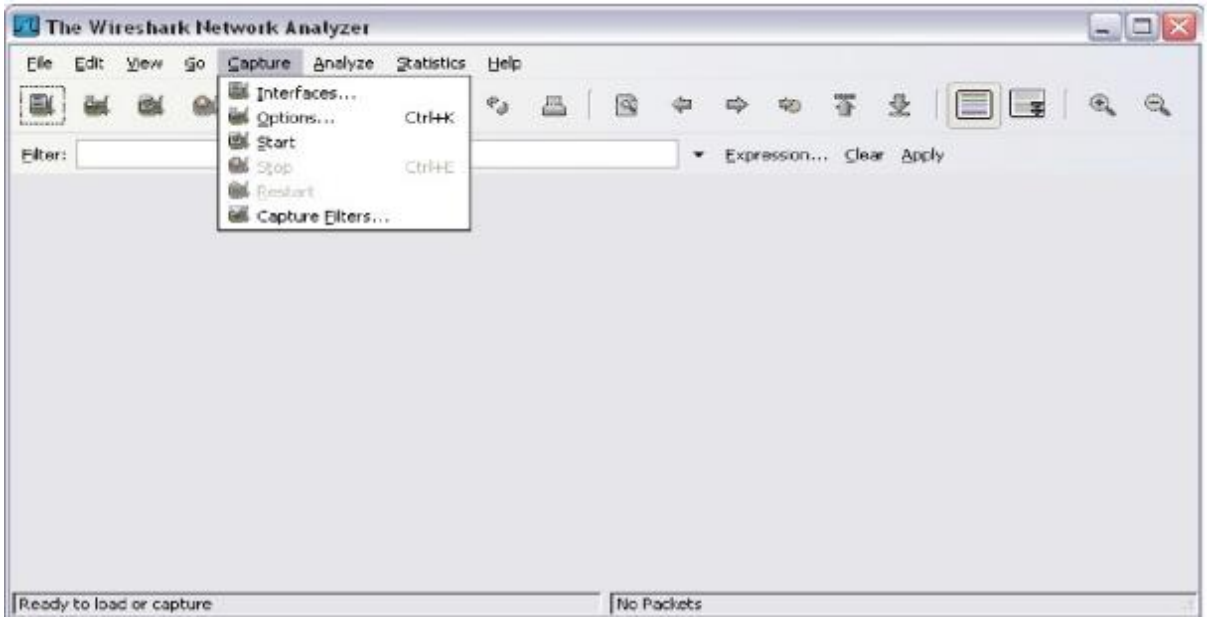
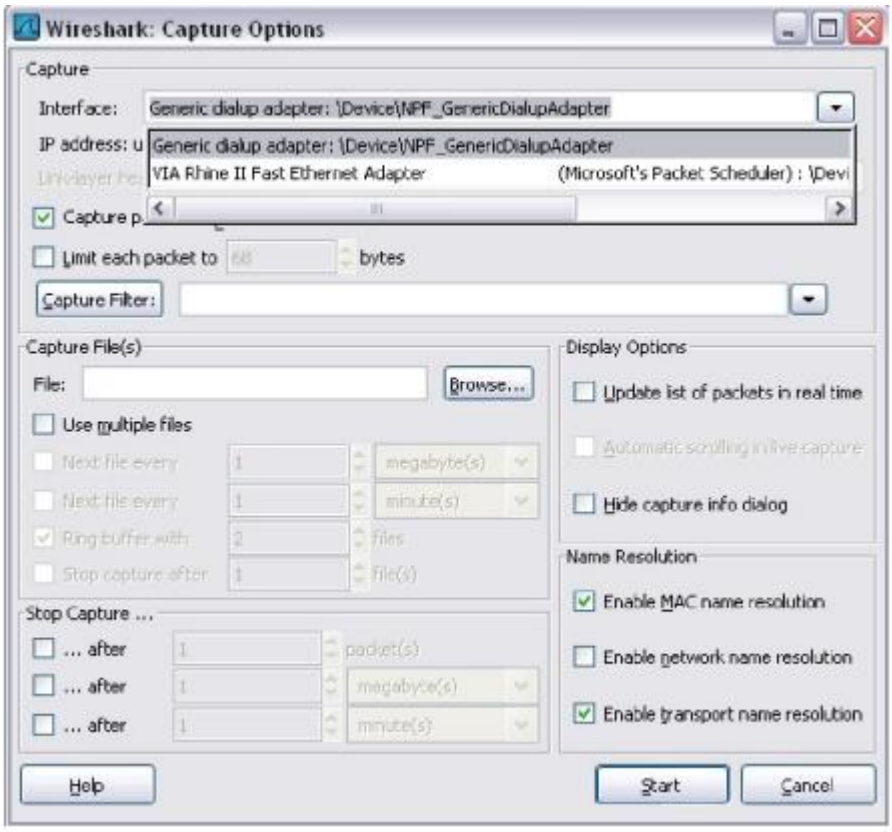
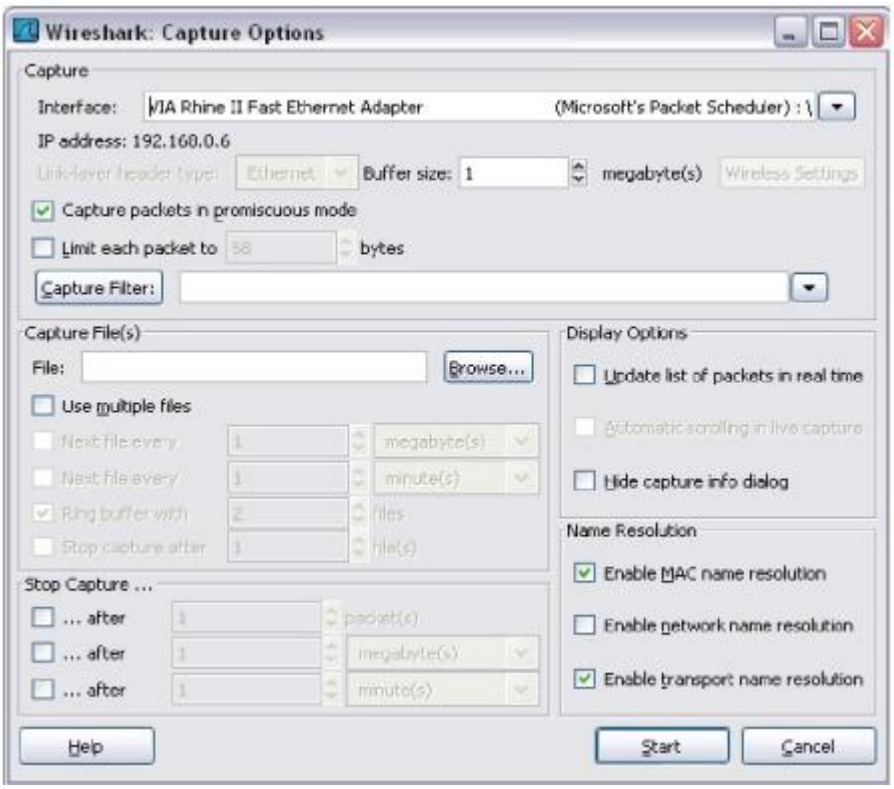
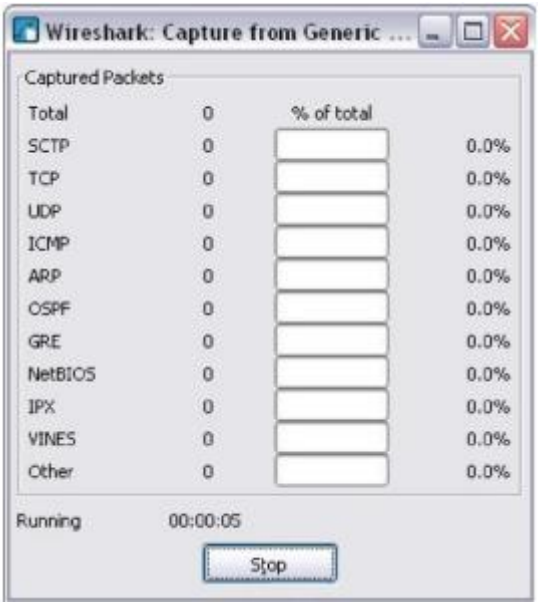
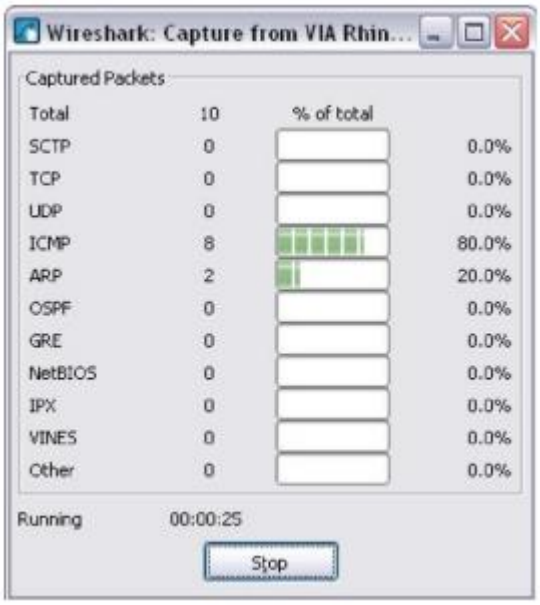
EXP5: Use of Wireshark tool to capture and examine packets

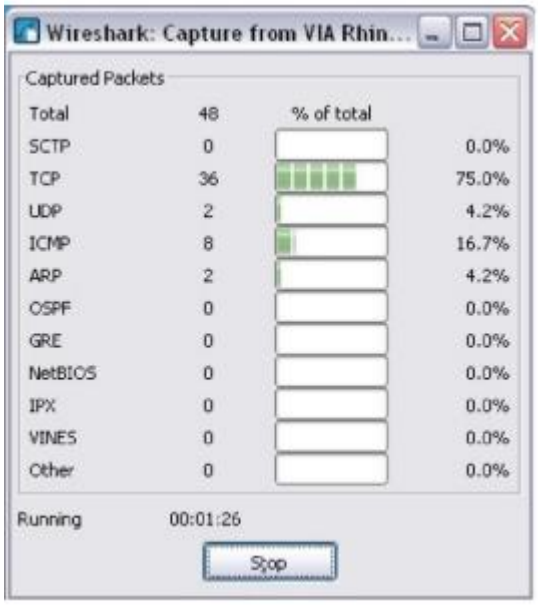


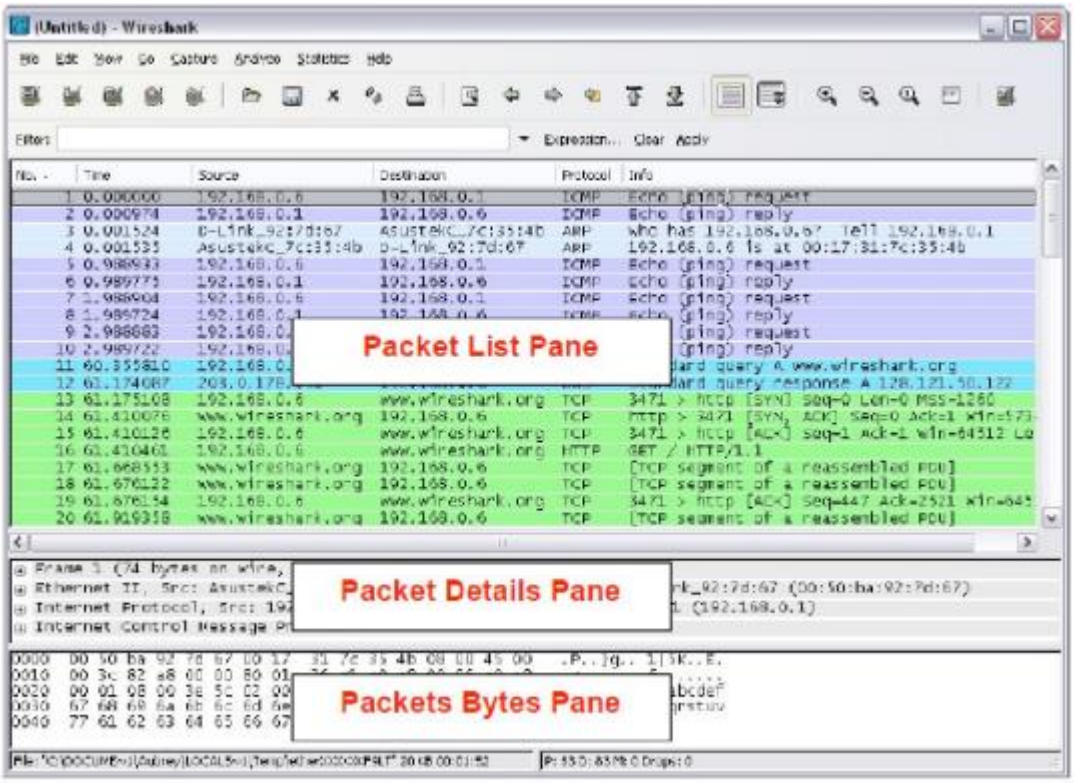



Wireshark: Capture Options
Capture
Interface: VIA Rhine II Fast Ethernet Adapter (Microsoft's Packet Scheduler) : \
IP address: 192.160.0.6
Link-layer header type: Ethernet Buffer size: 1 megabyte(s) Wireless Settings
Capture packets in promiscuous mode
Limit each packet to 68 bytes
Capture Filter:
Capture File(s)
File: Browse...
Use multiple files
Next file every 1 megabyte(s)
Next file every 1 minute(s)
Ring buffer with 2 files
Stop capture after 1 file(s)
Stop Capture ...
... after 1 packet(s)
... after 1 megabyte(s)
... after 1 minute(s)
Display Options
Update list of packets in real time
Automatic scrolling in live capture
Hide capture info dialog
Name Resolution
Enable MAC name resolution
Enable network name resolution
Enable transport name resolution
Help
Start
Cancel


Wireshark: Capture from Generic ...
Captured Packets
Total 0 % of total
SCTP 0 0.0%
TCP 0 0.0%
UDP 0 0.0%
ICMP 0 0.0%
ARP 0 0.0%
OSPF 0 0.0%
GRE 0 0.0%
NetBIOS 0 0.0%
IPX 0 0.0%
VINES 0 0.0%
Other 0 0.0%
Running 00:00:05
Stop


Wireshark: Capture from VIA Rhin...
Captured Packets
Total 10 % of total
SCTP 0 0.0%
TCP 0 0.0%
UDP 0 0.0%
ICMP 8 80.0%
ARP 2 20.0%
OSPF 0 0.0%
GRE 0 0.0%
NetBIOS 0 0.0%
IPX 0 0.0%
VINES 0 0.0%
Other 0 0.0%
Running 00:00:25
Stop


Wireshark: Capture from VIA Rhin...
Captured Packets
Total 48 % of total
SCTP 0 0.0%
TCP 36 75.0%
UDP 2 4.2%
ICMP 8 16.7%
ARP 2 4.2%
OSPF 0 0.0%
GRE 0 0.0%
NetBIOS 0 0.0%
IPX 0 0.0%
VINES 0 0.0%
Other 0 0.0%
Running 00:01:26
Stop



No.	Time	Source	Destination	Protocol	Info
1	0.000000	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
2	2.000032	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
3	4.000059	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
4	4.072858	QuantaCo_bd:0c:7c	Broadcast	ARP	Who has 10.1.1.254? Tell 10.1.1.1
5	4.073609	Cisco_cf:66:40	QuantaCo_bd:0c:7c	ARP	10.1.1.254 is at 00:0c:85:cf:66:40
6	4.073626	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
7	4.074122	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
8	5.067535	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
9	5.068007	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
10	6.000113	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
11	6.067548	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
12	6.068019	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
13	6.084103	Cisco_9f:6c:c9	Cisco_9f:6c:c9	LOOP	Reply
14	7.067603	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
15	7.068131	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
16	8.000126	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
17	9.975700	Cisco_9f:6c:c9	CDP/VTP/DTP/PAgP/U	DTP	Dynamic Trunking Protocol
18	10.000134	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =

```
Frame 6 (74 bytes on wire, 74 bytes captured)
    Arrival Time: Jan 10, 2007 01:54:07.860436000
    [Time delta from previous packet: 0.000017000 seconds]
    [Time since reference or first frame: 4.073626000 seconds]
    Frame Number: 6
    Packet Length: 74 bytes
    Capture Length: 74 bytes
    [Frame is marked: False]
    [Protocols in frame: eth:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp]
Ethernet II, Src: QuantaCo_bd:0c:7c (00:c0:9f:bd:0c:7c), Dst: Cisco_cf:66:40 (00:0c:85:cf:66:40)
  Destination: Cisco_cf:66:40 (00:0c:85:cf:66:40)
  Source: QuantaCo_bd:0c:7c (00:c0:9f:bd:0c:7c)
    Type: IP (0x0800)
Internet Protocol, Src: 10.1.1.1 (10.1.1.1), Dst: 192.168.254.254 (192.168.254.254)
    Version: 4
    Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 60
    Identification: 0x0bf7 (3063)
  Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (0x01)
  Header checksum: 0x6421 [correct]
    Source: 10.1.1.1 (10.1.1.1)
    Destination: 192.168.254.254 (192.168.254.254)
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x2a5c [correct]
    Identifier: 0x0300
    Sequence number: 0x2000
```

```
C:\Users\singh>tracert 8.8.8.8

Tracing route to google-public-dns-a.google.com [8.8.8.8]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.1.1
  2    13 ms    20 ms    15 ms  120.57.48.1
  3    14 ms    13 ms    13 ms  triband-del-59.180.212.202.bol.net.in [59.180.212.202]
  4    14 ms    14 ms    14 ms  triband-del-59.180.210.150.bol.net.in [59.180.210.150]
  5    14 ms    13 ms    13 ms  125.20.37.21
  6    14 ms    16 ms    14 ms  182.79.181.230
  7    60 ms    59 ms    60 ms  182.79.190.57
  8    67 ms   101 ms    92 ms  182.79.198.162
  9    63 ms    63 ms    62 ms  72.14.197.166
 10    55 ms    55 ms    54 ms  108.170.253.121
 11   122 ms    89 ms    88 ms  216.239.63.213
 12    87 ms    86 ms    86 ms  216.239.47.109
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22    88 ms    88 ms    87 ms  google-public-dns-a.google.com [8.8.8.8]

Trace complete.
```

Source	Destination	Protocol	Ler	Info
192.168.1.101	192.168.1.1	DNS	…	Standard query 0x8c5e PTR 8.8.8.8.in-addr.arpa
192.168.1.101	192.168.1.1	DNS	…	Standard query 0x8c5e PTR 8.8.8.8.in-addr.arpa
192.168.1.1	192.168.1.101	DNS	…	Standard query response 0x8c5e PTR 8.8.8.8.in-addr.arpa PTR goog
192.168.1.1	192.168.1.101	DNS	…	Standard query response 0x8c5e PTR 8.8.8.8.in-addr.arpa PTR goog
192.168.1.101	8.8.8.8	ICMP	…	Echo (ping) request id=0x0001, seq=206/52736, ttl=1 (no response
192.168.1.1	192.168.1.101	ICMP	…	Time-to-live exceeded (Time to live exceeded in transit)
192.168.1.101	8.8.8.8	ICMP	…	Echo (ping) request id=0x0001, seq=207/52992, ttl=1 (no response
192.168.1.1	192.168.1.101	ICMP	…	Time-to-live exceeded (Time to live exceeded in transit)
192.168.1.101	8.8.8.8	ICMP	…	Echo (ping) request id=0x0001, seq=208/53248, ttl=1 (no response
192.168.1.1	192.168.1.101	ICMP	…	Time-to-live exceeded (Time to live exceeded in transit)
192.168.1.101	192.168.1.1	DNS	…	Standard query 0x247f PTR 1.1.168.192.in-addr.arpa

```
192.168.1.101 8.8.8.8       ICMP   … Echo (ping) request  id=0x0001, seq=268/3073, ttl=21 (no respon
192.168.1.101 8.8.8.8       ICMP   … Echo (ping) request  id=0x0001, seq=269/3329, ttl=22 (reply in
8.8.8.8       192.168.1.101 ICMP   … Echo (ping) reply    id=0x0001, seq=269/3329, ttl=46 (request i
192.168.1.101 8.8.8.8       ICMP   … Echo (ping) request  id=0x0001, seq=270/3585, ttl=22 (reply in
8.8.8.8       192.168.1.101 ICMP   … Echo (ping) reply    id=0x0001, seq=270/3585, ttl=46 (request i
192.168.1.101 8.8.8.8       ICMP   … Echo (ping) request  id=0x0001, seq=271/3841, ttl=22 (reply in
8.8.8.8       192.168.1.101 ICMP   … Echo (ping) reply    id=0x0001, seq=271/3841, ttl=46 (request i
```