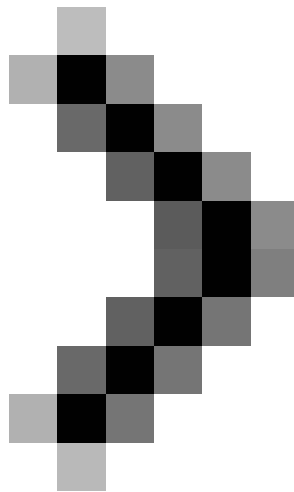
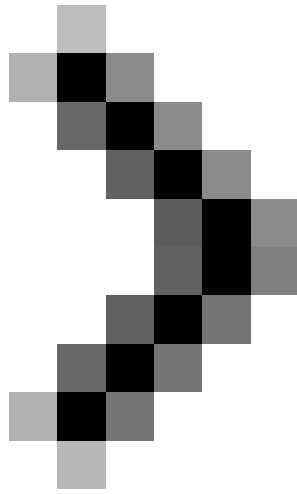


Working with Network Monitor (Part 5)

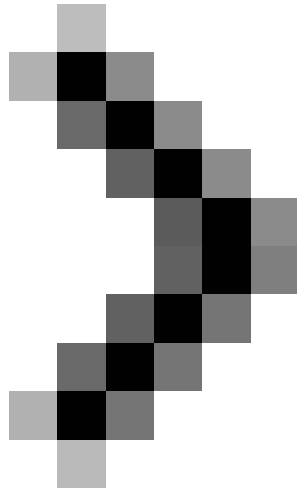
In the previous article of this series, we demonstrated that even capturing a simple network will give a lot of result packages that you don't really need. And also showed you how to filter out 'junk' packages to see only the



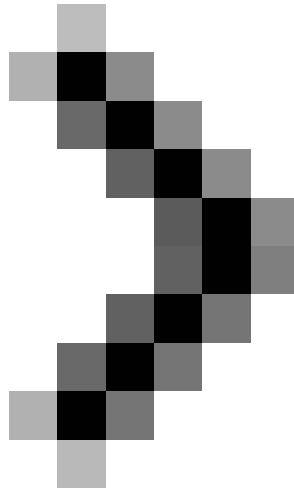
Working with Network Monitor (Part 1)



Working with Network Monitor (Part 2)



Working with Network Monitor (Part 3)



Working with Network Monitor (Part 4)

Brien M. Posey

In the previous article of this series, we demonstrated that even capturing a simple network will give a lot of result packages that you don't really need. And also showed you how to filter out 'junk' packages to see only the packages that you really care about. Now we want to continue to show you how to analyze the rest of the packages so that you can see what they include.

In the previous section of the previous section, the captured and filtered set of packages is similar to the one shown in Figure A. As explained in the first part of this article, I captured the data shown in the figure. by starting the capture, then executing the PING command and finally stopping the capture. My goal is to simplify things if possible. If you look at Figure A, you can see where the ICMP packets have been broadcast and where the replies have been received.

161	3.384868	LOCAL	000FB546EAAA	ICMP	Echo: From 147.100.100.34 To 147.100.100.99	FUBAR	Tasmania
162	3.384868	000FB546EAAA	LOCAL	ICMP	Echo Reply: To 147.100.100.34 From 147.100.100.99	Tasmania	FUBAR
230	4.386308	LOCAL	000FB546EAAA	ICMP	Echo: From 147.100.100.34 To 147.100.100.99	FUBAR	Tasmania
231	4.386308	000FB546EAAA	LOCAL	ICMP	Echo Reply: To 147.100.100.34 From 147.100.100.99	Tasmania	FUBAR
284	4.746826	000FB546EAAA	LOCAL	LDAP	ProtocolOp: SearchRequest (3)	Tasmania	FUBAR
285	4.746826	LOCAL	000FB546EAAA	LDAP	ProtocolOp: SearchResponse (4)	FUBAR	Tasmania
288	4.746826	000FB546EAAA	LOCAL	LDAP	ProtocolOp: BindRequest (0)	Tasmania	FUBAR
289	4.756840	LOCAL	000FB546EAAA	LDAP	ProtocolOp: BindResponse (1)	FUBAR	Tasmania
290	4.756840	000FB546EAAA	LOCAL	LDAP	ProtocolOp: SearchRequest (3)	Tasmania	FUBAR
291	4.756840	LOCAL	000FB546EAAA	LDAP	ProtocolOp: SearchResponse (4)	FUBAR	Tasmania
292	4.756840	000FB546EAAA	LOCAL	LDAP	ProtocolOp: SearchRequest (3)	Tasmania	FUBAR
293	4.756840	LOCAL	000FB546EAAA	LDAP	ProtocolOp: SearchResponse (4)	FUBAR	Tasmania
294	4.756840	000FB546EAAA	LOCAL	LDAP	ProtocolOp: SearchRequest (3)	Tasmania	FUBAR
295	4.756840	LOCAL	000FB546EAAA	LDAP	ProtocolOp: SearchResponse (4)	FUBAR	Tasmania
296	4.756840	000FB546EAAA	LOCAL	LDAP	ProtocolOp: SearchRequest (3)	Tasmania	FUBAR
297	4.756840	LOCAL	000FB546EAAA	LDAP	ProtocolOp: SearchResponse (4)	FUBAR	Tasmania
298	4.756840	000FB546EAAA	LOCAL	LDAP	ProtocolOp: SearchRequest (3)	Tasmania	FUBAR
299	4.756840	LOCAL	000FB546EAAA	LDAP	ProtocolOp: SearchResponse (4)	FUBAR	Tasmania
300	4.756840	000FB546EAAA	LOCAL	LDAP	ProtocolOp: SearchRequest (3)	Tasmania	FUBAR
301	4.756840	LOCAL	000FB546EAAA	LDAP	ProtocolOp: SearchResponse (4)	FUBAR	Tasmania
302	4.756840	000FB546EAAA	LOCAL	ICMP	Echo: From 147.100.100.99 To 147.100.100.34	Tasmania	FUBAR
303	4.756840	LOCAL	000FB546EAAA	ICMP	Echo Reply: To 147.100.100.99 From 147.100.100.34	FUBAR	Tasmania
306	4.766855	000FB546EAAA	LOCAL	ICMP	Echo: From 147.100.100.99 To 147.100.100.34	Tasmania	FUBAR
307	4.766855	LOCAL	000FB546EAAA	ICMP	Echo Reply: To 147.100.100.99 From 147.100.100.34	FUBAR	Tasmania
309	4.766855	000FB546EAAA	LOCAL	SMB	C negotiate, Dialect = NT LM 0.12	Tasmania	FUBAR
310	4.766855	LOCAL	000FB546EAAA	SMB	E negotiate, Dialect # = 5	FUBAR	Tasmania
311	4.766855	000FB546EAAA	LOCAL	SMB	C session setup & X	Tasmania	FUBAR
314	4.766855	LOCAL	000FB546EAAA	SMB	E session setup & X	FUBAR	Tasmania
315	4.766855	000FB546EAAA	LOCAL	SMB	C tree connect & X, Share = \\FUBAR.PRODUCT...	Tasmania	FUBAR
316	4.766855	LOCAL	000FB546EAAA	SMB	E tree connect & X, Type = IPC	FUBAR	Tasmania
317	4.766855	000FB546EAAA	LOCAL	SMB	C NT create & X, File = \HETLLOGON	Tasmania	FUBAR
318	4.766855	LOCAL	000FB546EAAA	SMB	E NT create & X, FID = 0x8007	FUBAR	Tasmania
319	4.766855	000FB546EAAA	LOCAL	NSRPC	c/o RPC Bind: UUID 12345678-1234-AB...	Tasmania	FUBAR
320	4.766855	LOCAL	000FB546EAAA	SMB	E write & X, Urcode 0x74	FUBAR	Tasmania
321	4.766855	000FB546EAAA	LOCAL	SMB	C read & X, FID = 0x8007, Read 0x400 at 0x0...	Tasmania	FUBAR
322	4.766855	LOCAL	000FB546EAAA	NSRPC	c/o RPC Bind Ack: call 0x1 assoc grp 0...	FUBAR	Tasmania
323	4.766855	000FB546EAAA	LOCAL	NSRPC	c/o RPC Request: call 0x1 sprnum 0x22 ...	Tasmania	FUBAR
324	4.766855	LOCAL	000FB546EAAA	R_LOGON	Error: Bad Opcode (Function does not exist)	FUBAR	Tasmania
325	4.766855	000FB546EAAA	LOCAL	SMB	C close file, FID = 0x8007	Tasmania	FUBAR
326	4.766855	LOCAL	000FB546EAAA	SMB	E close file	FUBAR	Tasmania
327	4.766855	000FB546EAAA	LOCAL	LDAP	ProtocolOp: UnbindRequest (2)	Tasmania	FUBAR
365	5.387748	LOCAL	000FB546EAAA	ICMP	Echo: From 147.100.100.34 To 147.100.100.99	FUBAR	Tasmania
366	5.387748	000FB546EAAA	LOCAL	ICMP	Echo Reply: To 147.100.100.34 From 147.100.100.99	Tasmania	FUBAR
416	6.389188	LOCAL	000FB546EAAA	ICMP	Echo: From 147.100.100.34 To 147.100.100.99	FUBAR	Tasmania
417	6.389188	000FB546EAAA	LOCAL	ICMP	Echo Reply: To 147.100.100.34 From 147.100.100.99	Tasmania	FUBAR

Figure 1: Really useful when filtering out unimportant packages

If this is a real life capture, there is no need to delve into the data because you can tell exactly what is going on by observing the Description column. But in the real world, things aren't that simple. To determine exactly what is going on inside a trace, it is necessary to look inside specific data packets.

There is nothing special to introduce to you in the ICMP package. In this case, let's look at some of the captured LDAP packets. You probably already know, LDAP stands for Light Weight Directory Access Protocol. LDAP is the protocol used to read information from Active Directory and also write information to Active Directory.

There are two reasons we want to show you how to analyze an LDAP package. First, in real world traces to the Windows network, LDAP packets are a very general case. The existence of LDAP packages in such a common way that you will need to decipher their meaning. The second reason is to understand what package is working. The technologies we want to show you can be used to look at the content within packages, which means that not every package will mean anything unless you are an expert on protocol.

Consider inside a package

Let's start by looking inside the box 284. The description simply says that this frame is a search request. However, in fact, it shows that a machine emitting this LDAP search request doesn't really give you that much. One way to know what this search request includes is to look inside the package.

Before opening the package, click on the icons to change the details panel and the hex panel. When all three panels are displayed, select the package you want to consider. When you are done selecting the package, you will see a screen similar to the one shown in Figure B.

284	4.746826	000FB546EAAA4	LOCAL	LDAP	ProtocolOp: SearchReq
285	4.746826	LOCAL	000FB546EAAA4	LDAP	ProtocolOp: SearchResp
288	4.746826	000FB546EAAA4	LOCAL	LDAP	ProtocolOp: BindRequest
289	4.756840	LOCAL	000FB546EAAA4	LDAP	ProtocolOp: BindResponse
290	4.756840	000FB546EAAA4	LOCAL	LDAP	ProtocolOp: SearchReq
291	4.756840	LOCAL	000FB546EAAA4	LDAP	ProtocolOp: SearchResp
292	4.756840	000FB546EAAA4	LOCAL	LDAP	ProtocolOp: SearchReq
293	4.756840	LOCAL	000FB546EAAA4	LDAP	ProtocolOp: SearchResp
294	4.756840	000FB546EAAA4	LOCAL	LDAP	ProtocolOp: SearchReq
295	4.756840	LOCAL	000FB546EAAA4	LDAP	ProtocolOp: SearchResp
296	4.756840	000FB546EAAA4	LOCAL	LDAP	ProtocolOp: SearchReq
297	4.756840	LOCAL	000FB546EAAA4	LDAP	ProtocolOp: SearchResp
298	4.756840	000FB546EAAA4	LOCAL	LDAP	ProtocolOp: SearchReq
299	4.756840	LOCAL	000FB546EAAA4	LDAP	ProtocolOp: SearchResp
300	4.756840	000FB546EAAA4	LOCAL	LDAP	ProtocolOp: SearchReq

```

+ FRAME: Base frame properties
+ ETHERNET: EType = Internet IP (IPv4)
+ IP: Protocol = TCP - Transmission Control; Packet ID = 4972; Total IP Length
+ TCP: Control Bits: .AP..., len: 351, seq:4053217973-4053218324, ack:1281832
+ LDAP: ProtocolOp: SearchRequest (3)

```

00000030	FF FF C7 DD 00 00 30 84 00 00 01 59 02 02 04 8E	..0ä..@Y@+Ä
00000040	63 84 00 00 01 4F 04 00 0A 01 00 0A 01 00 02 01	cä..@0+.@@.@@.@@
00000050	00 02 01 78 01 01 00 87 0B 6F 62 6A 65 63 74 63	.@x@@.çobjectc
00000060	6C 61 73 73 30 84 00 00 01 2B 04 11 73 75 62 73	lass0ä..@+*subs
00000070	63 68 65 6D 61 53 75 62 65 6E 74 72 79 04 0D 64	chemaSubentry+&d
00000080	73 53 65 72 76 69 63 65 4E 61 6D 65 04 0E 6E 61	sServiceName+&na
00000090	6D 69 6E 67 43 6F 6E 74 65 78 74 73 04 14 64 65	mingContexts+&de
000000A0	66 61 75 6C 74 4E 61 6D 69 6E 67 43 6F 6E 74 65	faultNamingConte
000000B0	78 74 04 13 73 63 68 65 6D 61 4E 61 6D 69 6E 67	xt+&schemaNaming
000000C0	43 6F 6E 74 65 78 74 04 1A 63 6F 6E 66 69 67 75	Context+&-configu
000000D0	72 61 74 69 6F 6E 4E 61 6D 69 6E 67 43 6F 6E 74	rationNamingCont
000000E0	65 78 74 04 17 72 6F 6F 74 44 6F 6D 61 69 6E 4E	ext+&rootDomainN
000000F0	61 6D 69 6E 67 43 6F 6E 74 65 78 74 04 10 73 75	amingContext+&su
00000100	70 70 6F 72 74 65 64 43 6F 6E 74 72 6F 6C 04 14	pportedControl+&f
00000110	73 75 70 70 6F 72 74 65 64 4C 44 41 50 56 65 72	supportedLDAPVer
00000120	73 69 6F 6E 04 15 73 75 70 70 6F 72 74 65 64 4C	sion+&\$supportedL
00000130	44 41 50 50 6F 6C 69 63 69 65 73 04 17 73 75 70	DAPPolicies+&sup
00000140	70 6F 72 74 65 64 53 41 53 4C 4D 65 63 68 61 6E	portedSASLMechan
00000150	69 73 6D 73 04 0B 64 6E 73 48 6F 73 74 4E 61 6D	isms+&dnsHostNam
00000160	65 04 0F 6C 64 61 70 53 65 72 76 69 63 65 4E 61	e+&ldapServiceNa
00000170	6D 65 04 0A 73 65 72 76 65 72 4E 61 6D 65 04 15	me+&serverName+&\$
00000180	73 75 70 70 6F 72 74 65 64 43 61 70 61 62 69 6C	supportedCapabil
00000190	69 74 69 65 73	ities

Figure B: Content inside a package

The first thing to consider is the details panel. If you look at this panel you will see that there are a number of different items that are scalable (Frame, Ethernet, IP, TCP and LDAP). The reason for the different entries here is because the packages are typically primitive. The package that we are considering is an LDAP package, but computers do not mention primitive LDAP. LDAP is based on TCP protocol. TCP is a small part of the IP protocol. Each item in the details pane shows a separate summary class.

If you look at the hex panel, you will see the contents of the packages shown as hexa. Note that each byte is marked with black. The reason for this markup is because the bytes highlighted in black correspond to the part of the selected package in the details pane. In this particular case, the FRAME item is selected. This section shows the entire frame, which explains why the entire frame is blacked out. If we select the LDAP entry, only the bytes

corresponding to the LDAP data will be blacked out as shown in Figure C.

The screenshot shows a network analysis tool interface. At the top is a menu bar (File, Edit, Display, Tools, Options, Window, Help) and a toolbar with various icons. Below this is a table of network frames:

Frame	Time	Src MAC Addr	Dst MAC Addr	Protocol	Description
284	4.746826	000FB546EAA4	LOCAL	LDAP	ProtocolOp: SearchRequest (3)
285	4.746826	LOCAL	000FB546EAA4	LDAP	ProtocolOp: SearchResponse (4)
286	4.746826	LOCAL	000FB546EAA4	TCP	Control Bits: .AP..., len: 51
287	4.746826	000FB546EAA4	LOCAL	TCP	Control Bits: .A..., len:
288	4.746826	000FB546EAA4	LOCAL	LDAP	ProtocolOp: BindRequest (0)
289	4.756840	LOCAL	000FB546EAA4	LDAP	ProtocolOp: BindResponse (1)
290	4.756840	000FB546EAA4	LOCAL	LDAP	ProtocolOp: SearchRequest (3)
291	4.756840	LOCAL	000FB546EAA4	LDAP	ProtocolOp: SearchResponse (4)
292	4.756840	000FB546EAA4	LOCAL	LDAP	ProtocolOp: SearchRequest (3)
293	4.756840	LOCAL	000FB546EAA4	LDAP	ProtocolOp: SearchResponse (4)
294	4.756840	000FB546EAA4	LOCAL	LDAP	ProtocolOp: SearchRequest (3)
295	4.756840	LOCAL	000FB546EAA4	LDAP	ProtocolOp: SearchResponse (4)
296	4.756840	000FB546EAA4	LOCAL	LDAP	ProtocolOp: SearchRequest (3)
297	4.756840	LOCAL	000FB546EAA4	LDAP	ProtocolOp: SearchResponse (4)
298	4.756840	000FB546EAA4	LOCAL	LDAP	ProtocolOp: SearchRequest (3)

Below the frame list, the details for the selected frame (Frame 284) are shown:

- FRAME: Base frame properties
- ETHERNET: EType = Internet IP (IPv4)
- IP: Protocol = TCP - Transmission Control; Packet ID = 4972; Total IP Length = 391;
- TCP: Control Bits: .AP..., len: 351, seq:4053217973-4053218324, ack:1281832858, win
- LDAP: ProtocolOp: SearchRequest (3)

At the bottom, a hex dump of the selected frame is displayed, with the right column containing ASCII characters that are partially blacked out:

```

00000000 00 0F B5 46 E8 03 00 0F B5 46 EA A4 08 00 45 00  .O F + . O F N m . E.
00000010 01 87 13 6C 40 00 80 06 F6 B6 93 64 64 63 93 64  @c#10.C*+|ôddcôd
00000020 64 22 29 32 01 85 F1 97 32 B5 4C 67 37 9A 50 18  d")Z@arü2Lg7UPt
00000030 FF FF C7 DD 00 00 30 84 00 00 01 59 02 02 04 8E  . . .0a..OY@+A
00000040 63 84 00 00 01 4F 04 00 0A 01 00 0A 01 00 02 01  çâ..00+.00.00.00
00000050 00 02 01 78 01 01 00 87 0B 6F 62 6A 65 63 74 63  .@x@.çobjectc
00000060 6C 61 73 73 30 84 00 00 01 2B 04 11 73 75 62 73  lass0a..@+*subs
00000070 63 68 65 6D 61 53 75 62 65 6E 74 72 79 04 0D 64  chemaSubentry+d
00000080 73 53 65 72 76 69 63 65 4E 61 6D 65 04 0E 6E 61  sServiceName+&na
00000090 6D 69 6E 67 43 6F 6E 74 65 78 74 73 04 14 64 65  mingContexts+7de
000000A0 66 61 75 6C 74 4E 61 6D 69 6E 67 43 6F 6E 74 65  faultNamingConte
000000B0 78 74 04 13 73 63 68 65 6D 61 4E 61 6D 69 6E 67  xt+!$schemaNaming
000000C0 43 6F 6E 74 65 78 74 04 1A 63 6F 6E 66 69 67 75  Context+~configu
000000D0 72 61 74 69 6F 6E 4E 61 6D 69 6E 67 43 6F 6E 74  rationNamingCont
000000E0 65 78 74 04 17 72 6F 6F 74 44 6F 6D 61 69 6E 4E  ext+;rootDomainN
000000F0 61 6D 69 6E 67 43 6F 6E 74 65 78 74 04 10 73 75  mingContext+>su
00000100 70 70 6F 72 74 65 64 43 6F 6E 74 72 6F 6C 04 14  pportedControl+fl
00000110 73 75 70 70 6F 72 74 65 64 4C 44 41 50 56 65 72  supportedLDAPVer
00000120 73 69 6F 6E 04 15 73 75 70 70 6F 72 74 65 64 4C  sion+$supportedL
00000130 44 41 50 50 6F 6C 69 63 69 65 73 04 17 73 75 70  DAPolicies+;sup
00000140 70 6F 72 74 65 64 53 41 53 4C 4D 65 63 68 61 6E  portedSASLMechan
00000150 69 73 6D 73 04 0B 64 6E 73 48 6F 73 74 4E 61 6D  isms+&dnsHostNam
00000160 65 64 6E 6C 64 61 50 53 6F 73 75 69 69 65 4F 61  &ldwServiceN
  
```

Figure C: Panel hex blackens the currently selected part of the package

You can see that each of these packages is expandable. By clicking on the plus sign next to each item, it can log content inside the package. Usually we can completely see the exact package by looking inside the frame. If you look closely at Figure C, you can pick up some words that can be read inside the content. However, this readable data is actually very difficult to read in practice. Words start on this line and end on the next line and are often divided by confusing symbols. Blackening also makes this part more difficult to read. A better way to see the

contents of this package is to extend the LDAP portion of the package from within the details pane. Expanding the LDAP panel will show you that this particular package is an LDAP search request as shown in Figure D. This means that the package has been sent trying to query Active Directory.

Frame	Time	Src MAC Addr	Dst MAC Addr	Protocol	Description
284	4.746826	000FB546EAA4	LOCAL	LDAP	ProtocolOp: SearchRequest
285	4.746826	LOCAL	000FB546EAA4	LDAP	ProtocolOp: SearchResponse
286	4.746826	LOCAL	000FB546EAA4	TCP	Control Bits: .AP..., len
287	4.746826	000FB546EAA4	LOCAL	TCP	Control Bits: .A..., len
288	4.746826	000FB546EAA4	LOCAL	LDAP	ProtocolOp: BindRequest (
289	4.756840	LOCAL	000FB546EAA4	LDAP	ProtocolOp: BindResponse
290	4.756840	000FB546EAA4	LOCAL	LDAP	ProtocolOp: SearchRequest
291	4.756840	LOCAL	000FB546EAA4	LDAP	ProtocolOp: SearchResponse
292	4.756840	000FB546EAA4	LOCAL	LDAP	ProtocolOp: SearchRequest
293	4.756840	LOCAL	000FB546EAA4	LDAP	ProtocolOp: SearchResponse
294	4.756840	000FB546EAA4	LOCAL	LDAP	ProtocolOp: SearchRequest
295	4.756840	LOCAL	000FB546EAA4	LDAP	ProtocolOp: SearchResponse
296	4.756840	000FB546EAA4	LOCAL	LDAP	ProtocolOp: SearchRequest
297	4.756840	LOCAL	000FB546EAA4	LDAP	ProtocolOp: SearchResponse
298	4.756840	000FB546EAA4	LOCAL	LDAP	ProtocolOp: SearchRequest

```

+ FRAME: Base frame properties
+ ETHERNET: EType = Internet IP (IPv4)
+ IP: Protocol = TCP - Transmission Control; Packet ID = 4972; Total IP Length =
+ TCP: Control Bits: .AP..., len: 351, seq:4053217973-4053218324, ack:1281832858
- LDAP: ProtocolOp: SearchRequest (3)
  - LDAP: MessageID = 1166 (0x48E)
    + LDAP: ProtocolOp = SearchRequest
  
```

00000000	00 0F B5 46 E8 03 00 0F B5 46 EA A4 08 00 45 00	.0 F 5 46 E8 03 00 0F B5 46 EA A4 08 00 45 00
00000010	01 87 13 6C 40 00 80 06 F6 B6 93 64 64 63 93 64	@c#1 8 .C + ôddcôd
00000020	64 22 29 32 01 85 F1 97 32 B5 4C 67 37 9A 50 18	d")2@â û2 Lg7Û
00000030	FF FF C7 DD 00 00 30 84 00 00 01 59 02 02 04 8E	.0â .0Y00+
00000040	53 84 00 00 01 4F 04 00 0A 01 00 0A 01 00 02 01	çâ..0+ 00 00 00
00000050	00 02 01 78 01 01 00 87 0B 6F 62 6A 65 63 74 63	.00x00.ç0objectc
00000060	6C 61 73 73 30 84 00 00 01 2B 04 11 73 75 62 73	lass0â..0+ +subs
00000070	63 68 65 6D 61 53 75 62 65 6E 74 72 79 04 0D 64	chemaSubentry+ d
00000080	73 53 65 72 76 69 63 65 4E 61 6D 65 04 0E 6E 61	sServiceName+ na
00000090	6D 69 6E 67 43 6F 6E 74 65 78 74 73 04 14 64 65	mingContexts+ de
000000A0	66 61 75 6C 74 4E 61 6D 69 6E 67 43 6F 6E 74 65	faultNamingConte
000000B0	78 74 04 13 73 63 68 65 6D 61 4E 61 6D 69 6E 67	xt+ !schemaNaming
000000C0	43 6F 6E 74 65 78 74 04 1A 63 6F 6E 66 69 67 75	Context+ -configu
000000D0	72 61 74 69 6F 6E 4E 61 6D 69 6E 67 43 6F 6E 74	rationNamingCont
000000E0	65 78 74 04 17 72 6F 6F 74 44 6F 6D 61 69 6E 4E	ext+ ;rootDomainN
000000F0	61 6D 69 6E 67 43 6F 6E 74 65 78 74 04 10 73 75	amingContext+ su
00000100	70 70 6F 72 74 65 64 43 6F 6E 74 72 6F 6C 04 14	pportedControl+
00000110	73 75 70 70 6F 72 74 65 64 4C 44 41 50 56 65 72	supportedLDAPVer
00000120	73 69 6F 6E 04 15 73 75 70 70 6F 72 74 65 64 4C	sion+ supportedL
00000130	44 41 50 50 6F 6C 69 63 69 65 73 04 17 73 75 70	DAPolicies+ ;sup
00000140	70 6F 72 74 65 64 53 41 53 4C 4D 65 63 68 61 6E	portedSASLMechan
00000150	69 73 6D 73 04 0B 64 6E 73 48 6F 73 74 4E 61 6D	isms+ dnsHostNam

Figure D: Opening the LDAP section we will see this is the LDAP search request package

So now we know what the purpose of this package is, but we still don't know what this package is actually doing. An LDAP request is required to query information from Active Directory, but what information does it want to query? If you open the LDAP section: ProtocolOp = SearchRequest, you can see that one of the sub-

items labeled Attribute Description List is shown in Figure E. If you look at this image, you will see that Attribute Description List corresponds to Clearer data section is displayed in hex frame.

The screenshot shows a network analysis tool interface with a list of frames and a detailed view of an LDAP search request.

Frame	Time	Src MAC Addr	Dst MAC Addr	Protocol	Description
284	4.746826	000FB546EAA4	LOCAL	LDAP	ProtocolOp: SearchRequest
285	4.746826	LOCAL	000FB546EAA4	LDAP	ProtocolOp: SearchResponse
286	4.746826	LOCAL	000FB546EAA4	TCP	Control Bits: .AP..., len: 351
287	4.746826	000FB546EAA4	LOCAL	TCP	Control Bits: .A..., len: 351
288	4.746826	000FB546EAA4	LOCAL	LDAP	ProtocolOp: BindRequest
289	4.756840	LOCAL	000FB546EAA4	LDAP	ProtocolOp: BindResponse
290	4.756840	000FB546EAA4	LOCAL	LDAP	ProtocolOp: SearchRequest
291	4.756840	LOCAL	000FB546EAA4	LDAP	ProtocolOp: SearchResponse
292	4.756840	000FB546EAA4	LOCAL	LDAP	ProtocolOp: SearchRequest
293	4.756840	LOCAL	000FB546EAA4	LDAP	ProtocolOp: SearchResponse
294	4.756840	000FB546EAA4	LOCAL	LDAP	ProtocolOp: SearchRequest
295	4.756840	LOCAL	000FB546EAA4	LDAP	ProtocolOp: SearchResponse
296	4.756840	000FB546EAA4	LOCAL	LDAP	ProtocolOp: SearchRequest
297	4.756840	LOCAL	000FB546EAA4	LDAP	ProtocolOp: SearchResponse
298	4.756840	000FB546EAA4	LOCAL	LDAP	ProtocolOp: SearchRequest

The detailed view of the selected frame (Frame 290) shows the following structure:

- FRAME: Base frame properties
- ETHERNET: EType = Internet IP (IPv4)
- IP: Protocol = TCP - Transmission Control; Packet ID = 4972; Total IP Length = 351
- TCP: Control Bits: .AP..., len: 351, seq:4053217973-4053218324, ack:12818324
- LDAP: ProtocolOp: SearchRequest (3)
 - LDAP: MessageID = 1166 (0x48E)
 - LDAP: ProtocolOp = SearchRequest
 - LDAP: Base Object =
 - LDAP: Scope = Base Object
 - LDAP: Deref Aliases = Never Deref Aliases
 - LDAP: Size Limit = No Limit
 - LDAP: Time Limit = 0x00000078
 - LDAP: Attrs Only = 0 (0x0)
 - LDAP: Filter
 - LDAP: Attribute Description List**

The hex dump below shows the raw data for the Attribute Description List field, with the following ASCII representation:

```

00000000 00 0F B5 46 E8 03 00 0F B5 46 EA A4 08 00 45 00  .c|F#v.c|F#v.E.
00000010 01 87 13 6C 40 00 80 06 F6 B6 93 64 64 63 93 64  @g!!lQ.C#+||dddcod
00000020 64 22 29 32 01 85 F1 97 32 B5 4C 67 37 9A 50 18  d")2@a+u2Lg7UPf
00000030 FF FF C7 DD 00 00 30 84 00 00 01 59 02 02 04 8E  ||..0a..@Y+++A
00000040 63 84 00 00 01 4F 04 00 0A 01 00 0A 01 00 02 01  ca..@+.@@.@@.@@
00000050 00 02 01 78 01 01 00 87 0B 6F 62 6A 65 63 74 63  .@@x@@.c$objectc
00000060 6C 61 73 73 30 84 00 00 01 2B 04 11 73 75 62 73  lass0a..@+*subs
00000070 63 68 65 6D 61 53 75 62 65 6E 74 72 79 04 0D 64  schemaSubentry+Ad
00000080 73 53 65 72 76 69 63 65 4E 61 6D 65 04 0E 6E 61  sServiceName+$na
00000090 6D 69 6E 67 43 6F 6E 74 65 78 74 73 04 14 64 65  mingContexts+$[de
000000A0 66 61 75 6C 74 4E 61 6D 69 6E 67 43 6F 6E 74 65  faultNamingConte
000000B0 78 74 04 13 73 63 68 65 6D 61 4E 61 6D 69 6E 67  xt+!$schemaNaming
000000C0 43 6F 6E 74 65 78 74 04 1A 63 6F 6E 66 69 67 75  Context+~configu
000000D0 72 61 74 69 6F 6E 4E 61 6D 69 6E 67 43 6F 6E 74  rationNamingCont
000000E0 65 78 74 04 17 72 6F 6F 74 44 6F 6D 61 69 6E 4E  ext+!rootDomainN
000000F0 61 6D 69 6E 67 43 6F 6E 74 65 78 74 04 10 73 75  amingContext+*su
00000100 70 70 6F 72 74 65 64 43 6F 6E 74 72 6F 6C 04 14  pportedControl+T
00000110 73 75 70 70 6F 72 74 65 64 4C 44 41 50 56 65 72  supportedLDAPVer
00000120 73 69 6F 6E 04 15 73 75 70 70 6F 72 74 65 64 4C  sion+$supportedL
00000130 44 41 50 50 6F 6C 69 63 69 65 73 04 17 73 75 70  DAPPolicies+!sup
00000140 70 6F 72 74 65 64 53 41 53 4C 4D 65 63 68 61 6E  portedSASLMechan
00000150 69 73 6D 73 04 0B 64 6E 73 48 6F 73 74 4E 61 6D  isms+*dnsHostNam
00000160 65 64 6F 6C 64 61 61 78 53 65 78 76 69 69 65 4E 61  t+!dn$ServiceNam

```

Figure E: LDAP search requests are always padded with an attribute description list.

You will also see in this figure, the list item describing properties is fully expandable. If you open this section, you can see that Network Monitor correctly displays which LDAP attributes the frame is requesting data as shown in Figure F.

Frame	Time	Src MAC Addr	Dst MAC Addr	Protocol	Description
284	4.746826	000FB546EAA4	LOCAL	LDAP	ProtocolOp: SearchReq
285	4.746826	LOCAL	000FB546EAA4	LDAP	ProtocolOp: SearchRes
286	4.746826	LOCAL	000FB546EAA4	TCP	Control Bits: .A....
287	4.746826	000FB546EAA4	LOCAL	TCP	Control Bits: .A....
288	4.746826	000FB546EAA4	LOCAL	LDAP	ProtocolOp: BindReques
289	4.756840	LOCAL	000FB546EAA4	LDAP	ProtocolOp: BindRespor
290	4.756840	000FB546EAA4	LOCAL	LDAP	ProtocolOp: SearchReq
291	4.756840	LOCAL	000FB546EAA4	LDAP	ProtocolOp: SearchRes
292	4.756840	000FB546EAA4	LOCAL	LDAP	ProtocolOp: SearchReq
293	4.756840	LOCAL	000FB546EAA4	LDAP	ProtocolOp: SearchRes
294	4.756840	000FB546EAA4	LOCAL	LDAP	ProtocolOp: SearchReq
295	4.756840	LOCAL	000FB546EAA4	LDAP	ProtocolOp: SearchRes
296	4.756840	000FB546EAA4	LOCAL	LDAP	ProtocolOp: SearchReq
297	4.756840	LOCAL	000FB546EAA4	LDAP	ProtocolOp: SearchRes
298	4.756840	000FB546EAA4	LOCAL	LDAP	ProtocolOp: SearchReq


```

LDAP: Size Limit = No Limit
LDAP: Time Limit = 0x00000078
LDAP: Attrs Only = 0 (0x0)
+ LDAP: Filter
- LDAP: Attribute Description List
  LDAP: Attribute Type =subschemaSubentry
  LDAP: Attribute Type =dsServiceName
  LDAP: Attribute Type =namingContexts
  LDAP: Attribute Type =defaultNamingContext
  LDAP: Attribute Type =schemaNamingContext
  LDAP: Attribute Type =configurationNamingContext
  LDAP: Attribute Type =rootDomainNamingContext
  LDAP: Attribute Type =supportedControl
  LDAP: Attribute Type =supportedLDAPVersion
  LDAP: Attribute Type =supportedLDAPPolicies
  LDAP: Attribute Type =supportedSASLMechanisms
  LDAP: Attribute Type =dnsHostName
  LDAP: Attribute Type =ldapServiceName
  LDAP: Attribute Type =serverName
  LDAP: Attribute Type =supportedCapabilities
  
```


00000000	00 0F B5 46 E8 03 00 0F B5 46 EA A4 08 00 45 00	.0 F#v.0 F0h. E.
00000010	01 87 13 6C 40 00 80 06 F6 B6 93 64 64 63 93 64	@c#l@.C#+- ôddcôd
00000020	64 22 29 32 01 85 F1 97 32 B5 4C 67 37 9A 50 18	d")2@âû2Lg7UP†
00000030	FF FF C7 DD 00 00 30 84 00 00 01 59 02 02 04 8E	. .0ä. .@Y00+Ä
00000040	63 84 00 00 01 4F 04 00 0A 01 00 0A 01 00 02 01	cä. .00+.00.00.00
00000050	00 02 01 78 01 01 00 87 0B 6F 62 6A 65 63 74 63	.00x00.c#objectc
00000060	6C 61 73 73 30 84 00 00 01 2B 04 11 73 75 62 73	lass0ä. .0+*#subs
00000070	63 68 65 6D 61 53 75 62 65 6E 74 72 79 04 0D 64	chemaSubentry†#d
00000080	73 53 65 72 76 69 63 65 4E 61 6D 65 04 0E 6E 61	sServiceName+Sha
00000090	6D 69 6E 67 43 6F 6E 74 65 78 74 73 04 14 64 65	mingContexts†#de
000000A0	66 61 75 6C 74 4E 61 6D 69 6E 67 43 6F 6E 74 65	faultNamingConte
000000B0	78 74 04 13 73 63 68 65 6D 61 4E 61 6D 69 6E 67	xt†#schemaNaming
000000C0	43 6F 6E 74 65 78 74 04 1A 63 6F 6E 66 69 67 75	Context†-configu
000000D0	72 61 74 69 6F 6E 4E 61 6D 69 6E 67 43 6F 6E 74	rationNamingCont
000000E0	65 78 74 04 17 72 6F 6F 74 44 6F 6D 61 69 6E 4E	ext†#rootDomainN
000000F0	61 6D 69 6E 67 43 6F 6E 74 65 78 74 04 10 73 75	amingContext†#su
00000100	70 70 6F 72 74 65 64 43 6F 6E 74 72 6F 6C 04 14	pportedControl†#E
00000110	73 75 70 70 6F 72 74 65 64 4C 44 41 50 56 65 72	supportedLDAPVer
00000120	73 69 6F 6E 04 15 73 75 70 70 6F 72 74 65 64 4C	sion†\$supportedL
00000130	44 41 50 50 6F 6C 69 63 69 65 73 04 17 73 75 70	DAPPolicies†#sup
00000140	70 6F 72 74 65 64 53 41 53 4C 4D 65 63 68 61 6E	portedSASLMechan
00000150	69 73 6D 73 04 0B 64 6E 73 48 6F 73 74 4E 61 6D	isms†#dnsHostNam
00000160	65 64 6F 6E 64 61 61 73 65 65 73 76 69 69 65 6F	†#ldapServiceName

Figure F: Network Monitor displays a list of properties for the component where the LDAP query is trying to query the data.

Conclude

So, through this series, I have basically introduced how to use Network Monitor. Microsoft will soon release version 3 of Network Monitor, but everything that I have introduced to you in this article will still work well until the new version is released.

You finished reading the article "**Working with Network Monitor (Part 5)**" 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.
