**ELEC3506/9506 Communication Networks**

**-Lab Report 2**



Zhixuan Lin(530034414) -Contributinos(50%) -ELEC3506

Xinran He(540662177) -Contributions(50%) -ELEC9506

Table of Contents

Introduction……………………………………………………………………………2

Phase 1: ICMP - Ping…………………………………………………………………2

Phase 1: ICMP - Traceroute…………………………………………………………3

Credit…………………………………………………………………………………4

Phase 2: Ip……………………………………………………………………………5

Appendix………………………………………………………………………………8

(All the screen shots are in Appendix)

**Introduction**

The primary objective of this laboratory was to explore fundamental concepts of the Internet Control Message Protocol (ICMP) and the Internet Protocol (IP) through practical experimentation using Wireshark. In the first phase, ICMP was investigated by generating and analyzing packets created by the Ping and Traceroute programs. This enabled the identification of ICMP message types, structures, and their role in connectivity verification and path discovery. In the second phase, attention was directed towards IP datagrams, with emphasis on examining header fields, tracing packet flows, and observing fragmentation under varying packet sizes. By combining theoretical knowledge with packet-level observations, this lab provided hands-on experience in understanding how control messages and datagram structures support reliable communication in packet-switched networks.

**Phase 1: ICMP - Ping**

**Set Up**

1. Open the Windows Command Prompt
2. Start Wireshark and begin packet capturing
3. Enter "ping -n 10 www.ust.hk" in the command line.

This command sends 10 ICMP Echo Request packets to the target host (the server of the Hong Kong University of Science and Technology).

1. Wait for the command to be completed.
2. Enter the filtering condition "icmp" in Wireshark.

Q1. What is the IP address of your host? What is the IP address of the destination

host?

Source(Host) IP Address: 10.170.56.60

Destination IP Address: 143.89.209.9

Q2. Why is it that an ICMP packet does not have source and destination port

numbers?

ICMP operates at the Network Layer (Layer 3) and directly carries within the IP data packet. The port number, on the other hand, is a concept of the Transport Layer (Layer 4, TCP/UDP) and is used to distinguish different application processes. ICMP is only used to transmit network control information (such as echo requests/responses, error reports), and it is not bound to a specific process, so it does not require a port number.

Q3. Examine one of the ping request packets sent by your host. What are the ICMP

type and code numbers? What other fields does this ICMP packet have? How

many bytes are the checksum, sequence number and identifier fields?

Type: 8 (Echo Request)

Code: 0; Other fields: Checksum, Identifier, Sequence

Number, Data

Field sizes:

Checksum: 2 bytes

Identifier: 2 bytes

Sequence Number: 2 bytes

Q4. Examine the corresponding ping reply packet. What are the ICMP type and code

numbers? What other fields does this ICMP packet have? How many bytes are the

checksum, sequence number and identifier fields?

Type: 0 (Echo Reply)

Code: 0; Other fields: Checksum, Identifier, Sequence

Number, Data

Field sizes:

Checksum: 2 bytes

Identifier: 2 bytes

Sequence Number: 2 bytes

**Phase 1: ICMP - Traceroute**

**Set Up**

1. Open the Windows Command Prompt
2. Start Wireshark and begin packet capturing
3. Enter "tracert www.inria.fr" in the command line.

This command will send a series of ICMP Echo Request packets to the target host (INRIA, with IP address 128.93.162.83), and gradually increase the TTL value.

1. Wait for the command to be completed.
2. Enter the filtering condition "icmp" in Wireshark.

Q5. What is the IP address of your host? What is the IP address of the target

destination host?

Host IP Address: 10.170.56.60

Destination IP Adress: 128.93.162.83

Q6. If ICMP sent UDP packets instead (as in Unix/Linux), would the IP protocol

number still be 01 for the probe packets? If not, what would it be?

No. ICMP packets use protocol number 1 in the IP header. If Traceroute used UDP instead, the protocol number would be 17 (UDP).

Q7. Examine the ICMP echo packet in your screenshot. Is this different from the

ICMP ping query packets in the first half of this lab? If yes, how so?

Yes. Both are ICMP Echo Request (Type 8, Code 0), but there are key differences:

In Ping, packets are sent with a fixed TTL (e.g., 128) to reach the final destination directly. In Traceroute, the TTL is deliberately varied (1, 2, 3 …), so intermediate routers return ICMP Time Exceeded messages. This allows discovery of each hop along the path.

Q8. Examine the ICMP error packet in your screenshot. It has more fields than the

ICMP echo packet. What is included in those fields?

The ICMP Time Exceeded packet includes:

ICMP header (Type = 11, Code = 0, Checksum)

Additional fields (unused, often 0)

The IP header of the original datagram

The first 8 bytes of the payload of the original datagram

This extra information helps the sender identify which packet caused the error.

Q9. Examine the last three ICMP packets received by the source host. How are these

packets different from the ICMP error packets? Why are they different?

The last three are ICMP Echo Replies (Type 0, Code 0), not error packets. They come from the final destination host (128.93.162.83) rather than intermediate routers. Difference: At this stage, the TTL value was sufficient for the packet to reach the target, so the destination host returned normal Echo Replies instead of “Time Exceeded” errors.

Q10. Within the tracert measurements, is there a link whose delay is significantly

longer than others? Refer to the screenshot in Figure 4, is there a link whose

delay is significantly longer than others? On the basis of the router names, can

you guess the location of the two routers on the end of this link?

Yes. In the traceroute result, most hops had RTTs around a few hundred milliseconds, but there was a noticeable jump of about 40–50 ms when the packets moved from an international backbone router (GÉANT network) to the French academic network (RENATER). This longer delay is caused by a long-distance link (very likely the transatlantic connection). One router is on the international backbone, and the other is in France (RENATER), near the final destination inria.fr.

**Credit**

**Set Up**

1. Open Wireshark and filter: icmp or udp.
2. Run your UDP client and send a UDP frame with an unconventional destination port (such as 40000+) to a "live" host.
3. Observe the returned message.

Phenomenon: After sending UDP probes to unconventional ports, an ICMP Destination Unreachable - Port Unreachable (Type 3, Code 3) was captured from the target IP.

Conclusion: The target host is reachable, but the UDP port is not open (hence the "port unreachable" response).

Key points marked in the screenshot:

Circle Type=3, Code=3 in the ICMP message.

Circle out the original IP/UDP header of the loopback in its load, and confirm that the IP and port numbers are consistent with those of the probe frame;

3) (Optional) The time difference between the two frames = RTT.

If a UDP response is received → the port is open; if there is no return → it is mostly discarded by the firewall.

**Phase 2: Ip**

**Set Up**

1. Open Wireshark and start capturing packets.

2) Windows,PingPlotter

Open PingPlotter → Address to Trace: gaia.cs.umass.edu (IP: 128.119.245.12); of times to Trace: set to 3.

Edit → Advanced Options → Packet Options → Packet Size = 56 → Trace.

Change Packet Size to 2000 → Resume.

Change Packet Size to 3500 → Resume.

After the process is over, stop capturing packets in Wireshark and save them.

Run separately:

traceroute gaia.cs.umass.edu 56

traceroute gaia.cs.umass.edu 2000

traceroute gaia.cs.umass.edu 3500

After completion, stop capturing packets in Wireshark and save.

1. Select the first ICMP Echo Request message sent by your computer, and expand

the Internet Protocol part of the packet in the packet details window.

What is the IP address of your computer?

Host IP: 10.170.56.60 ; Destination IP: 128.119.245.12

1. Within the IP packet header, what is the value in the upper layer protocol field?

Upper-layer protocol in the IP header: ICMP (protocol number 1) for these traceroute/echo packets.

3. How many bytes are in the IP header? How many bytes are in the payload *of the*

*IP datagram*? Explain how you determined the number of payload bytes.

Using one Echo Request as example: Wireshark shows Frame length = 70 B; subtract 14 B Ethernet header → IP Total Length = 56 B. With IHL = 20 B, the IP payload = 36 B (= 8 B ICMP header + 28 B data).

4. Has this IP datagram been fragmented? Explain how you determined whether or

not the datagram has been fragmented.

Not fragmented. Evidence/logic: the IP datagram is far below Ethernet’s 1500-byte MTU; fragmented packets would have MF=1 and/or Fragment offset > 0.

5. Which fields in the IP datagram *always* change from one datagram to the next

within this series of ICMP messages sent by your computer?

Fields that always change across your host’s Echo Requests: TTL, Header Checksum, and typically Identification (new IP datagram each time). (Procedure: sort by Source and step through ICMP as instructed.)

6. Which fields stay constant? Which of the fields *must* stay constant? Which fields

must change? Why?

**Stay constant:** Version (IPv4), Src/Dst IP, Protocol (= ICMP), IHL, and (in the unfragmented case) Flags/Fragment Offset.  
**Must change:** **TTL** (for hop discovery) and the **Header Checksum** (recomputed), and **Identification** (to distinguish IP datagrams).

7. Describe the pattern you see in the values in the Identification field of the IP

Datagram

Identification pattern: monotonically increasing per new IP datagram (typical +1), enabling fragment reassembly and datagram distinction.

1. What is the value in the Identification field and the TTL field?

For first-hop ICMP Time-Exceeded replies: check any returned packet from the nearest router—these are ICMP “TTL exceeded” messages destined to your host. Read the router’s TTL (as sent by the router; usually constant per router) and its Identification from the IP header. Example lines show such replies.

9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent

to your computer by the nearest (first hop) router? Why?

Across those first-hop replies:

TTL: remains constant for that router (it uses a fixed initial TTL).

Identification: varies per reply (new IP datagram each time). Evidence: multiple Time-Exceeded packets from the same hop.

10. Find the first ICMP Echo Request message that was sent by your computer after

you changed the Packet Size in pingplotter to be 2000. Has that message been

fragmented across more than one IP datagram? [Note: if you find your packet has

not been fragmented, you should download the zip file

http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip and extract the ip

ethereal-trace-1packet trace. If your computer has an Ethernet interface, a packet

size of 2000 should cause fragmentation.3]

After raising Packet Size to 2000 B (per guide), the Echo Request is fragmented on Ethernet (MTU 1500 B).

1. Print out the first fragment of the fragmented IP datagram. What information in

the IP header indicates that the datagram been fragmented? What information in

the IP header indicates whether this is the first fragment versus a latter fragment?

How long is this IP datagram?

First fragment (how to identify & length):

Fragmented: MF=1 and/or Fragment offset ≥ 0.

First fragment: Fragment offset = 0, MF = 1.

IP Total Length of first fragment: 1500 B (= 20-B IP header + 1480-B data).

12. Print out the second fragment of the fragmented IP datagram. What information in

the IP header indicates that this is not the first datagram fragment? Are the more

fragments? How can you tell?

Second fragment: Fragment offset = 1480/8 = 185 (non-zero), and if MF = 1 then more fragments follow; only the last fragment has MF = 0.

13. What fields change in the IP header between the first and second fragment?

Fields that change between fragment #1 and #2: Total Length, Flags/MF, Fragment offset, and Header Checksum.  
Fields that remain the same: Identification, Src/Dst IP, Protocol, Version, IHL.

1. How many fragments were created from the original datagram?

With Packet Size = 3500 B, number of fragments over Ethernet: 3 fragments

1: data 1480 B → IP TL = 1500, offset=0, MF=1

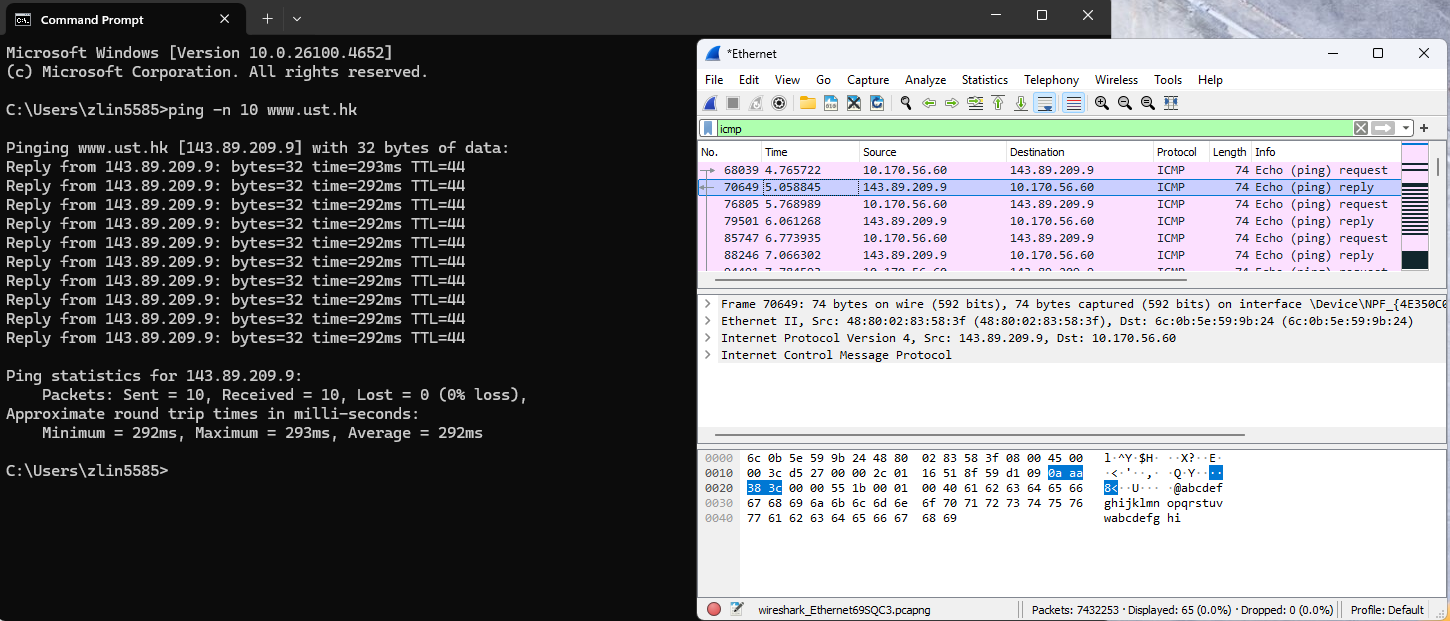
2: data 1480 B → IP TL = 1500, offset=185, MF=1

3: data 540 B → IP TL = 560, offset=370, MF=0

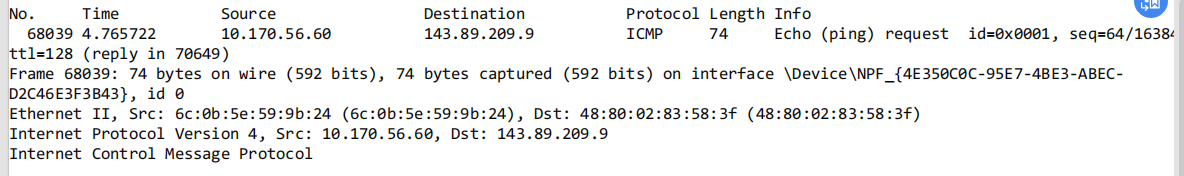
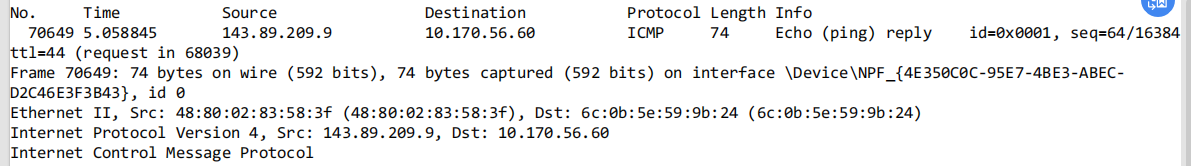
15. What fields change in the IP header among the fragments?

Among those 3500-B fragments, the same rule as Q13: Identification identical across all fragments; Total Length, Fragment offset, Flags/MF, and thus Header Checksum differ; other IP-header fields stay the same.

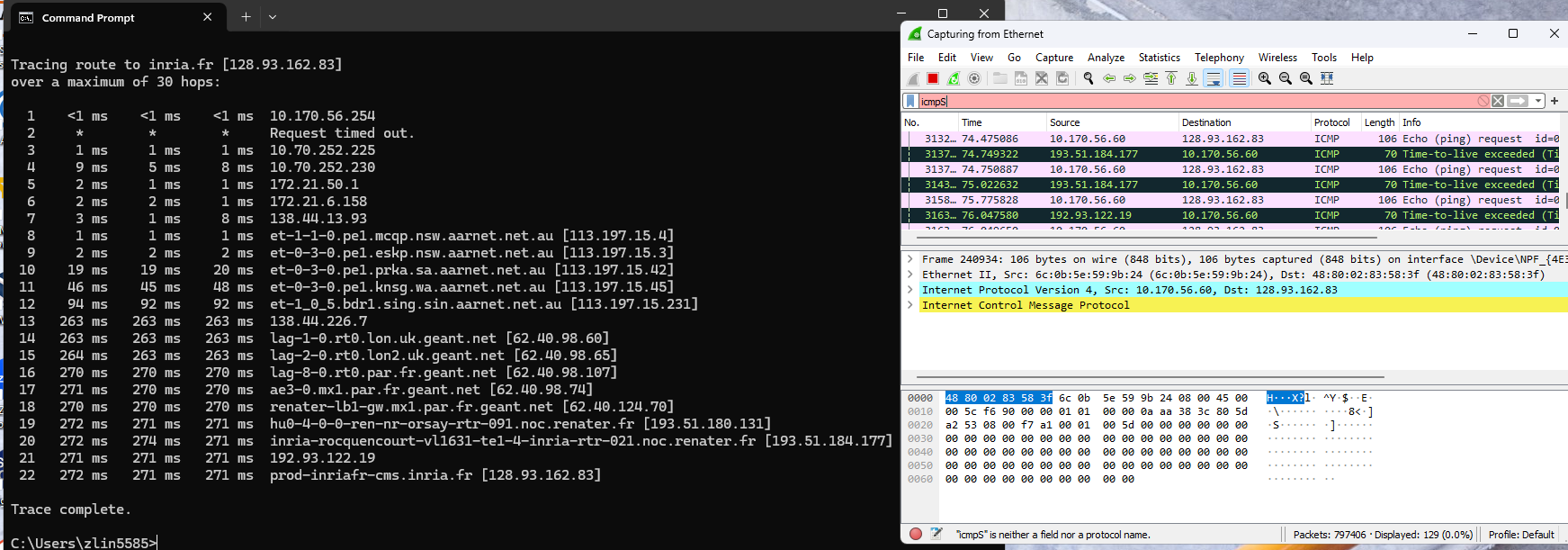
**Appendix**



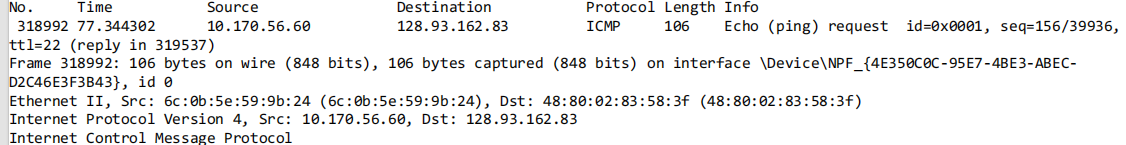
Phase 1: ICMP - Ping Set Up

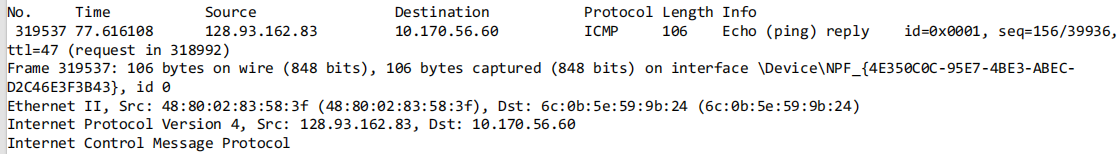


Phase 1: ICMP - Ping Reply and Request

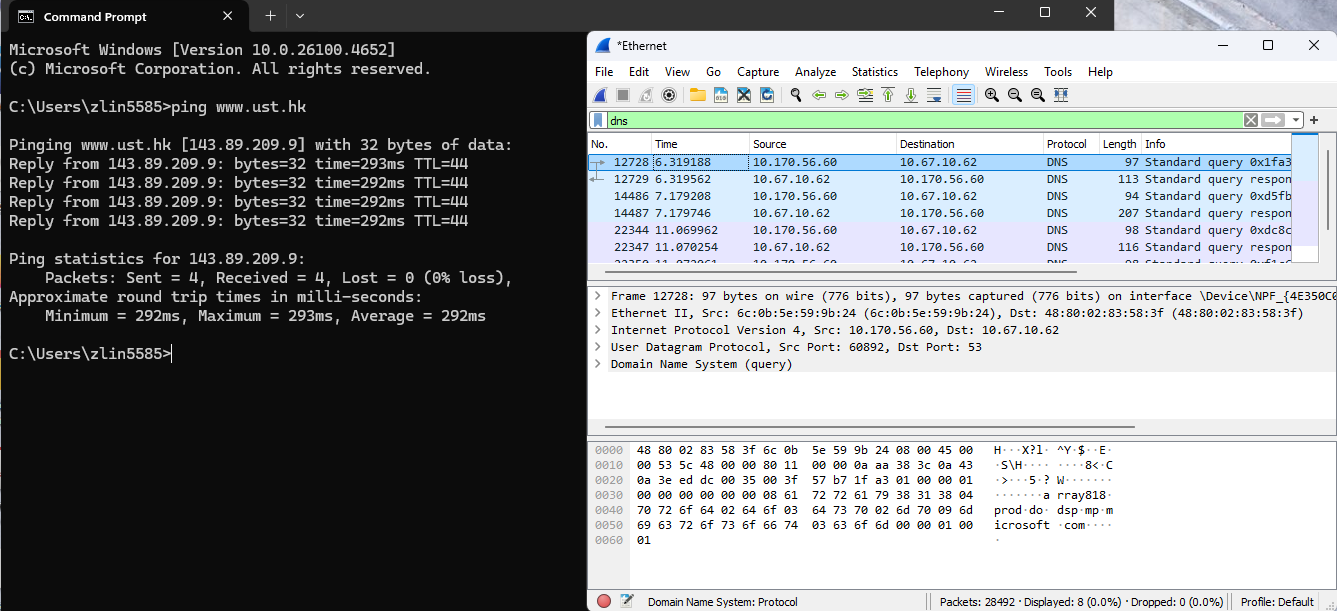


Phase 1: ICMP - Traceroute Set Up

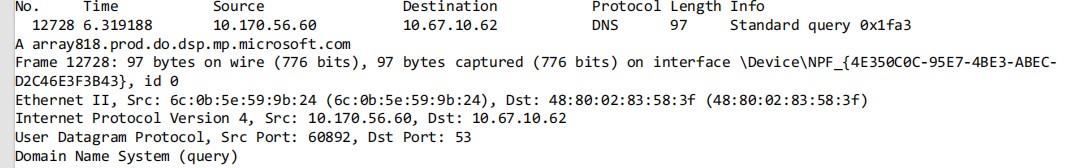


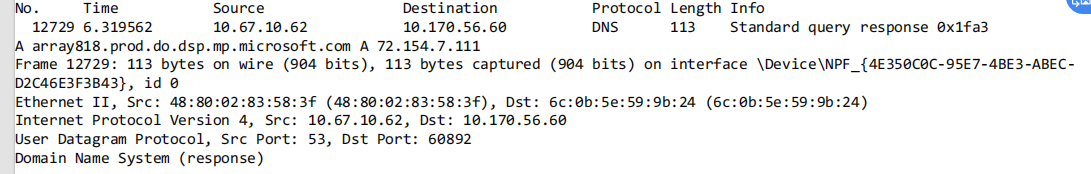


Phase 1: ICMP - Traceroute Reply and Request

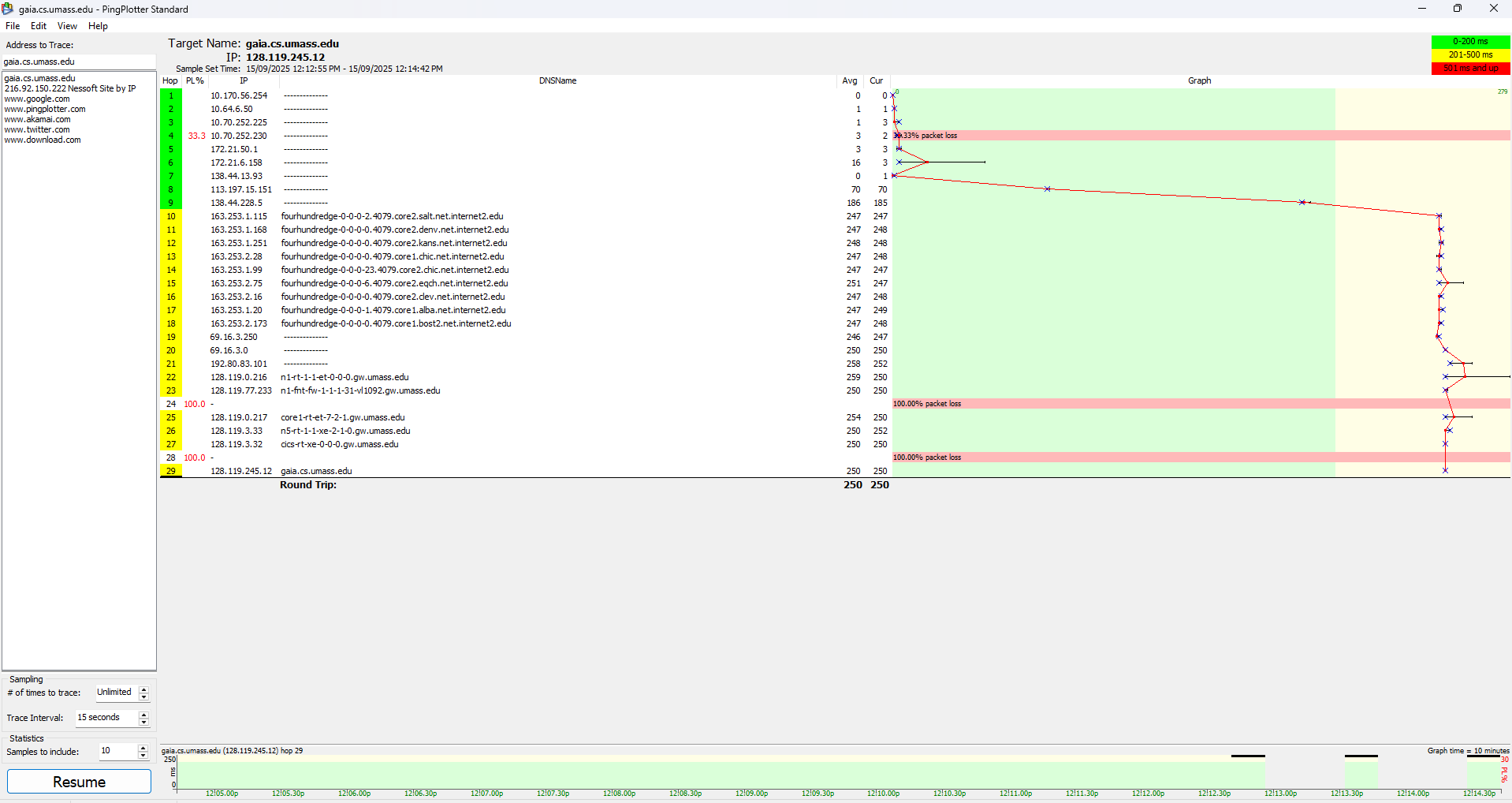
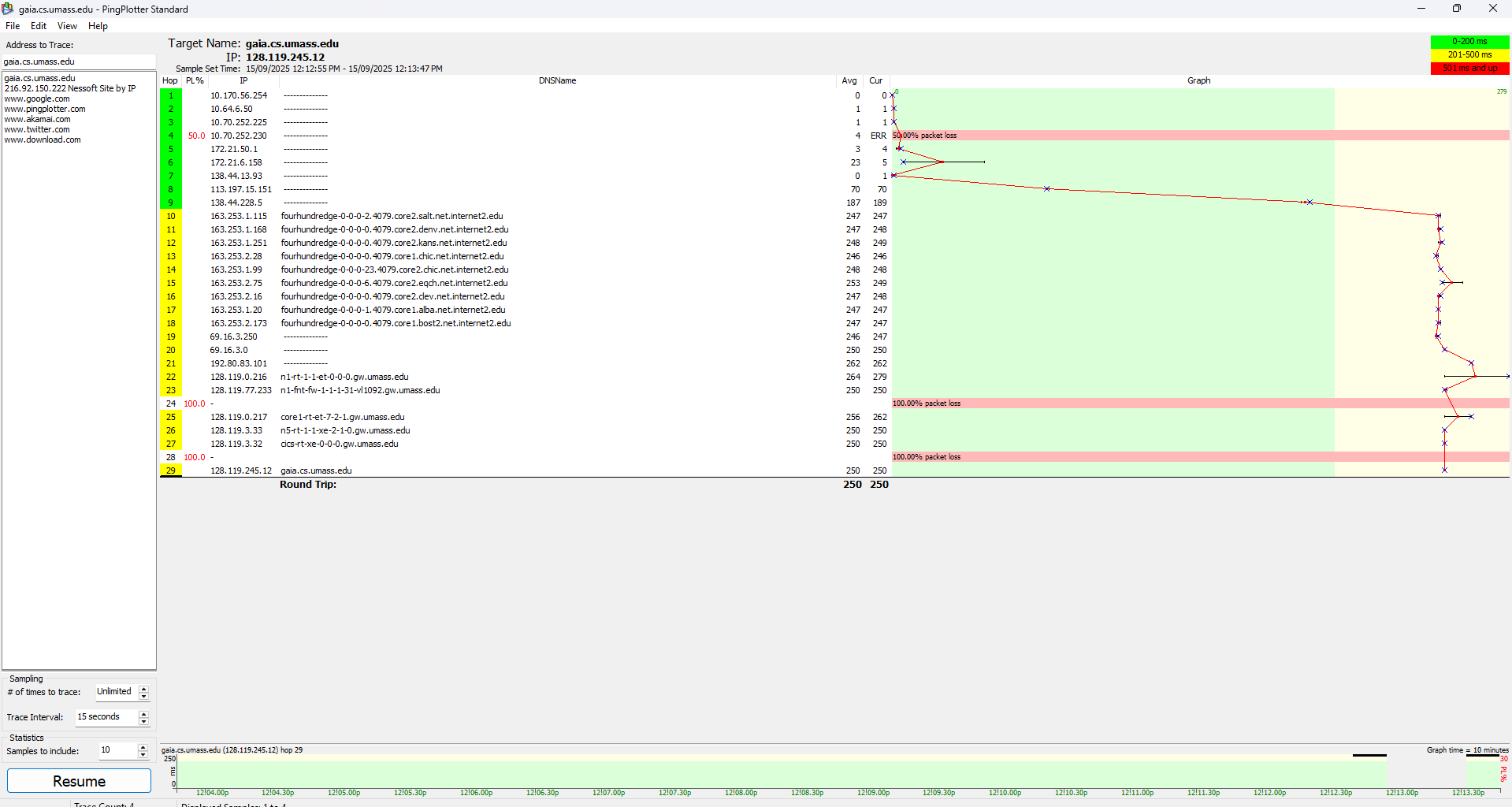
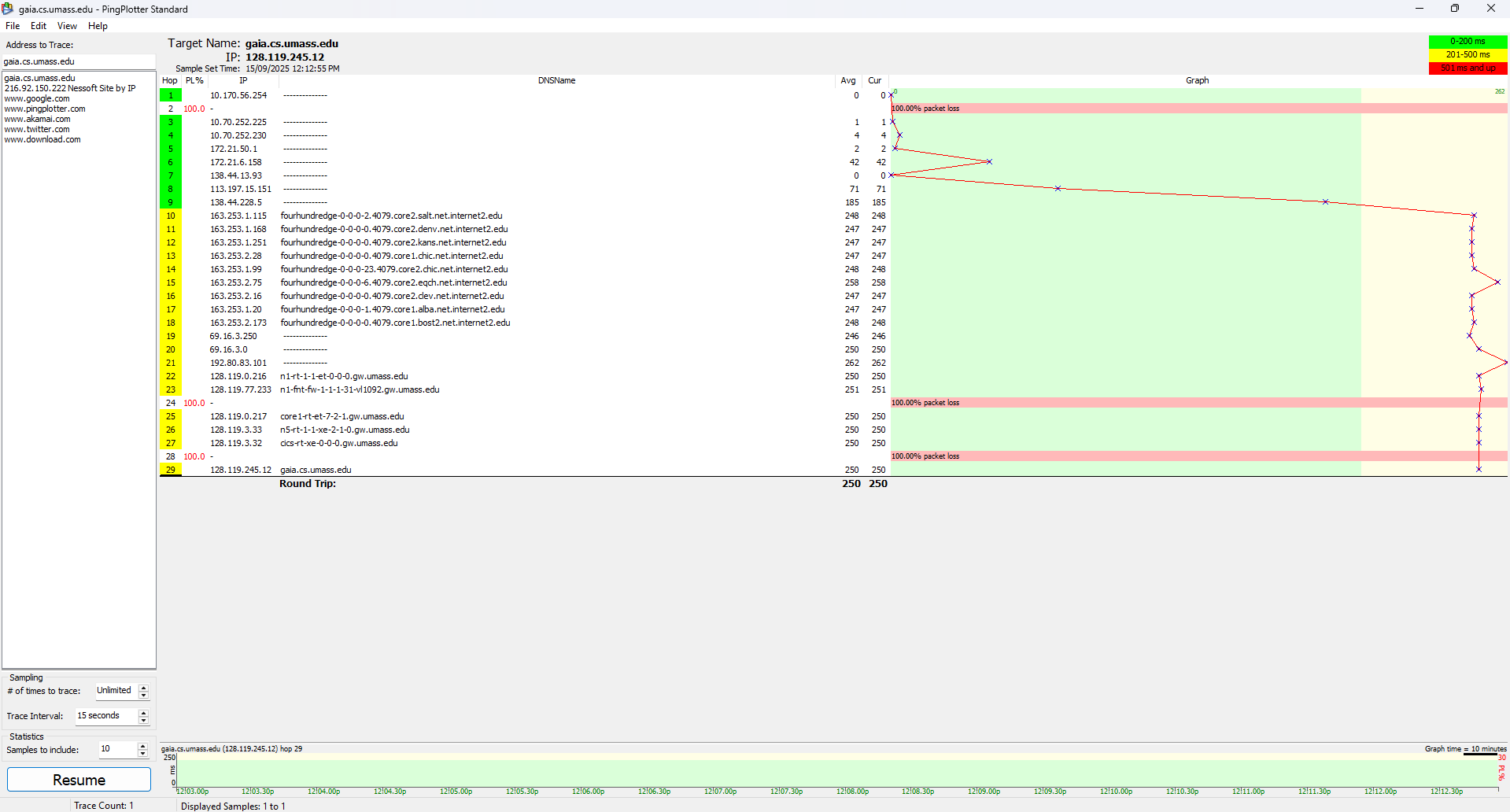


Credit Set Up





Credit Query and Response



Phase 2: IP - Packet Size:56,2000,3500