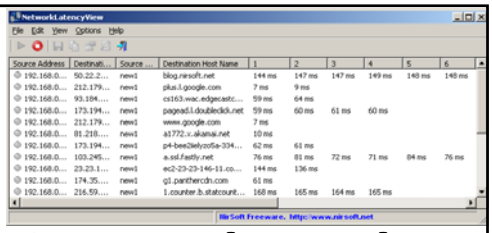


Monitorización de conexiones de red TCP en Windows con NirSoft – NetworkLatencyView y herramientas complementarias

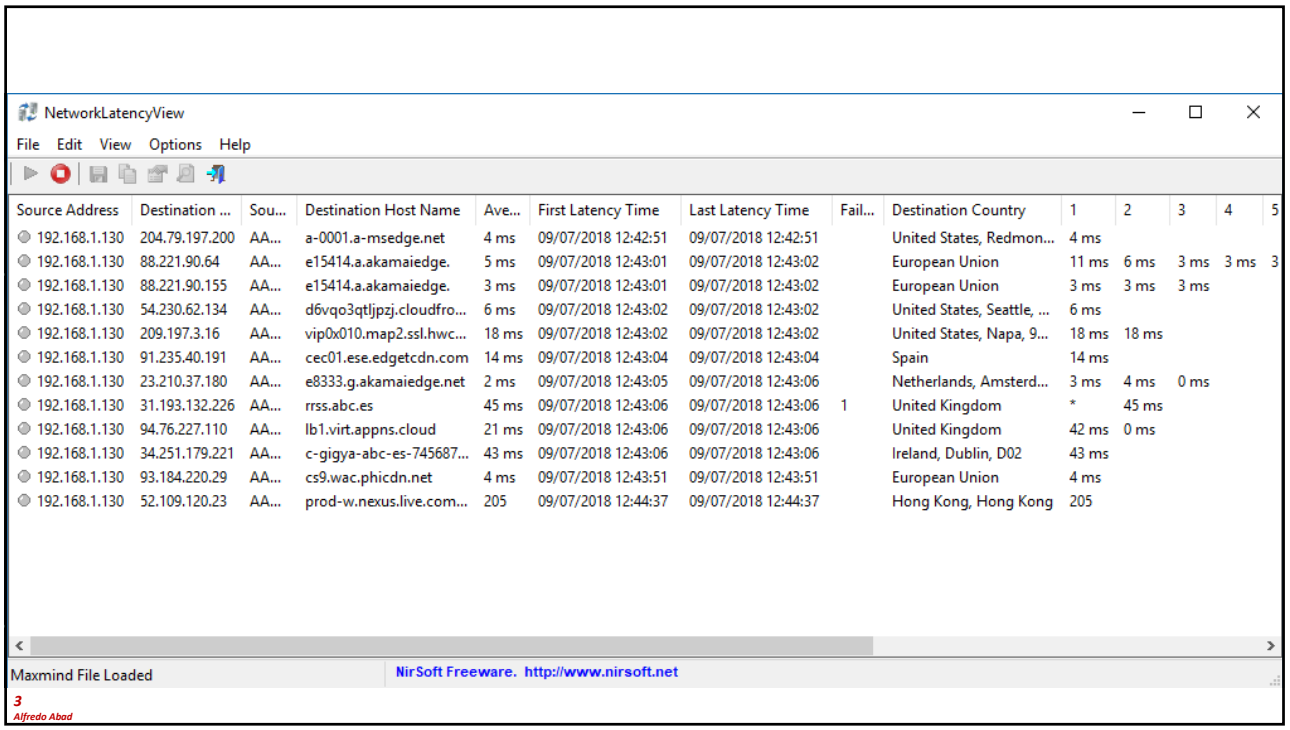
PARP203_NetworkLatencyView.pptx

Alfredo Abad

UA: 9-ago-2018

NetworkLatencyView de NirSoft

- NetworkLatencyView es una herramienta sencilla para Windows que escucha las conexiones TCP en su sistema y calcula la latencia de la red (en milisegundos) por cada conexión TCP detectada en su sistema
  - Para cada dirección IP, NetworkLatencyView muestra hasta 10 valores de latencia de red y su promedio
  - El valor de latencia calculado por NetworkLatencyView es muy similar al resultado que obtiene al hacer ping a la misma dirección IP
- NetworkLatencyView también le permite exportar fácilmente la información de latencia al archivo text / csv / tab-delimited / html / xml, o copiar la información al portapapeles y luego pegarla en Excel u otra aplicación



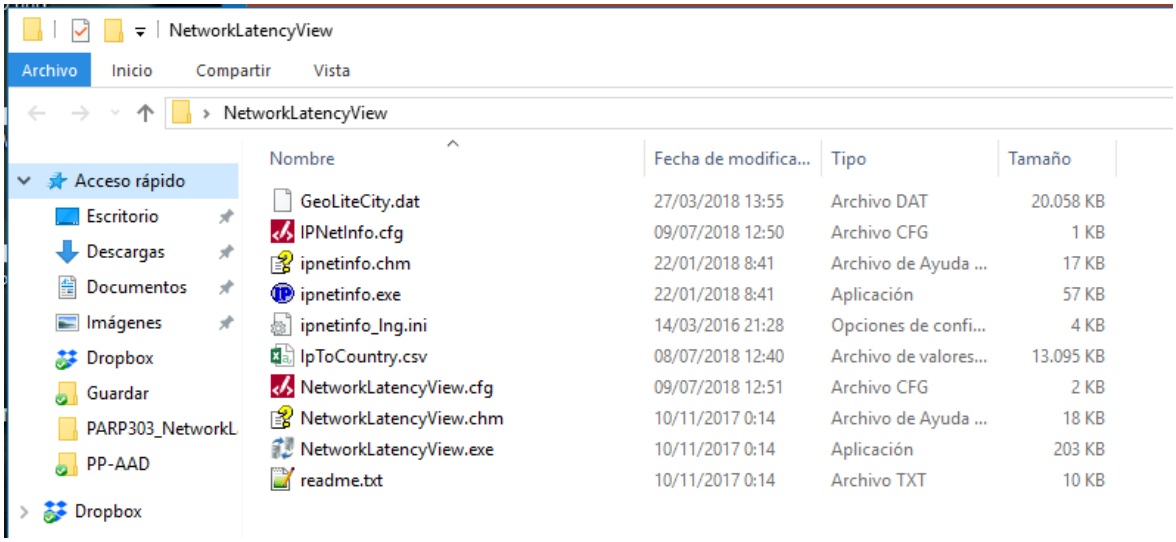
3
Alfredo Abad

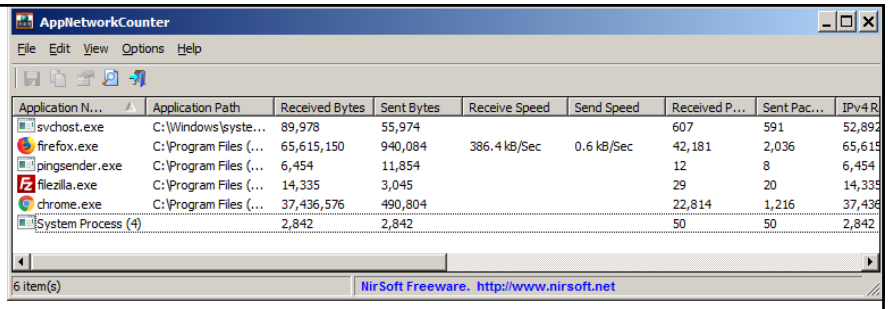
Procedimiento

- Seguir las instrucciones de la página oficial de NetworkLatencyView
  - https://www.nirsoft.net/utils/network_latency_view.html
- Descargar, como se recomienda, las aplicaciones complementarias IPNetInfo, así como las bases de datos de geolocalización
  - http://software77.net/geo-ip/
  - https://dev.maxmind.com/geoip/legacy/geolite/
- Recuerda que debes ejecutar la aplicación con cuenta de administración
- Descarga las librerías WinPcap o instala NetworkMonitor para poder hacer una captura de tráfico
- Navega por diversos lugares, ensayando las diversas opciones de la aplicación: visualizar latencias, exportar resultados, ver geolocalizaciones, filtrados por puertos, etc.

4
Alfredo Abad

Vista del directorio de instalación de aplicaciones





AppNetworkCounter (aplicación complementaria)

https://www.redeszone.net/2018/04/22/appnetworkcounter-medir-trafico-aplicaicones/

http://www.nirsoft.net/utils/app_network_counter.html

AppNetworkCounter es una aplicación gratuita para Windows creada para permitirnos tener el control sobre el uso que hacen las aplicaciones que tenemos instaladas en nuestro ordenador de la red. Gracias a esta herramienta vamos a poder ver, en tiempo real, el ancho de banda que está utilizando cada aplicación y proceso de nuestro ordenador conectado a Internet, además de los bytes y paquetes que las aplicaciones envían a través de los protocolos TCP y UDP y todos los paquetes IPv4 e IPv6 generados por estos procesos.

Para entregar

- Procedimiento de instalación del escenario
- Ejecución sin captura a fichero
- Ejecución con captura en modo promiscuo (WinPcap o similar)
- Filtrado de puertos
- Investigación de geolocalización y de las compañías involucradas en las páginas web que visites
- Exportación de resultados