

MiTeC Network Scanner

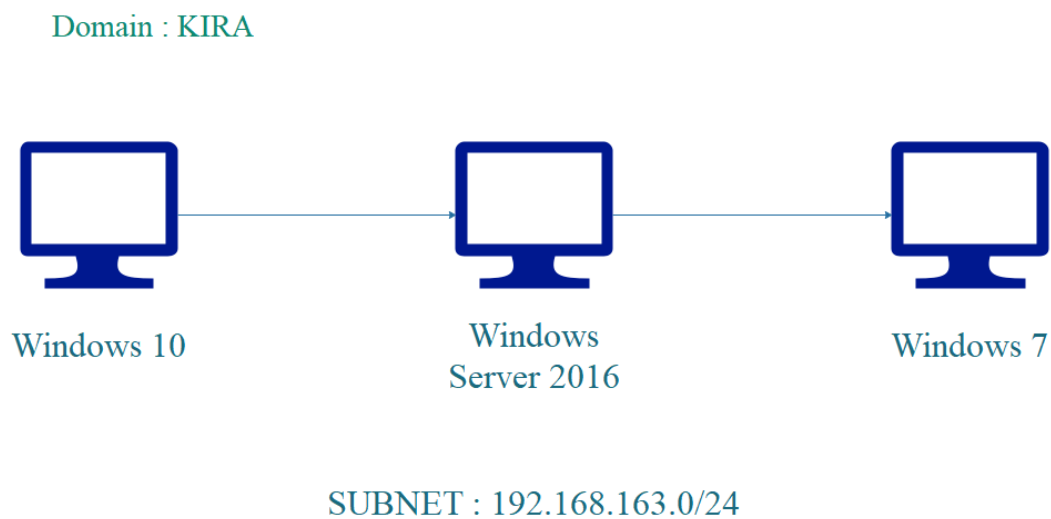
Giới Thiệu

Đây là 1 công cụ để quét ICMP, Port, IP, NetBIOS, ActiveDirectory và SNMP đa luồng miễn phí với nhiều tính năng nâng cao. Nó dành cho cả quản trị viên hệ thống và người dùng phổ thông quan tâm đến bảo mật máy tính. Chương trình thực hiện quét ping, quét các cổng TCP và UDP đã mở, chia sẻ tài nguyên và dịch vụ.

Các Tính Năng Quét

- ActiveDirectory
- Network neighbourhood
- Ping (ICMP)
- IP Address
- MAC Address (even across routers)
- MAC Vendor
- Device name
- Device domain/workgroup
- Logged user
- Operating system
- BIOS, Model and CPU
- System time and Up time
- Device description
- Type flags (SQL server, Domain controller etc.)
- Remote device date and time
- TCP and UDP port scanning
- SNMP services.
- Installed services on device
- Shared resources
- Sessions
- Open Files
- Running processes
- Terminal sessions
- Event Log
- Installed software
- SAM accounts
- WMI Queries
- Powerful Whols client

<https://www.mitec.cz/netscan.html>



Giới thiệu

Domain: KIRA

Đảm bảo các máy phải ping được đến Windows 10 (Máy Tính Scanner) và các máy phải join domain

Máy Windows Server 2016 : Domain Controller (192.168.163.133)

Windows 7 : Client (192.168.163.130)

Windows 10: Máy tính Scanner (192.168.163.137)

Mục Tiêu

- Lấy info hardware , os , software
- Lấy info các partition trên máy

Lấy info hardware, OS , software

```
Administrator: C:\Windows\system32\cmd.exe

C:\Users\administrator>ping 192.168.163.130

Pinging 192.168.163.130 with 32 bytes of data:
Reply from 192.168.163.130: bytes=32 time<1ms TTL=128
Reply from 192.168.163.130: bytes=32 time<1ms TTL=128
Reply from 192.168.163.130: bytes=32 time<1ms TTL=128
Reply from 192.168.163.130: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.163.130:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

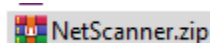
C:\Users\administrator>ping 192.168.163.133

Pinging 192.168.163.133 with 32 bytes of data:
Reply from 192.168.163.133: bytes=32 time<1ms TTL=128
Reply from 192.168.163.133: bytes=32 time<1ms TTL=128
Reply from 192.168.163.133: bytes=32 time<1ms TTL=128
Reply from 192.168.163.133: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.163.133:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms



C:\Users\administrator>
```

Đầu tiên phải đảm bảo máy scanner ping được đến các máy trong domain

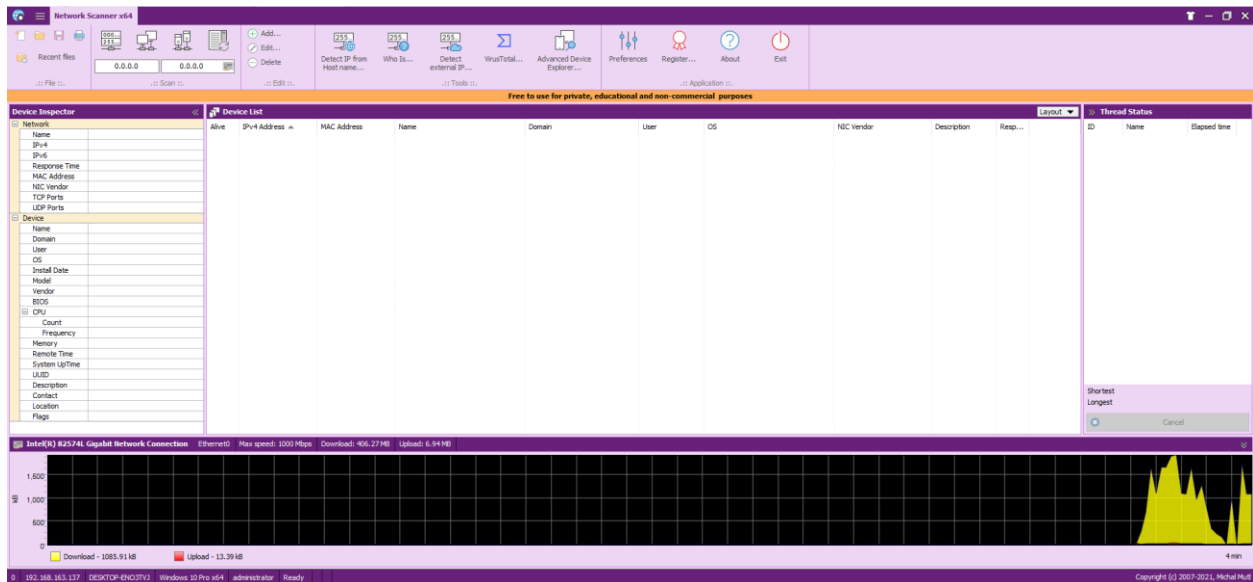


<https://www.mitec.cz/Downloads/NetScanner.zip>

Sau khi tải tool về ta sẽ có định dạng file nén như thế này

Name	Date modified	Type	Size
 NetScanner	3/6/2021 6:47 PM	Application	4,077 KB
 NetScanner64	3/6/2021 6:47 PM	Application	5,212 KB

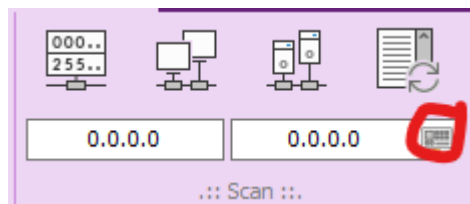
Sau khi giải nén xong mình có 2 File 1 là dành cho máy tính chạy 32 bit (NetScanner)và 1 là dành cho máy tính chạy 64 bit (NetScanner64) . Mở chương trình phù hợp với máy tính của mình



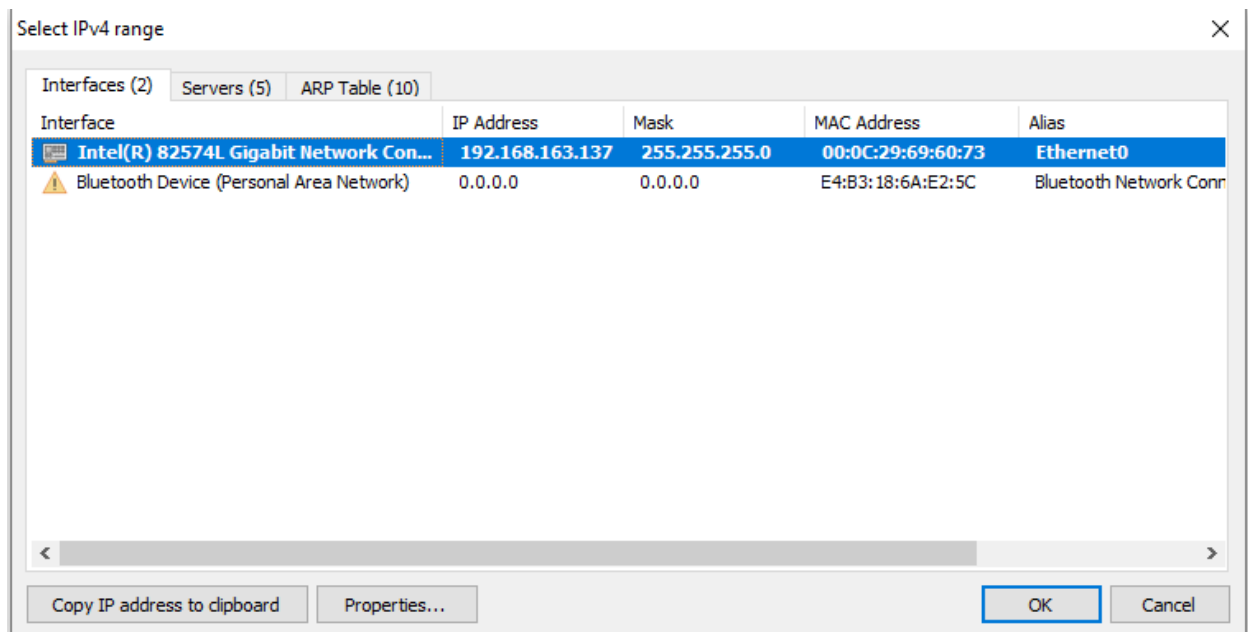
Sau khi mở lên chúng ta có giao diện như thế này

Chúng ta có 1 giao diện vô cùng trực quan và có cả lưu lượng mạng đang sử dụng trên cổng được show ra với dạng đồ thị màu vàng bên dưới

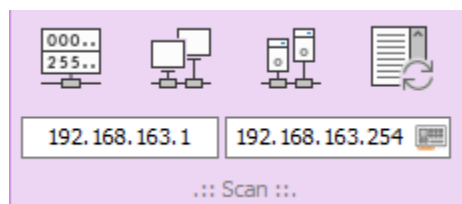
Đầu tiên ta sẽ chọn card mạng để từ card mạng này ta sẽ lấy được thông tin lớp mạng cần quét



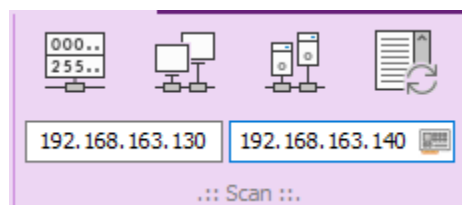
Đầu tiên chọn card mạng bằng cách bấm vào icon như hình trên



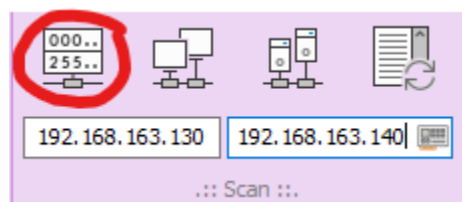
Mình sẽ chọn card mạng đang kết nối đến hệ thống mạng ở đây là Intel 82574L Gigabit Network. Sau đó bấm OK



Lúc này toàn bộ ip trong lớp mạng đã được vào ô Scan . Ở bài lab này mình chỉ dùng 3 con máy để test nên mình sẽ giới hạn lại lớp mạng cho quá trình quét được nhanh hơn



Mình chọn dãy ip cần thiết với nhu cầu của mình



Sau đó bấm vào icon này để quét hệ thống mạng

Device List (3)										Thread Status (11)		
Alive	IPv4 Address	MAC Address	Name	Domain	User	OS	NIC Vendor	Description	Resp...	ID	Name	Elapsed time
	192.168.163.130	00-0C-29-CD-0D-55	KMA-PC	KIRA	Administrator	Windows 7	VMware Inc.		ICM...	1	192.168.163.130	00:00:00
	192.168.163.133	00-0C-29-43-BE-09	WIN-DG7C3SPFRVS	KIRA	Administrator	Windows 10	VMware Inc.		ICM...	2	192.168.163.131	00:00:08
	192.168.163.137	00-0C-29-69-60-73	DESKTOP-ENO3TVJ.kira.com	KIRA	Administrator	Windows 10	VMware Inc.		ICM...	3	192.168.163.132	00:00:08

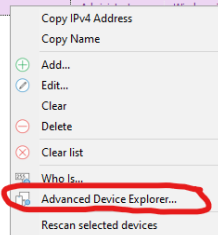
Alive	IPv4 Address	MAC Address	Name	Domain	User	OS	NIC Vendor	Description	Resp...
	192.168.163.130	00-0C-29-CD-0D-55	KMA-PC	KIRA	Administrator	Windows 7	VMware Inc.		ICM...
	192.168.163.133	00-0C-29-43-BE-09	WIN-DG7C3SPFRVS	KIRA	Administrator	Windows Server 2016 Datacenter	VMware Inc.		ICM...
	192.168.163.137	00-0C-29-69-60-73	DESKTOP-ENO3TVJ.kira.com	KIRA	Administrator	Windows 10	VMware Inc.		ICM...

Ở bên phải là dãy ip mình đã quét thì những máy tính khả dụng sẽ được hiện tick xanh lá cây

Sau khi quét xong thì ta đã quét được 3 máy trong hệ thống mạng này ta sẽ có những thông tin như địa chỉ ip của máy tính , Name của máy tính , Domain , User đang login vào máy tính đó

Chúng ta thử xem thông tin thử của máy tính windows 7

	192.168.163.130	00-0C-29-CD-0D-55	KMA-PC	KIRA	Administrator	Windows 7	VMware Inc.		ARP...
	192.168.163.133	00-0C-29-43-BE-09	WIN-DG7C3SPFRVS	KIRA	Administrator	Windows Server 2016 Datacenter	VMware Inc.		ICM...
	192.168.163.137	00-0C-29-69-60-73	DESKTOP-ENO3TVJ.kira.com	KIRA	Administrator	Windows 10	VMware Inc.		ICM...



Chọn máy tính muốn show thông tin và chuột phải vào chọn Advanced Device Explorer

Advanced Device Explorer

KMA-PC 192.168.163.130

Username: Password: Login Logoff

Dashboard

Network

Name	KMA-PC
IPv4	192.168.163.130
IPv6	
Response Time	ARP: 0 ms
MAC Address	00-0C-29-CD-0D-55
NIC Vendor	VMware Inc.
TCP Ports	
UDP Ports	

Device

Name	KMA-PC
Domain	KIRA
User	Administrator
OS	Windows 7
Install Date	
Model	
Vendor	
BIOS	

CPU

Count	
Frequency	

Remote Shutdown... Remote Execute... Wake on LAN Refresh

Ping Status - 0 ms

ms 1.0 0.8 0.6 0.4 0.2 0.0

2 min

Export data...

Lúc này ta đã thấy được những thông tin sơ sơ về máy tính windows 7 . Để có thể show hết các thông tin của máy tính windows 7 chúng ta cần đăng nhập bằng User Administrator của domain (Hoặc nếu quản trị viên không cho ta tài khoản User Administrator thì họ chỉ cần tạo cho ta 1 User thuộc group Admin cũng được)

192.168.163.130

Username: Password: Login Logoff

Dashboard

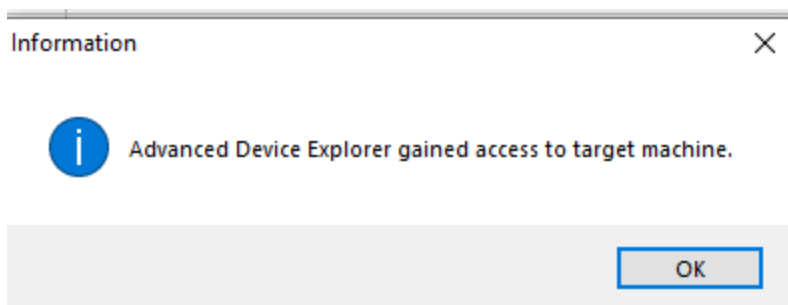
Chúng ta tiến hành đăng nhập User Administrator và để lấy thông tin máy

192.168.163.130

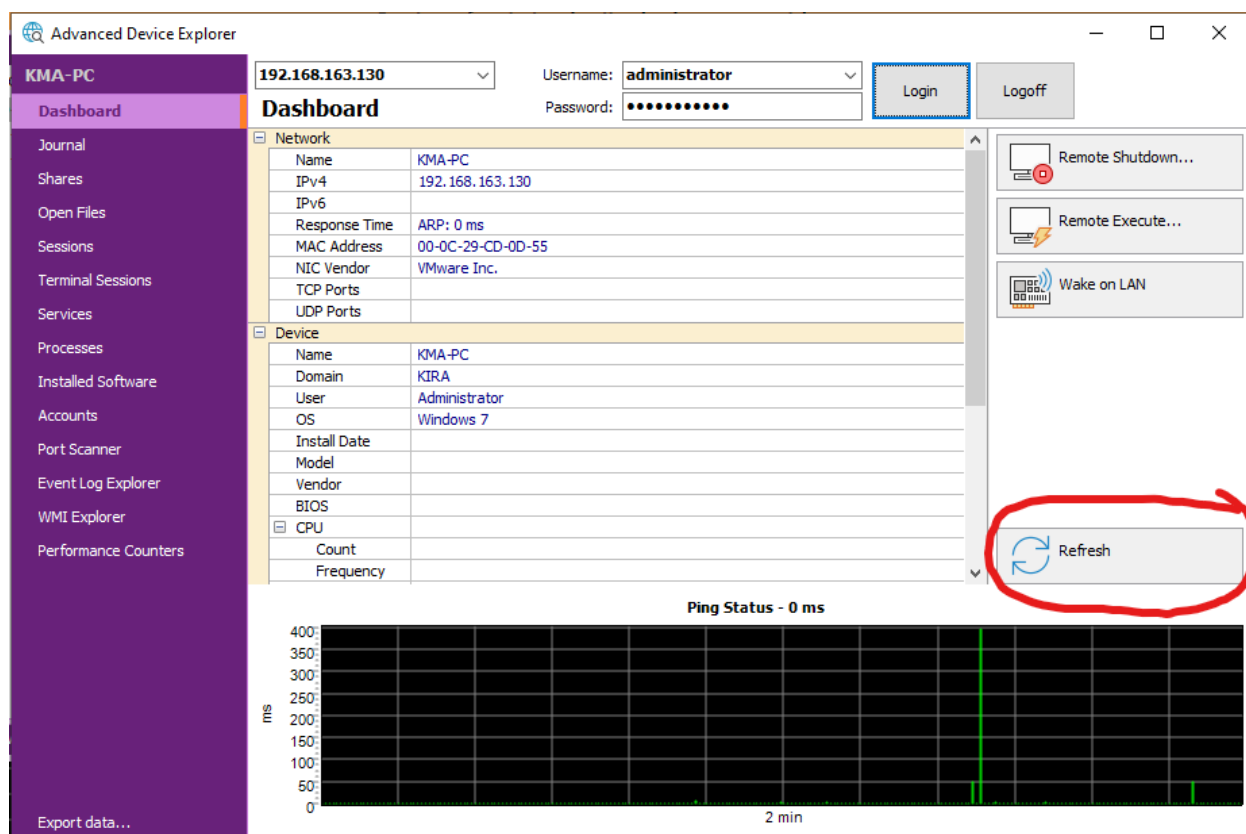
Username: administrator Password: Login Logoff

Dashboard

Sau đó bấm Login



Ta sẽ nhận được thông báo rằng đã có thể truy cập đến máy tính cần lấy thông tin và bấm OK



Sau đó bấm Refresh để cập nhập thông tin

Device	
Name	KMA-PC
Domain	KIRA
User	Administrator
OS	Windows 7
Install Date	8/25/2021 6:15:59 AM
Model	VMware Virtual Platform
Vendor	VMware, Inc.
BIOS	PhoenixBIOS 4.0 Release 6.0 INTEL - 6040000
CPU	Intel Core i7-5700HQ 2.70GHz
Count	1
Frequency	2693 MHz
Memory	2048 MB
Remote Time	11/29/2021 9:26:28 PM
System UpTime	00:46:00
UUID	22BB4D56-9714-B901-45BD-9993D2CD0D55
Description	
Contact	
Location	
Flags	WORKSTATION,SERVER,NT,POTENTIAL_BROWSER,MASTER_BROWSER
Server	WORKSTATION

Ping Status - 0 ms

Lúc này ta đã có thông tin về máy tính windows 7 như Name,Domain, OS đang sử dụng , Máy tính này được tạo ra vào ngày mấy , thông tin BIOS . CPU , RAM , v.v.v

Tiếp đến ta sẽ lấy thông tin các tiến trình đang chạy trên máy windows 7

Bằng cách sử dụng câu truy vấn WMI Chọn tab

KMA-PC

Dashboard

Journal

Shares

Open Files

Sessions

Terminal Sessions

Services

Processes

Installed Software

Accounts

Port Scanner

Event Log Explorer

WMI Explorer

Performance Counters

192.168.163.130

Username: administrator

Password:

Login

Dashboard

Device	
Name	KMA-PC
Domain	KIRA
User	Administrator
OS	Windows 7
Install Date	8/25/2021 6:15:59 AM
Model	VMware Virtual Platform
Vendor	VMware, Inc.
BIOS	PhoenixBIOS 4.0 Release 6.0 INTEL - 6040000
CPU	Intel Core i7-5700HQ 2.70GHz
Count	1
Frequency	2693 MHz
Memory	2048 MB
Remote Time	11/29/2021 9:26:28 PM
System UpTime	00:46:00
UUID	22BB4D56-9714-B901-45BD-9993D2CD0D55
Description	
Contact	
Location	
Flags	WORKSTATION,SERVER,NT,POTENTIAL_BROWSER,MASTER_BROWSER
Server	WORKSTATION

Ping Status - 0 ms

Advanced Device Explorer

KMA-PC

192.168.163.130 Username: administrator Password: [REDACTED] Login Logoff

WMI Explorer

Query: select Caption,ThreadCount,WorkingSetSize from win32_process Execute

#	Caption	Handle	ThreadCount	WorkingSetSize
0	System Idle Process	0	2	24576
1	System	4	96	4448256
2	smss.exe	268	3	950272
3	csrss.exe	364	9	3690496
4	wininit.exe	416	3	3756032
5	services.exe	500	7	10809344
6	lsass.exe	532	8	12230656
7	lsmd.exe	540	9	4026368
8	svchost.exe	660	9	9232384
9	vm3dservice.exe	720	3	3018752
10	svchost.exe	760	7	7872512
11	svchost.exe	840	20	17227776
12	svchost.exe	908	18	79003648
13	svchost.exe	952	32	33701888
14	svchost.exe	432	12	10842112
15	svchost.exe	1084	16	45137920
16	spoolsv.exe	1224	12	7925760
17	svchost.exe	1252	19	12009472
18	svchost.exe	1380	18	12603392
19	VGAAuthService.exe	1456	4	5025792
20	vmtoolsd.exe	1524	11	14708736
21	WmiPrvSE.exe	1876	11	13770752
22	msdtc.exe	1064	12	5619712
23	svchost.exe	1440	6	4014080
24	svchost.exe	2284	13	33529856

38 item(s)

Export data...

Ta sẽ thấy được các thông tin Processes đang chạy trên máy tính windows 7 bằng câu lệnh

select Caption,ProcessId,ThreadCount,WorkingSetSize from win32_process

Advanced Device Explorer

KMA-PC

192.168.163.130 Username: administrator Password: [REDACTED] Login Logoff

WMI Explorer

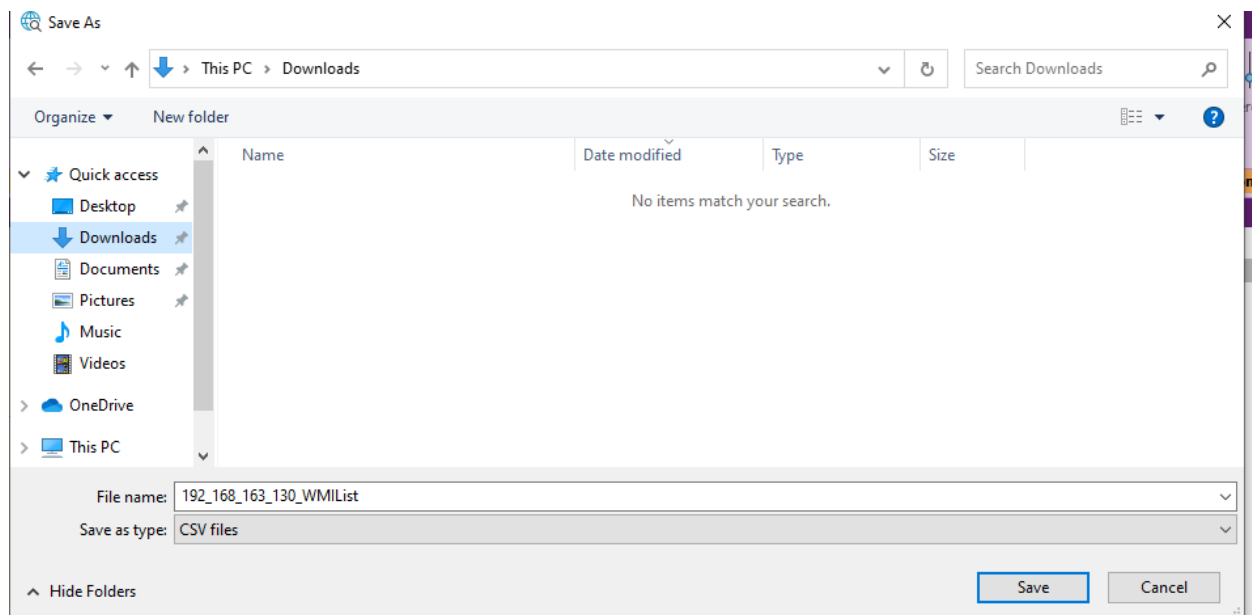
Query: select Caption,ProcessId,ThreadCount,WorkingSetSize from win32_process Execute

#	Caption	Handle	ThreadCount	WorkingSetSize
0	System Idle Process	0	2	24576
1	System	4	96	4448256
2	smss.exe	268	3	950272
3	csrss.exe	364	9	3690496
4	wininit.exe	416	3	3756032
5	services.exe	500	7	10809344
6	lsass.exe	532	8	12230656
7	lsmd.exe	540	9	4026368
8	svchost.exe	660	9	9232384
9	vm3dservice.exe	720	3	3018752
10	svchost.exe	760	7	7872512
11	svchost.exe	840	20	17227776
12	svchost.exe	908	18	79003648
13	svchost.exe	952	32	33701888
14	svchost.exe	432	12	10842112
15	svchost.exe	1084	16	45137920
16	spoolsv.exe	1224	12	7925760
17	svchost.exe	1252	19	12009472
18	svchost.exe	1380	18	12603392
19	VGAAuthService.exe	1456	4	5025792
20	vmtoolsd.exe	1524	11	14708736
21	WmiPrvSE.exe	1876	11	13770752
22	msdtc.exe	1064	12	5619712
23	svchost.exe	1440	6	4014080
24	svchost.exe	2284	13	33529856

38 item(s)

Export data...

Ta có thể xuất data ra bằng cách bấm Export data

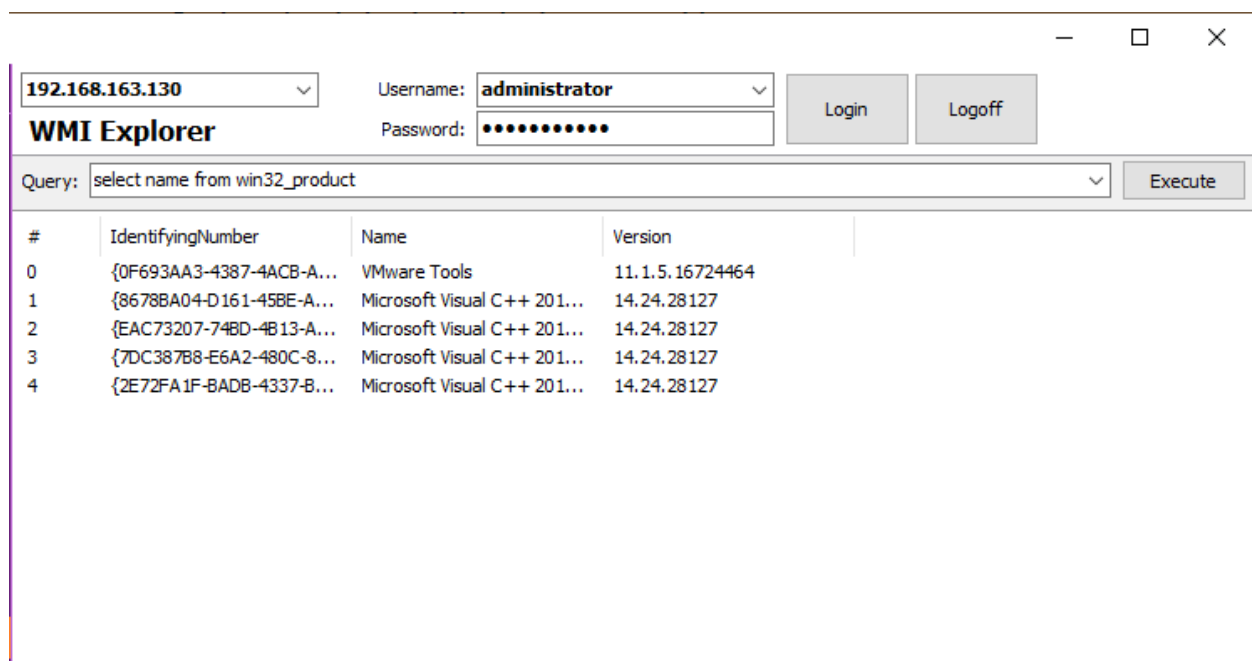


Sau đó chọn nơi lưu và Save lại

Chúng ta cũng có thể lấy thông tin các Software đang cài đặt trên máy tính windows 7 bằng câu lệnh sau

select name from win32_product

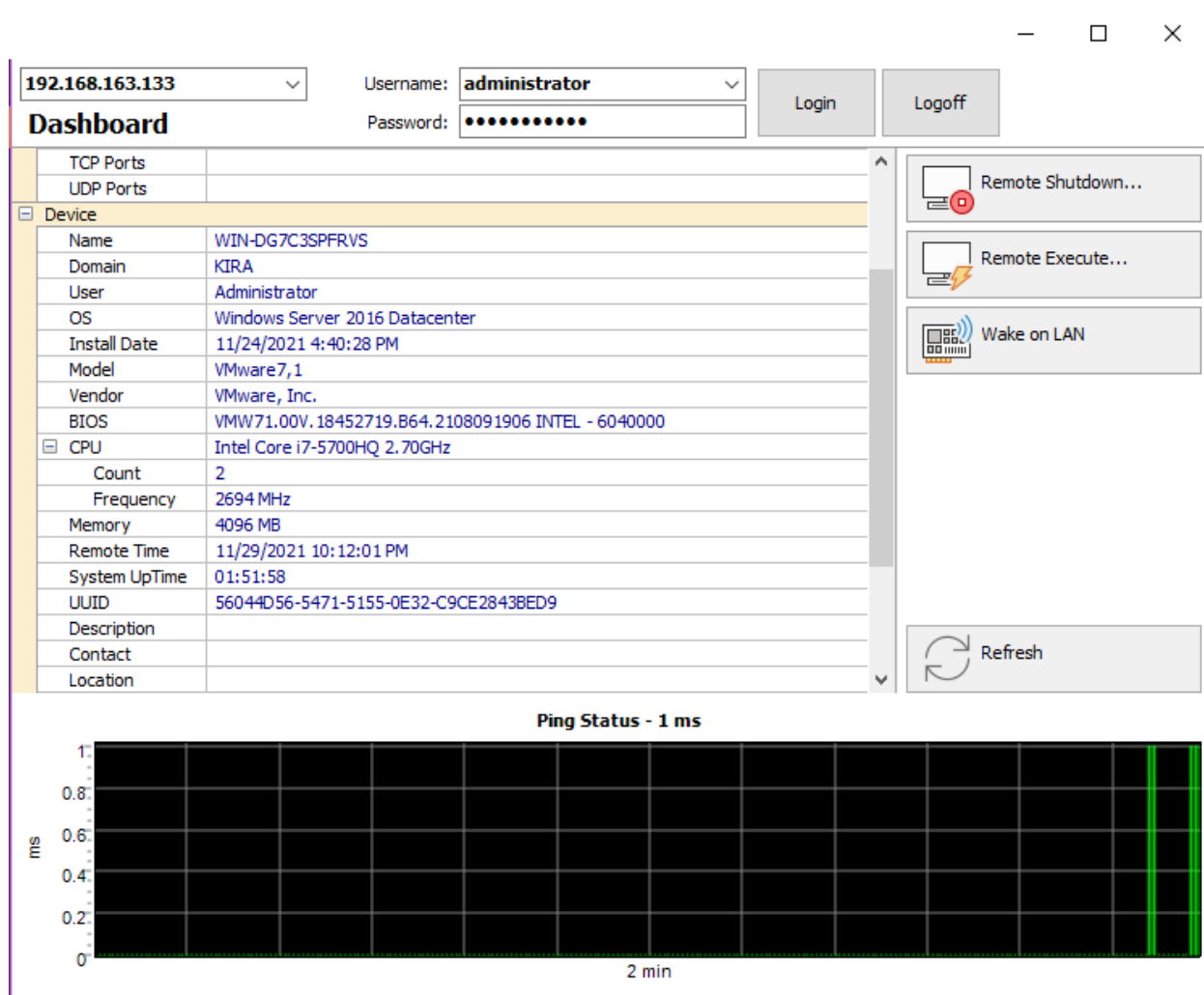
Câu lệnh này khá tốn 1 ít thời gian mong mọi người chờ đợi tầm (2p30s)



Sau đó ta có thể xuất data tương tự như trên

Sau khi lấy được thông tin máy tính windows 7

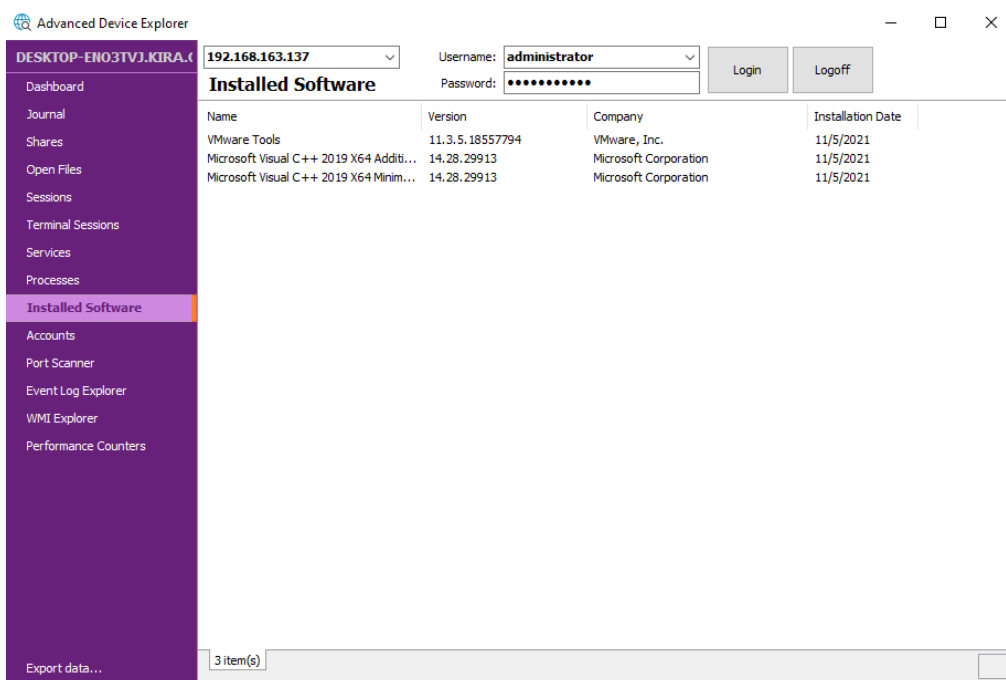
Chúng ta thấy các thông tin từ máy tính domain controller và máy windows 10 tương tự như trên



Domain	KIRA
User	Administrator
OS	Windows 10
Install Date	11/26/2021 11:10:17 AM
Model	VMware Virtual Platform
Vendor	VMware, Inc.
BIOS	PhoenixBIOS 4.0 Release 6.0 INTEL - 6040000
CPU	Intel Core i7-5700HQ 2.70GHz
Count	2
Frequency	2694 MHz
Memory	2048 MB
Remote Time	11/29/2021 10:13:33 PM
System UpTime	01:26:03
UUID	026C4D56-BD7C-CFF5-7E84-185BAE696073
Description	
Contact	
Location	
Flags	WORKSTATION,SERVER,NT
Server	WORKSTATION
Server	SERVER
Server	NT

Ở trên con máy Scanner thì thông tin tiến trình cũng như ứng dụng đang cài đặt cho máy được hiện ra cụ thể hơn còn những máy khác chúng ta phải sử dụng câu truy vấn WMI Explorer

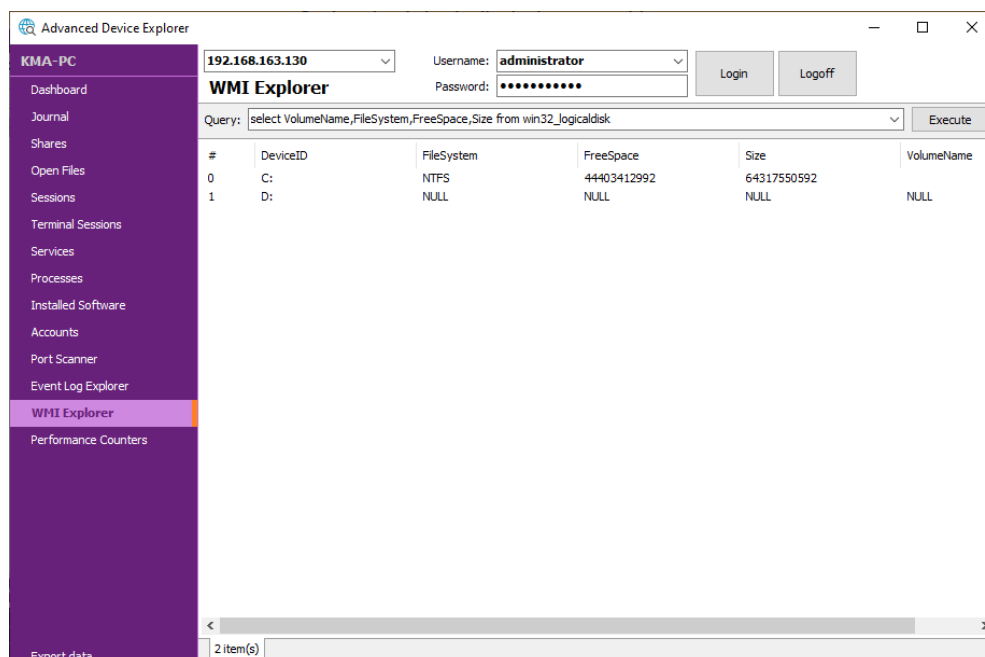
Advanced Device Explorer						
DESKTOP-ENO3TVJ.KIRA.(192.168.163.137)		Username: administrator		Login Logoff		
Password:						
Dashboard	Processes					
Journal	PID	Session ID	Name	Working Set	Threads	Username
Shares	316	0	smss.exe		2	SYSTEM
Open Files	436	0	csrss.exe	508.00 KB	12	
Sessions	512	1	csrss.exe	380.00 KB	11	
Terminal Sessions	532	0	wininit.exe		1	SYSTEM
Services	576	1	winlogon.exe	80.00 KB	6	SYSTEM
	652	0	services.exe	4.03 MB	7	SYSTEM
	676	0	lsass.exe	3.71 MB	9	SYSTEM
	792	0	svchost.exe	11.47 MB	19	SYSTEM
	820	1	fontdrvhost.exe		5	
	828	0	fontdrvhost.exe		5	
	912	0	svchost.exe	7.77 MB	10	NETWORK SERVICE
	996	1	dwm.exe	26.43 MB	15	
	396	0	svchost.exe	17.27 MB	51	SYSTEM
	688	0	svchost.exe	2.53 MB	20	SYSTEM
	1048	0	svchost.exe	2.58 MB	23	LOCAL SERVICE
	1052	0	svchost.exe	4.88 MB	11	LOCAL SERVICE
	1068	0	svchost.exe		7	LOCAL SERVICE
	1076	0	svchost.exe	264.00 KB	4	LOCAL SERVICE
	1196	0	svchost.exe	2.46 MB	17	NETWORK SERVICE
	1276	0	svchost.exe	292.00 KB	3	LOCAL SERVICE
	1424	0	svchost.exe		11	LOCAL SERVICE
	1548	0	svchost.exe		4	NETWORK SERVICE
	1656	0	svchost.exe	3.48 MB	14	LOCAL SERVICE
	1736	0	Memory Compression	155.60 MB	34	SYSTEM
	1888	0	svchost.exe	1.93 MB	9	LOCAL SERVICE
	2000	0	svchost.exe		4	LOCAL SERVICE
	2004	0	svchost.exe		3	LOCAL SERVICE
	1672	0	svchost.exe		7	SYSTEM
Export data...	76 item(s)					



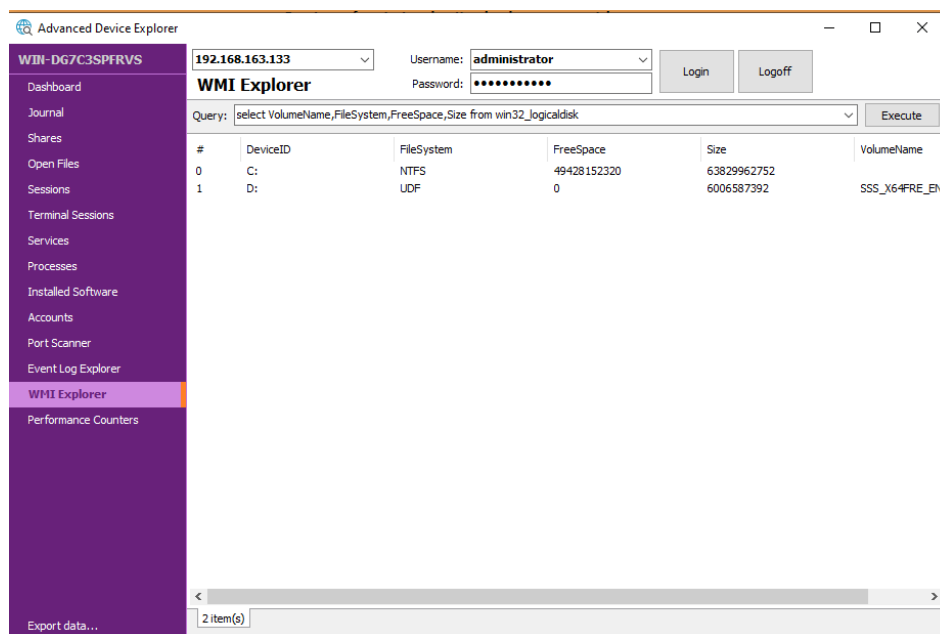
Lấy info các partition trên máy

Ở đây để lấy thông tin dung lượng các partition trên máy ta phải sử dụng câu lệnh truy vấn WMI như sau

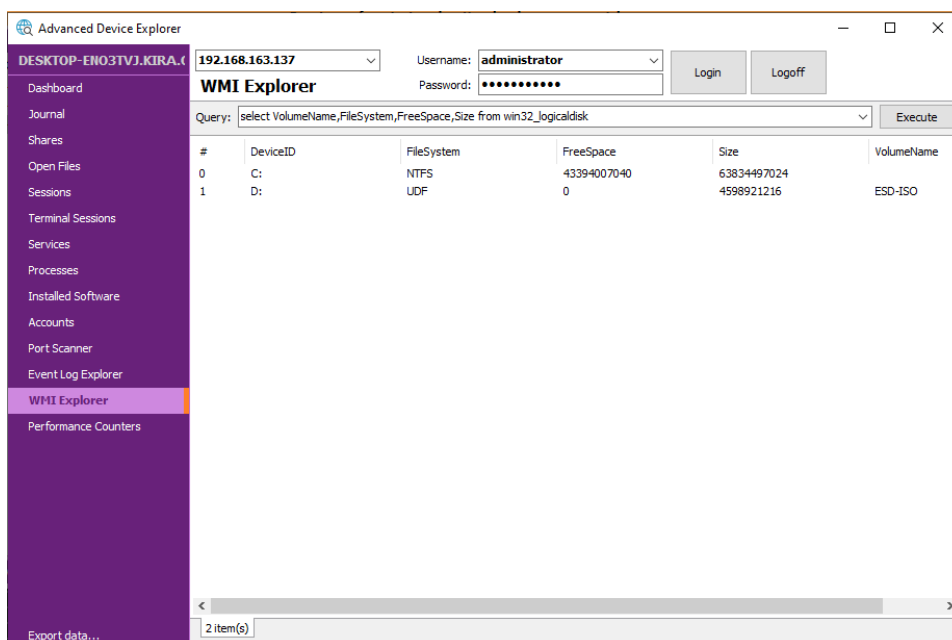
select VolumeName,FileSystem,FreeSpace,Size from win32_logicaldisk



Dung lượng các Partition trên máy windows 7



Dung lượng các Partition trên máy windows server 2016



Dung lượng các Partition trên máy windows 10

Video Demo

<https://www.youtube.com/watch?v=6YVDoqJ87Wo>