

Source Address	Destination	Source	Destination Host Name	1	2	3	4	5	6
192.168.0...	50.22.2...	newt	blog.nirsoft.net	144 ms	147 ms	147 ms	149 ms	148 ms	148 ms
192.168.0...	212.179...	newt	plus.google.com	7 ms	9 ms				
192.168.0...	93.184...	newt	cs131.msc.edgeware...	59 ms	64 ms				
192.168.0...	173.194...	newt	pagespeed.l.google.com	59 ms	60 ms	61 ms	60 ms		
192.168.0...	212.179...	newt	www.google.com	7 ms					
192.168.0...	81.218...	newt	at772-x.akama.net	10 ms					
192.168.0...	173.194...	newt	ph-bw2w01c01a-394...	62 ms	61 ms				
192.168.0...	103.245...	newt	a.saf.Fastly.net	76 ms	81 ms	72 ms	71 ms	84 ms	76 ms
192.168.0...	23.23.1...	newt	ec2-23-23-146-11.co...	144 ms	136 ms				
192.168.0...	174.35...	newt	g2.dnethrds.com	61 ms					
192.168.0...	216.59...	newt	l.counter-0.statcount...	168 ms	165 ms	164 ms	165 ms		

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

PARP203\_NetworkLatencyView.pptx

Alfredo Abad

UA: 9-ago-2018

1

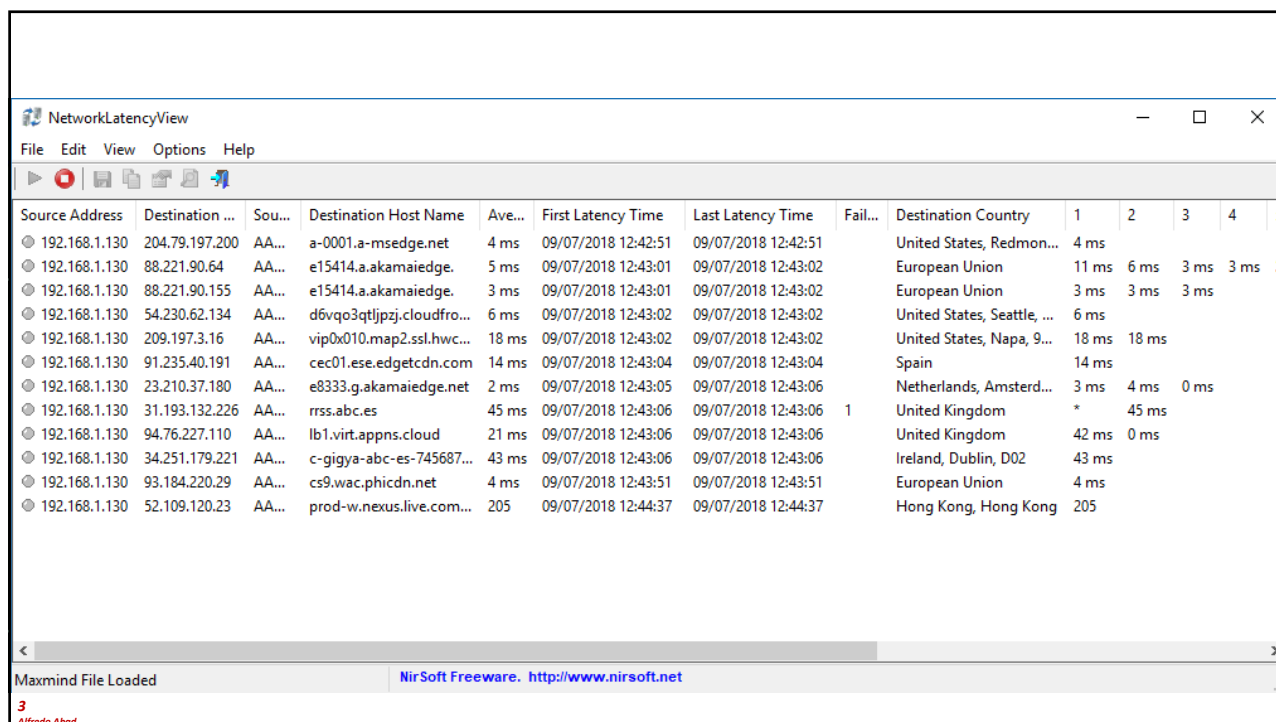
Alfredo Abad

## 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

2

Alfredo Abad



NetworkLatencyView

File Edit View Options Help

Source Address	Destination ...	Sou...	Destination Host Name	Ave...	First Latency Time	Last Latency Time	Fail...	Destination Country	1	2	3	4	5
192.168.1.130	204.79.197.200	AA...	a-0001.a-msedge.net	4 ms	09/07/2018 12:42:51	09/07/2018 12:42:51		United States, Redmon...	4 ms				
192.168.1.130	88.221.90.64	AA...	e15414.a.akamaiedge.	5 ms	09/07/2018 12:43:01	09/07/2018 12:43:02		European Union	11 ms	6 ms	3 ms	3 ms	3
192.168.1.130	88.221.90.155	AA...	e15414.a.akamaiedge.	3 ms	09/07/2018 12:43:01	09/07/2018 12:43:02		European Union	3 ms	3 ms	3 ms		
192.168.1.130	54.230.62.134	AA...	d6vqo3qtijpzj.cloudfro...	6 ms	09/07/2018 12:43:02	09/07/2018 12:43:02		United States, Seattle, ...	6 ms				
192.168.1.130	209.197.3.16	AA...	vip0x010.map2.ssl.hwc...	18 ms	09/07/2018 12:43:02	09/07/2018 12:43:02		United States, Napa, 9...	18 ms	18 ms			
192.168.1.130	91.235.40.191	AA...	cec01.es.edgetcdn.com	14 ms	09/07/2018 12:43:04	09/07/2018 12:43:04		Spain	14 ms				
192.168.1.130	23.210.37.180	AA...	e8333.g.akamaiedge.net	2 ms	09/07/2018 12:43:05	09/07/2018 12:43:06		Netherlands, Amsterd...	3 ms	4 ms	0 ms		
192.168.1.130	31.193.132.226	AA...	rrss.abc.es	45 ms	09/07/2018 12:43:06	09/07/2018 12:43:06	1	United Kingdom	*	45 ms			
192.168.1.130	94.76.227.110	AA...	lb1.virt.appns.cloud	21 ms	09/07/2018 12:43:06	09/07/2018 12:43:06		United Kingdom	42 ms	0 ms			
192.168.1.130	34.251.179.221	AA...	c-gigya-abc-es-745687...	43 ms	09/07/2018 12:43:06	09/07/2018 12:43:06		Ireland, Dublin, D02	43 ms				
192.168.1.130	93.184.220.29	AA...	cs9.wac.phicdn.net	4 ms	09/07/2018 12:43:51	09/07/2018 12:43:51		European Union	4 ms				
192.168.1.130	52.109.120.23	AA...	prod-w.nexus.live.com...	205	09/07/2018 12:44:37	09/07/2018 12:44:37		Hong Kong, Hong Kong	205				

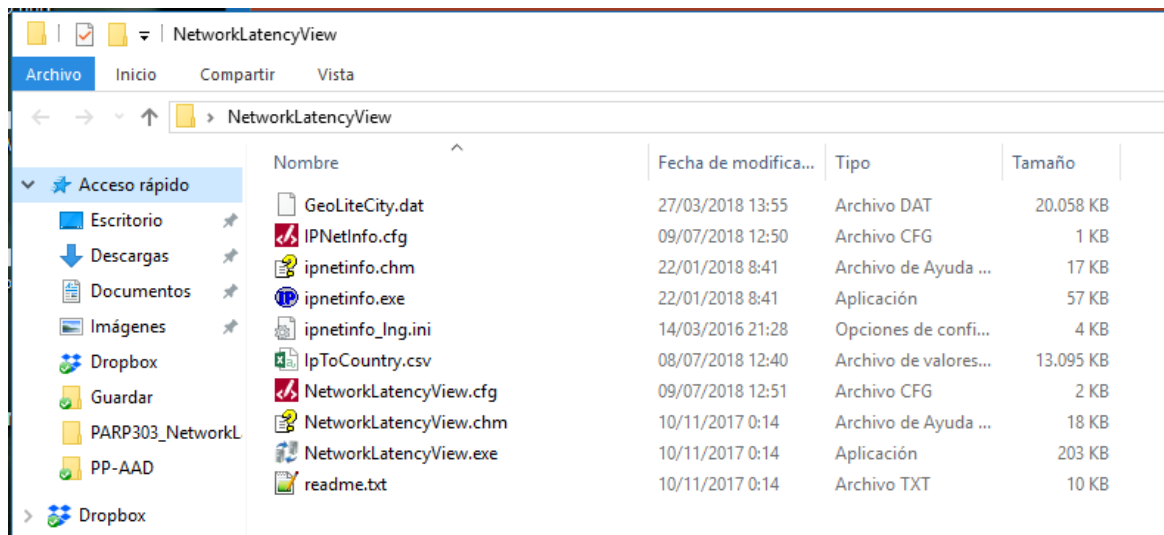
Maxmind File Loaded NirSoft Freeware. <http://www.nirsoft.net>

3  
Alfredo Abad

## Procedimiento

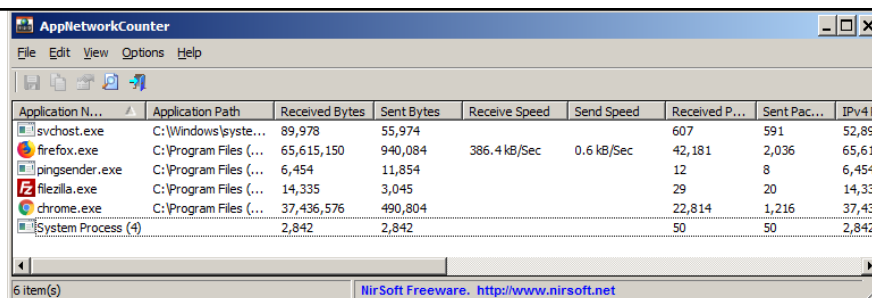
- Seguir las instrucciones de la página oficial de NetworkLatencyView
  - [https://www.nirsoft.net/utils/network\\_latency\\_view.html](https://www.nirsoft.net/utils/network_latency_view.html)
- Descargar, como se recomienda, las aplicaciones complementarias IPNetInfo, así como las bases de datos de 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.

## Vista del directorio de instalación de aplicaciones



5

Alfredo Abad



## AppNetworkCounter (aplicación complementaria)

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

[http://www.nirsoft.net/utills/app\\_network\\_counter.html](http://www.nirsoft.net/utills/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.

6

Alfredo Abad

## 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