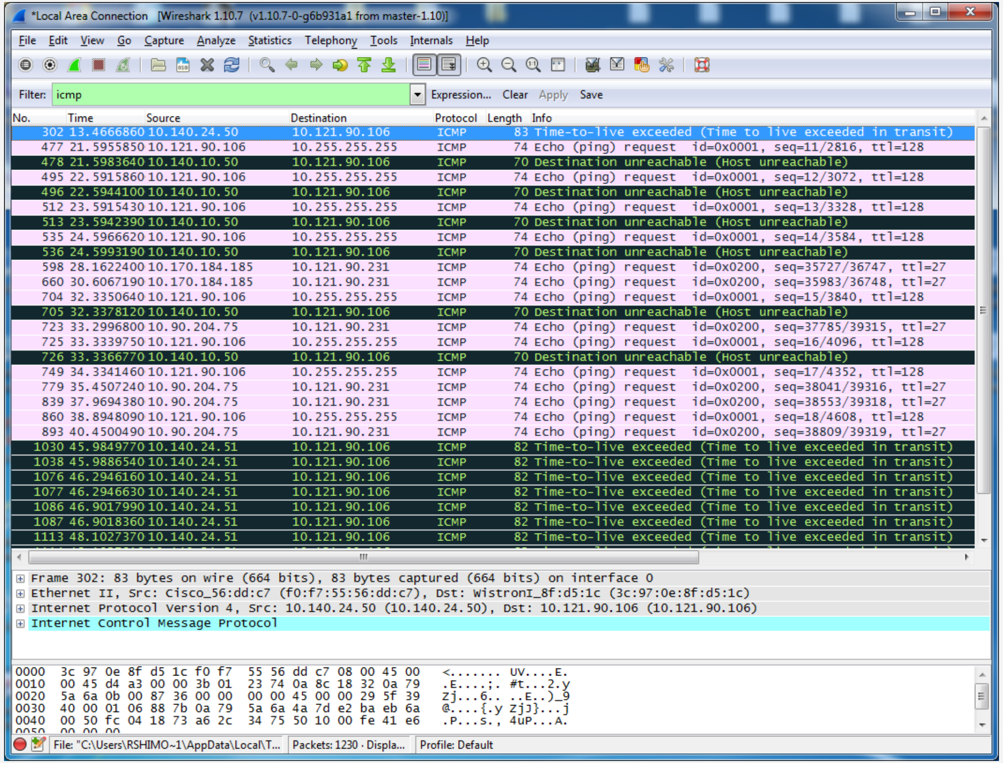
Protocols

Understanding Protocols

- What are Protocols?
- How protocols work:
  - Encapsulation of data
  - Traffic flow concepts from source to destination
- Dissecting an ICMP transmission
  - Ping is used to troubleshoot network connectivity

Wireshark & Protocols


*Local Area Connection [Wireshark 1.10.7 (v1.10.7-0-g6b931a1 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: icmp

No.	Time	Source	Destination	Protocol	Length	Info
302	13.4666860	10.140.24.50	10.121.90.106	ICMP	83	Time-to-live exceeded (Time to live exceeded in transit)
477	21.5955850	10.121.90.106	10.255.255.255	ICMP	74	Echo (ping) request id=0x0001, seq=11/2816, ttl=128
478	21.5983640	10.140.10.50	10.121.90.106	ICMP	70	Destination unreachable (Host unreachable)
495	22.5915860	10.121.90.106	10.255.255.255	ICMP	74	Echo (ping) request id=0x0001, seq=12/3072, ttl=128
496	22.5944100	10.140.10.50	10.121.90.106	ICMP	70	Destination unreachable (Host unreachable)
512	23.5915430	10.121.90.106	10.255.255.255	ICMP	74	Echo (ping) request id=0x0001, seq=13/3328, ttl=128
513	23.5942390	10.140.10.50	10.121.90.106	ICMP	70	Destination unreachable (Host unreachable)
535	24.5966620	10.121.90.106	10.255.255.255	ICMP	74	Echo (ping) request id=0x0001, seq=14/3584, ttl=128
536	24.5993190	10.140.10.50	10.121.90.106	ICMP	70	Destination unreachable (Host unreachable)
598	28.1622400	10.170.184.185	10.121.90.231	ICMP	74	Echo (ping) request id=0x0200, seq=35727/36747, ttl=27
660	30.6067190	10.170.184.185	10.121.90.231	ICMP	74	Echo (ping) request id=0x0200, seq=35983/36748, ttl=27
704	32.3350640	10.121.90.106	10.255.255.255	ICMP	74	Echo (ping) request id=0x0001, seq=15/3840, ttl=128
705	32.3378120	10.140.10.50	10.121.90.106	ICMP	70	Destination unreachable (Host unreachable)
723	33.2996800	10.90.204.75	10.121.90.231	ICMP	74	Echo (ping) request id=0x0200, seq=37785/39315, ttl=27
725	33.3339750	10.121.90.106	10.255.255.255	ICMP	74	Echo (ping) request id=0x0001, seq=16/4096, ttl=128
726	33.3366770	10.140.10.50	10.121.90.106	ICMP	70	Destination unreachable (Host unreachable)
749	34.3341460	10.121.90.106	10.255.255.255	ICMP	74	Echo (ping) request id=0x0001, seq=17/4352, ttl=128
779	35.4507240	10.90.204.75	10.121.90.231	ICMP	74	Echo (ping) request id=0x0200, seq=38041/39316, ttl=27
839	37.9694380	10.90.204.75	10.121.90.231	ICMP	74	Echo (ping) request id=0x0200, seq=38553/39318, ttl=27
860	38.8948090	10.121.90.106	10.255.255.255	ICMP	74	Echo (ping) request id=0x0001, seq=18/4608, ttl=128
893	40.4500490	10.90.204.75	10.121.90.231	ICMP	74	Echo (ping) request id=0x0200, seq=38809/39319, ttl=27
1030	45.9849770	10.140.24.51	10.121.90.106	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
1038	45.9886540	10.140.24.51	10.121.90.106	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
1076	46.2946160	10.140.24.51	10.121.90.106	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
1077	46.2946630	10.140.24.51	10.121.90.106	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
1086	46.9017990	10.140.24.51	10.121.90.106	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
1087	46.9018360	10.140.24.51	10.121.90.106	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
1113	48.1027370	10.140.24.51	10.121.90.106	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)

```
⊞ Frame 302: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0
⊞ Ethernet II, Src: Cisco_56:dd:c7 (f0:f7:55:56:dd:c7), Dst: WistronI_8f:d5:1c (3c:97:0e:8f:d5:1c)
⊞ Internet Protocol Version 4, Src: 10.140.24.50 (10.140.24.50), Dst: 10.121.90.106 (10.121.90.106)
⊞ Internet Control Message Protocol
```

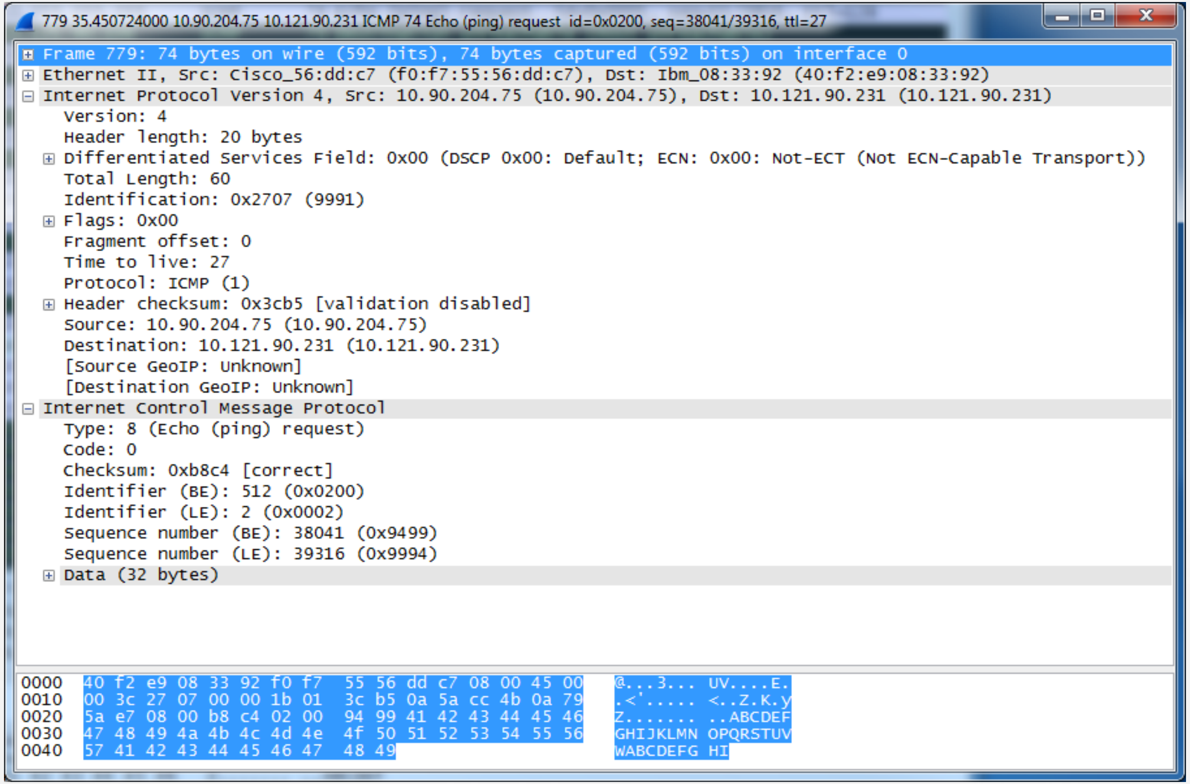
```
0000  3c 97 0e 8f d5 1c f0 f7  55 56 dd c7 08 00 45 00   <....... UV....E.
0010  00 45 d4 a3 00 00 3b 01  23 74 0a 8c 18 32 0a 79   .E....;. #t...2.y
0020  5a 6a 0b 00 87 36 00 00  00 00 45 00 00 29 5f 39   Zj...6.. ..E..)_9
0030  40 00 01 06 88 7b 0a 79  5a 6a 4a 7d e2 ba eb 6a   @....{.y ZjJ}...j
0040  00 50 fc 04 18 73 a6 2c  34 75 50 10 00 fe 41 e6   .P...s., 4uP...A.
0050  00 00 00
```

File: "C:\Users\RSHIMO~1\AppData\Local\T... | Packets: 1230 · Displa... | Profile: Default

Network Lab

- Capture a ping (ICMP) from source to destination
  - Use Wireshark to capture traffic
- Troubleshooting problems
  - Use Wireshark to analyze traffic
  - Review traffic to analyze network, protocols, and traffic flow
  - Time to Live (TTL)

Dissecting the ICMP Packet



779 35.450724000 10.90.204.75 10.121.90.231 ICMP 74 Echo (ping) request id=0x0200, seq=38041/39316, ttl=27

```
⊞ Frame 779: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
⊞ Ethernet II, Src: Cisco_56:dd:c7 (f0:f7:55:56:dd:c7), Dst: Ibm_08:33:92 (40:f2:e9:08:33:92)
⊟ Internet Protocol Version 4, Src: 10.90.204.75 (10.90.204.75), Dst: 10.121.90.231 (10.121.90.231)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 60
    Identification: 0x2707 (9991)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 27
    Protocol: ICMP (1)
  ⊞ Header checksum: 0x3cb5 [validation disabled]
    Source: 10.90.204.75 (10.90.204.75)
    Destination: 10.121.90.231 (10.121.90.231)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊟ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xb8c4 [correct]
    Identifier (BE): 512 (0x0200)
    Identifier (LE): 2 (0x0002)
    Sequence number (BE): 38041 (0x9499)
    Sequence number (LE): 39316 (0x9994)
  ⊞ Data (32 bytes)
```

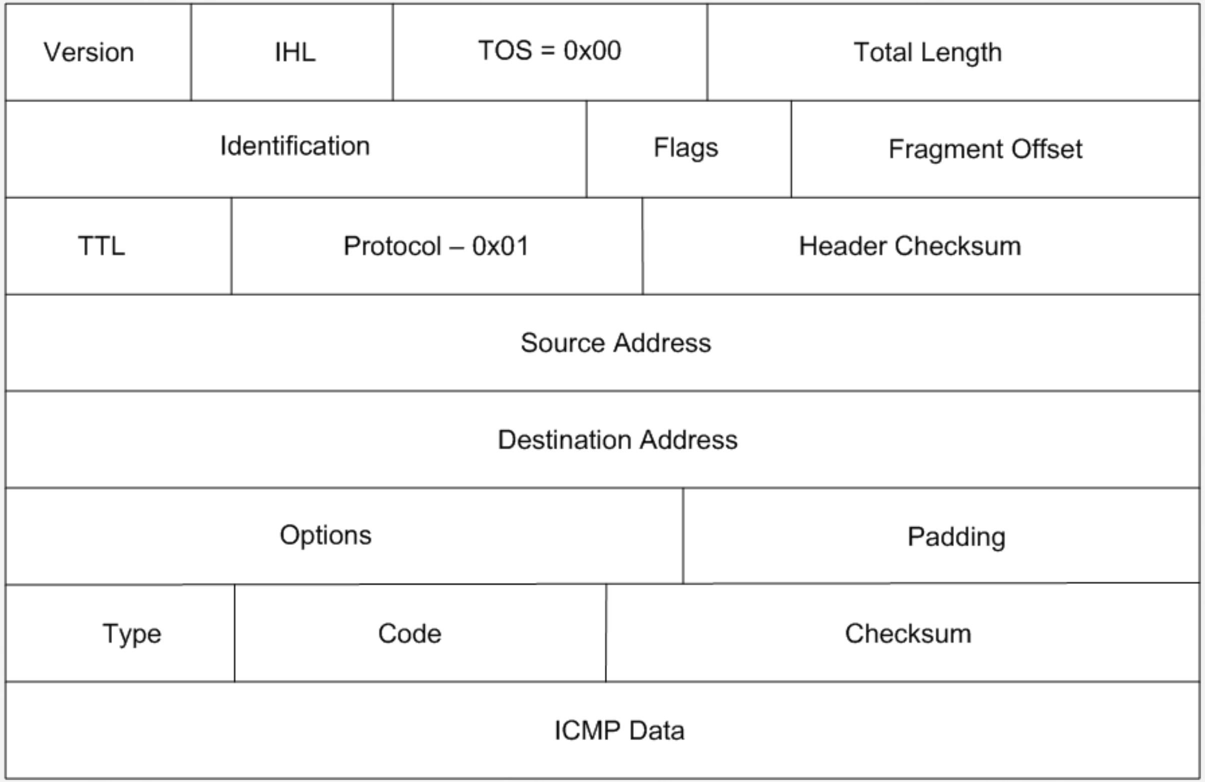
```
0000  40 f2 e9 08 33 92 f0 f7  55 56 dd c7 08 00 45 00   @...3... UV....E.
0010  00 3c 27 07 00 00 1b 01  3c b5 0a 5a cc 4b 0a 79   .<'..... <..Z.K.y
0020  5a e7 08 00 b8 c4 02 00  94 99 41 42 43 44 45 46   Z....... ..ABCDEF
0030  47 48 49 4a 4b 4c 4d 4e  4f 50 51 52 53 54 55 56   GHIJKLMN OPQRSTUV
0040  57 41 42 43 44 45 46 47  48 49                     WABCDEFG HI
```

Internet Control Message Protocol (ICMP)

» ICMP used to troubleshoot problems

- Commonly used with ping and traceroute
- Part of the TCP/IP protocol suite (Layer 3)
- Relays query messages
- Uses control messages

IP Header Information



Version

IHL

TOS = 0x00

Total Length

Identification

Flags

Fragment Offset

TTL

Protocol – 0x01

Header Checksum

Source Address

Destination Address

Options

Padding

Type

Code

Checksum

ICMP Data

Traffic Flow Analysis

- Data captured for analysis can reveal many issues
  - Dropped packets
  - Incorrect gateway assignment
  - Incorrect path
  - Latency
  - Many others…
- Source to destination
  - Ping will show you via ICMP connectivity from source to destination