

Herramientas de escaneo de red en Windows: Network Manager y NETworkManager

<https://sourceforge.net/projects/sortbytenm/>
<https://github.com/BornToBeRoot/NETworkManager>

PARP304-Tools-NETworkManager.pptx

Alfredo Abad

UA:9-jul-2018

1

Alfredo Abad

Premisas y procedimiento

- Se trata de estudiar las posibilidades de dos herramientas portables para Windows (de nombre similar, pero distintas): Network Manager y NETworkManager
 - (No confundir con NetworkManager de los sistemas Linux)
 - Puedes empezar a leer por aquí:
<https://www.redeszona.net/2018/06/23/networkmanager-herramienta-redes-windows/>
- Procedimiento:
 - Descárgalas
 - Instálalas sobre un sistema Windows
 - Ejecútalas y estudia todas sus posibilidades
- Haz un mapa mental con todas las posibilidades que presenta cada una de las herramientas

2

Alfredo Abad

Network Manager (I)

Network Manager

Wi-Fi

Local IP: 192.168.1.130
Public IP: 188.78.233.231
Download: 120 B
Upload: 637 B
960 b
4.98 Kb

2.11 GB

Total: 133 MB

Control Panel

Tools Settings Help

IPv4 IPv6

Wi-Fi

Property	Value	Value
Address IP & Mask	192.168.1.130	255.255.255.0
Gateway IP & Metric	192.168.1.1	0
DNS Server	192.168.1.1	
DHCP Enabled	IP & DNS	
DHCP Server	192.168.1.1	
NetBIOS over TCP/IP	DHCP Enabled	
MTU	1500	

Interface tools

Adapter GUID: B200F3CB-505A-4CB5-B1ED-A045787A2882
Description: Qualcomm Atheros AR5006X Wireless Network
Type: Wireless IEEE 802.11
Interface Index: 14
MAC Address: 00:1B:9E:A1:C8:EC
Interface Metric: 55

Download: 0 B
Upload: 0 B
0 b
0 b

Lowest IPv4 metrics

Gateway Metric: 0
Route Metric: 55

2.11 GB

Total: 133 MB

Public IPv4: 188.78.233.231
Public IPv6: No global IP

NetworkManagerWIN

Archivo Inicio Compartir Vista

NetworkManagerWIN

Nombre	Fecha de modifica...	Tipo	Tamaño
Launcher.exe	25/06/2018 21:55	Aplicación	365 KB
License.txt	14/08/2015 2:26	Archivo TXT	17 KB
Network_Manager.log	09/07/2018 17:17	Documento de tex	1 KB
Network_Manager_x64.exe	25/06/2018 21:55	Aplicación	3.837 KB
Network_Manager_x86.exe	25/06/2018 21:55	Aplicación	3.846 KB

3

Alfredo Abad

Network Manager (II)

IP Sessions

All connected processes

svchost.exe (920)
(4)
Dropbox.exe (7816)
KMSSSS.exe (2384)
svchost.exe (1372)
NvBackend.exe (5372)
(0)
wininit.exe (544)
svchost.exe (372)
svchost.exe (880)
spoolsv.exe (1888)
lsass.exe (684)
services.exe (636)
Telegram.exe (7448)
SearchUI.exe (7896)
firefox.exe (6008)
firefox.exe (4728)
firefox.exe (6716)
firefox.exe (4628)
firefox.exe (3404)
firefox.exe (5356)
Network_Manager_x64.exe (8860)
POWERPNT.EXE (1708)
svchost.exe (3368)
dasHost.exe (3200)
svchost.exe (1632)

Process	Local Address	Local Port	Remote Address	Remote Port	Protocol	State
svchost.exe (920)	0.0.0.0	135	0.0.0.0	0	TCP	Listen
(4)	192.168.1.130	139	0.0.0.0	0	TCP	Listen
Dropbox.exe (7816)	127.0.0.1	843	0.0.0.0	0	TCP	Listen
KMSSSS.exe (2384)	0.0.0.0	1688	0.0.0.0	0	TCP	Listen
svchost.exe (1372)	0.0.0.0	5040	0.0.0.0	0	TCP	Listen
Dropbox.exe (7816)	0.0.0.0	17500	0.0.0.0	0	TCP	Listen
Dropbox.exe (7816)	127.0.0.1	17600	0.0.0.0	0	TCP	Listen
NvBackend.exe (5372)	127.0.0.1	23408	0.0.0.0	0	TCP	Listen
(0)	127.0.0.1	23408	127.0.0.1	61652	TCP	Time wai
(0)	127.0.0.1	23408	127.0.0.1	61655	TCP	Time wai
(0)	127.0.0.1	23408	127.0.0.1	61651	TCP	Time wai
(0)	127.0.0.1	23408	127.0.0.1	61654	TCP	Time wai
(0)	127.0.0.1	23408	127.0.0.1	61653	TCP	Time wai
(0)	127.0.0.1	23408	127.0.0.1	61656	TCP	Time wai
(0)	127.0.0.1	23408	127.0.0.1	61650	TCP	Time wai
(0)	127.0.0.1	23408	127.0.0.1	61657	TCP	Time wai
wininit.exe (544)	0.0.0.0	49664	0.0.0.0	0	TCP	Listen
svchost.exe (372)	0.0.0.0	49665	0.0.0.0	0	TCP	Listen
svchost.exe (880)	0.0.0.0	49666	0.0.0.0	0	TCP	Listen
spoolsv.exe (1888)	0.0.0.0	49667	0.0.0.0	0	TCP	Listen
lsass.exe (684)	0.0.0.0	49668	0.0.0.0	0	TCP	Listen
services.exe (636)	0.0.0.0	49669	0.0.0.0	0	TCP	Listen
svchost.exe (372)	192.168.1.130	59544	13.92.209.232	443	TCP	Establish
Telegram.exe (7448)	192.168.1.130	59562	149.154.167.51	443	TCP	Establish
Dropbox.exe (7816)	127.0.0.1	59664	127.0.0.1	59665	TCP	Establish

[Process path]

☐ Detect remote UDP IPs and ports

☐ Resolve IP

☐ Get bytes

Route remote IP

Copy remote IP end point

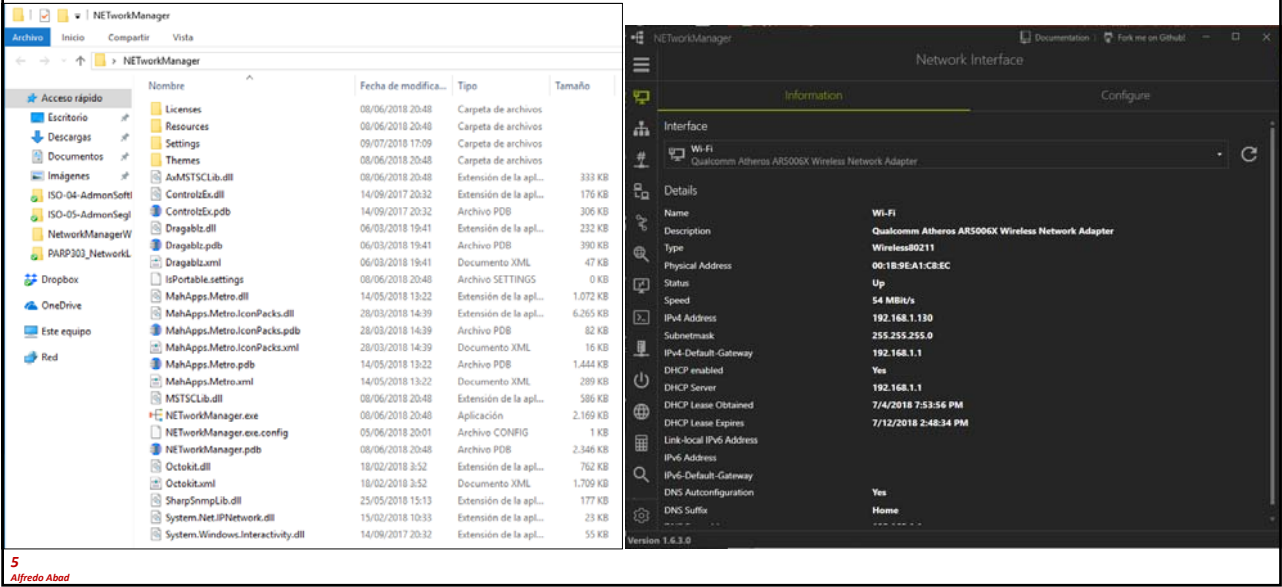
Show IPv4 Sessions Only

TCP & UDP

4

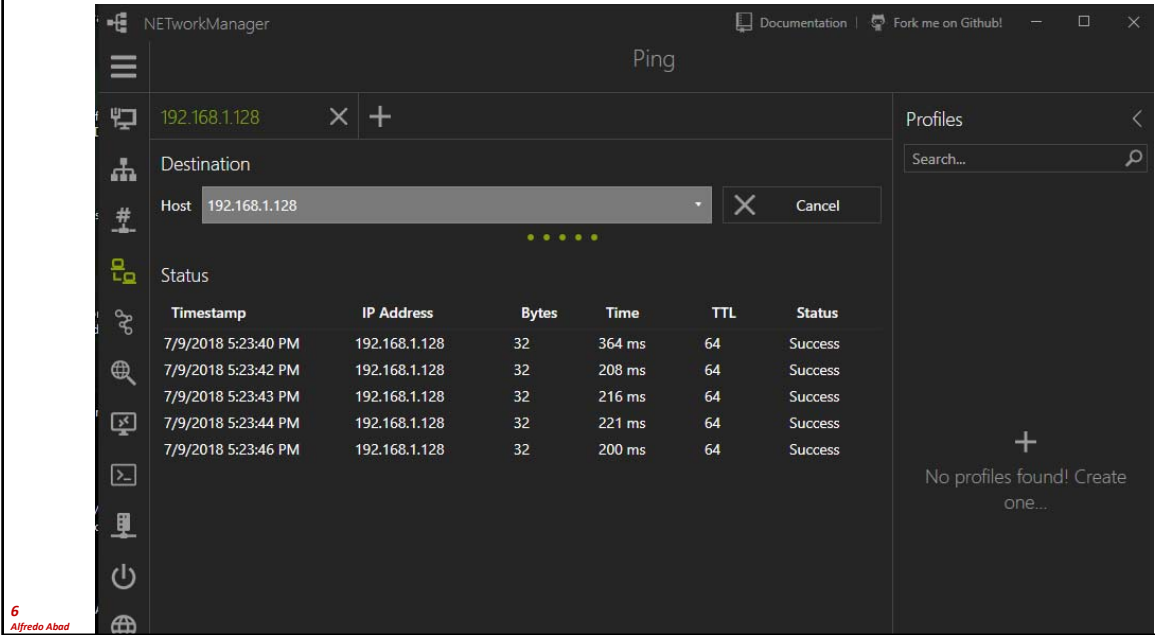
Alfredo Abad

NETworkManager (I)



5
Alfredo Abad

NETworkManager (II)



6
Alfredo Abad

