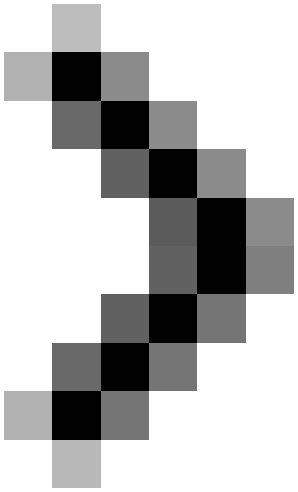
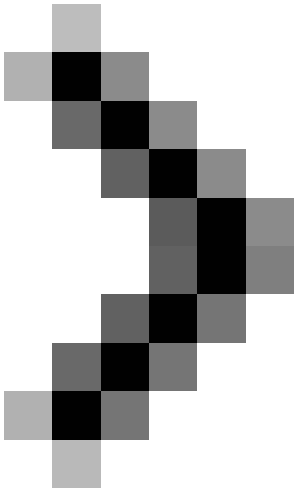
Managing Windows Networks using Script - Part 8: Handling remote scripting errors using Network Monitor 3.0

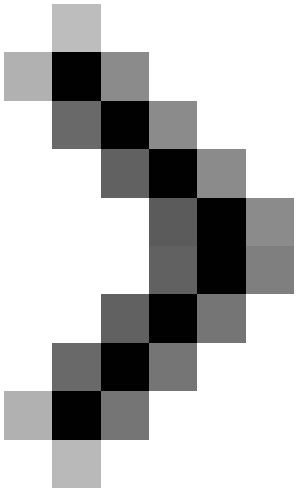
In Part 7, we started troubleshooting the error that occurred when trying to remotely change the IP address on an XP computer using the ChangeIPAddress.vbs script that was previously developed.



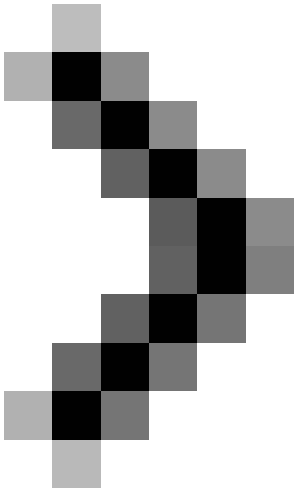
Part 1: Basic concepts



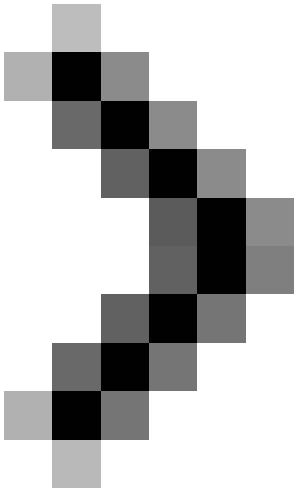
Part 2: Complete the script



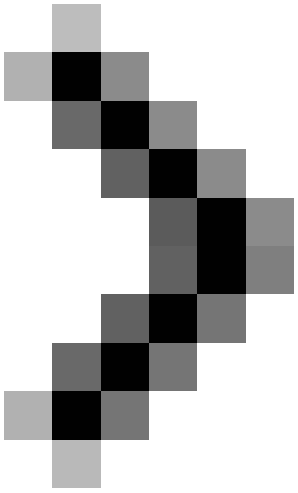
Part 3: Understanding WMI



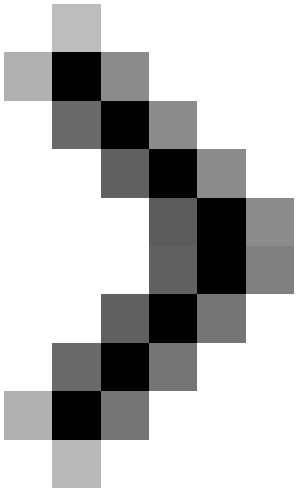
Part 4: Use Win32_NetworkAdapterConfiguration



Part 5: Overcoming challenges



Part 6: The first steps for remote scripting



Part 7: Troubleshooting errors

Mitch Tulloch

In Part 7, we started troubleshooting the error that occurred when trying to remotely change the IP address on an XP computer using the ChangeIPAddress.vbs script that was previously developed. The error is:

SWbemObjectEx: The remote procedure call failed

In the previous section, we mentioned that we have contacted some reputable experts in handling this error, and the best answer to get it is a hotfix that can corrupt WMI functionality and results. The script is working but with it there is an error.

A reader contacted me with the comment below:

In my opinion this is not a bug in the hotfix. Notice that you are changing the IP address of XP2. The remote call procedure failed because it lost the connection with XP2 on the original address (172.16.11.43). It then depends on the time (about 1 minute) to search for XP2 new IP address (172.16.11.65) before removing the old address. Imagine you only infiltrated a server like an administrator and changed the server's IP address. Will you lose connection? It will hang for a moment. But changing the default port on the server will not disconnect an existing connection (assuming you do this from the same subnet). If you try to change the default port setting from a remote location, you must be delayed .

So how can we check this explanation?

Use Network Monitor 3.0

Microsoft recently released a new version of Network Monitor, which is part of Microsoft Systems Management Server. Network Monitor 3.0 has several improvements over the previous version, namely:

1. Improved user interface displays frames when they are active in real time.
2. Multiple simultaneous capture sessions and simultaneous capture on multiple network adapters.
3. The ability to display network 'conversations', ie specific session protocols.
4. Support for Vista, Windows XP and Windows Server 2003 (both 32 bit and 64 bit).
5. The new filter panel allows you to use specified filters.

We are using NM3 to catch traces from the computer on which the ChangeIPAddress.vbs script is running. Here is the setup section to check:

Administrator machine workstation
Name: test124.test.com
IP address: 172.16.11.124 (static)

Destination machine
Name: test125.test.com
IP address: 172.16.11.125 (static)

Domain controller
Name: dc181.test.com
IP address: 172.16.11.181

However, before running ChangeIPAddress.vbs on test124 to change the IP address of test125, look at NM3 a bit.

When you launch NM3, it will have the interface as shown in Figure 1:

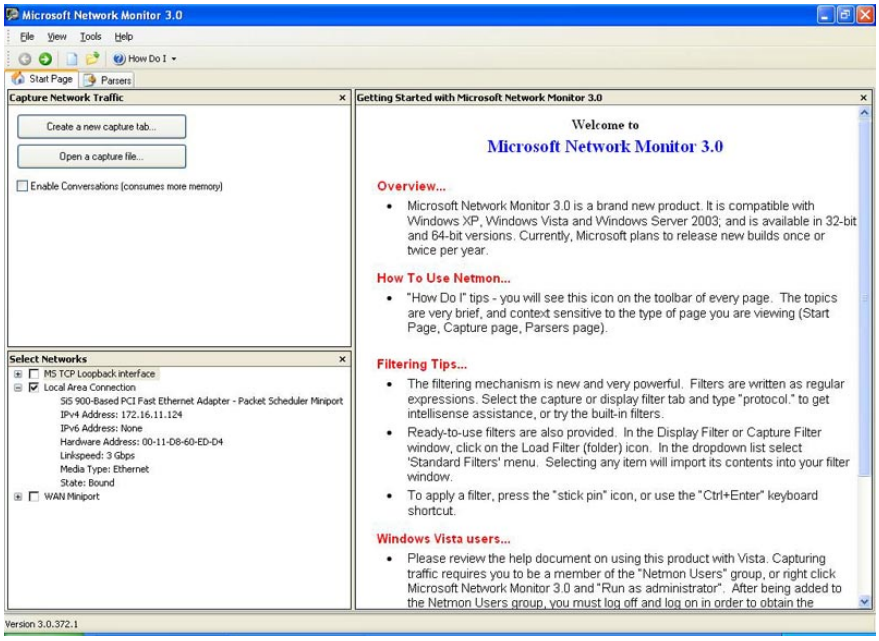


Figure 1: Network Monitor 3.0 window when opened

Before proceeding, select the Enable Conversations checkbox so that we can see the type of session protocol that appears during the trace.

Now click on the New Capture tab. This allows you to open a new tab called Capture1 that can be used to create network traces.

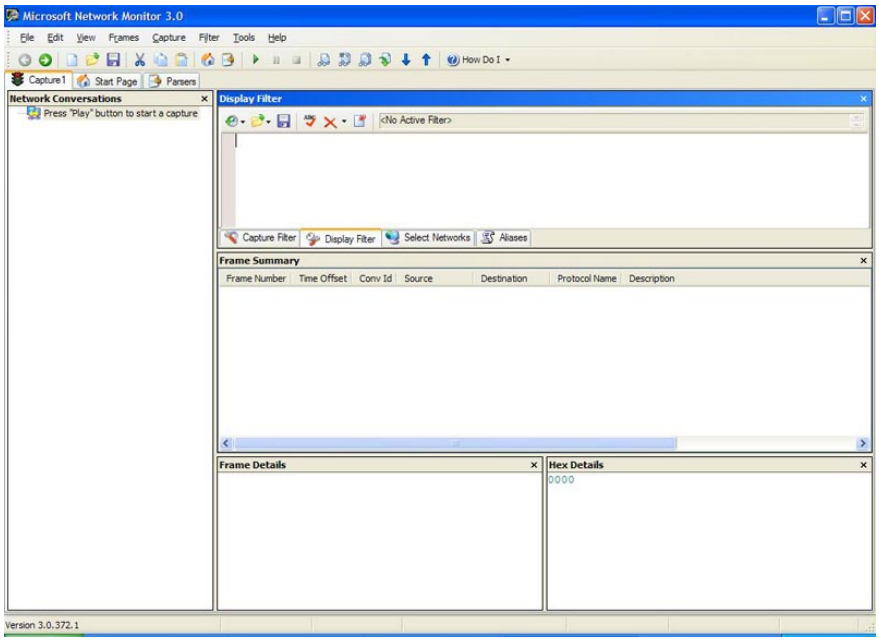


Figure 2: Open a new capture tab

Please check NM3 in a simple way. Click the Play button to start a capture, then from computer test124 open a command window and enter ping 172.16.11.125 which means we are pinging test125 to test124. The result is shown in Figure 3 below:

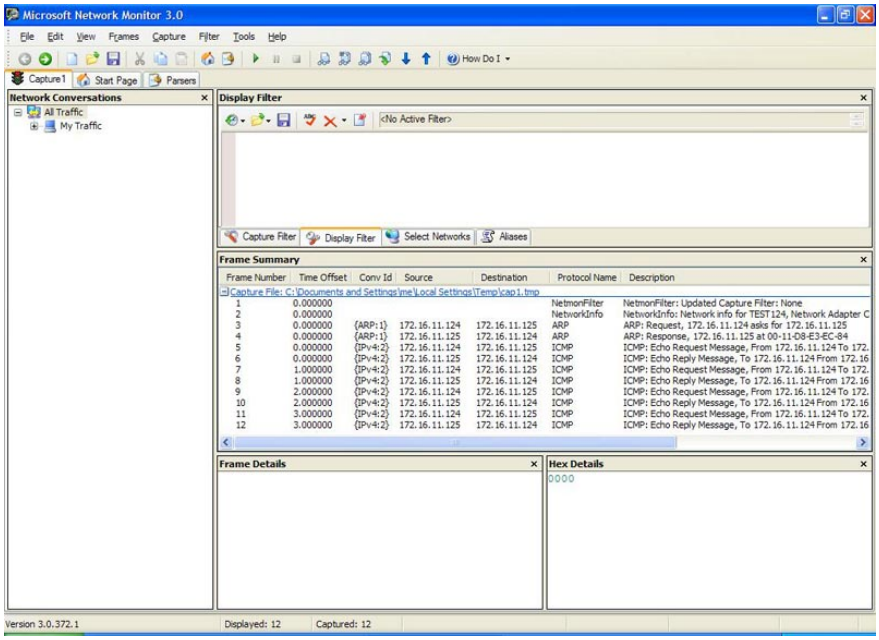


Figure 3: Analysis of ping 172.16.11.125

This is what we expect: two ARP packets (an ARP request followed by an ARP response) and a series of ICMP packets (Echo Request messages are given after Echo Reply messages). If you know the basic TCP / IP network connection, this is completely understandable.

Look at the 'conversation' situation that happened in Figure 4. Open the My Traffic button to display it:

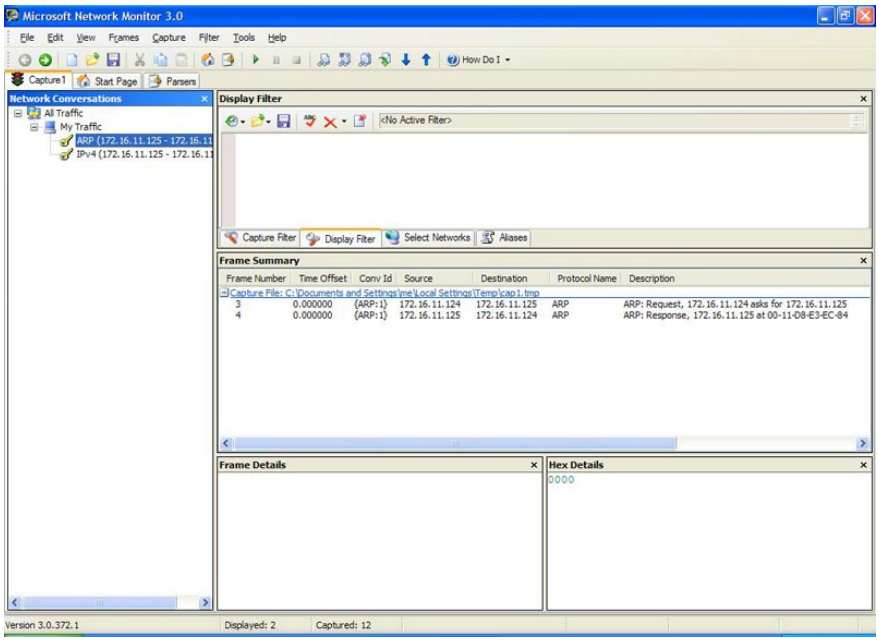


Figure 4: 'Conversations'
Note that two "conversations" have appeared: ARP and IPv4 (ICMP).

Now select the ARP Request package and look inside it (Figure 5):

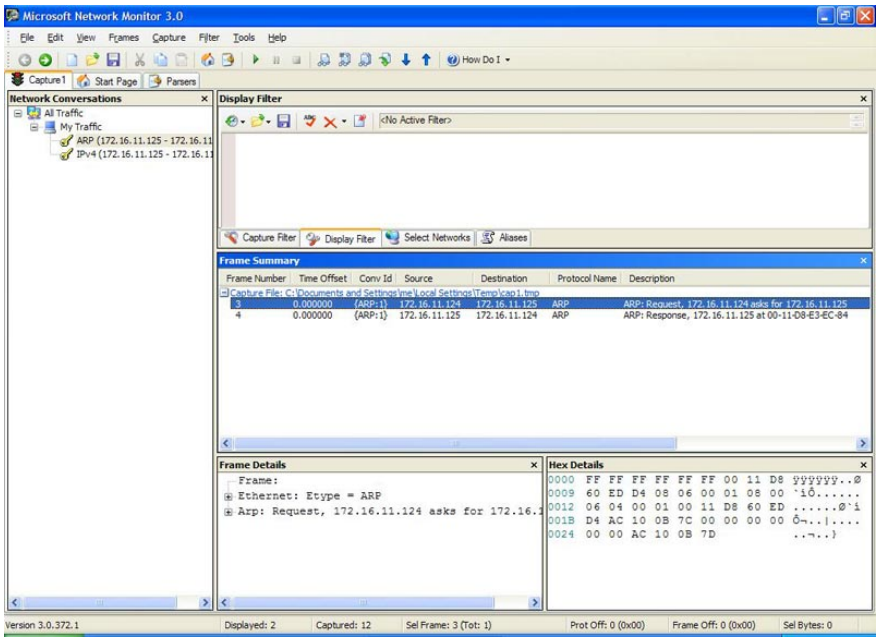


Figure 5: Examining a package

We have been introduced briefly about NM3, now use it to handle some errors.

Trace times

We started by restarting both workstations and clearing the cache (ARP, NDS, .), then opening the command prompt on computer test124, typing ChangeIPAddress.vbs 172.16.11.144 to change the IP address. of the test125 computer from 172.16.11.125 to 172.16.11.144. Figure 6 below is the results obtained:

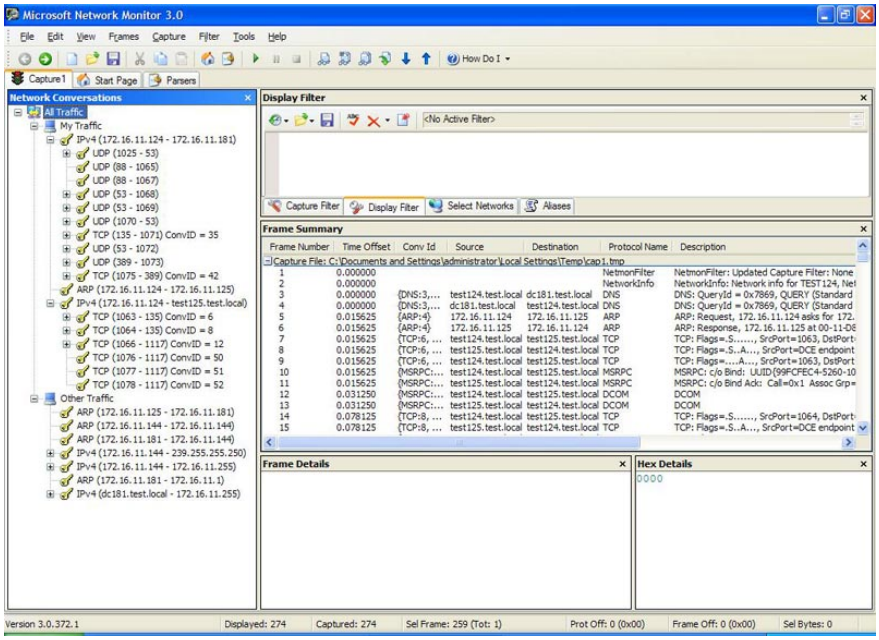


Figure 6: Results obtained when running ChangeIPAddress.vbs 172.16.11.144

Figure 6 is an overview of what happened. Retained the last 90 seconds and had 274 frames kept. The error message appears around frame 241 and the command window returns at frame 274. There is a lot of traffic that we can analyze! Look at Figure 6 above, we can start analyzing it:

1. 3-4 frames show the name TEST125 existing under the IP address 172.16.11.125 using DNS.
2. Frames 5-6 show the existing 172.16.11.125 IP address within the MAC address using ARP.
3. Frames 7-9 show the 'handshake' procedure of TCP (SYN, SYN / ACK, ACK) appearing between test124 and test125 computers.
4. 10-11 frames represent existing RPC constraints established between two computers.
5. Frames 12-13 represent the existing DCOM used on RCP (WMI uses DCOM to 'shake hands' remote calls).

We cannot see all 274 frames in the drawing, so we copied the information about all frames into a text file. You can click here to see the information about all frames when running ChangeIPAddress.vbs.

When troubleshooting common sense you have to start with what you know rather than what you don't understand. With that in mind, we understand that the other script (ChangeGateway.vbs) we developed in the previous article worked without generating any error messages. So before considering carefully in the file ChangeIPAddress.txt, restart your workstations and perform another capture, which will show the results of running ChangeGateway.vbs command 172.16.11.2 1 on test124 to replace Change the default port of test125 from 172.16.11.1 to 172.16.11.2 (specify the parameter measured by 1). This is what the second capture shows (Figure 7):

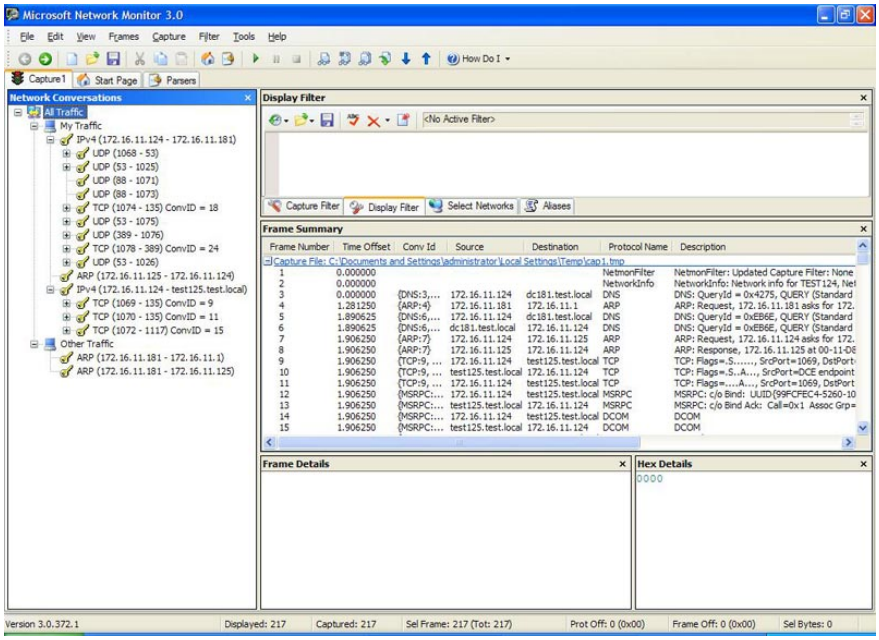


Figure 7: Results running ChangeGateway.vbs 172.16.11.2 1

Now there are only 217 frames to analyze (!) And you can go here to see the summary of all the frames.

Analysis of capture for ChangeGateway.vbs

Now let's try and analyze this second capture (working without generating errors) by dividing the summary of the frames into sections, which is one of them:

1 0.000000 NetmonFilter NetmonFilter: Updated Capture Filter: None
2 0.000000 NetworkInfo NetworkInfo: Network info for TEST124, Network Adapter Count = 1

Only NM3 header - ignored

3 0.000000 {DNS: 3, UDP: 2, IPv4: 1} 172.16.11.124 dc181.test.local DNS DNS: QueryId = 0x4275, QUERY (Standard query), Query for 124.11.16.172.in-addr.arpa of type SOA on class Internet
4 1.281250 {ARP: 4} 172.16.11.181 172.16.11.1 ARP ARP: Request, 172.16.11.181 asks for 172.16.11.1
5 1.890625 {DNS: 6, UDP: 5, IPv4: 1} 172.16.11.124 dc181.test.local DNS DNS: QueryId = 0xEB6E, QUERY (Standard query), Query for test125.test.local of type Host Addr on Internet class
6 1.890625 {DNS: 6, UDP: 5, IPv4: 1} dc181.test.local 172.16.11.124 DNS DNS: QueryId = 0xEB6E, QUERY (Standard query), Response - Success
7 1.906250 {ARP: 7} 172.16.11.124 172.16.11.125 ARP ARP: Request, 172.16.11.124 asks for 172.16.11.125
8 1.906250 {ARP: 7} 172.16.11.125 172.16.11.124 ARP ARP: Response, 172.16.11.125 at 00-11-D8-E3-EC-84

Name and address (DNS and ARP)

9 1.906250 {TCP: 9, IPv4: 8} 172.16.11.124 test125.test.local TCP TCP: Flags = .S ., SrcPort = 1069, DstPort = DCE endpoint resolution (135), Len = 0, Seq = 1441244938, Ack = 0, Win = 65535 (scale factor 0) = 65535
10.906250 {TCP: 9, IPv4: 8} test125.test.local 172.16.11.124 TCP TCP: Flags = .S.A ., SrcPort = DCE endpoint resolution (135), DstPort = 1069, Len = 0, Seq = 871910569, Ack = 1441244939, Win = 65535 (scale factor 0) =

65535
11 1.906250 {TCP: 9, IPv4: 8} 172.16.11.124 test125.test.local TCP TCP: Flags = . A ., SrcPort = 1069, DstPort = DCE endpoint resolution (135), Len = 0, Seq = 1441244939, Ack = 871910570, Win = 65535 (scale factor 0) = 65535

Test124 established a TVP connection with test125.

12 1.906250 {MSRPC: 10, TCP: 9, IPv4: 8} 172.16.11.124 test125.test.local MSRPC MSRPC: c / o Bind: UUID {99FCFEC4-5260-101B-BBCB-00AA0021347A} DCOM-IObjectExporter Call = 0x1 Assoc Grp = 0x0 Xmit = 0x16D0 Recv = 0x16D0
13 1.906250 {MSRPC: 10, TCP: 9, IPv4: 8} test125.test.local 172.16.11.124 MSRPC MSRPC: c / o Ack: Call = 0x1 Assoc Grp = 0x32E9 Xmit = 0x16D0 Recv = 0x16D0
14 1.906250 {MSRPC: 10, TCP: 9, IPv4: 8} 172.16.11.124 test125.test.local DCOM DCOM
15 1.906250 {MSRPC: 10, TCP: 9, IPv4: 8} test125.test.local 172.16.11.124 DCOM DCOM

Test124 establishes an RCP binding with test125 and calls DCOM.

16 1.921875 {TCP: 11, IPv4: 8} 172.16.11.124 test125.test.local TCP TCP: Flags = .S ., SrcPort = 1070, DstPort = DCE endpoint resolution (135), Len = 0, Seq = 3003512395, Ack = 0, Win = 65535 (scale factor 0) = 65535
17 1.921875 {TCP: 11, IPv4: 8} test125.test.local 172.16.11.124 TCP TCP: Flags = .S.A ., SrcPort = DCE endpoint resolution (135), DstPort = 1070, Len = 0, Seq = 4088700167, Ack = 3003512396, Win = 65535 (scale factor 0) = 65535
18 1.921875 {TCP: 11, IPv4: 8} 172.16.11.124 test125.test.local TCP TCP: Flags = . A ., SrcPort = 1070, DstPort = DCE endpoint resolution (135), Len = 0, Seq = 3003512396, Ack = 4088700168, Win = 65535 (scale factor 0) = 65535

3-way TCP handshake between two computers.

19 1.921875 {UDP: 12, IPv4: 1} 172.16.11.124 dc181.test.local KerberosV5 KerberosV5: TGS Request Realm: TEST.LOCAL Sname: RPCSS / test125.test.local
20 1.921875 {UDP: 12, IPv4: 1} dc181.test.local 172.16.11.124 KerberosV5 KerberosV5: TGS Response Cname: Administrator

Kerberos authentication

21 1.921875 {MSRPC: 13, TCP: 11, IPv4: 8} 172.16.11.124 test125.test.local MSRPC MSRPC: c / o Bind: UUID {000001A0-0000-0000-C000-000000000046} DCOM-IRemoteSCMActivator Call = 0x2 Assoc Grp = 0x32E9 Xmit = 0x16D0 Recv = 0x16D0
22 1.921875 {ARP: 14} 172.16.11.181 172.16.11.125 ARP ARP: Request, 172.16.11.181 asks for 172.16.11.125
23 1.921875 {MSRPC: 13, TCP: 11, IPv4: 8} test125.test.local 172.16.11.124 MSRPC MSRPC: c / o Ack: Call = 0x2 Assoc Grp = 0x32E9 Xmit = 0x16D0 Recv = 0x16D0
24 1.921875 {MSRPC: 13, TCP: 11, IPv4: 8} 172.16.11.124 test125.test.local MSRPC MSRPC: Alter Cont: UUID {000001A0-0000-0000-C000-000000000046} DCOM-IRemoteSCMActivator Call = 0x2
25 1.921875 {MSRPC: 13, TCP: 11, IPv4: 8} test125.test.local 172.16.11.124 MSRPC MSRPC: Alter Cont Resp: Call = 0x2 Assoc Grp = 0x32E9 Xmit = 0x16D0 Recv = 0x16D0
26 1.921875 {MSRPC: 13, TCP: 11, IPv4: 8} 172.16.11.124 test125.test.local DCOM DCOM
27 1.937500 {MSRPC: 13, TCP: 11, IPv4: 8} test125.test.local 172.16.11.124 DCOM DCOM

Many RPC and DCOM. We think that 'Alter Cont' indicates that interstitial content is being used, but in fact it is not guaranteed. It should have been OK when the script worked without generating any errors.

28 1.937500 {TCP: 15, IPv4: 8} 172.16.11.124 test125.test.local TCP TCP: Flags = .S ., SrcPort = 1072, DstPort = 1117, Len = 0, Seq = 3011418470, Ack = 0, Win = 65535 (scale factor 0) = 65535
29 1.937500 {TCP: 15, IPv4: 8} test125.test.local 172.16.11.124 TCP TCP: Flags = .S.A ., SrcPort = 1117, DstPort = 1072, Len = 0, Seq = 554832695, Ack = 3011418471, Win = 65535 (scale factor 0) = 65535
30 1.937500 {TCP: 15, IPv4: 8} 172.16.11.124 test125.test.local TCP TCP: Flags = . A ., SrcPort = 1072, DstPort = 1117, Len = 0, Seq = 3011418471, Ack = 554832696, Win = 65535 (scale factor 0) = 65535

Another TCP handshake

31 1.937500 {UDP: 16, IPv4: 1} 172.16.11.124 dc181.test.local KerberosV5 KerberosV5: TGS Request Realm: TEST.LOCAL Sname: TEST125 $
32 1.937500 {UDP: 16, IPv4: 1} dc181.test.local 172.16.11.124 KerberosV5 KerberosV5: TGS Response Cname: Administrator

Continue with Kerberos

33 1.937500 {MSRPC: 17, TCP: 15, IPv4: 8} 172.16.11.124 test125.test.local MSRPC MSRPC: c / o Bind: UUID {00000143-0000-0000-C000-000000000046} DCOM-IRemUnknown2 Call = 0x1 Assoc Grp = 0x0 Xmit = 0x16D0 Recv = 0x16D0
34 1.937500 {MSRPC: 17, TCP: 15, IPv4: 8} test125.test.local 172.16.11.124 MSRPC MSRPC: c / o Bind Ack: Call = 0x1 Assoc Grp = 0x333D Xmit = 0x16D0 Recv = 0x16D0
35 1.937500 {MSRPC: 17, TCP: 15, IPv4: 8} 172.16.11.124 test125.test.local MSRPC MSRPC: c / o Alter Cont: UUID {00000143-0000-0000-C000-000000000046} DCOM-IRemUnknown2 Call = 0x1
36 1.937500 {MSRPC: 17, TCP: 15, IPv4: 8} test125.test.local 172.16.11.124 MSRPC MSRPC Alter Cont Resp: Call = 0x1 Assoc Grp = 0x333D Xmit = 0x16D0 Recv = 0x16D0
37 1.937500 {MSRPC: 17, TCP: 15, IPv4: 8} 172.16.11.124 test125.test.local DCOM DCOM
38 1.937500 {MSRPC: 17, TCP: 15, IPv4: 8} test125.test.local 172.16.11.124 DCOM DCOM
39 1.937500 {MSRPC: 17, TCP: 15, IPv4: 8} 172.16.11.124 test125.test.local MSRPC MSRPC: Alter Cont: UUID {D4781CD6-E5D3-44DF-AD94-930EFE48A887} WMI-IWbemLoginClientID Call = 0x2
40 1.937500 {MSRPC: 17, TCP: 15, IPv4: 8} test125.test.local 172.16.11.124 MSRPC MSRPC: Alter Cont Resp: Call = 0x2 Assoc Grp = 0x333D Xmit = 0x16D0 Recv = 0x16D0
41 1.937500 {MSRPC: 17, TCP: 15, IPv4: 8} 172.16.11.124 test125.test.local DCOM DCOM
42 1.937500 {MSRPC: 17, TCP: 15, IPv4: 8} test125.test.local 172.16.11.124 DCOM DCOM
43 1.937500 {MSRPC: 17, TCP: 15, IPv4: 8} 172.16.11.124 test125.test.local MSRPC MSRPC: Alter Cont: UUID {F309AD18-D86A-11D0-A075-00C04FB68820} WMI-IWbemLevel1Login Call = 0x3
44 1.937500 {MSRPC: 17, TCP: 15, IPv4: 8} test125.test.local 172.16.11.124 MSRPC MSRPC: Alter Cont Resp: Call = 0x3 Assoc Grp = 0x333D Xmit = 0x16D0 Recv = 0x16D0
45 1.937500 {MSRPC: 17, TCP: 15, IPv4: 8} 172.16.11.124 test125.test.local DCOM DCOM
46 1.937500 {MSRPC: 17, TCP: 15, IPv4: 8} test125.test.local 172.16.11.124 DCOM DCOM
47 1.937500 {MSRPC: 17, TCP: 15, IPv4: 8} 172.16.11.124 test125.test.local DCOM DCOM
48 1.937500 {MSRPC: 17, TCP: 15, IPv4: 8} test125.test.local 172.16.11.124 DCOM DCOM
49 1.953125 {MSRPC: 17, TCP: 15, IPv4: 8} 172.16.11.124 test125.test.local MSRPC MSRPC: Alter Cont: UUID {9556DC99-828C-11CF-A37E-00AA003240C7} WMI-IWbemServices Call = 0x5
50 1.953125 {MSRPC: 17, TCP: 15, IPv4: 8} test125.test.local 172.16.11.124 MSRPC MSRPC: Alter Cont Resp: Call = 0x5 Assoc Grp = 0x333D Xmit = 0x16D0 Recv = 0x16D0
51 1.953125 {MSRPC: 17, TCP: 15, IPv4: 8} 172.16.11.124 test125.test.local DCOM DCOM

52 1.953125 {MSRPC: 17, TCP: 15, IPv4: 8} test125.test.local 172.16.11.124 DCOM DCOM
53 1.953125 {MSRPC: 17, TCP: 15, IPv4: 8} 172.16.11.124 test125.test.local DCOM DCOM
54 1.953125 {MSRPC: 17, TCP: 15, IPv4: 8} test125.test.local 172.16.11.124 DCOM DCOM
55 1.953125 {MSRPC: 17, TCP: 15, IPv4: 8} 172.16.11.124 test125.test.local MSRPC MSRPC: Alter Cont: UUID {1C1C45EE-4395-11D2-B60B-00104B703EFD} WMI-IWbemFetchSmartEnum Call = 0x7
56 1.953125 {MSRPC: 17, TCP: 15, IPv4: 8} test125.test.local 172.16.11.124 MSRPC MSRPC: Alter Cont Resp: Call = 0x7 Assoc Grp = 0x333D Xmit = 0x16D0 Recv = 0x16D0
57 1.953125 {MSRPC: 17, TCP: 15, IPv4: 8} 172.16.11.124 test125.test.local DCOM DCOM
58 1.953125 {MSRPC: 17, TCP: 15, IPv4: 8} test125.test.local 172.16.11.124 DCOM DCOM
59 1.953125 {MSRPC: 17, TCP: 15, IPv4: 8} 172.16.11.124 test125.test.local MSRPC MSRPC: Alter Cont: UUID {423EC01E-2E35-11D2-B604-00104B703EFD} WMI-IWbemWCOSmartEnum Call = 0x8
60 1.953125 {MSRPC: 17, TCP: 15, IPv4: 8} test125.test.local 172.16.11.124 MSRPC MSRPC Alter Cont Resp: Call = 0x8 Assoc Grp = 0x333D Xmit = 0x16D0 Recv = 0x16D0
61 1.953125 {MSRPC: 17, TCP: 15, IPv4: 8} 172.16.11.124 test125.test.local DCOM DCOM
62 2.015625 {MSRPC: 17, TCP: 15, IPv4: 8} test125.test.local 172.16.11.124 DCOM DCOM

There are many RPC / DCOM here. It may seem mysterious but if you look closely you will see some of the existing WMI such as WMI-IWbemLoginClientID, WMI-IWbemLevel1Login, WMI-IWbemServices, WMI-IWbemFetchSmartEnum, . Searching on MSDN shows us more information about what happens. For example, this page tells us that 'IwbemServices interface is used for clients and providers to be able to access WMI services' so it is like existing WMI interfaces. call on the remote computer (using DCOM) by the host computer running the script from it. Some interfaces are not really confusing for readers.

The most confusing thing for the first reader is that the TCP clusters with RPC 'Continued Response' packets seem to indicate that connections made earlier are being used for many other purposes. We will skip some frames in this next section.

63 2.015625 {TCP: 15, IPv4: 8} test125.test.local 172.16.11.124 TCP TCP: [Continuation to # 62] Flags = . A ., SrcPort = 1117, DstPort = 1072, Len = 1460 , Seq = 554835972 - 554837432, Ack = 3011421991, Win = 65061 (scale factor 0) = 65061
64 2.015625 {TCP: 15, IPv4: 8} 172.16.11.124 test125.test.local TCP TCP: Flags = . A ., SrcPort = 1072, DstPort = 1117, Len = 0, Seq = 3011421991, Ack = 554837432, Win = 65535 (scale factor 0) = 65535
65 2.015625 {TCP: 15, IPv4: 8} test125.test.local 172.16.11.124 TCP TCP: [Continuation to # 62] Flags = . A ., SrcPort = 1117, DstPort = 1072, Len = 1460 , Seq = 554837432 - 554838892, Ack = 3011421991, Win = 65061 (scale factor 0) = 65061
66 2.015625 {TCP: 15, IPv4: 8} 172.16.11.124 test125.test.local TCP TCP: Flags = . A ., SrcPort = 1072, DstPort = 1117, Len = 0, Seq = 3011421991, Ack = 554838892, Win = 65535 (scale factor 0) = 65535
67 2.015625 {TCP: 15, IPv4: 8} test125.test.local 172.16.11.124 TCP TCP: [Continuation to # 62] Flags = . PA ., SrcPort = 1117, DstPort = 1072, Len = 1449, Seq = 554838892 - 554840341, Ack = 3011421991, Win = 65061 (scale factor 0) = 65061
68 2.015625 {MSRPC: 17, TCP: 15, IPv4: 8} test125.test.local 172.16.11.124 MSRPC MSRPC: c / o Continued Response: WMI-IWbemWCOSmartEnum Call = 0x8 Context = 0x5 Hint = 0x198C Cancels = 0x0
.
.
.
155 2.031250 {MSRPC: 17, TCP: 15, IPv4: 8} test125.test.local 172.16.11.124 MSRPC MSRPC: c / o Continued Response: WMI-IWbemServices Call = 0x9 Context = 0x3 Hint = 0x904 Cancels = 0x0
156 2.031250 {TCP: 15, IPv4: 8} test125.test.local 172.16.11.124 TCP TCP: [Continuation to # 155] Flags = .

PA ., SrcPort = 1117, DstPort = 1072, Len = 929, Seq = 554924260 - 554925189, Ack = 3011422236, Win = 64816 (scale factor 0) = 64816
157 2.031250 {TCP: 15, IPv4: 8} 172.16.11.124 test125.test.local TCP TCP: Flags = . A ., SrcPort = 1072, DstPort = 1117, Len = 0, Seq = 3011422236, Ack = 554925189, Win = 65535 (scale factor 0) = 65535
158 2.031250 {MSRPC: 17, TCP: 15, IPv4: 8} 172.16.11.124 test125.test.local DCOM DCOM
159 2.031250 {TCP: 15, IPv4: 8} 172.16.11.124 test125.test.local TCP TCP: [Continuation # 158] Flags = . PA ., SrcPort = 1072, DstPort = 1117, Len = 1, Seq = 3011423696 - 3011423697, Ack = 554925189, Win = 65535 (scale factor 0) = 65535
160 2.031250 {TCP: 15, IPv4: 8} test125.test.local 172.16.11.124 TCP TCP: Flags = . A ., SrcPort = 1117, DstPort = 1072, Len = 0, Seq = 554925189, Ack = 3011423697, Win = 65535 (scale factor 0) = 65535

We have a DCOM cluster followed by TCP connection endings with FIN / ACK, so it is predicted that the script might have done its job and is cleaning up.

161 2.062500 {MSRPC: 17, TCP: 15, IPv4: 8} test125.test.local 172.16.11.124 DCOM DCOM
162 2.062500 {MSRPC: 17, TCP: 15, IPv4: 8} 172.16.11.124 test125.test.local DCOM DCOM
163 2.062500 {MSRPC: 17, TCP: 15, IPv4: 8} test125.test.local 172.16.11.124 DCOM DCOM
164 2.062500 {MSRPC: 17, TCP: 15, IPv4: 8} 172.16.11.124 test125.test.local DCOM DCOM
165 2.062500 {MSRPC: 17, TCP: 15, IPv4: 8} test125.test.local 172.16.11.124 DCOM DCOM
166 2.062500 {MSRPC: 17, TCP: 15, IPv4: 8} 172.16.11.124 test125.test.local DCOM DCOM
167 2.062500 {MSRPC: 17, TCP: 15, IPv4: 8} test125.test.local 172.16.11.124 DCOM DCOM
168 2.062500 {MSRPC: 17, TCP: 15, IPv4: 8} 172.16.11.124 test125.test.local DCOM DCOM
169 2.062500 {MSRPC: 17, TCP: 15, IPv4: 8} test125.test.local 172.16.11.124 DCOM DCOM
170 2.078125 {TCP: 15, IPv4: 8} 172.16.11.124 test125.test.local TCP TCP: Flags = F . A ., SrcPort = 1072, DstPort = 1117, Len = 0, Seq = 3011424421, Ack = 554926046, Win = 64678 (scale factor 0) = 64678
171 2.078125 {TCP: 15, IPv4: 8} test125.test.local 172.16.11.124 TCP TCP: Flags = . A ., SrcPort = 1117, DstPort = 1072, Len = 0, Seq = 554926046, Ack = 3011424422, Win = 64811 (scale factor 0) = 64811
172 2.078125 {TCP: 15, IPv4: 8} test125.test.local 172.16.11.124 TCP TCP: Flags = F . A ., SrcPort = 1117, DstPort = 1072, Len = 0, Seq = 554926046, Ack = 3011424422, Win = 64811 (scale factor 0) = 64811
173 2.078125 {TCP: 15, IPv4: 8} 172.16.11.124 test125.test.local TCP TCP: Flags = . A ., SrcPort = 1072, DstPort = 1117, Len = 0, Seq = 3011424422, Ack = 554926047, Win = 64678 (scale factor 0) = 64678
174 2.093750 {TCP: 9, IPv4: 8} 172.16.11.124 test125.test.local TCP TCP: Flags = . A ., SrcPort = 1069, DstPort = DCE endpoint resolution (135), Len = 0, Seq = 1441245035, Ack = 871910766, Win = 65339 (scale factor 0) = 65339
175 2.093750 {TCP: 11, IPv4: 8} 172.16.11.124 test125.test.local TCP TCP: Flags = . A ., SrcPort = 1070, DstPort = DCE endpoint resolution (135), Len = 0, Seq = 3003514721, Ack = 4088701653, Win = 65535 (scale factor 0) = 65535
176 2.546875 {TCP: 18, IPv4: 1} 172.16.11.124 dc181.test.local TCP TCP: Flags = .S ., SrcPort = 1074, DstPort = DCE endpoint resolution (135), Len = 0, Seq = 4283854964, Ack = 0, Win = 65535 (scale factor 0) = 65535
177 2.546875 {TCP: 18, IPv4: 1} dc181.test.local 172.16.11.124 TCP TCP: Flags = .S.A ., SrcPort = DCE endpoint resolution (135), DstPort = 1074, Len = 0, Seq = 2447011944, Ack = 4283854965, Win = 16384 (scale factor 0) = 16384
178 2.546875 {TCP: 18, IPv4: 1} 172.16.11.124 dc181.test.local TCP TCP: Flags = . A ., SrcPort = 1074, DstPort = DCE endpoint resolution (135), Len = 0, Seq = 4283854965, Ack = 2447011945, Win = 65535 (scale factor 0) = 65535

Here are some DNS and LDAP that appear between test124 and domain controller. It is not clear why it happened, but we will ignore some of them when they appear too much:

179 2.546875 {MSRPC: 19, TCP: 18, IPv4: 1} 172.16.11.124 dc181.test.local MSRPC MSRPC: c / o Bind: UUID {E1AF8308-5D1F-11C9-91A4-08002B14A0FA} Endpoint Mapper Call = 0x1 Assoc Grp = 0x0 Xmit = 0x16D0 Recv = 0x16D0
180 2.546875 {MSRPC: 19, TCP: 18, IPv4: 1} dc181.test.local 172.16.11.124 MSRPC MSRPC: c / o Bind Ack: Call = 0x1 Assoc Grp = 0x7DAD Xmit = 0x16D0 Recv = 0x16D0
181 2.546875 {MSRPC: 19, TCP: 18, IPv4: 1} 172.16.11.124 dc181.test.local EPM EPM: Request: ept_map: NDR, Tracking Server Service v1.0, RPC v5, 0.0.0.0:135 (0x87) [DCE endpoint resolution (135)]
182 2.546875 {MSRPC: 19, TCP: 18, IPv4: 1} dc181.test.local 172.16.11.124 EPM EPM: Response: ept_map: 0x16C9A0D6 - EP_S_NOT_REGISTERED
183 2,546875 {DNS: 21, UDP: 20, IPv4: 1} 172.16.11.124 dc181.test.local DNS DNS: QueryId = 0x896A, QUERY (Standard query), Query for _ldap._tcp.Default-First-Site._sites. dc._msdcs.test.local of type SRV on class Internet
184 2,546875 {DNS: 21, UDP: 20, IPv4: 1} dc181.test.local 172.16.11.124 DNS DNS: QueryId = 0x896A, QUERY (Standard query), Response - Success
185 2.546875 {LDAP: 23, UDP: 22, IPv4: 1} 172.16.11.124 dc181.test.local LDAP LDAP: Search Request, MessageID: 4, BaseObject: NULL, SearchScope: base Object, SearchAlias: neverDerefAliases
186 2,546875 {LDAP: 23, UDP: 22, IPv4: 1} dc181.test.local 172.16.11.124 LDAP LDAP: Search Result Entry, MessageID: 4, Status: Success
.
.
.
212 6.546875 {DNS: 32, UDP: 5, IPv4: 1} 172.16.11.124 dc181.test.local DNS DNS: QueryId = 0x266D, QUERY (Standard query), Query for download.windowsupdate.com of the Host Addr on class Internet type
213 6.546875 {ARP: 4} 172.16.11.181 172.16.11.1 ARP ARP: Request, 172.16.11.181 asks for 172.16.11.1
214 7.546875 {DNS: 32, UDP: 5, IPv4: 1} 172.16.11.124 dc181.test.local DNS DNS: QueryId = 0x266D, QUERY (Standard query), Query for download.windowsupdate.com of the Host Addr on class Internet type
215 8.546875 {DNS: 32, UDP: 5, IPv4: 1} 172.16.11.124 dc181.test.local DNS DNS: QueryId = 0x266D, QUERY (Standard query), Query for download.windowsupdate.com of the Host Addr on class Internet type
216 9.281250 {ARP: 4} 172.16.11.181 172.16.11.1 ARP ARP: Request, 172.16.11.181 asks for 172.16.11.1

At this point, the script is ready to finish so we have finished capturing.

Analysis of Capture for ChangeIPAddress.vbs

Now we have a little idea of ??what a capture of the successful remote control script looks like:

1. Some DNS and ARP
2. Setting up of TCP sessions with 3-way handshake.
3. RPC and DCOM constraints
4. Many TCP handshakes
5. Kerberos (computers in a domain)
6. Multiple RPC / DCOM
7. Many TCP handshakes, many Kerberos, RPC / DCOM are associated with TCP communications.
8. Many DCOM are followed by previously established TCP sessions.

All of that takes about 2 seconds.

Now let's look at the capture for ChangeIPAddress.vbs (the script generated an RPC error when running it remotely) and see how it differs from the above scenarios.

1 0.000000 NetmonFilter NetmonFilter: Updated Capture Filter: None
2 0.000000 NetworkInfo NetworkInfo: Network info for TEST124, Network Adapter Count = 1

It is Netmon

3 0.000000 {DNS: 3, UDP: 2, IPv4: 1} test124.test.local dc181.test.local DNS DNS: QueryId = 0x7869, QUERY (Standard query), Query for test125.test.local of type Host Addr on Internet class
4 0.000000 {DNS: 3, UDP: 2, IPv4: 1} dc181.test.local test124.test.local DNS DNS: QueryId = 0x7869, QUERY (Standard query), Response - Success
5 0.015625 {ARP: 4} 172.16.11.124 172.16.11.125 ARP ARP: Request, 172.16.11.124 asks for 172.16.11.125
6 0.015625 {ARP: 4} 172.16.11.125 172.16.11.124 ARP ARP: Response, 172.16.11.125 at 00-11-D8-E3-EC-84
7 0.015625 {TCP: 6, IPv4: 5} test124.test.local test125.test.local TCP TCP: Flags = .S ., SrcPort = 1063, DstPort = DCE endpoint resolution (135), Len = 0, Seq = 539163285, Ack = 0, Win = 65535 (scale factor 0) = 65535
8 0.015625 {TCP: 6, IPv4: 5} test125.test.local test124.test.local TCP TCP: Flags = .S.A ., SrcPort = DCE endpoint resolution (135), DstPort = 1063, Len = 0, Seq = 981335265, Ack = 539163286, Win = 65535 (scale factor 0) = 65535
9 0.015625 {TCP: 6, IPv4: 5} test124.test.local test125.test.local TCP TCP: Flags = . A ., SrcPort = 1063, DstPort = DCE endpoint resolution (135), Len = 0, Seq = 539163286, Ack = 981335266, Win = 65535 (scale factor 0) = 65535

ARP, then NDS, TCP handshake - as before.

10 0.015625 {MSRPC: 7, TCP: 6, IPv4: 5} test124.test.local test125.test.local MSRPC MSRPC: c / o Bind: UUID {99FCFEC4-5260-101B-BBCB-00AA0021347A} DCOM-IObjectExporter Call = 0x1 Assoc Grp = 0x0 Xmit = 0x16D0 Recv = 0x16D0
11 0.015625 {MSRPC: 7, TCP: 6, IPv4: 5} test125.test.local test124.test.local MSRPC MSRPC: c / o Bind Ack: Call = 0x1 Assoc Grp = 0x32EA Xmit = 0x16D0 Recv = 0x16D0
12 0.031250 {MSRPC: 7, TCP: 6, IPv4: 5} test124.test.local test125.test.local DCOM DCOM
13 0.031250 {MSRPC: 7, TCP: 6, IPv4: 5} test125.test.local test124.test.local DCOM DCOM
14 0.078125 {TCP: 8, IPv4: 5} test124.test.local test125.test.local TCP TCP: Flags = .S ., SrcPort = 1064, DstPort = DCE endpoint resolution (135), Len = 0, Seq = 1367843928, Ack = 0, Win = 65535 (scale factor 0) = 65535
15 0.078125 {TCP: 8, IPv4: 5} test125.test.local test124.test.local TCP TCP: Flags = .S.A ., SrcPort = DCE endpoint resolution (135), DstPort = 1064, Len = 0, Seq = 3625279350, Ack = 1367843929, Win = 65535 (scale factor 0) = 65535
16 0.078125 {TCP: 8, IPv4: 5} test124.test.local test125.test.local TCP TCP: Flags = . A ., SrcPort = 1064, DstPort = DCE endpoint resolution (135), Len = 0, Seq = 1367843929, Ack = 3625279351, Win = 65535 (scale factor 0) = 65535
17 0.078125 {UDP: 9, IPv4: 1} test124.test.local dc181.test.local KerberosV5 KerberosV5: TGS Request Realm: TEST.LOCAL Sname: RPCSS / test125.test.local
18 0.078125 {UDP: 9, IPv4: 1} dc181.test.local test124.test.local KerberosV5 KerberosV5: TGS Response Cname: Administrator

RPC, then DCOM, another TCP handshake, Kerberos. It looks the same as before.

19 0.078125 {MSRPC: 10, TCP: 8, IPv4: 5} test124.test.local test125.test.local MSRPC MSRPC: c / o Bind: UUID {000001A0-0000-0000-C000-000000000046} DCOM-IRemoteSCMActivator Call = 0x2 Assoc Grp = 0x32EA Xmit = 0x16D0 Recv = 0x16D0
20 0.093750 {ARP: 11} 172.16.11.125 172.16.11.181 ARP ARP: Request, 172.16.11.125 asks for 172.16.11.181
21 0.093750 {MSRPC: 10, TCP: 8, IPv4: 5} test125.test.local test124.test.local MSRPC MSRPC: c / o Ack: Call = 0x2 Assoc Grp = 0x32EA Xmit = 0x16D0 Recv = 0x16D0
22 0.093750 {MSRPC: 10, TCP: 8, IPv4: 5} test124.test.local test125.test.local MSRPC MSRPC: c / o Alter Cont: UUID {000001A0-0000-0000-C000-000000000046} DCOM-IRemoteSCMActivator Call = 0x2
23 0.093750 {MSRPC: 10, TCP: 8, IPv4: 5} test125.test.local test124.test.local MSRPC MSRPC: Alter Cont Resp: Call = 0x2 Assoc Grp = 0x32EA Xmit = 0x16D0 Recv = 0x16D0
24 0.093750 {MSRPC: 10, TCP: 8, IPv4: 5} test124.test.local test125.test.local DCOM DCOM
25 0.093750 {MSRPC: 10, TCP: 8, IPv4: 5} test125.test.local test124.test.local DCOM DCOM
26 0.093750 {TCP:12, IPv4:5} test124.test.local test125.test.local TCP TCP: Flags=.S., SrcPort=1066, DstPort=1117, Len=0, Seq=1180773456, Ack=0, Win=65535 (scale factor 0) = 65535
27 0.093750 {TCP:12, IPv4:5} test125.test.local test124.test.local TCP TCP: Flags=.S.A., SrcPort=1117, DstPort=1066, Len=0, Seq=539972629, Ack=1180773457, Win=65535 (scale factor 0) = 65535
28 0.093750 {TCP:12, IPv4:5} test124.test.local test125.test.local TCP TCP: Flags=.A., SrcPort=1066, DstPort=1117, Len=0, Seq=1180773457, Ack=539972630, Win=65535 (scale factor 0) = 65535
29 0.093750 {UDP:13, IPv4:1} test124.test.local dc181.test.local KerberosV5 KerberosV5: TGS Request Realm: TEST.LOCAL Sname: TEST125$
30 0.109375 {UDP:13, IPv4:1} dc181.test.local test124.test.local KerberosV5 KerberosV5: TGS Response Cname: Administrator

Cùng m?u

31 0.109375 {MSRPC:14, TCP:12, IPv4:5} test124.test.local test125.test.local MSRPC MSRPC: c/o Bind: UUID{00000143-0000-0000-C000-000000000046} DCOM-IRemUnknown2 Call=0x1 Assoc Grp=0x0 Xmit=0x16D0 Recv=0x16D0
32 0.109375 {MSRPC:14, TCP:12, IPv4:5} test125.test.local test124.test.local MSRPC MSRPC: c/o Bind Ack: Call=0x1 Assoc Grp=0x333E Xmit=0x16D0 Recv=0x16D0
33 0.109375 {MSRPC:14, TCP:12, IPv4:5} test124.test.local test125.test.local MSRPC MSRPC: c/o Alter Cont: UUID{00000143-0000-0000-C000-000000000046} DCOM-IRemUnknown2 Call=0x1
34 0.109375 {MSRPC:14, TCP:12, IPv4:5} test125.test.local test124.test.local MSRPC MSRPC: c/o Alter Cont Resp: Call=0x1 Assoc Grp=0x333E Xmit=0x16D0 Recv=0x16D0
35 0.109375 {MSRPC:14, TCP:12, IPv4:5} test124.test.local test125.test.local DCOM DCOM
36 0.109375 {MSRPC:14, TCP:12, IPv4:5} test125.test.local test124.test.local DCOM DCOM
37 0.109375 {MSRPC:14, TCP:12, IPv4:5} test124.test.local test125.test.local MSRPC MSRPC: c/o Alter Cont: UUID{D4781CD6-E5D3-44DF-AD94-930EFE48A887} WMI-IWbemLoginClientID Call=0x2
38 0.109375 {MSRPC:14, TCP:12, IPv4:5} test125.test.local test124.test.local MSRPC MSRPC: c/o Alter Cont Resp: Call=0x2 Assoc Grp=0x333E Xmit=0x16D0 Recv=0x16D0
39 0.109375 {MSRPC:14, TCP:12, IPv4:5} test124.test.local test125.test.local DCOM DCOM
40 0.109375 {MSRPC:14, TCP:12, IPv4:5} test125.test.local test124.test.local DCOM DCOM
41 0.109375 {MSRPC:14, TCP:12, IPv4:5} test124.test.local test125.test.local MSRPC MSRPC: c/o Alter Cont: UUID{F309AD18-D86A-11D0-A075-00C04FB68820} WMI-IWbemLevel1Login Call=0x3
42 0.109375 {MSRPC:14, TCP:12, IPv4:5} test125.test.local test124.test.local MSRPC MSRPC: c/o Alter Cont Resp: Call=0x3 Assoc Grp=0x333E Xmit=0x16D0 Recv=0x16D0
43 0.109375 {MSRPC:14, TCP:12, IPv4:5} test124.test.local test125.test.local DCOM DCOM

44 0.109375 {MSRPC:14, TCP:12, IPv4:5} test125.test.local test124.test.local DCOM DCOM
45 0.109375 {MSRPC:14, TCP:12, IPv4:5} test124.test.local test125.test.local DCOM
COM
46 0.109375 {MSRPC:14, TCP:12, IPv4:5} test125.test.local test124.test.local DCOM DCOM
47 0.109375 {MSRPC:14, TCP:12, IPv4:5} test124.test.local test125.test.local MSRPC MSRPC: c/o Alter Cont: UUID{9556DC99-828C-11CF-A37E-00AA003240C7} WMI-IWbemServices Call=0x5
48 0.109375 {MSRPC:14, TCP:12, IPv4:5} test125.test.local test124.test.local MSRPC MSRPC: c/o Alter Cont Resp: Call=0x5 Assoc Grp=0x333E Xmit=0x16D0 Recv=0x16D0
49 0.109375 {MSRPC:14, TCP:12, IPv4:5} test124.test.local test125.test.local DCOM DCOM
50 0.109375 {MSRPC:14, TCP:12, IPv4:5} test125.test.local test124.test.local DCOM DCOM
51 0.109375 {MSRPC:14, TCP:12, IPv4:5} test124.test.local test125.test.local DCOM DCOM
52 0.109375 {MSRPC:14, TCP:12, IPv4:5} test125.test.local test124.test.local DCOM DCOM
53 0.109375 {MSRPC:14, TCP:12, IPv4:5} test124.test.local test125.test.local MSRPC MSRPC: c/o Alter Cont: UUID{1C1C45EE-4395-11D2-B60B-00104B703EFD} WMI-IWbemFetchSmartEnum Call=0x7 54 0.109375 {MSRPC:14, TCP:12, IPv4:5} test125.test.local test124.test.local MSRPC MSRPC: c/o Alter Cont Resp: Call=0x7 Assoc Grp=0x333E Xmit=0x16D0 Recv=0x16D0
55 0.109375 {MSRPC:14, TCP:12, IPv4:5} test124.test.local test125.test.local DCOM DCOM
56 0.109375 {MSRPC:14, TCP:12, IPv4:5} test125.test.local test124.test.local DCOM DCOM
57 0.109375 {MSRPC:14, TCP:12, IPv4:5} test124.test.local test125.test.local MSRPC MSRPC: c/o Alter Cont: UUID{423EC01E-2E35-11D2-B604-00104B703EFD} WMI-IWbemWCOSmartEnum Call=0x8
58 0.109375 {MSRPC:14, TCP:12, IPv4:5} test125.test.local test124.test.local MSRPC MSRPC: c/o Alter Cont Resp: Call=0x8 Assoc Grp=0x333E Xmit=0x16D0 Recv=0x16D0
59 0.109375 {MSRPC:14, TCP:12, IPv4:5} test124.test.local test125.test.local DCOM DCOM

Toàn b? c?m RPC/DCOM, gi?ng các d?u hi?u khác.

60 0.187500 {TCP:6, IPv4:5} test124.test.local test125.test.local TCP TCP: Flags=.A., SrcPort=1063, DstPort=DCE endpoint resolution(135), Len=0, Seq=539163382, Ack=981335462, Win=65339 (scale factor 0) = 65339
61 0.187500 {MSRPC:14, TCP:12, IPv4:5} test125.test.local test124.test.local DCOM DCOM
62 0.187500 {TCP:12, IPv4:5} test125.test.local test124.test.local TCP TCP: [Continuation to #61]Flags=.A., SrcPort=1117, DstPort=1066, Len=1460, Seq=539975906 - 539977366, Ack=1180776977, Win=65061 (scale factor 0) = 65061
63 0.187500 {TCP:12, IPv4:5} test124.test.local test125.test.local TCP TCP: Flags=.A., SrcPort=1066, DstPort=1117, Len=0, Seq=1180776977, Ack=539977366, Win=65535 (scale factor 0) = 65535
64 0.187500 {TCP:12, IPv4:5} test125.test.local test124.test.local TCP TCP: [Continuation to #61]Flags=.A., SrcPort=1117, DstPort=1066, Len=1460, Seq=539977366 - 539978826, Ack=1180776977, Win=65061 (scale factor 0) = 65061
65 0.187500 {TCP:12, IPv4:5} test124.test.local test125.test.local TCP TCP: Flags=.A., SrcPort=1066, DstPort=1117, Len=0, Seq=1180776977, Ack=539978826, Win=65535 (scale factor 0) = 65535
66 0.187500 {TCP:12, IPv4:5} test125.test.local test124.test.local TCP TCP: [Continuation to #61]Flags=.PA., SrcPort=1117, DstPort=1066, Len=1449, Seq=539978826 - 539980275, Ack=1180776977, Win=65061 (scale factor 0) = 65061
67 0.187500 {MSRPC:14, TCP:12, IPv4:5} test125.test.local test124.test.local MSRPC MSRPC: c/o Continued Response: WMI-IWbemWCOSmartEnum Call=0x8 Context=0x5 Hint=0x198C Cancels=0x0
.
.
.

148 0.187500 {MSRPC:14, TCP:12, IPv4:5} test125.test.local test124.test.local MSRPC MSRPC: c/o Continued Response: WMI-IWbemServices Call=0x9 Context=0x3 Hint=0x1F84 Cancels=0x0
149 0.187500 {TCP:12, IPv4:5} test125.test.local test124.test.local TCP TCP: [Continuation to #148]Flags=.A., SrcPort=1117, DstPort=1066, Len=1460, Seq=540058365 - 540059825, Ack=1180777222, Win=64816 (scale factor 0) = 64816
150 0.187500 {TCP:12, IPv4:5} test124.test.local test125.test.local TCP TCP: Flags=.A., SrcPort=1066, DstPort=1117, Len=0, Seq=1180777222, Ack=540059825, Win=65535 (scale factor 0) = 65535
151 0.187500 {TCP:12, IPv4:5} test125.test.local test124.test.local TCP TCP: [Continuation to #148]Flags=.A., SrcPort=1117, DstPort=1066, Len=1460, Seq=540059825 - 540061285, Ack=1180777222, Win=64816 (scale factor 0) = 64816
152 0.187500 {TCP:12, IPv4:5} test125.test.local test124.test.local TCP TCP: [Continuation to #148]Flags=.PA., SrcPort=1117, DstPort=1066, Len=1449, Seq=540061285 - 540062734, Ack=1180777222, Win=64816 (scale factor 0) = 64816
153 0.187500 {TCP:12, IPv4:5} test124.test.local test125.test.local TCP TCP: Flags=.A., SrcPort=1066, DstPort=1117, Len=0, Seq=1180777222, Ack=540062734, Win=65535 (scale factor 0) = 65535
154 0.187500 {MSRPC:14, TCP:12, IPv4:5} test125.test.local test124.test.local MSRPC MSRPC: c/o Continued Response: WMI-IWbemServices Call=0x9 Context=0x3 Hint=0x904 Cancels=0x0
155 0.187500 {TCP:12, IPv4:5} test125.test.local test124.test.local TCP TCP: [Continuation to #154]Flags=.PA., SrcPort=1117, DstPort=1066, Len=929, Seq=540064194 - 540065123, Ack=1180777222, Win=64816 (scale factor 0) = 64816
156 0.187500 {TCP:12, IPv4:5} test124.test.local test125.test.local TCP TCP: Flags=.A., SrcPort=1066, DstPort=1117, Len=0, Seq=1180777222, Ack=540065123, Win=65535 (scale factor 0) = 65535
157 0.187500 {MSRPC:14, TCP:12, IPv4:5} test124.test.local test125.test.local DCOM DCOM
RPC together with TCP. You can see the WMI interface calls happening.
RPC cùng v?i TCP. B?n có th? nhìn th?y các cu?c g?i giao di?n WMI ?ang di?n ra.
158 0.218750 {ARP:15} 172.16.11.144 172.16.11.144 ARP ARP: Request, 172.16.11.144 asks for 172.16.11.144

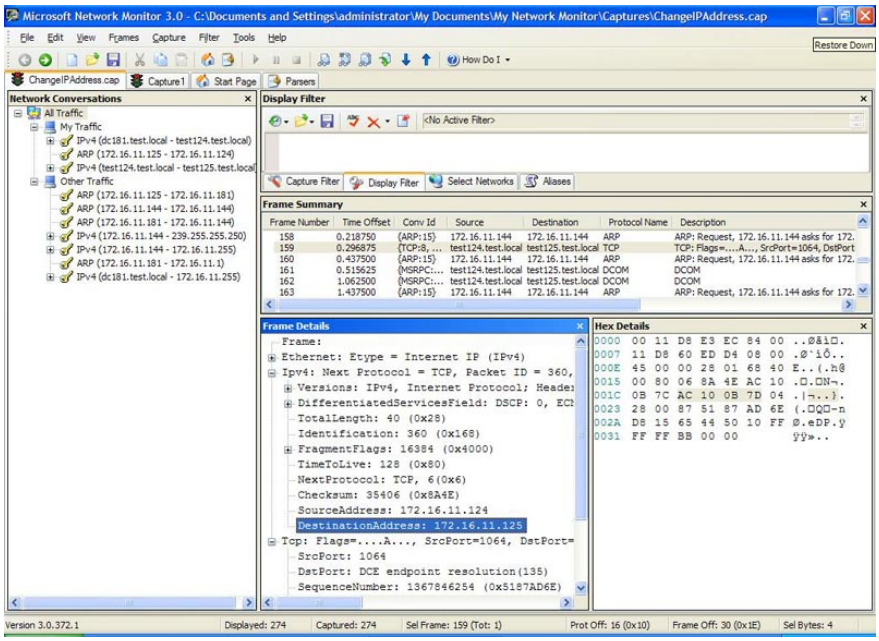
K?ch b?n trên ?ã thay ??i thành công ??a ch? IP c?a máy tính m?c tiêu (test125) t? 172.16.11.125 thành 172.16.11.144, v?y t?i sao máy tính m?c tiêu s? d?ng ARP ?? th? và chuy?n ??a ch? IP c?a nó vào thành ??a ch? MAC? ?i?u này là m?t ví d? ARP không có lý do, ?i?u ?ã x?y ra khi m?t nút nào ?ó kh?i t?o yêu c?u ARP cho ?? a ch? IP c?a nó. V?y t?i sao máy tính m?c tiêu th?c hi?n ?i?u này? ?? b?o ??m ??a ch? IP m?i không b? s? d?ng b ?i b?t k? nút m?ng khác nào trong m?ng. Máy tính m?c tiêu ??a ra m?t vài yêu c?u ARP và n?u không có ?áp ? ng ARP nào ???c nh?n thì nó s? ??a ra quy?t ??nh r?ng ??a ch? m?i c?a nó là duy nh?t ??i v?i m?ng và ??a ch? ? ó có th? ???c gi? l?i. Tuy nhiên n?u m?t nút khác ??a ra m?t ?áp ?ng ARP cho yêu c?u này thì ?ây s? là nút ??u tiên th?a nh?n có m?t ??a ch? xung ??t trên m?ng và nó vô hi?u hóa ??a ch? IP c?a nó (gán thành 0.0.0.0).

? ?ây, m?i th? d??ng nh? ???c gi?i quy?t – b?n có th? th?y ?i?u này b?i s? th?t r?ng th?i gian bên trong các gói ? ang t?ng ?áng k?. Nh?ng gì ?ó x?y ra ti?p theo là nút mã ngu?n (test124) c? g?ng phúc ?áp TCP v?i máy tính m? c tiêu nh?ng không g?p ? v? trí nào:

159 0.296875 {TCP:8, IPv4:5} test124.test.local test125.test.local TCP TCP: Flags=.A., SrcPort=1064, DstPort=DCE endpoint resolution(135), Len=0, Seq=1367846254, Ack=3625280836, Win=65535 (scale factor 0) = 65535
160 0.437500 {ARP:15} 172.16.11.144 172.16.11.144 ARP ARP: Request, 172.16.11.144 asks for 172.16.11.144
161 0.515625 {MSRPC:14, TCP:12, IPv4:5} test124.test.local test125.test.local DCOM DCOM
162 1.062500 {MSRPC:14, TCP:12, IPv4:5} test124.test.local test125.test.local DCOM DCOM

163 1.437500 {ARP:15} 172.16.11.144 172.16.11.144 ARP ARP: Request, 172.16.11.144 asks for 172.16.11.144
164 2.265625 {MSRPC:14, TCP:12, IPv4:5} test124.test.local test125.test.local DCOM DCOM
165 2.453125 {ARP:15} 172.16.11.144 172.16.11.144 ARP ARP: Request, 172.16.11.144 asks for 172.16.11.144
166 3.437500 {ARP:15} 172.16.11.144 172.16.11.144 ARP ARP: Request, 172.16.11.144 asks for 172.16.11.144
167 4.437500 {ARP:15} 172.16.11.144 172.16.11.144 ARP ARP: Request, 172.16.11.144 asks for 172.16.11.144
168 4.671875 {MSRPC:14, TCP:12, IPv4:5} test124.test.local test125.test.local DCOM DCOM

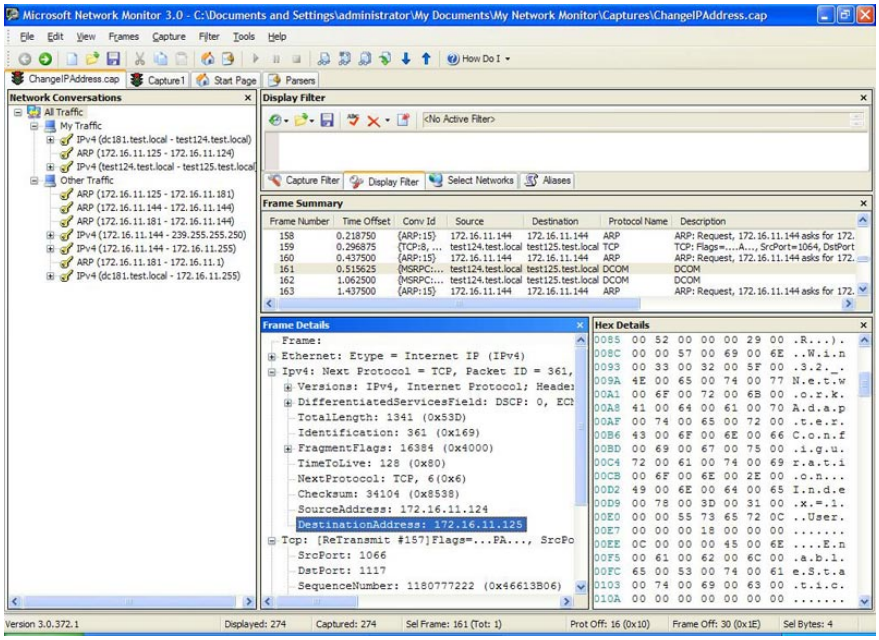
Hãy xem xét gói 159 ? trên (Hình 8):



Hình 8: Các v?n ?? k?t n?i TCP

L?u ý t? hình này r?ng máy tính ngu?n (test124) v?n cho r?ng máy ?ích có ??a ch? IP là 172.16.11.125, và nó v?n c? g?ng g?i tín hi?u ACK ??n test125 ?? duy trì k?t n?i TCP ???c thành l?p tr??c ?ó.

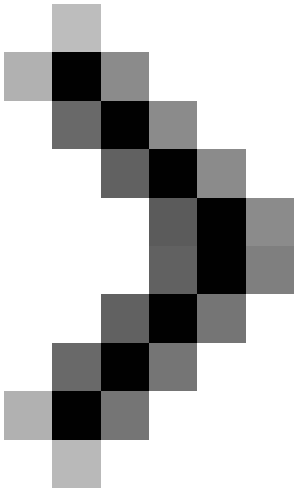
Hãy xem khung 161 (Hình 9):



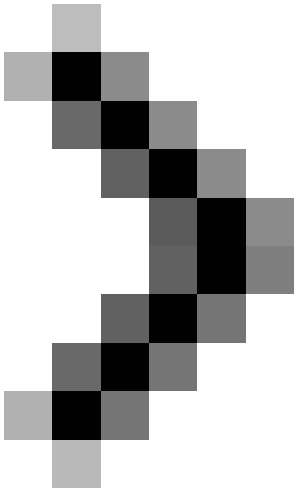
Hình 9: Các v?n ?? RPC/DCOM

L?u ý r?ng vi?c k?t n?i RPC ???c thành l?p tr??c ?ó b?ng máy tính ngu?n (test124) v?i máy tính ?ích (test125), ? ang c? g?ng tri?u g?i DCOM ?? g?i EnableStatic Method c?a l?p Win32_NetworkAdapterConfiguration. (?? có th? xem ???c v?n ?? này, b?n hãy nhìn vào ph?n c?a s? Hex Details, n?i có th? xem t?i tr?ng hex c?a gói RPC ???c hi?n th? d??i d?ng v?n b?n Unicode). Tuy nhiên trong vi?c c? g?ng tri?u g?i DCOM, máy tính ngu?n v?n ngh? ??a ch? ?ích c?a máy tính m?c tiêu là 172.16.11.125 (xem ph?n Frame Details trong hình v?).

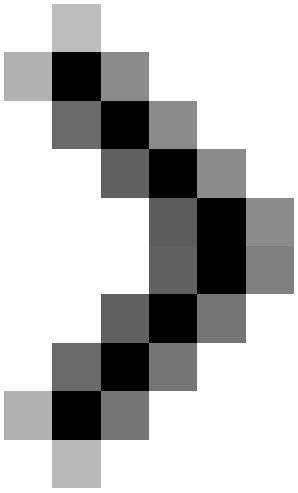
Ph?n còn l?i c?a ChangeIPAddress.vbs c?ng r?t thú v? ?? phân tích tuy nhiên chúng ta ?ã nh?n ra ???c lý do t?i sao k?ch b?n ?i?u khi?n xa không ch?y ?úng cách. Rõ ràng nó làm vi?c n?u chúng ta s? d?ng cách gi?i quy?t On Error Resume Next mà chúng ta ?ã ?? c?p ??n trong bài vi?t tr??c.



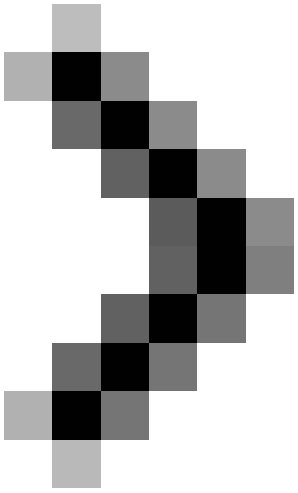
Ph?n 9: Tìm hi?u k?ch b?n ?i?u khi?n xa



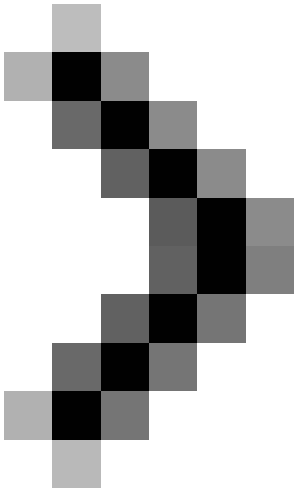
Ph?n 10: Các th? thu?t c?a k?ch b?n ?i?u khi?n xa



Ph?n 11: Các th? thu?t k?ch b?n khác



Ph?n 12: Các thu?c tính c?a l?p WMI



Ph?n 13: K?ch b?n tr? v? t?t c? các giá tr?

You finished reading the article "**Managing Windows Networks using Script - Part 8: Handling remote scripting errors using Network Monitor 3.0**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.