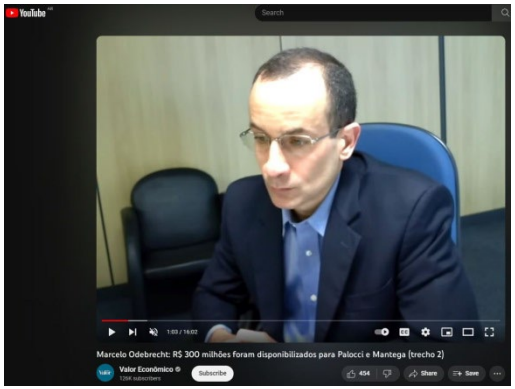
DIGITAL EVIDENCE

"Digital evidence is any information of evidentiary value that is stored or transmitted in digital form."



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.

- The increasing incorporation of digital evidence in judicial processes confronts investigators with new challenges and new knowledge.

- The substantive legislation has been updated but not the procedural rules.

- Digital evidence is incorporated into criminal proceedings through traditional means of evidence.

- In unforeseen cases, the principle of freedom of evidence is used.

CHALLENGES OF DIGITAL EVIDENCE

- Growing use of cell phones, cloud computing and increasing storage capacity of smartphones, disks and USB drives.
- It forces investigators to conduct proactive research.
- Computer-savvy criminals: anti-forensic techniques: encryption, use of Tor browser, TAILS, Whonix, use of cryptocurrencies.
- Lack of specific protocols on acquisition, securing and preservation of digital evidence.
- Lack of budget to acquire new technological investigation tools and to incorporate more human resources. Lack of knowledge updating.
- Transnational character of digital evidence.

CHARACTERISTICS OF DIGITAL EVIDENCE

I. RELEVANCE

II. CONFIABILITY

III. SUFFICIENCY

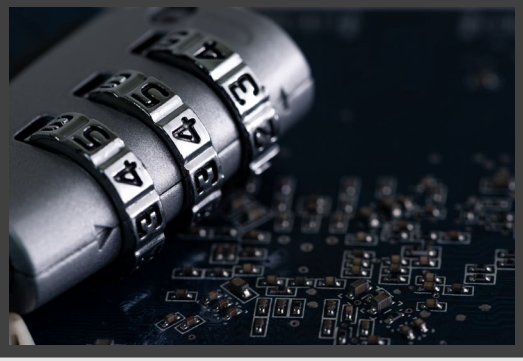
- IS DIGITAL: I.E. A SET OF BITS. MINIMUM UNIT OF INFORMATION (0 or 1)
- RESIDES IN A PHYSICAL MEDIUM, BUT IT IS NOT THE PHYSICAL MEDIUM.
- INTANGIBLE
- HAS METADATA
- CAN BE DUPLICATED WITHOUT LIMITS AND ITS COPY WILL BE IDENTICAL TO THE ORIGINAL.
- IS VOLATILE
- CAN BE EASILY MODIFIED, ALTERED OR DELETED (including remotely)
- NEEDS TO BE SAFEGUARDED
- MAY BE EVIDENCE OF STORAGE, PROCESSING OR TRAFFIC.

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

It is a mathematical algorithm that transforms any arbitrary block of data into a new series of characters with a fixed length. Regardless of the length of the input data, the output hash value will always have the same length.

Computer expertise

Safeguarding information during investigation

HASH (SHA 1 – 256 -512 – MD5)

Incorporation of documents to the process

METADATA

(It is the data of the data)

METADATA IN A DIGITAL PHOTOGRAPH

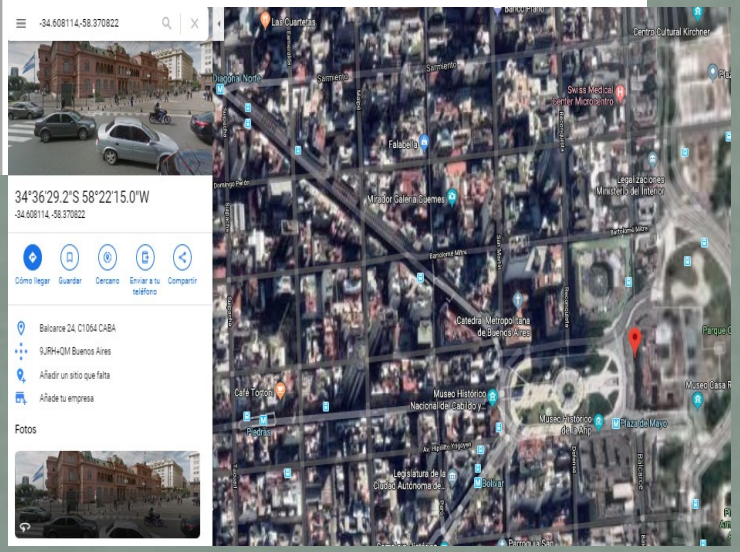
Basic Image Information

Target file: IMG_20191127_183902.jpg

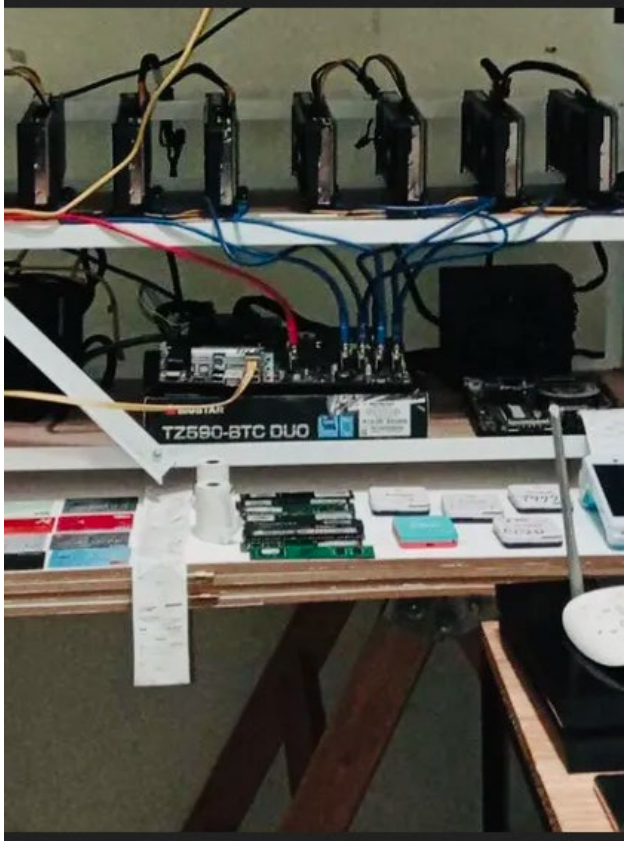
Camera:	Huawei DUB-LX3
Lens:	3 mm
Exposure:	Auto exposure, Program AE, 1/1,167 sec, f/2, ISO 101
Flash:	none
Date:	**November 27, 2019** 6:39:04PM (timezone not specified) (2 months, 5 days, 42 minutes, 15 seconds ago, assuming image timezone of 3 hours behind GMT)
Location:	Latitude/longitude: **34**° 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



Sources of digital evidence



- Not every electronic device stores digital evidence.

CHAIN OF CUSTODY IN CRIMINAL PROCEEDINGS

"A process that tracks the movement of evidence throughout its collection, safeguarding, and analysis lifecycle, documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose of any transfer." NIST.

Digital Evidence Chain of Custody Protocols or Manuals: ISO/IEC 27037 Standards

It goes from the collection of evidence to its final disposition.

Documented with chain of custody forms/tags, labels, etc.

Extraction or collection of evidence. Preservation and packaging of evidence. Transport or moving of the evidence. Transfer of the evidence, either to the laboratories for analysis, or to the different prosecutors' offices for custody. Custody and final preservation until the hearing is held.

Safeguarding of due process guarantees

The criminal process involves police personnel, prosecutors, experts, judges, etc.

Computer Forensics

- The process used to acquire, preserve, analyze and report evidence using scientific methods that are demonstrably reliable, accurate and repeatable, so that they can be used in legal proceedings (NIST -NISTIR 8006).

SOURCES: OPEN COMPUTER SYSTEMS, COMMUNICATION SYSTEM, CONVERGENT COMPUTER SYSTEMS

STORAGE DEVICES: FORENSIC IMAGING: BIT BY BIT COPY WITH HASH ASSIGNMENT.CELL PHONES: LOGICAL EXTRACTION, FILE SYSTEM OR PHYSICAL (SIM CARD - REMOVABLE MEMORY).

THE EXPERT CAN PERFORM TASKS IN THE LABORATORY OR AT THE SCENE (MEMORY DUMPS, NETWORK DUMPS, TRIAGE, FORENSIC COPYING).

VOLATILE EVIDENCE: IF THE PC OR LAPTOP IS TURNED ON IT CAN EXTRACT RAM MEMORY, LOGGED USERS, RUNNING PROCESSES, IDENTIFY ENCRYPTION, KEY CONNECTIONS, NETWORK CONFIGURATION.

INITIAL ACTS - ACQUISITION - ANALYSIS - DOCUMENTATION - PRESENTATION.

ART 14: THE CONVENTION MAY BE APPLIED TO "THE COLLECTION OF ELECTRONIC EVIDENCE OF ANY CRIME".

IN-COUNTRY EVIDENCE MEASURES

- Quick preservation of data stored on computer media
- Storage and quick partial disclosure of traffic data
- Order of submission
- Search and seizure
- Real-time traffic data collection
- Content data interception

INTERNATIONAL COOPERATION

- Quick storage
- Quick disclosure of stored data
- Mutual assistance regarding access to data/traffic and content
- Cross-border access to public or consensual data
- 24/7 Network

- Digital evidence transnationality

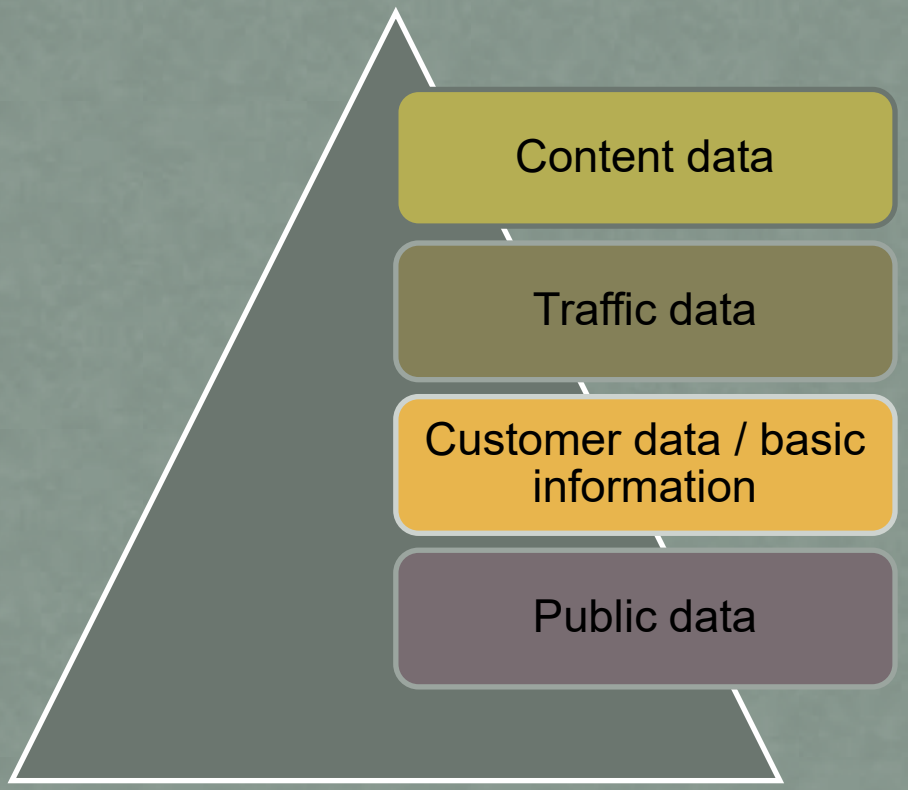
•Formal and informal international cooperation (UNCAC, UNTOC, MLAT, 24/7 Network, INTERPOL).

•International case law: "United States vs Microsoft Corp." - Cloud Act - RGDP

•Voluntary cooperation of service providers.

•Second protocol to the Budapest Convention (2022)

- DIFFERENT LEVELS OF RIGHTS AFFECTED



As we move up the pyramid, "probable cause" will be required to carry out the evidentiary proceeding, protecting principles such as proportionality, exceptionality, necessity, etc.

Conservation actions and request for reports

facebook

Law Enforcement Online Requests

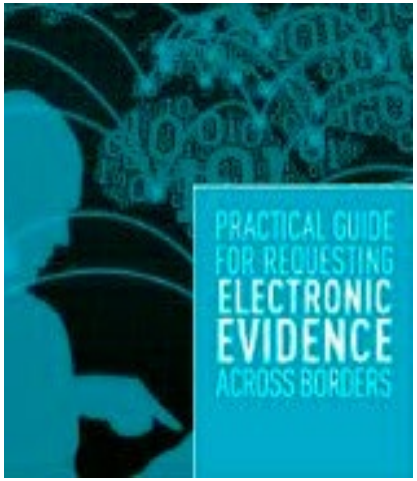
Request Secure Access to the Law Enforcement Online Request System

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

MODERN TECHNIQUES OF CRIMINAL INVESTIGATION

- OPEN SOURCE INTELLIGENCE
- UNDERCOVER DIGITAL AGENT
- DIGITAL SURVEILLED DELIVERY
- USE OF DRONES
- ACOUSTIC CYBER SURVEILLANCE / IMAGES

THE ONLINE EVIDENCE

THE WEB

Haga clic para agregar texto

Haga clic para agregar texto

ARPANET 1960 / 1970

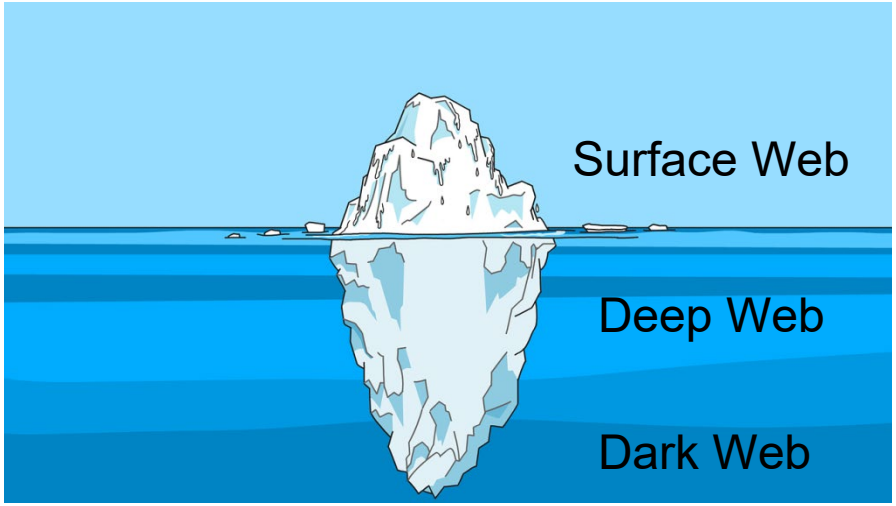
WORLD WIDE WEB 1990 (protocolo HTTP – lenguaje HTML – URL)

IoT – IA – BIG DATA

PROTOCOLO TCP/IP 1980

REDES SOCIALES - PRIMER IPHONE 2000

Three levels of the Web



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

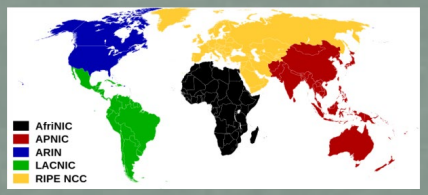
IP

IPV4: 181.46.139.15

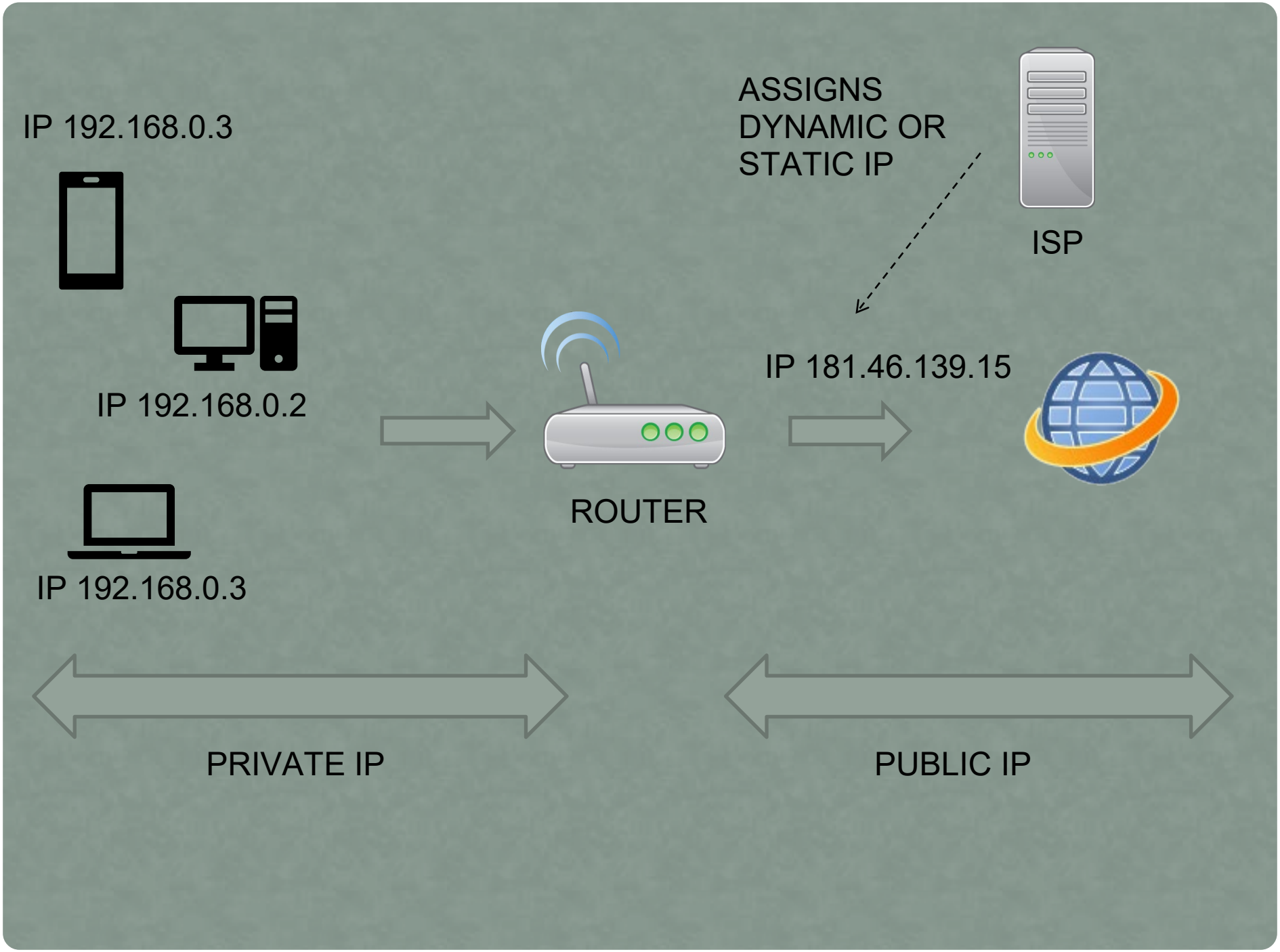
IPV6:
1030:0000:0000:0000:0005:0700:100c:348b

- THE IP ADDRESS IDENTIFIES DEVICES CONNECTED TO A NETWORK USING THE IP PROTOCOL.
- IPV4: IP ADDRESSES OF FOUR DECIMAL NUMBERS SEPARATED BY A DOT. MAXIMUM 12 CHARACTERS.
- THERE ARE FOUR BILLION IPV4 ADDRESSES. THAT IS WHY THE IPV6 PROTOCOL STARTED TO BE USED.

ICANN



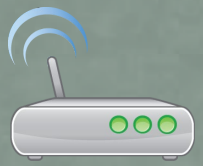
ISP
Internet Service Provider


IP 192.168.0.3
ASSIGNS
DYNAMIC OR
STATIC IP
ISP
IP 192.168.0.2
IP 181.46.139.15
ROUTER
IP 192.168.0.3
PRIVATE IP
PUBLIC IP

DOMAIN NAME SYSTEM

A person types in his browser: www.google.com

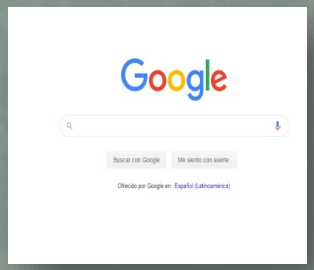
DNS CACHE MEMORY



MODEM - ROUTER

DNS RESOLVER (ISP Internet service provider)

GOOGLE server
IP 172.217.3.196



Server sends the web page to the browser

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

*DNS SERVERS ARE LIKE TELEPHONE DIRECTORIES THAT ALLOW TO KNOW THE IP ASSIGNED TO EACH DOMAIN.Google.com = IP 172.217.3.196

HTTPS :// WWW. OECD. ORG

Internet Protocol | Subdomain | 2do level domain | 1er level domain TLD

DomainTools PROFILE CONNECT MONITOR SUPPORT Whois Lookup

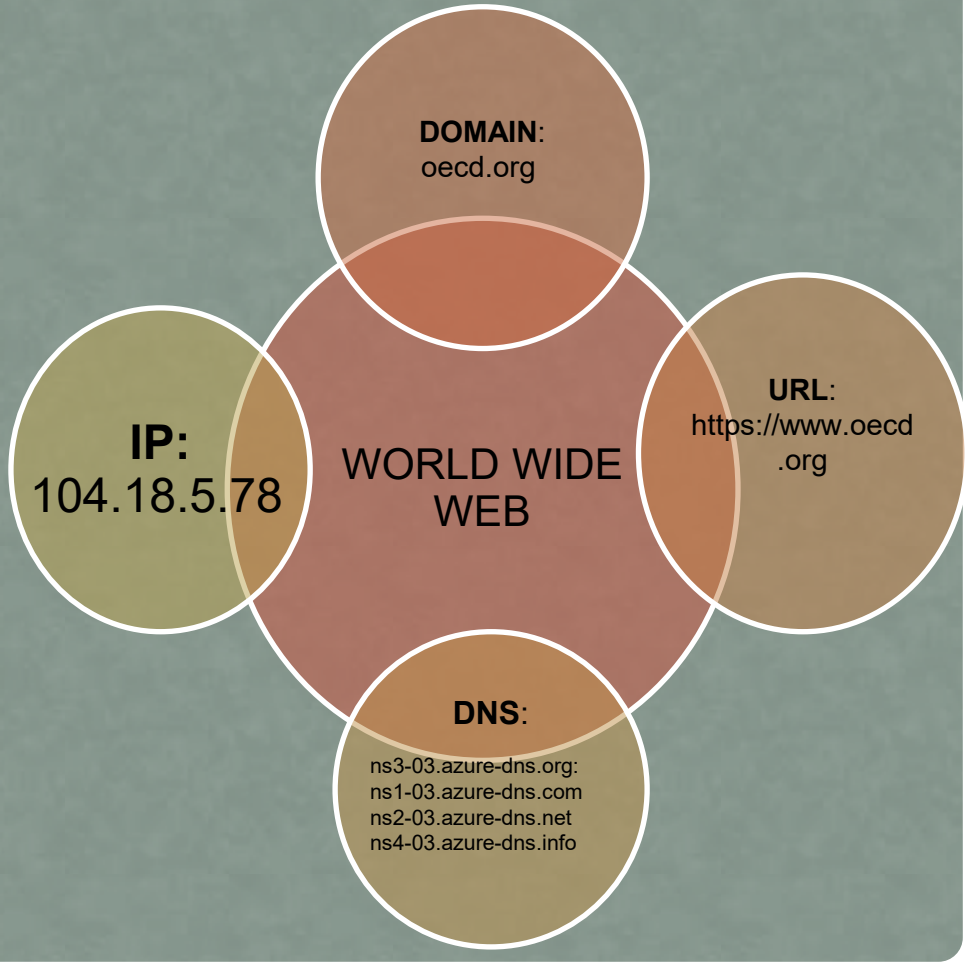
Home > Whois Lookup > Oecd.org

Whois Record for Oecd.org

Domain Profile

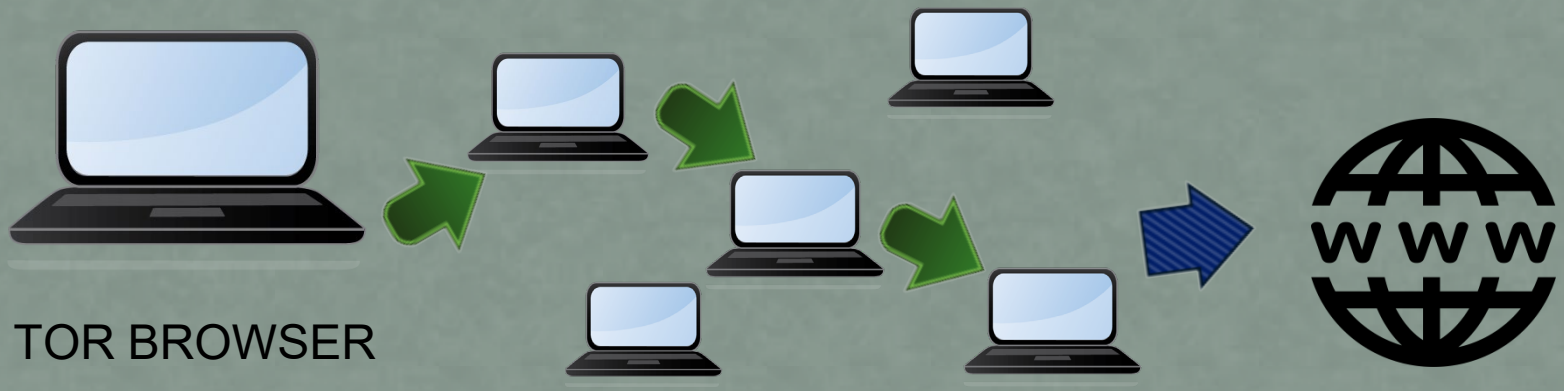
Registrar	Network Solutions, LLC IANA ID: 2 URL: http://www.networksolutions.com Whois Server: whois.networksolutions.com domain.operations@web.com (p) +1.8777228662
Registrar Status	clientTransferProhibited
Dates	10,541 days old Created on 1994-12-13 Expires on 2029-12-12 Updated on 2023-03-23
Name 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)



WEB CONNECTION

PROXY - VPN

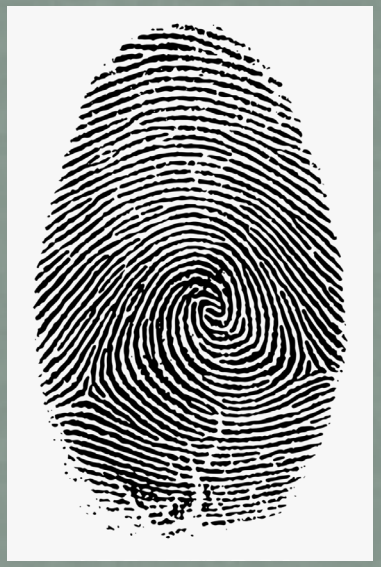


TOR BROWSER

The browser's footprint

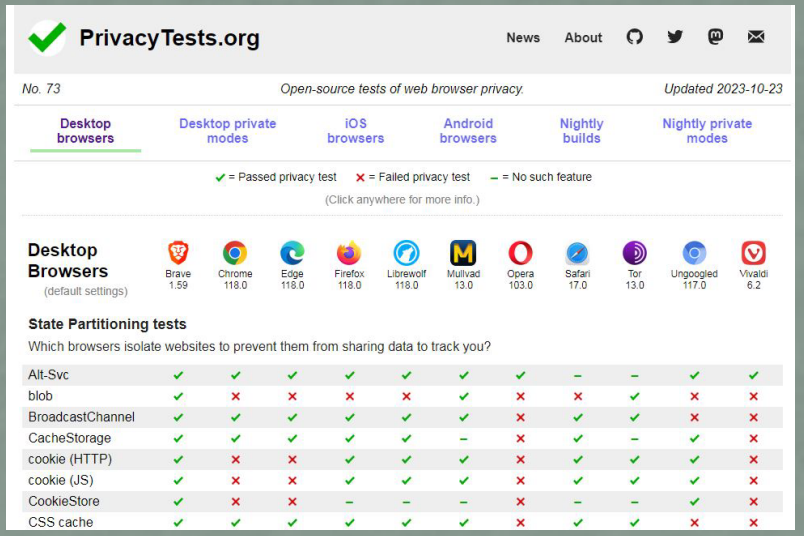
Websites can identify the public IP and perform tracking through cookies.

The information sent by your browser can make it unique and identifiable among millions of Internet users (e.g. browser type, operating system, screen resolution, fonts used).



https://coveryourtracks.eff.org

https://whoer.net/es



PrivacyTests.org

News About

No. 73 — Open-source tests of web browser privacy. — Updated 2023-10-23

Desktop browsers | Desktop private modes | iOS browsers | Android browsers | Nightly builds | Nightly private modes

✓ = Passed privacy test ✗ = Failed privacy test – = No such feature

(Click anywhere for more info.)

Desktop Browsers (default settings)

	Brave 1.59	Chrome 118.0	Edge 118.0	Firefox 118.0	Librewolf 118.0	Mullvad 13.0	Opera 103.0	Safari 17.0	Tor 13.0	Ungoogled 117.0	Vivaldi 6.2
State Partitioning tests											
Which browsers isolate websites to prevent them from sharing data to track you?											
Alt-Svc	✓	✓	✓	✓	✓	✓	✓	–	–	✓	✓
blob	✓	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗
BroadcastChannel	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✗
CacheStorage	✓	✓	✓	✓	✓	–	✗	✓	–	✓	✗
cookie (HTTP)	✓	✗	✗	✓	✓	✓	✗	✓	✓	✓	✗
cookie (JS)	✓	✗	✗	✓	✓	✓	✗	✓	✓	✓	✗
CookieStore	✓	✗	✗	–	–	–	✗	–	–	✓	✗
CSS cache	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✗

Some recommendations before starting an open source investigation on the Internet.