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


jaja que suerte
Tengo mi Antivirus !!

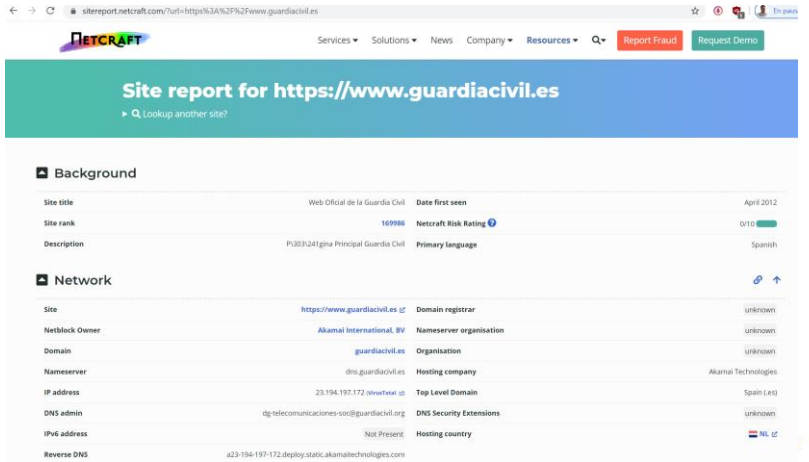
Obtener información abierta

- 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**:

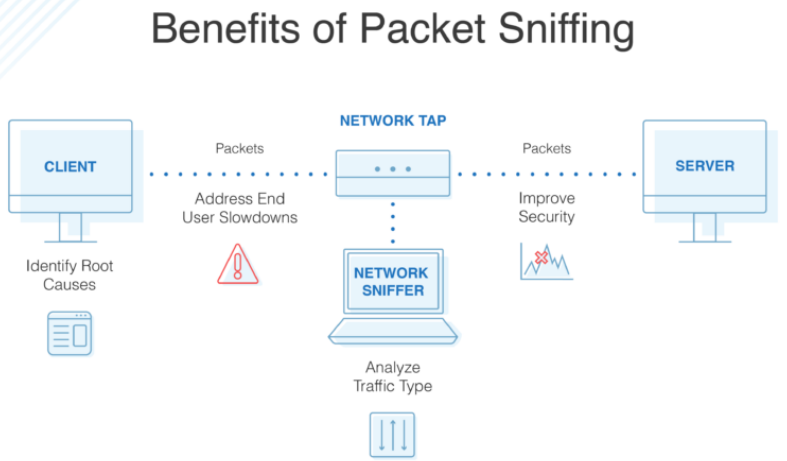
https://sitereport.netcraft.com



Actividades con Netcraft

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

Packet Sniffing



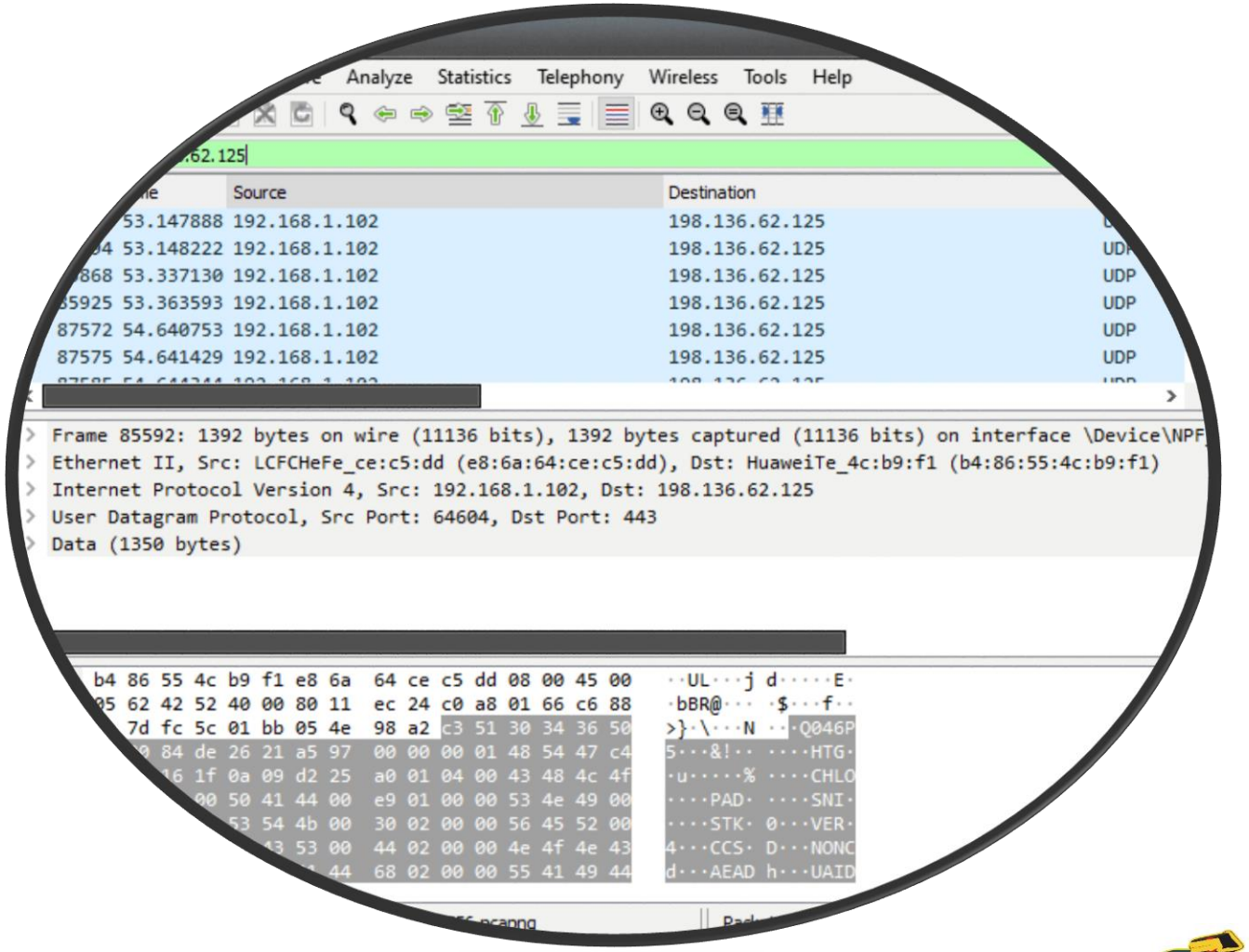
FUENTE: dnsstuff.com

- 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)

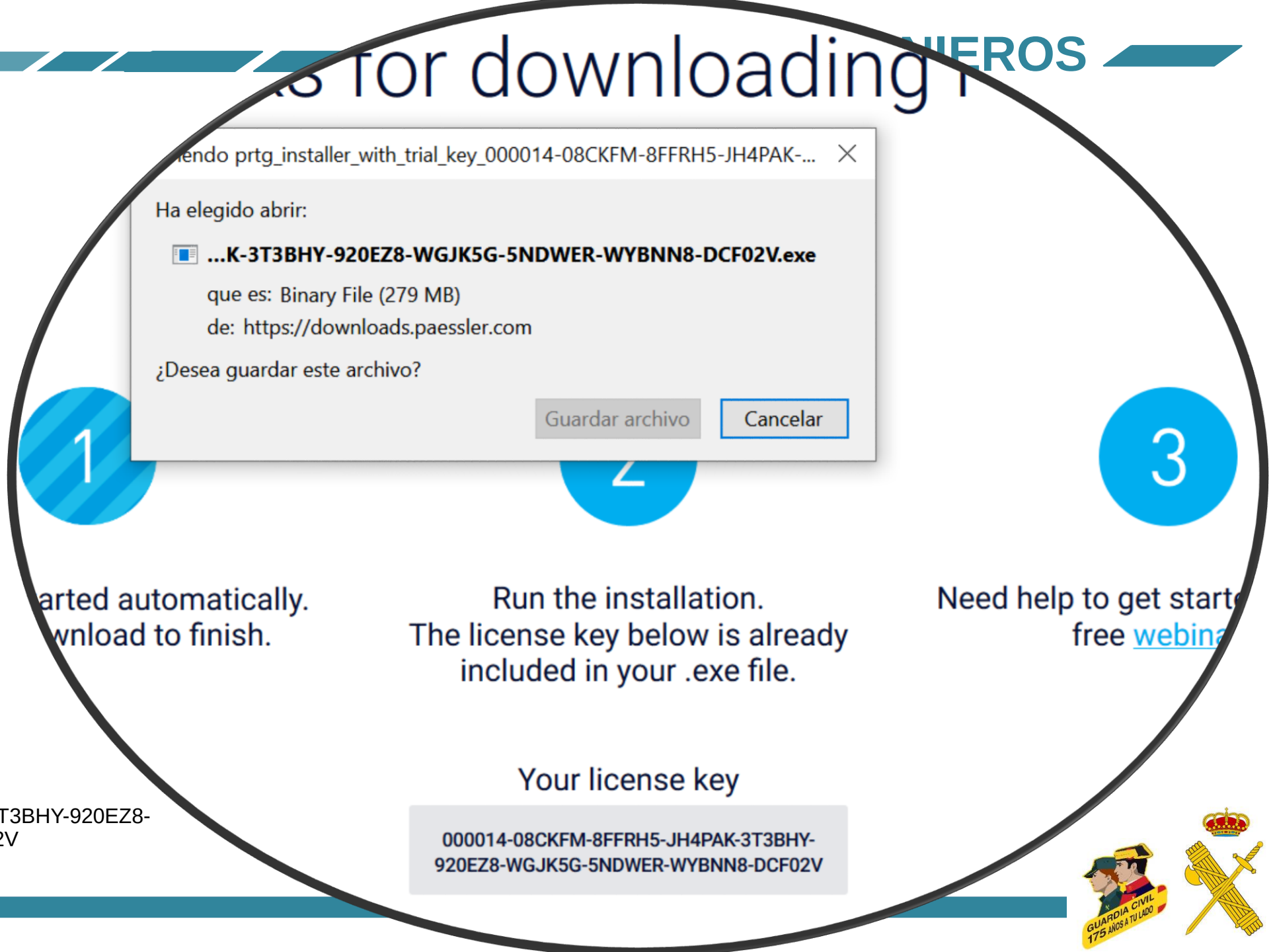
Comparar sniffers

- 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


Analyze Statistics Telephony Wireless Tools Help
Source Destination
53.147888 192.168.1.102 198.136.62.125
53.148222 192.168.1.102 198.136.62.125 UDP
53.337130 192.168.1.102 198.136.62.125 UDP
53.363593 192.168.1.102 198.136.62.125 UDP
54.640753 192.168.1.102 198.136.62.125 UDP
54.641429 192.168.1.102 198.136.62.125 UDP
Frame 85592: 1392 bytes on wire (11136 bits), 1392 bytes captured (11136 bits) on interface \Device\NPF
Ethernet II, Src: LCFCHeFe_ce:c5:dd (e8:6a:64:ce:c5:dd), Dst: HuaweiTe_4c:b9:f1 (b4:86:55:4c:b9:f1)
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 198.136.62.125
User Datagram Protocol, Src Port: 64604, Dst Port: 443
Data (1350 bytes)

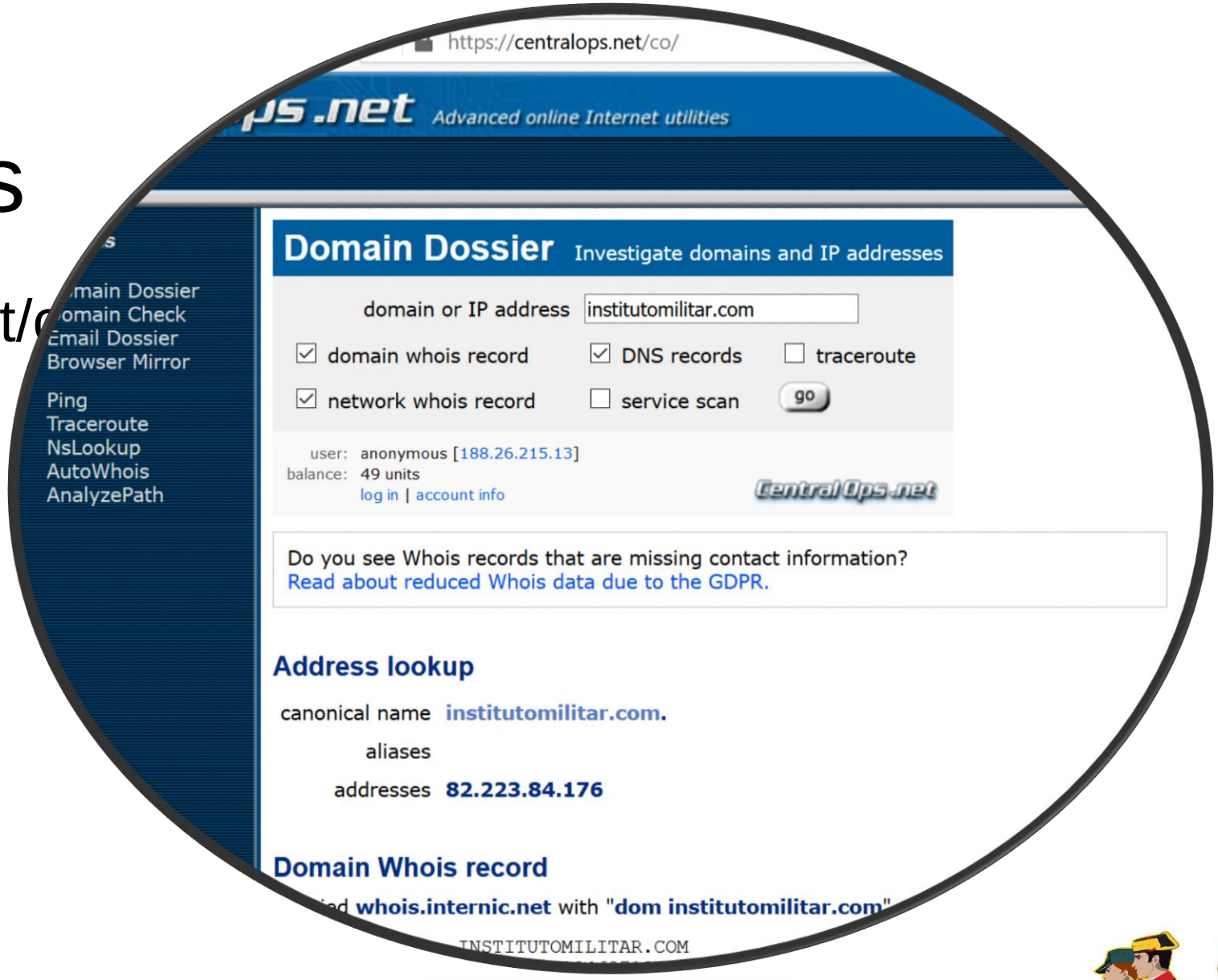
PRTG



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

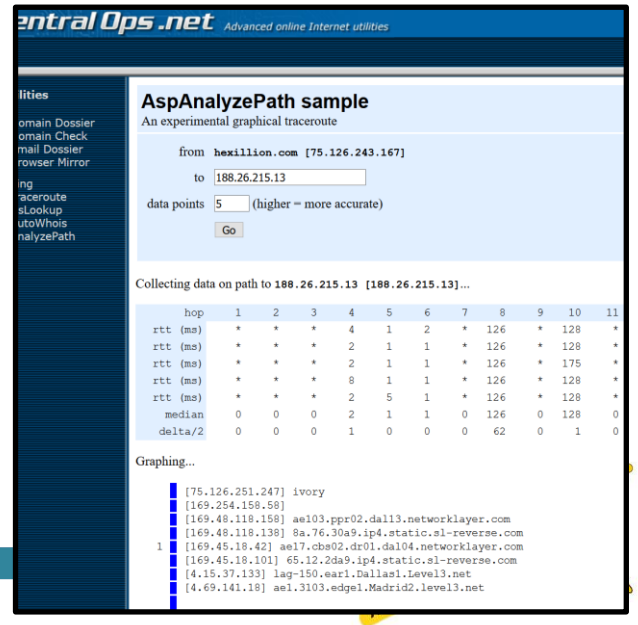
Central OPs

- https://centralops.net/c

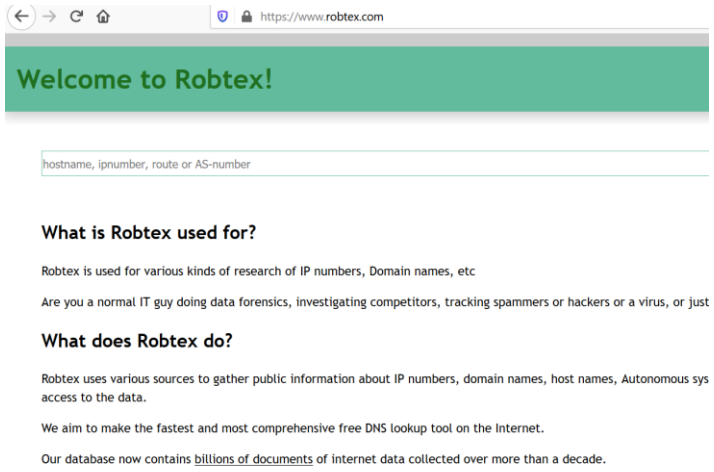


Actividades Central Ops

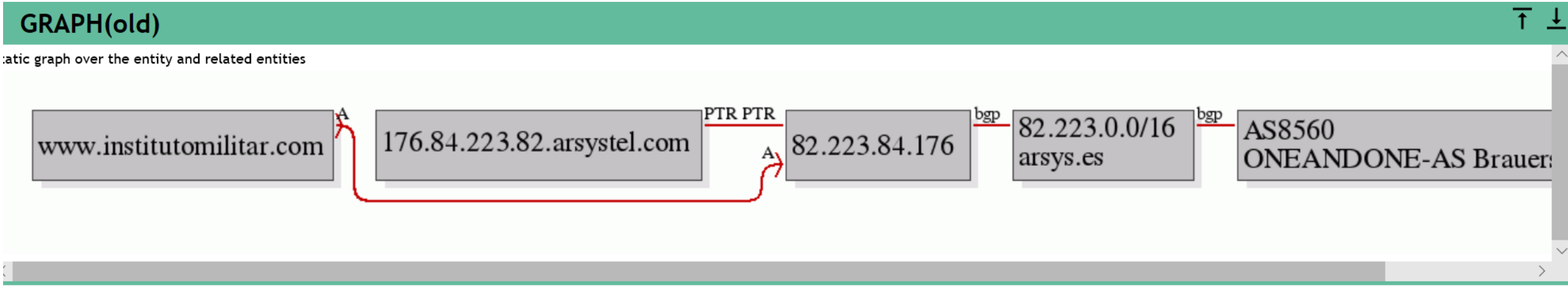
- 1.- Hacer domain checker de nuestra web
- 2.- Investigar sobre un email
- 3.- Qué información está dando nuestro navegador
- 4.- Hacer un pingeado desde el servidor Ops
- 5.- Un trazado de ruta
- 6.- Un whois automático
- 7.- Analizar una ruta de un sitio a otro



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



ACADEMIA DE INGENIEROS

Laboratorio de captura

Capitán GC Jesús S. Cano Carrillo