

Source Address	Destination Address	Source Port	Destination Port	Host Name	1	2	3	4	5	6
192.168.0...	50.22.2...	new1	blog.nirsoft.net		144 ms	147 ms	147 ms	149 ms	148 ms	148 ms
192.168.0...	212.179...	new1	plus1.google.com		7 ms	9 ms				
192.168.0...	192.168.0...	new1	cctv13.cctvgo.com		59 ms	64 ms				
192.168.0...	173.194...	new1	gutenberg.libsyn.com		69 ms	60 ms	61 ms	60 ms		
192.168.0...	212.179...	new1	www.google.com		7 ms					
192.168.0...	81.218...	new1	al772.v.akamai.net		10 ms					
192.168.0...	173.194...	new1	pr-bee2wlyzofse-324...		62 ms	61 ms				
192.168.0...	103.246...	new1	a-sd.fasty.net		76 ms	81 ms	72 ms	71 ms	84 ms	76 ms
192.168.0...	29.23.1...	new1	ec02-29-146-11.co...		144 ms					
192.168.0...	174.35...	new1	gl.pancreatic.com		61 ms					
192.168.0...	216.59...	new1	1.counter.b.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

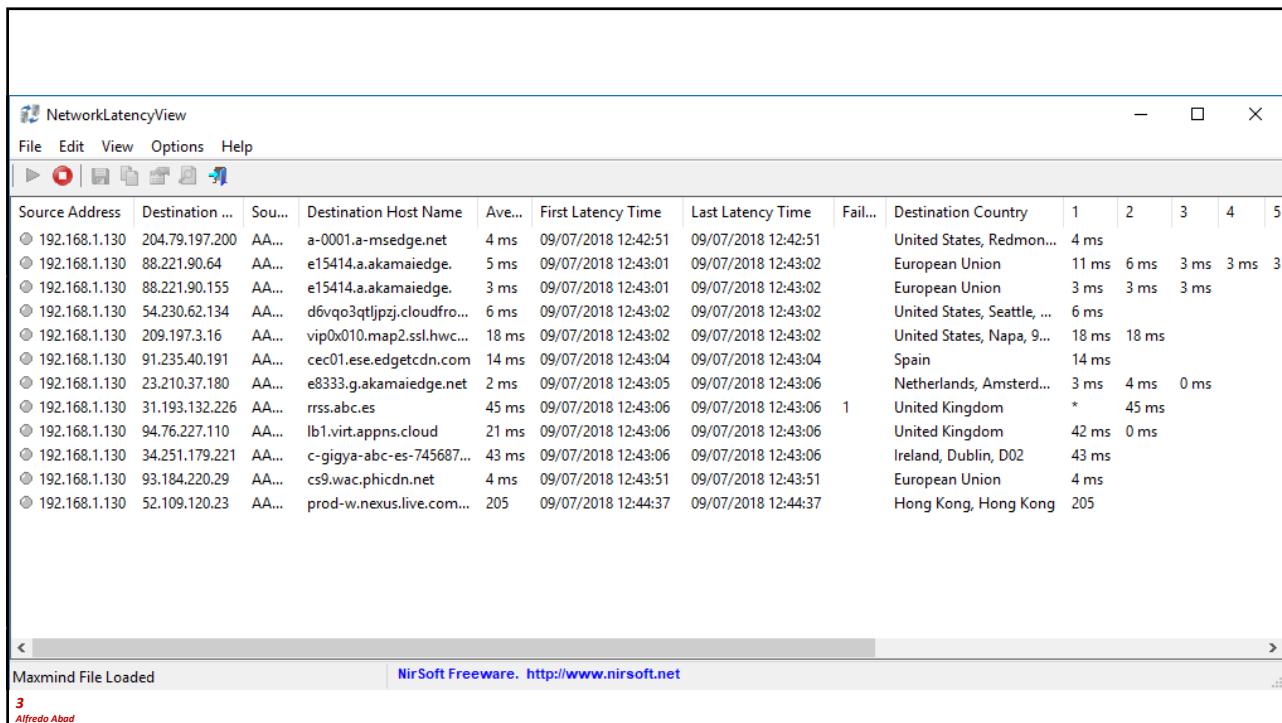
UA: 9-agosto-2018

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



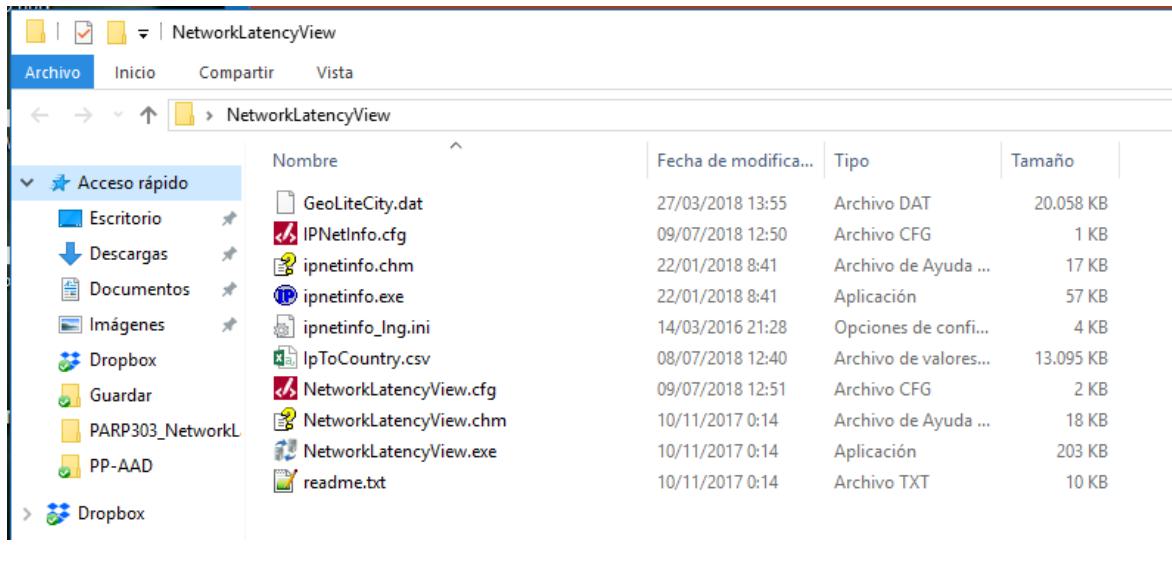
The screenshot shows the NetworkLatencyView application window. The main pane displays a table of network traffic data with the following columns: Source Address, Destination IP, Destination Port, Sou..., Destination Host Name, Ave..., First Latency Time, Last Latency Time, Fail..., Destination Country, and five columns for latency values (1, 2, 3, 4, 5). Below the table, there are navigation arrows and status messages: 'Maxmind File Loaded' and 'NirSoft Freeware. <http://www.nirsoft.net>'.

Source Address	Destination IP	Destination Port	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...		d6vqo3qtjlpzj.cloudfr...	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.ese.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, Amsterda...	3 ms	4 ms	0 ms		
192.168.1.130	31.193.132.226	AA...		rss.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				

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.

Vista del directorio de instalación de aplicaciones

5
Alfredo Abad

AppNetworkCounter									
Application N...	Application Path	Received Bytes	Sent Bytes	Receive Speed	Send Speed	Received P...	Sent Pac...	IPv4 R...	
svchost.exe	C:\Windows\system...	89,978	55,974			607	591	52,892	
firefox.exe	C:\Program Files (...)	65,615,150	940,084	386.4 kB/Sec	0.6 kB/Sec	42,181	2,036	65,615	
pingsender.exe	C:\Program Files (...)	6,454	11,854			12	8	6,454	
filezilla.exe	C:\Program Files (...)	14,335	3,045			29	20	14,335	
chrome.exe	C:\Program Files (...)	37,436,576	490,804			22,814	1,216	37,436	
System Process (4)		2,842	2,842			50	50	2,842	

AppNetworkCounter (aplicación complementaria)

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

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.

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