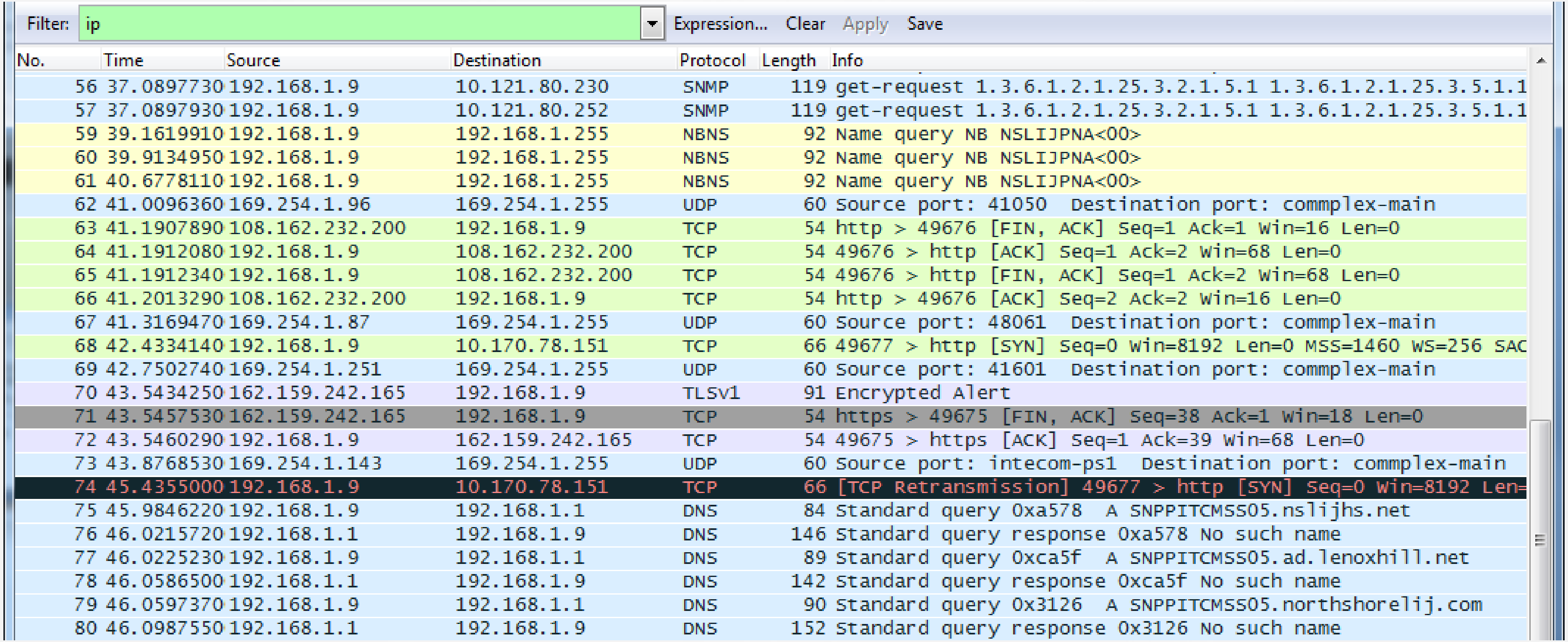
TCP/IP

Understanding TCP/IP

- Transmission Control Protocol / Internet Protocol (TCP/IP)
- What is TCP/IP and why is it important?
  - The most commonly used protocol stack in use today
- TCP/IP routing
  - IP routing

Wireshark & TCP/IP



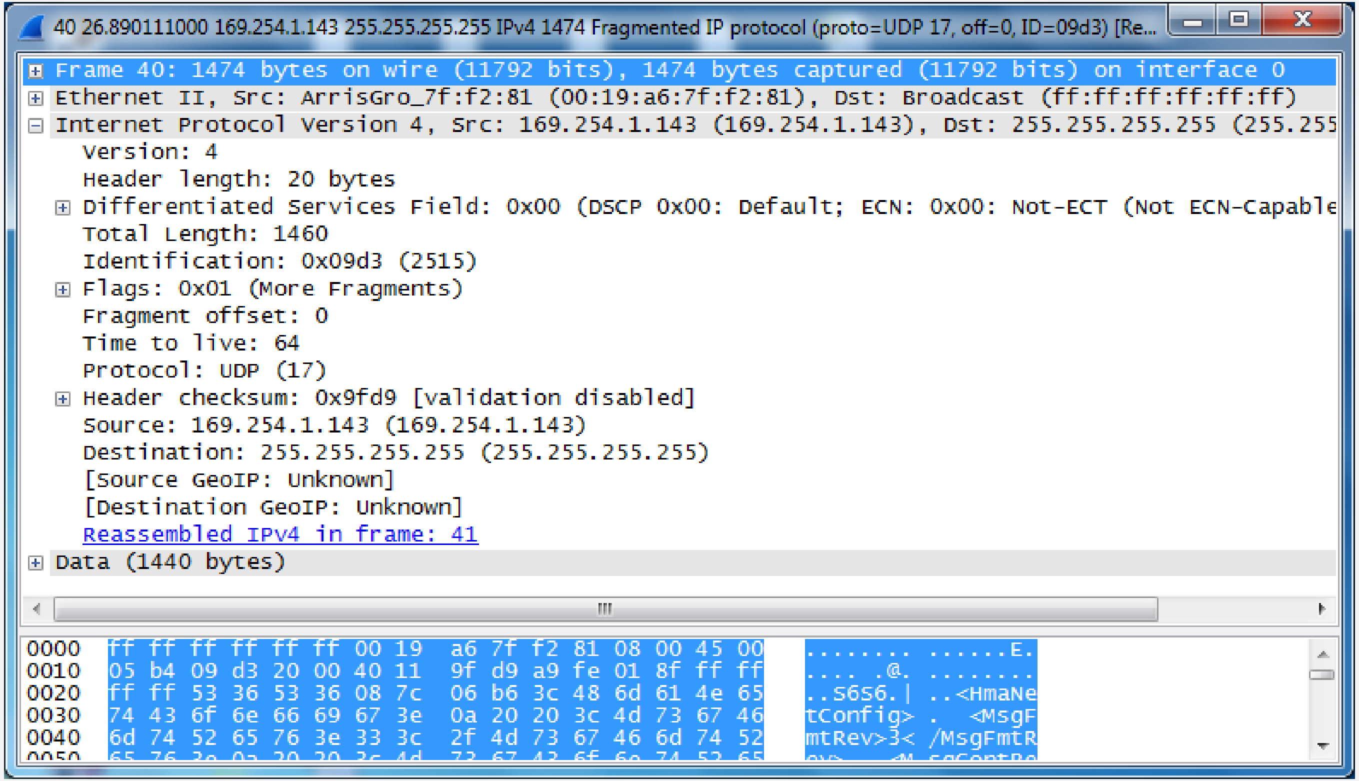
Filter: ip

No.	Time	Source	Destination	Protocol	Length	Info
56	37.0897730	192.168.1.9	10.121.80.230	SNMP	119	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1
57	37.0897930	192.168.1.9	10.121.80.252	SNMP	119	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1
59	39.1619910	192.168.1.9	192.168.1.255	NBNS	92	Name query NB NSLIJPNA<00>
60	39.9134950	192.168.1.9	192.168.1.255	NBNS	92	Name query NB NSLIJPNA<00>
61	40.6778110	192.168.1.9	192.168.1.255	NBNS	92	Name query NB NSLIJPNA<00>
62	41.0096360	169.254.1.96	169.254.1.255	UDP	60	Source port: 41050 Destination port: commplex-main
63	41.1907890	108.162.232.200	192.168.1.9	TCP	54	http > 49676 [FIN, ACK] Seq=1 Ack=1 Win=16 Len=0
64	41.1912080	192.168.1.9	108.162.232.200	TCP	54	49676 > http [ACK] Seq=1 Ack=2 Win=68 Len=0
65	41.1912340	192.168.1.9	108.162.232.200	TCP	54	49676 > http [FIN, ACK] Seq=1 Ack=2 Win=68 Len=0
66	41.2013290	108.162.232.200	192.168.1.9	TCP	54	http > 49676 [ACK] Seq=2 Ack=2 Win=16 Len=0
67	41.3169470	169.254.1.87	169.254.1.255	UDP	60	Source port: 48061 Destination port: commplex-main
68	42.4334140	192.168.1.9	10.170.78.151	TCP	66	49677 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SAC
69	42.7502740	169.254.1.251	169.254.1.255	UDP	60	Source port: 41601 Destination port: commplex-main
70	43.5434250	162.159.242.165	192.168.1.9	TLSv1	91	Encrypted Alert
71	43.5457530	162.159.242.165	192.168.1.9	TCP	54	https > 49675 [FIN, ACK] Seq=38 Ack=1 Win=18 Len=0
72	43.5460290	192.168.1.9	162.159.242.165	TCP	54	49675 > https [ACK] Seq=1 Ack=39 Win=68 Len=0
73	43.8768530	169.254.1.143	169.254.1.255	UDP	60	Source port: intecom-ps1 Destination port: commplex-main
74	45.4355000	192.168.1.9	10.170.78.151	TCP	66	[TCP Retransmission] 49677 > http [SYN] Seq=0 Win=8192 Len=
75	45.9846220	192.168.1.9	192.168.1.1	DNS	84	Standard query 0xa578 A SNPPITCMSS05.nslijhs.net
76	46.0215720	192.168.1.1	192.168.1.9	DNS	146	Standard query response 0xa578 No such name
77	46.0225230	192.168.1.9	192.168.1.1	DNS	89	Standard query 0xca5f A SNPPITCMSS05.ad.lenoxhill.net
78	46.0586500	192.168.1.1	192.168.1.9	DNS	142	Standard query response 0xca5f No such name
79	46.0597370	192.168.1.9	192.168.1.1	DNS	90	Standard query 0x3126 A SNPPITCMSS05.northshorelij.com
80	46.0987550	192.168.1.1	192.168.1.9	DNS	152	Standard query response 0x3126 No such name

Why Analyze TCP/IP?

- Troubleshooting problems
  - Use Wireshark to capture traffic
  - Review traffic to analyze network, protocols, and traffic flow
- Common issues include
  - Layer 3 routing
  - Incorrect TCP/IP configuration (IP, subnet mask, gateway)

IP Packet



40 26.890111000 169.254.1.143 255.255.255.255 IPv4 1474 Fragmented IP protocol (proto=UDP 17, off=0, ID=09d3) [Re...

```
⊞ Frame 40: 1474 bytes on wire (11792 bits), 1474 bytes captured (11792 bits) on interface 0
⊞ Ethernet II, Src: ArrisGro_7f:f2:81 (00:19:a6:7f:f2:81), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊟ Internet Protocol Version 4, Src: 169.254.1.143 (169.254.1.143), Dst: 255.255.255.255 (255.255
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable
    Total Length: 1460
    Identification: 0x09d3 (2515)
  ⊞ Flags: 0x01 (More Fragments)
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (17)
  ⊞ Header checksum: 0x9fd9 [validation disabled]
    Source: 169.254.1.143 (169.254.1.143)
    Destination: 255.255.255.255 (255.255.255.255)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
    Reassembled IPv4 in frame: 41
⊞ Data (1440 bytes)
```

```
0000  ff ff ff ff ff ff 00 19  a6 7f f2 81 08 00 45 00   ........ ......E.
0010  05 b4 09 d3 20 00 40 11  9f d9 a9 fe 01 8f ff ff   .... .@. ........
0020  ff ff 53 36 53 36 08 7c  06 b6 3c 48 6d 61 4e 65   ..S6S6.| ..<HmaNe
0030  74 43 6f 6e 66 69 67 3e  0a 20 20 3c 4d 73 67 46   tConfig> .  <MsgF
0040  6d 74 52 65 76 3e 33 3c  2f 4d 73 67 46 6d 74 52   mtRev>3< /MsgFmtR
0050  65 76 3e 0a 20 20 3c 4d  73 67 43 6f 6e 74 52 65   ev>.  <M sgContRe
```

Capturing Protocol Data

- Protocol data captured can be inspected for issues
- Protocol analysis
  - Opens up the data for inspection
  - Helps find problems you cannot see without capturing data for inspection
- Traffic analysis
  - Used to find bandwidth, latency, and other network issues