



Guardia Civil

Mando de Apoyo
Jefatura de Servicios Técnicos

Seguridad en las Tecnologías de la Información y la comunicación

Laboratorio de captura de información

ACADEMIA DE INGENIEROS

Capitán GC Jesús
S. Cano Carrillo



Estado de Alarma, 25 de junio de 2020



ACADEMIA DE INGENIEROS





Obtener información abierta

- INTERNET ARCHIVE <http://web.archive.org/>
 - Web durante 20 años
 - Miles de millones de páginas web de millones de sitios web.
 - 510 mil millones de capturas web con marca de tiempo
- PRÁCTICA 1.- ¿Cuándo tenemos evidencias de que existe una web “institutomilitar.com”?
- PRÁCTICA 2.- ¿Cómo era la web del Mº de Defensa, en tiempos del presidente Zapatero y del presidente Rajoy?
- PRÁCTICA 3.- ¿Cómo era la web de Guardia Civil cuando inició su presidencia el presidente Sánchez?





Netcraft

- Servicios de seguridad de Internet: detección e interrupción de delitos cibernéticos, pruebas de aplicaciones y escaneo PCI, cuota de mercado de servidores web, sistemas operativos, proveedores de alojamiento, autoridades de certificación SSL y tecnologías web.
- **Site Report:** <https://sitereport.netcraft.com>
- **Search DNS results:**

<https://sitereport.netcraft.com>

Site report for <https://www.guardiacivil.es>

Background

Site title	Web Oficial de la Guardia Civil	Date first seen
Site rank	169986	Netcraft Risk Rating
Description	PU031241gns Principal Guardia Civil	Primary language

Network

Site	https://www.guardiacivil.es	Domain registrar
Netblock Owner	Akamai International, BV	Nameserver organisation
Domain	guardiacivil.es	Organization
Nameserver	dns.guardiacivil.es	Hosting company
IP address	23.194.197.172	Top Level Domain
DNS admin	dgt-telecomunicaciones-soc@guardiacivil.org	DNS Security Extensions
IPv6 address	Not Present	Hosting country
Reverse DNS	a23-194-197-172.deploy.static.akamaitechnologies.com	

GUARDIA CIVIL 175 AÑOS A TU LADO



Actividades con Netcraft

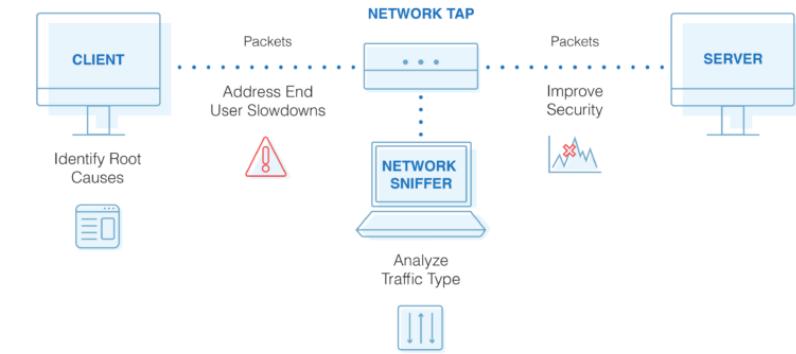
- INFORME 1.- Con institutomilitar.com
- INFORME 2.- Con www.guardiacivil.org
- INFORME 3.- Con alguna web que queráis



Packet Sniffing

- Identificar problemas
- Indagar lentitudes
- Analizar tráficos por tipos (ejemplo, tráfico stun)
- Mejorar anchos de banda
- Mejorar la seguridad (la actividad criminal pasa por la red)

Benefits of Packet Sniffing



FUENTE: dnsstuff.com



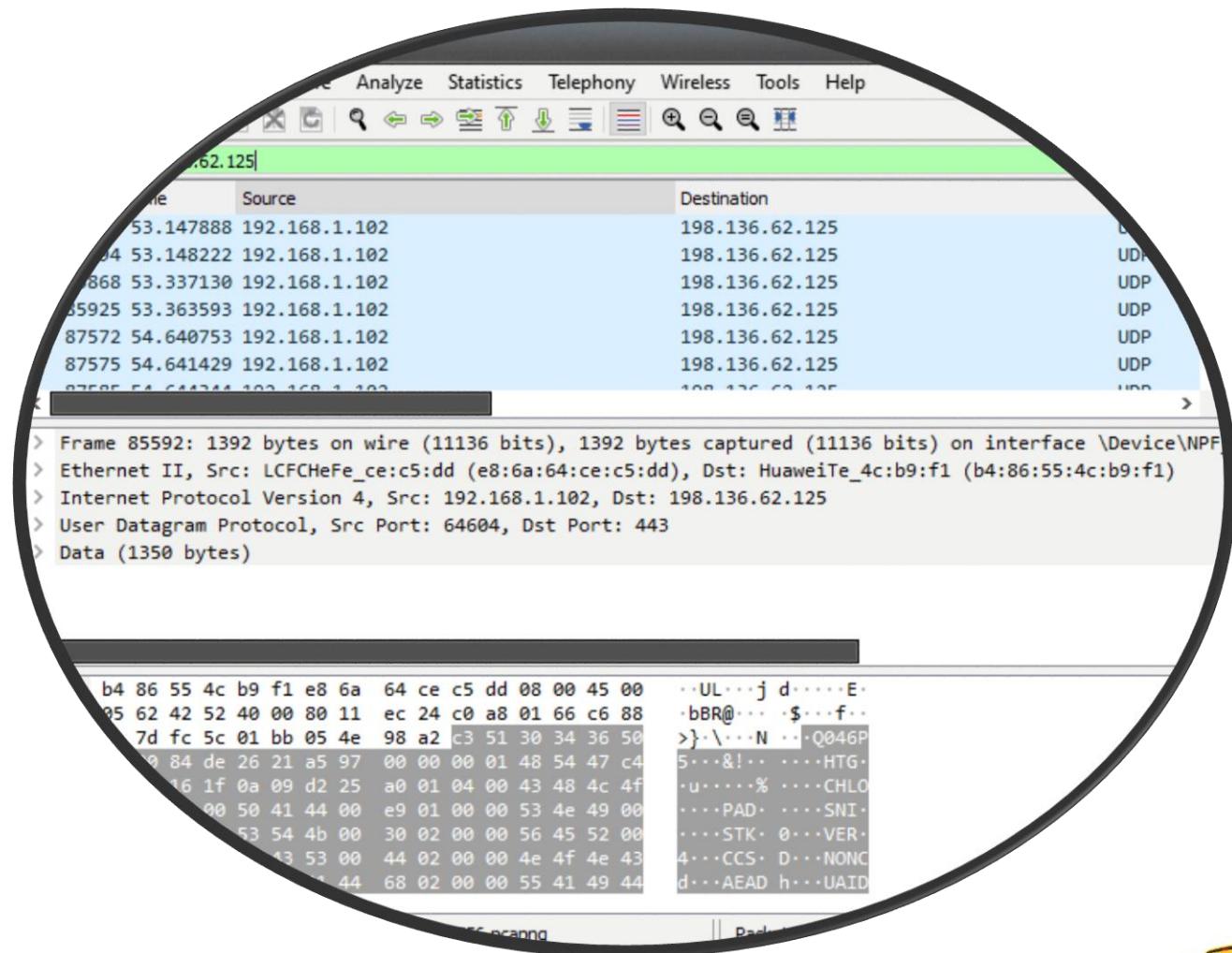
Comparar sniffers

- <https://www.wireshark.org/>
- https://www.paessler.com/packet_capture
- <https://www.manageengine.com/products/netflow/>
- <https://www.liveaction.com/products/omnipeek-network-protocol-analyzer/>
- <https://www.solarwinds.com/network-performance-monitor/use-cases/packet-sniffer?CMP=ORG-BLG-DNS>





Wireshark

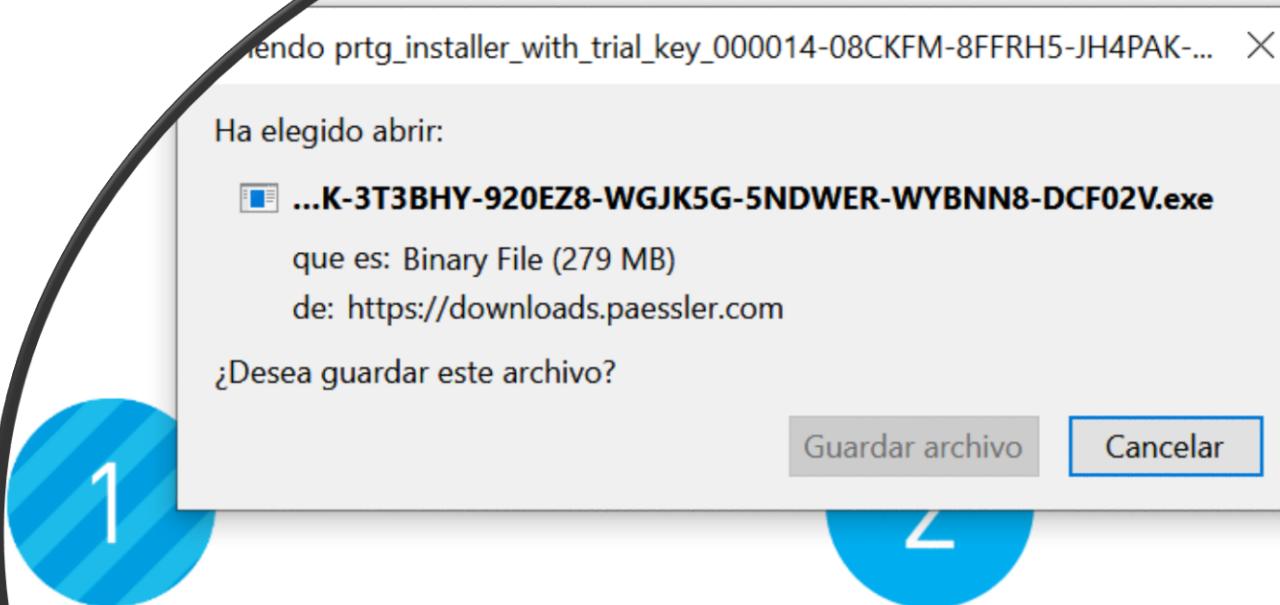




PRTG

000014-08CKFM-8FFRH5-JH4PAK-3T3BHY-920EZ8-WGJK5G-5NDWER-WYBNN8-DCF02V

WIFROS



Started automatically.
Download to finish.

Run the installation.
The license key below is already included in your .exe file.

Need help to get started?
free [webinar](#)

Your license key

000014-08CKFM-8FFRH5-JH4PAK-3T3BHY-920EZ8-WGJK5G-5NDWER-WYBNN8-DCF02V



Central OPs

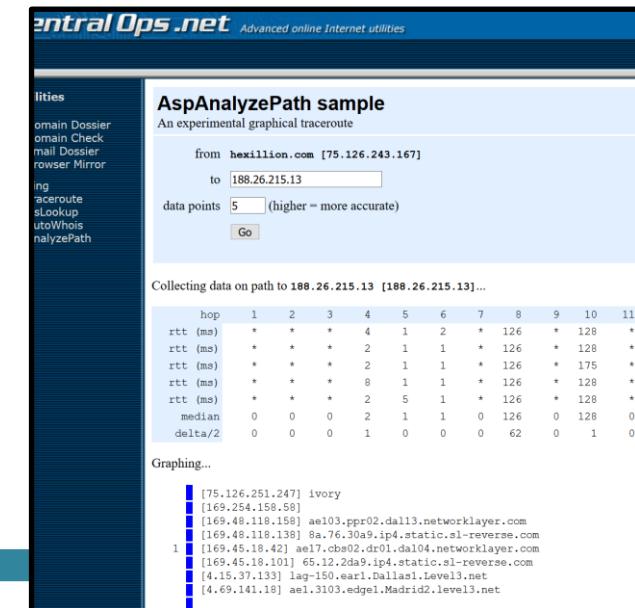
- <https://centralops.net/co/>

The screenshot shows the 'Domain Dossier' tool on the Central Ops.net website. The URL in the address bar is <https://centralops.net/co/>. The main interface is titled 'Domain Dossier' with the sub-instruction 'Investigate domains and IP addresses'. A search bar contains the domain 'institutomilitar.com'. Below the search bar are several checkboxes: 'domain whois record' (checked), 'DNS records' (checked), 'traceroute' (unchecked), 'network whois record' (checked), and 'service scan' (unchecked). A 'go' button is to the right of these checkboxes. Below the search area, it says 'user: anonymous [188.26.215.13]' and 'balance: 49 units'. There are 'log in' and 'account info' links. The 'Central Ops.net' logo is in the bottom right of this section. A message box below the search area asks if the user sees Whois records that are missing contact information, with a link to 'Read about reduced Whois data due to the GDPR'. The 'Address lookup' section shows the canonical name 'institutomilitar.com.', aliases (empty), and addresses '82.223.84.176'. The 'Domain Whois record' section shows the result of a WHOIS query: 'whois.internic.net with "dom institutomilitar.com"' and the text 'INSTITUTOMILITAR.COM'.



Actividades Central Ops

- 1.- Hacer domain checker de nuestra web
- 2.- Investigar sobre un email
- 3.- Qué información está dando nuestro navegador
- 4.- Hacer un pingrado desde el servidor Ops
- 5.- Un trazado de ruta
- 6.- Un whois automático
- 7.- Analizar una ruta de un sitio a otro





Robtex!

- Fuentes para recopilar información pública sobre IP, nombres de dominio, nombres de host, sistemas autónomos, rutas, etc. en una gran base de datos de acceso gratuito.
- www.robtex.com



What is Robtex used for?

Robtex is used for various kinds of research of IP numbers, Domain names, etc

Are you a normal IT guy doing data forensics, investigating competitors, tracking spammers or hackers or a virus, or just

What does Robtex do?

Robtex uses various sources to gather public information about IP numbers, domain names, host names, Autonomous sys access to the data.

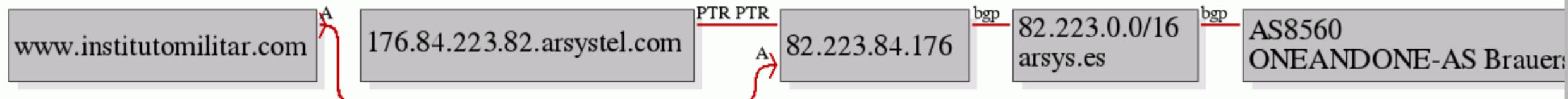
We aim to make the fastest and most comprehensive free DNS lookup tool on the Internet.

Our database now contains billions of documents of internet data collected over more than a decade.

GRAPH(old)



Static graph over the entity and related entities





Capitán GC Jesús S.
Cano Carrillo

ACADEMIA DE INGENIEROS

Laboratorio de captura

