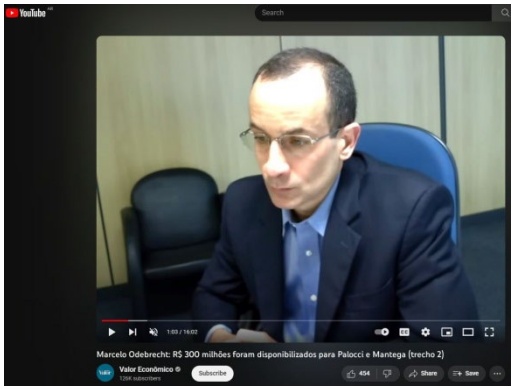
LA EVIDENCIA DIGITAL

“La evidencia digital es cualquier información de valor probatorio que se almacena o transmite en forma digital”



Caso Alvarado: habló el que desbloqueó el Iphone 8

Un teléfono que habla por sí solo

Hay 4.500 audios que son la evidencia central en el juicio contra el jefe narco. Arrojó el aparato al río cuando lo arrestaron.

Por José Maggi

Esta empresa con sede en Nueva York desencriptó el aparato.

El juicio contra la banda liderada por Esteban Alvarado tuvo ayer su novena jornada, en la que declaró como testigo el representante de la empresa norteamericana que desbloqueó el IPhone que el jefe narco arrojó a las aguas de Embalse Río Tercero, donde fue capturado. También lo hizo quien accedió al contenido del aparato: un técnico en análisis forense.

MÉXICO

En Instagram, Facebook y WhatsApp: así funciona el narcomenudeo a través de redes sociales

Páginas de Facebook e Instagram se dedican a distribuir marihuana y otras sustancias, además de diversos productos hechos con droga

4 de Octubre de 2019

Policiales

Tenían 185 millones de dólares en criptomonedas y los embargan por 4 billones de pesos acusados de lavar dinero para el Comando Vermelho

- Son tres brasileños acusados de ser miembros del poderoso grupo criminal.
- Su jefe, Marcelo Alves de Sousa, sigue prófugo. Era el titular de una billetera virtual por la que pasó ese monto millonario en dólares.

- La creciente incorporación de evidencia digital en los procesos judiciales enfrenta a los investigadores a nuevos desafíos y nuevos conocimientos.

- Se ha actualizado la legislación de fondo pero no las normas procesales.

- La evidencia digital se incorpora al proceso penal mediante los medios de prueba tradicionales.

- En los casos no previstos se recurre al principio de libertad probatoria.

DESAFIOS DE LA EVIDENCIA DIGITAL

- Creciente uso de teléfonos celulares, computación en la nube y aumento de la capacidad de almacenamiento de los smartphones, discos y unidades USB.
- Obliga a los investigadores a llevar a cabo investigaciones proactivas.
- Delincuentes con conocimientos informáticos: técnicas antiforense: encriptación, uso de navegador Tor, TAILS, Whonix, uso de criptomonedas.
- Falta de protocolos específicos sobre adquisición, aseguramiento y conservación de la evidencia digital.
- Falta de presupuesto para adquirir nuevas herramientas tecnológicas de investigación y para incorporar mayor recurso humano. Falta de actualización de conocimientos.
- Carácter transnacional de la evidencia digital.

CARACTERÍSTICAS DE LA EVIDENCIA DIGITAL

I. RELEVANCIA

II. CONFIABILIDAD

III. SUFICIENCIA

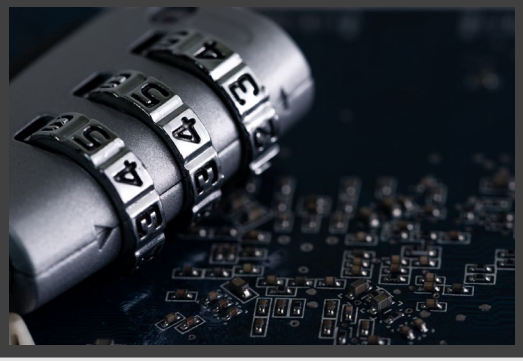
- ES DIGITAL: ES DECIR UN CONJUNTO DE BITS. UNIDAD MINIMA DE INFORMACION (0 o 1)
- RESIDE EN UN SOPORTE FISICO, PERO NO ES EL SOPORTE FISICO.
- INTANGIBLE
- POSEE METADATOS
- PUEDE DUPLICARSE SIN LIMITES Y SU COPIA SERA IDENTICA AL ORIGINAL
- ES VOLÁTIL
- PUEDE MODIFICARSE, ALTERARSE O ELIMINARSE FÁCILMENTE (incluso de manera remota)
- NECESITA SER RESGUARDADA
- PUEDE SER EVIDENCIA DE ALMACENAMIENTO, DE PROCESAMIENTO O DE TRÁFICO

OECD – Better Policies for Better Lives
@OECD

Each participant in the OECD LATIN AMERICA ACADEMY FOR TAX CRIME AND FINANCIAL INVESTIGATIONS course will receive USD 1,000 for attending at OSINT and digital evidence class. ☺

4:17 PM· Oct 29, 2023 · Twitter for Android

3 Retweets **16** Likes



- HASH

  Es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor **hash** de salida tendrá siempre la misma longitud.

Pericias informáticas

Resguardo de información durante la investigación

HASH (SHA 1 – 256 -512 – MD5)

Incorporación de documentos al proceso

- METADATOS

(Son los datos de los datos)

METADATOS EN UNA FOTOGRAFÍA DIGITAL

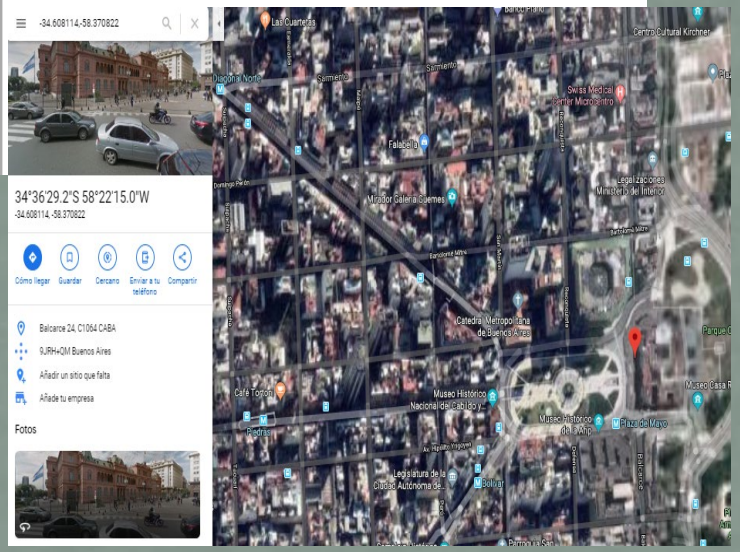
Basic Image Information

Target file: IMG_20191127_183902.jpg

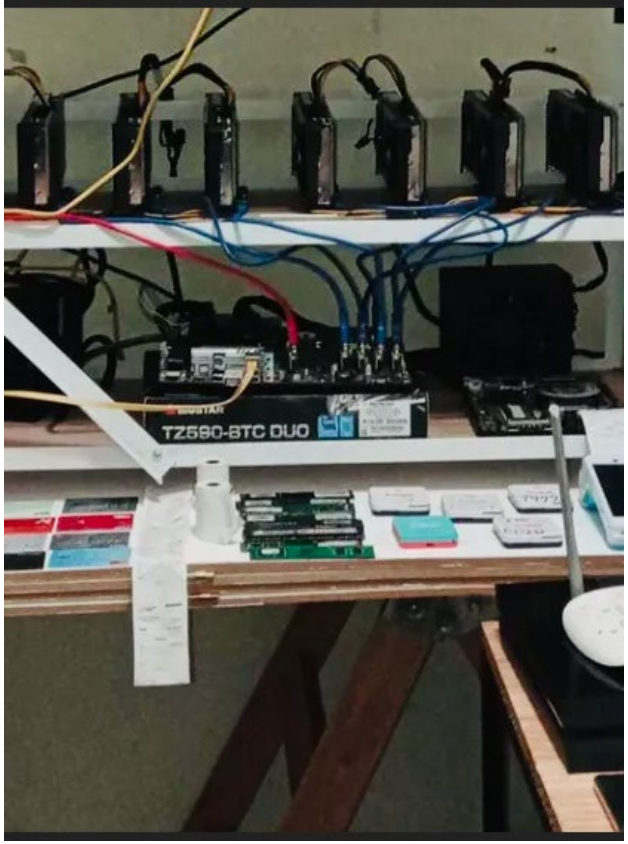
Camera:	Huawei DUB-LX3
Lens:	3 mm
Exposure:	Auto exposure, Program AE, 1/1,167 sec, f/2, ISO 101
Flash:	none
Date:	**November 27, 2019** 6:39:04PM (timezone not specified) (2 months, 5 days, 42 minutes, 15 seconds ago, assuming image timezone of 3 hours behind GMT)
Location:	Latitude/longitude: **34**° 36' 29.2" South, **58**° 22' 15" West (-34.608114, -58.370822) Map via embedded coordinates at: Google, Yahoo, WikiMapia, OpenStreetMap, Bing (also see the Google Maps pane below) Altitude: 0 meters (0 feet) below sea level Timezone guess from earthtools.org: 3 hours behind GMT
File:	**2,448** × **3,264** JPEG (**8.0** megapixels) 2,232,619 bytes (2.1 megabytes)
Color Encoding:	**WARNING:** Color space tagged as sRGB, without an embedded color profile. **Windows and Mac browsers and apps treat the colors randomly**. Images for the web are most widely viewable when in the sRGB color space and with an embedded color profile. See my Introduction to Digital-Image Color Spaces for more information.

1:1 Extracted **240** × **320** 17-kilobyte "`EXIF:ThumbnailImage`" JPG
Displayed here at 100% (1/104 the area of the original)

Click image to isolate; click this text to show histogram



Fuentes de evidencia digital



- No todo aparato electrónico almacena evidencia digital.

CADENA DE CUSTODIA EN EL PROCESO PENAL

"Un proceso que rastrea el movimiento de las pruebas a lo largo de su ciclo de vida de recogida, salvaguarda y análisis, documentando a cada persona que manejó las pruebas, la fecha/hora en que se recogieron o transfirieron y el propósito de cualquier transferencia". NIST.

Protocolos o Manuales de Cadena de custodia de la Evidencia digital:
Normas ISO/IEC 27037

Va desde la obtención de la evidencia hasta la disposición final de la misma.

Se documenta con los formularios de cadena de custodia / rótulos, etiquetas, etc.

Extracción o recolección de los indicios. Preservación y embalaje de la prueba. Transporte o traslado de la prueba. Traspaso de la misma, ya sea a los laboratorios para su análisis, o a las diferentes fiscalías para su custodia. Custodia y preservación final hasta que se realice la audiencia debate.

Resguardo de garantía del debido proceso

En el proceso penal interviene personal policial, fiscales, peritos, jueces

- Pericia informática

Informatica forense: El proceso utilizado para adquirir, preservar, analizar e informar sobre evidencia utilizando métodos científicos que son demostrablemente confiables, precisos y repetibles, de modo que puedan usarse en procedimientos judiciales (NIST – NISTIR 8006)

FUENTES: SISTEMAS DE COMPUTACION ABIERTOS, SISTEMA DE COMUNICACION, SISTEMAS CONVERGENTES DE COMPUTACIÓN

DISPOSITIVOS ALMACENAMIENTO: IMAGEN FORENSE: COPIA BIT A BIT CON ASIGNACIÓN DE HASH.TELEFONOS CELULARES: EXTRACCIÓN LOGICA, SISTEMA DE ARCHIVOS O FISICA (TARJETA SIM – MEMORIA EXTRAIBLE.

EL PERITO PUEDE REALIZAR TAREAS EN EL LABORATORIO O EN EL LUGAR DEL HECHO / ALLANAMIENTO (VOLCADOS DE MEMORIA, VOLCADOS DE RED, TRIAGE, COPIA FORENSE).

EVIDENCIA VOLATIL: SI LA PC O LAPTOP ESTA ENCENDIDA PUEDE EXTRAERSE MEMORIA RAM, USUARIOS LOGGEADOS, PROCESOS EN CURSO, IDENTIFICAR ENCRIPTAMIENTO, CLAVES CONEXIONES, CONFIGURACION DE RED.

ACTOS INCIALES– ADQUISICION – ANALISIS- DOCUMENTACION- PRESENTACION.

CONVENIO DE BUDAPEST

ART 14: EL CONVENIO SE PODRÁ APLICAR A "LA OBTENCION DE PRUEBAS ELECTRONICAS DE CUALQUIER DELITO"

MEDIDAS DE PRUEBA EN EL PAIS

- Conservación rápida de datos almacenados en medios informáticos
- Conservación y revelación parcial rápida de datos sobre tráfico
- Orden de presentación
- Registro y confiscación
- Obtención en tiempo real de datos de tráfico
- Interceptación de datos de contenido

COOPERACION INTERNACIONAL

- Conservación rápida
- Revelación rápida de datos conservados
- Asistencia mutua en relación al acceso a datos/ tráfico y contenido
- Acceso transfronterizo de datos públicos o con consentimiento
- Red 24/7

- Transnacionalidad de la evidencia digital

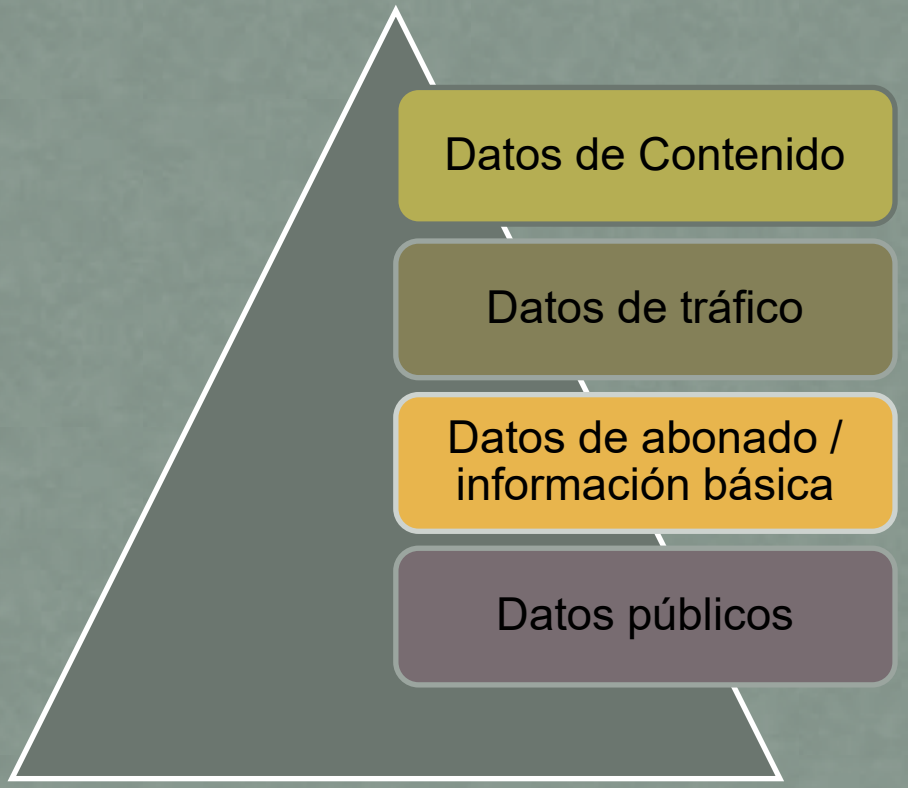
•Cooperación internacional formal e informal (UNCAC, UNTOC, MLAT, RED 24/7, INTERPOL).

•Jurisprudencia internacional: “United States vs Microsoft Corp.” – Cloud Act - RGDP

•Cooperación voluntaria de los proveedores de servicios.

•Segundo protocolo del Convenio Budapest (2022)

- DIFERENTES ESCALAS DE AFECTACIÓN DE DERECHOS



A medida que subimos en la pirámide se requerirá “causa probable” para llevar adelante la medida probatoria, resguardándose principios como el de proporcionalidad, excepcionalidad, necesidad, etc.

Medidas de conservación y pedido de informes

facebook

Law Enforcement Online Requests

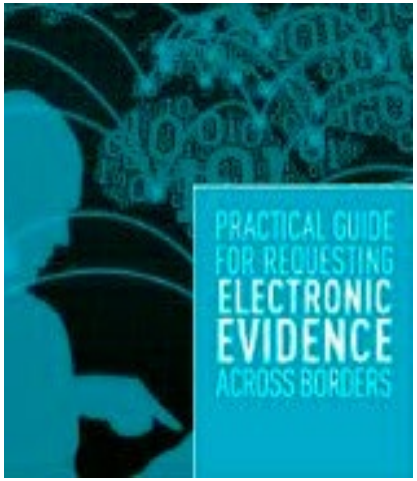
Request Secure Access to the Law Enforcement Online Request System

We disclose account records solely in accordance with our terms of service and applicable law.

If you are a law enforcement agent or emergency responder who is authorized to gather evidence in connection with an official investigation or in order to investigate an emergency involving the danger of serious physical injury or death, you may request records from Facebook through this system.

I am an authorized law enforcement agent or government employee investigating an emergency, and this is an official request

Solicitar acceso



Envíos de requerimientos judiciales

Confirme su identidad

Welcome to Twitter's online legal request submission site. You can submit your legal request (e.g., subpoena or court order) for account information or content removal by following the steps below. We also accept emergency disclosure requests from law enforcement through this site. All non-legal requests should be submitted through our Help Center forms.

Si usted es un agente de la policía, un representante gubernamental u otro tipo de entidad externa con la intención de enviar un requerimiento judicial válido, le solicitamos que introduzca su nombre completo y su dirección de correo electrónico oficial, y que confirme su autoridad marcando la casilla que aparece a continuación. No se permite ningún otro uso de este formulario.

Para obtener más información, consulte nuestras Directrices para agentes de policía, el artículo de ayuda Cómo acceder a tus datos de Twitter y la Política de privacidad de Twitter.

Nombre completo:*

Introduzca su nombre completo

Dirección de correo electrónico oficial:*

Introduzca su dirección de correo electrónico oficial

Se enviará a esta dirección de correo electrónico un mensaje que contiene un enlace de autorización para acceder al sitio.

Afirmo que dispongo de la autoridad legal necesaria para enviar este requerimiento y que su envío constituye un uso permitido de este sistema. *

Solicitar acceso

MODERNAS TECNICAS DE INVESTIGACION PENAL

- INVESTIGACION EN FUENTES ABIERTAS
- AGENTE ENCUBIERTO DIGITAL
- ENTREGA VIGILADA DIGITAL
- USO DE DRONES
- CIBERVIGILANCIA ACUSTICA / IMAGENES

LA EVIDENCIA ONLINE

LA WEB

ARPANET 1960 / 1970

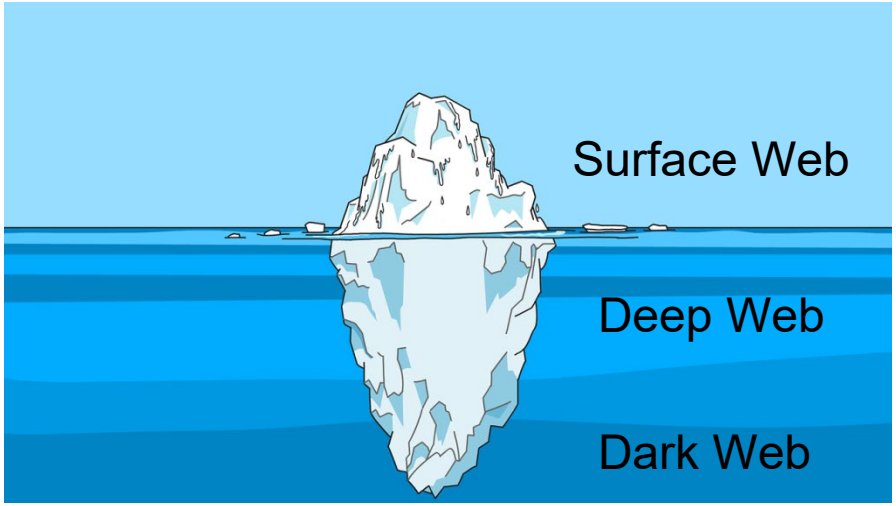
WORLD WIDE WEB 1990 (protocolo HTTP – lenguaje HTML – URL)

IoT – IA – BIG DATA

PROTOCOLO TCP/IP 1980

REDES SOCIALES - PRIMER IPHONE 2000

Tres niveles de la Web



https://www.kaspersky.es/blog/valor-darkweb/24602 **(2021)**

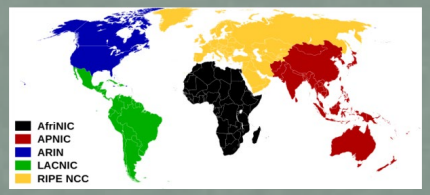
IP

IPV4: 181.46.139.15

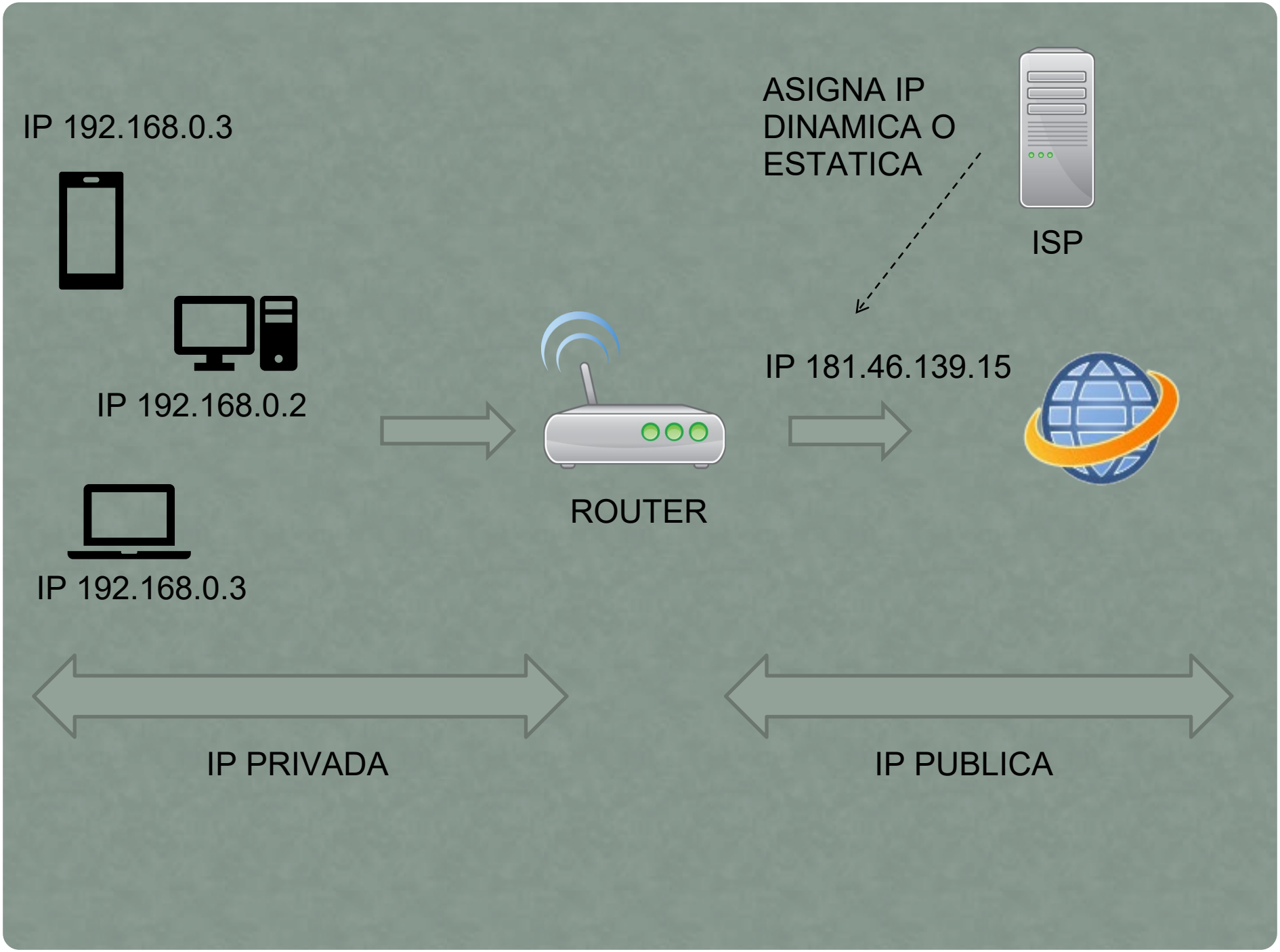
IPV6:
1030:0000:0000:0000:0005:0700:100c:348b

- LA DIRECCION IP IDENTIFICA DISPOSTIVOS CONECTADOS A UNA RED QUE UTILIZA EL PROTOLO IP
- IPV4: DIRECCIONES IP DE CUATRO NUMEROS DECIMALES SEPARADOS POR UN PUNTO. MAXIMO 12 CARACTERES.
- EXISTEN CUATRO MIL MILLONES DE DIRECCIONES IPV4. POR ESO COMENZO A UTILIZARSE EL PROTOCOLO IPV6.

ICANN



ISP
Internet Service Provider


IP 192.168.0.3
ASIGNA IP
DINAMICA O
ESTATICA
ISP
IP 192.168.0.2
IP 181.46.139.15
ROUTER
IP 192.168.0.3
IP PRIVADA
IP PUBLICA

SISTEMA DE NOMBRES DE DOMINIO

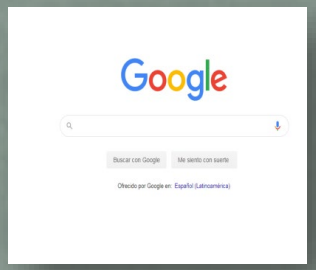
Una persona escribe en su navegador: www.google.com

MEMORIA CACHE DNS

MODEM - ROUTER

DNS RESOLVER (ISP proveedor de internet)

Servidor de GOOGLE
IP 172.217.3.196



Servidor envía la página web al navegador

Servidores DNS (Raíz o Root Server, 1er Nivel o TLD Server y 2do Nivel o Authoratative Name Server)

*Los servidores DNS son como guías Telefónicas que permiten conocer las IP asignada a cada dominio. Google.com = IP 172.217.3.196

HTTPS :// WWW. OECD. ORG

Protocolo de internet

Subdominio

Dominio 2do Nivel

Dominio 1er Nivel TLD

DomainTools PROFILE CONNECT MONITOR SUPPORT Whois Lookup

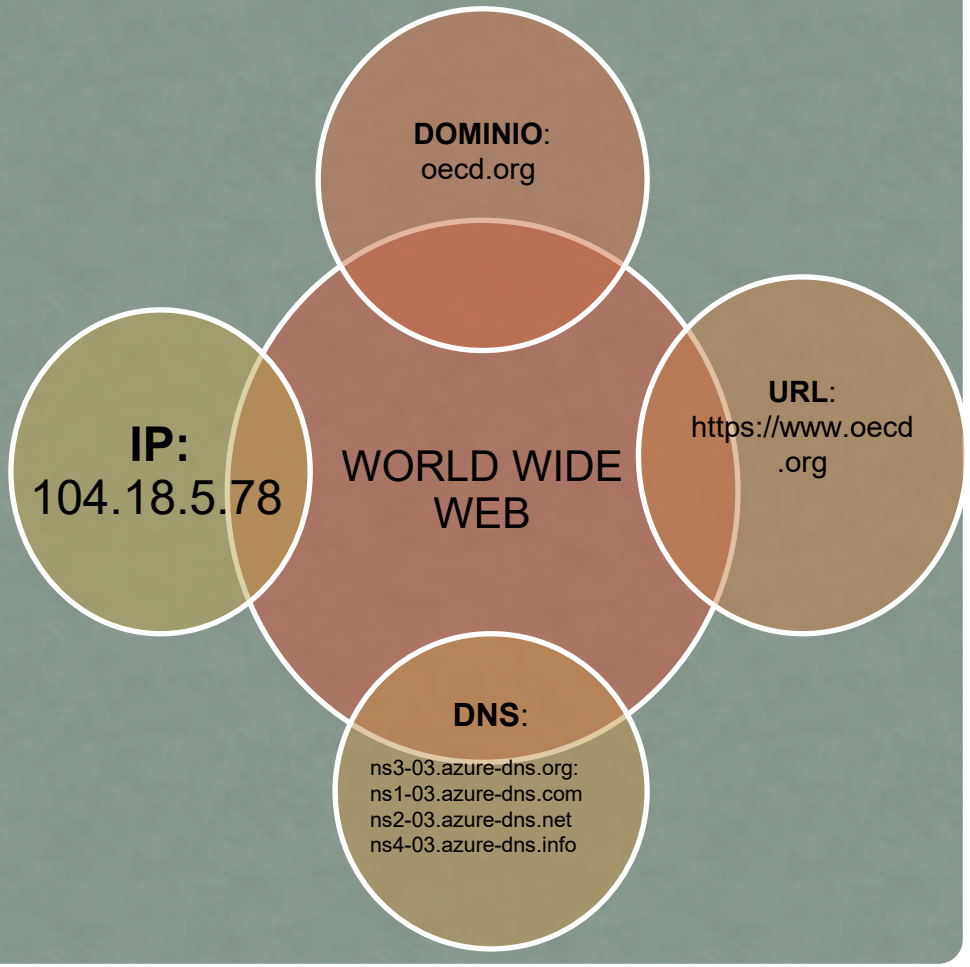
Home > Whois Lookup > Oecd.org

Whois Record for Oecd.org

Domain Profile

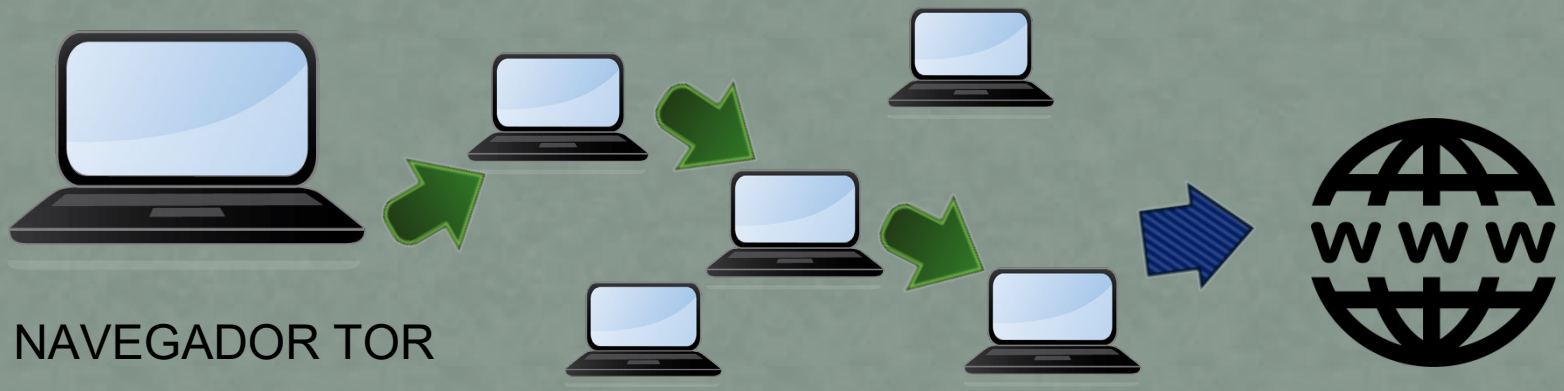
Registrar	Network Solutions, LLC IANA ID: 2 URL: http://www.networksolutions.com Whois Server: whois.networksolutions.com domain.operations@web.com (p) +1.8777228662
Registrar Status	clientTransferProhibited
Dates	10,541 days old Created on 1994-12-13 Expires on 2029-12-12 Updated on 2023-03-23
Name Servers	NS1-03.AZURE-DNS.COM (has 476,736 domains) NS2-03.AZURE-DNS.NET (has 256 domains) NS3-03.AZURE-DNS.ORG (has 161 domains) NS4-03.AZURE-DNS.INFO (has 58 domains)
IP Address	104.18.4.78 - 6 other sites hosted on this server
IP Location	- Noord-holland - Amsterdam - Cloudflare Inc.
ASN	AS13335 CLOUDFLARENET, US (registered Jul 14, 2010)
Domain Status	Registered And No Website
IP History	95 changes on 95 unique IP addresses over 18 years
Hosting History	5 changes on 3 unique name servers over 14 years

Whois Record (last updated on 2023-10-23)



CONEXIÓN A LA WEB

PROXY - VPN

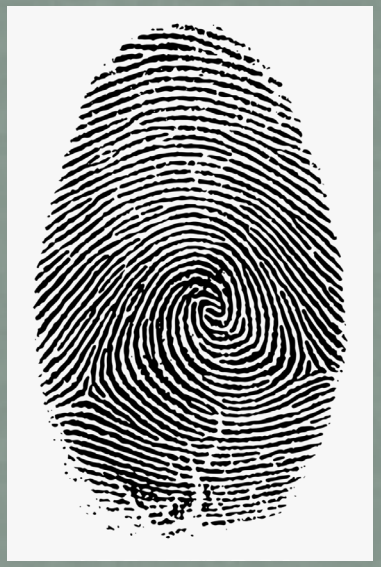


NAVEGADOR TOR

La huella del navegador

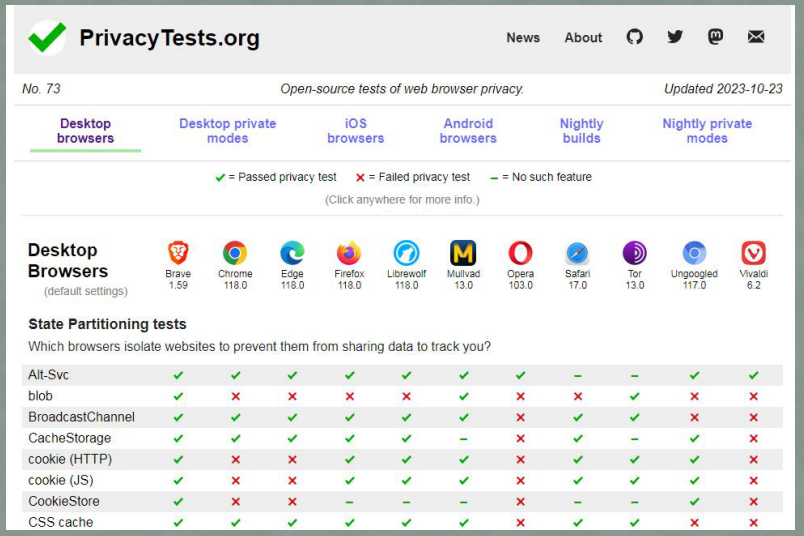
Los sitios web pueden identificar la IP pública y efectuar seguimientos a través de cookies.

La información que envía nuestro navegador lo puede convertir en único e identificable entre millones de usuarios de internet (Por ejemplo: tipo de navegador, sistema operativo, resolución de pantalla, fuentes utilizadas).



https://coveryourtracks.eff.org

https://whoer.net/es



Algunas recomendaciones antes de iniciar una investigación en fuentes abiertas en internet.