.com)

site:ejemplo.com

site:darfe.es

site:uned.es

filetype: devuelve webs que contengan documentos de un tipo de fichero concreto (por ejemplo: *SEO filetype:pdf*). *Podemos ir concatenando varios operadores básicos.*

site:ejemplo.com filetype:pdf

site:darfe.es filetype:pdf

site:upm.es filetype:pdf

Localiza documentos indexados.

Repetir con:

filetype:docx

filetype:xlsx

filetype:pptx

- Backups:

filetype:bak OR filetype:old

 Analizar:

- Títulos de documentos
- Autores
- Contexto del documento

Intitle, inurl e intext:

Intitle muestra los contenidos que tengan en el Title Tag la palabra después de los caracteres ":" (por ejemplo: *intitle:index of*, *intitle:examen*, *intitle:fotos*).

inurl busca páginas que contengan una palabra o frase específica dentro de esta URL.

intitle:"index of"

intitle:"examen"

intitle:"fotos"

Detectar listado de directorios, documentos,

site:ejemplo.com intitle:"index of"

site:empresa-ficticia.com filetype:pdf

site:upm.es intitle:"index of"

site:madrid.org intitle:"index of"

site:madrid.org intitle:"fotos"

site:upm.es intitle:"examen"

inurl:darfe.es intext:ciberseguridad

inurl:darfe.es allintext:ciberseguridad wifi

site:darfe.es intext:auditoria forense

inurl:darfe.es intext:auditoria forense

¿qué diferencia veis entre los dos últimos?

Posibles hallazgos:

- Listados de archivos
- Backups
- Versiones antiguas

Te proponemos que completes la lectura de este tema desde nuestro artículo “**OSINT en detalle (Parte 1)**”.

Este tema lo desarrollamos en detalle en el video 186 **(Obligatorio)**.

🌐 OSINT Google Dorks y buscadores avanzados - Charla 186 -
Aprendiendo Ciberseguridad paso a paso
<https://youtu.be/-JAcvgAWj68>



10.6. OSINT sobre personas y redes sociales (SOCMINT)

Este es uno de los temas más delicados de la serie. El OSINT sobre personas requiere **máxima ética, profesionalidad y cumplimiento legal**. Se analiza información pública, nunca privada.

El **People OSINT** es la disciplina dentro de la inteligencia de fuentes abiertas que se centra en el **análisis de la huella digital de personas físicas**, siempre a partir de información **pública, accesible y obtenida sin interacción directa con el objetivo**.

En el contexto profesional, el OSINT sobre personas no se utiliza para "espiar", sino para:

- Concienciación en ciberseguridad
- Evaluación de riesgos humanos
- Auditorías de exposición digital
- Fases de reconocimiento en Red Team
- Prevención de phishing, spear phishing y BEC

En este tema se establece una **base metodológica sólida**, ética y legal, que permita al alumno entender **qué información es relevante, cómo correlacionarla y cómo documentarla correctamente**.

SOCMINT como subdisciplina, marco ético y legal

Principio fundamental

Todo el People OSINT debe realizarse exclusivamente con información pública y sin interacción con la persona analizada.

Esto implica:

- No enviar mensajes
- No solicitar contactos
- No acceder a sistemas autenticados
- No suplantar identidades

Desde el punto de vista legal, el analista debe tener en cuenta:

- RGPD
- Principio de minimización
- Finalidad legítima (formación, auditoría, concienciación)

Huella digital personal

Definición técnica

La **huella digital** es el conjunto de rastros que una persona deja en Internet como resultado del uso de servicios digitales.

Incluye información:

- Explícita (publicada conscientemente)

- Implícita (generada sin intención)

Huella digital activa

Información que la persona publica de forma consciente:

- Perfiles en redes sociales
- Comentarios en foros
- Blogs personales
- Currículums online

Ejemplo:

- Perfil de LinkedIn con cargo, empresa y tecnologías

Huella digital pasiva

Información que aparece sin que la persona sea plenamente consciente:

- Metadatos de documentos
- Historial de repositorios
- Indexación por buscadores
- Comentarios antiguos

Ejemplo:

- PDF subido a una web con nombre de usuario del sistema operativo en los metadatos

Te proponemos que completes la lectura de este tema desde nuestro artículo “**OSINT en detalle (Parte 1)**”.

Este tema lo desarrollamos en detalle en el video 187 (**Obligatorio**).

🌐 OSINT sobre personas y redes sociales (SOCMINT) - Charla 187 - Aprendiendo Ciberseguridad paso a paso: <https://youtu.be/jsff9cEues>

