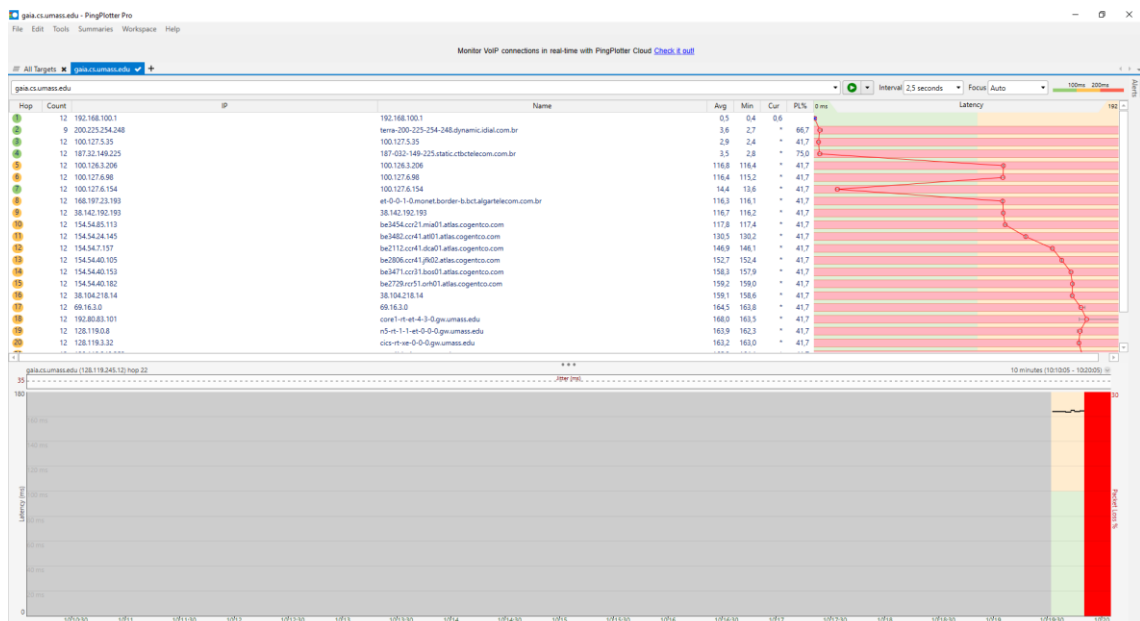
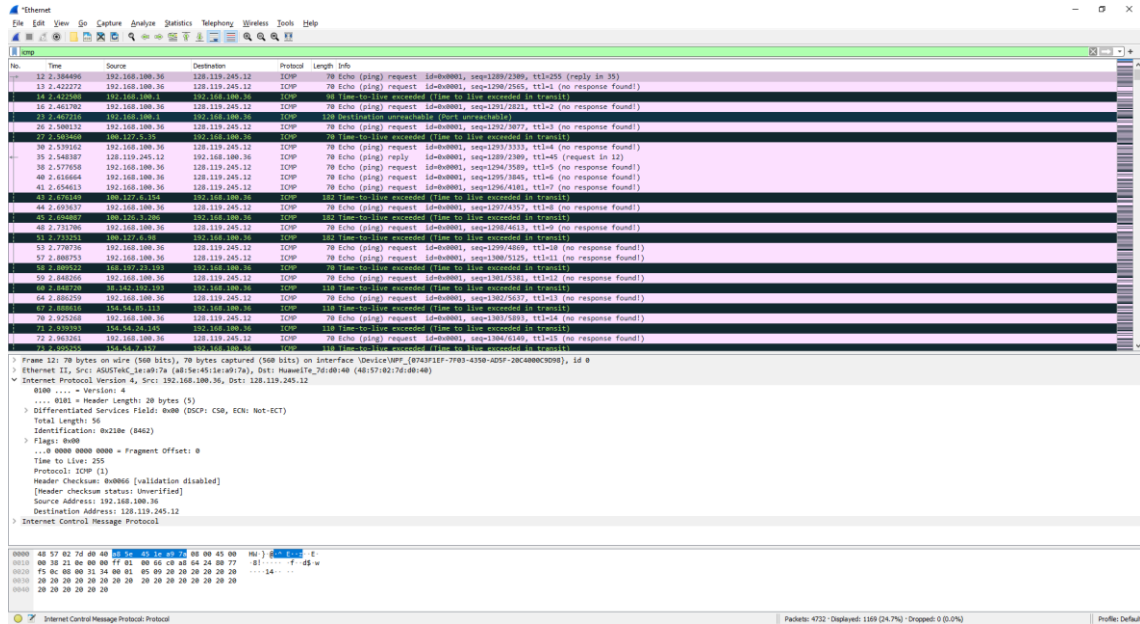


# GS1023 – REDE DE COMPUTADORES

## Computer Networking – J. F. Kurose and K. W. Ross – 7th Edition Chapter 2 – Camadas de Aplicação

Pedro Henrique Silva Santana – 12011BSI218 – pedro.santana@ufu.br  
Victor Hugo Martins Alves – 12011BSI217 – victor.alves1@ufu.br



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?**

Foi utilizado para a comunicação o protocolo ICMP, e o endereço IP do computador é 192.168.100.36

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

O valor do campo protocol é ICMP (1).

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.**

O IP header possui 20 bytes, já o payload possui 36 já que o valor total do tamanho do pacote é de 56.

4. **Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.**

Não pois na aba flags foi indicado o valor 0 para fragment offset.

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?**

Os campos que sempre mudam são: Identification, Time to live and Header checksum.

## 6. Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?

Os campos que se mantem constante são:

- Version - usando IPv4
- header length - para pacotes ICMP
- source IP – enviados de uma mesma fonte
- destination IP – enviados para um mesmo destino
- Differentiated Services – todos pacotes ICMP usam o mesmo tipo de serviço
- Upper Layer Protocol - para pacotes ICMP

Os campos que devem se mantem constante são:

- Version - usando IPv4
- header length - para pacotes ICMP
- source IP – enviados de uma mesma fonte
- destination IP – enviados para um mesmo destino
- Differentiated Services – todos pacotes ICMP usam o mesmo tipo de serviço
- Upper Layer Protocol - para pacotes ICMP

Os campos que devem mudar são:

- Identification – os pacotes IP devem possuir diferentes id's
- Time to live – valor é incrementado pelo pacote anterior
- Header checksum – Alteração da header necessita de um novo checksum

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

O padrão encontrado é que o valor de identificação é incrementado por cada requisição ICMP Echo.

The image shows a Wireshark packet capture of ICMP Echo (ping) requests and replies. The packet list on the left shows 72 packets. The packet details pane on the right shows the structure of the captured packet (Frame 13). The packet structure is as follows:

- Frame 13: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface vDeviceVMP\_07431F7F93-4350-A05F-28C400C3090, Id 0
- Ethernet II, Src: ASUSVME\_1a:00:70:4b:5a:45 (48:5e:45:1a:00:70), Dst: HuaweiE\_7d:d0:40 (48:57:02:7d:d0:40)
- Internet Protocol Version 4, Src: 192.168.100.36, Dst: 128.119.245.12
- 0000 .... = Version: 4
- 0000 .... = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 56
- Identification: 8428f (8403)
- Flags: 0x00
- 0000 .... = Reserved bit: Not set
- 0000 .... = Don't Fragment: Not set
- 0000 .... = More Fragments: Not set
- 0000 0000 0000 = Fragment Offset: 0
- Time to Live: 1
- Protocol: ICMP (1)
- Header Checksum: 0x4e45 (validation disabled)
- [Header checksum status: Unverified]
- Source Address: 192.168.100.36
- Destination Address: 128.119.245.12

The packet bytes pane at the bottom shows the raw data of the packet, including the IP header and ICMP payload.

## 8. What is the value in the Identification field and the TTL field?

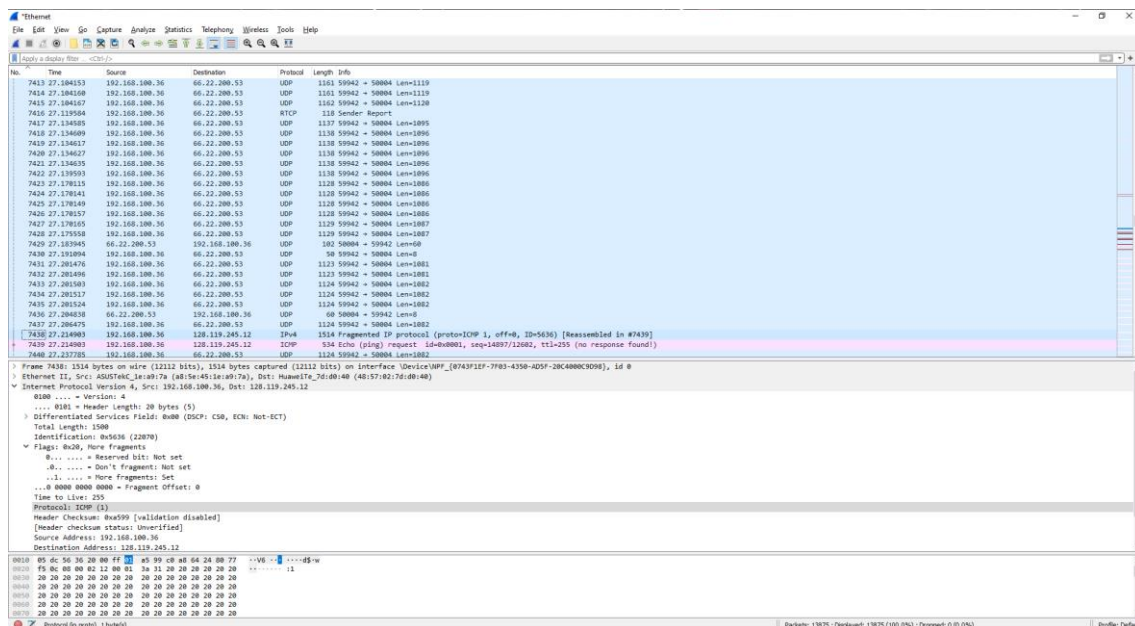
O Valor do campo Identification é 8463 e do campo Time to Live é 1.

## 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?

O campo Identification deve mudar para cada ICMP TTL-exceeded pois o mesmo possui um único valor e, caso dois ou mais IP datagrams possuam o mesmo Id, isso pode significar a fragmentação de um Ip datagram singular. Já o campo TTL permanece o mesmo devido ao fato de ser do mesmo hop. e

## 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 ipethereal-trace-1 packet trace. If your computer has an Ethernet interface, a packet size of 2000 should cause fragmentation.3 ]

O pacote foi fragmentado por mais de um IP datagram.



## 11. 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?

O pacote 7438, no campo more fragments é setado indicando que foi fragmentado. O offset 0 indica que este é o primeiro fragmento e possui tamanho total de 1500.

No.	Time	Source	Destination	Protocol	Length	Info
7413	27.184153	192.168.100.36	66.22.200.53	UDP	1161	59942 → 58004 Len=1119
7414	27.184169	192.168.100.36	66.22.200.53	UDP	1161	59942 → 58004 Len=1119
7415	27.184167	192.168.100.36	66.22.200.53	UDP	1162	59942 → 58004 Len=1120
7416	27.1139584	192.168.100.36	66.22.200.53	RTCP	118	Sender Report
7417	27.114535	192.168.100.36	66.22.200.53	UDP	1137	59942 → 58004 Len=1095
7418	27.114609	192.168.100.36	66.22.200.53	UDP	1138	59942 → 58004 Len=1096
7419	27.114617	192.168.100.36	66.22.200.53	UDP	1138	59942 → 58004 Len=1096
7420	27.114627	192.168.100.36	66.22.200.53	UDP	1138	59942 → 58004 Len=1096
7421	27.114635	192.168.100.36	66.22.200.53	UDP	1138	59942 → 58004 Len=1096
7422	27.119931	192.168.100.36	66.22.200.53	UDP	1138	59942 → 58004 Len=1096
7423	27.178115	192.168.100.36	66.22.200.53	UDP	1128	59942 → 58004 Len=1086
7424	27.178141	192.168.100.36	66.22.200.53	UDP	1128	59942 → 58004 Len=1086
7425	27.178149	192.168.100.36	66.22.200.53	UDP	1128	59942 → 58004 Len=1086
7426	27.178157	192.168.100.36	66.22.200.53	UDP	1128	59942 → 58004 Len=1086
7427	27.178155	192.168.100.36	66.22.200.53	UDP	1129	59942 → 58004 Len=1087
7428	27.178558	192.168.100.36	66.22.200.53	UDP	1129	59942 → 58004 Len=1087
7429	27.183945	66.22.200.53	192.168.100.36	UDP	182	58004 → 59942 Len=60
7430	27.112094	192.168.100.36	66.22.200.53	UDP	58	59942 → 58004 Len=6
7431	27.201476	192.168.100.36	66.22.200.53	UDP	1123	59942 → 58004 Len=1081
7432	27.201496	192.168.100.36	66.22.200.53	UDP	1123	59942 → 58004 Len=1081
7433	27.201503	192.168.100.36	66.22.200.53	UDP	1124	59942 → 58004 Len=1082
7434	27.201517	192.168.100.36	66.22.200.53	UDP	1124	59942 → 58004 Len=1082
7435	27.201524	192.168.100.36	66.22.200.53	UDP	1124	59942 → 58004 Len=1082
7436	27.204810	66.22.200.53	192.168.100.36	UDP	60	58004 → 59942 Len=6
7437	27.206475	192.168.100.36	66.22.200.53	UDP	1124	59942 → 58004 Len=1082
7438	27.214903	192.168.100.36	128.119.245.12	IPV4	1514	Fragmented IP protocol (proto=TCP, seq=1480712082, ttl=255 (no response found))
7439	27.214903	192.168.100.36	128.119.245.12	TCP	534	ECN (ping) request id=0x0001, seq=1480712082, ttl=255 (no response found)
7440	27.217755	192.168.100.36	66.22.200.53	UDP	1124	59942 → 58004 Len=1082

Frame 7439: 536 bytes on wire (4272 bits), 536 bytes captured (4272 bits) on interface eth0 (192.168.100.36) from source 192.168.100.36 to destination 192.168.100.36

Ethernet II, Src: ASUSMeE (a8:1e:45:1a:9b:7a), Dst: HuaweiE (d6:dd:4b:4b:57:02:7d:db:4b)

Internet Protocol Version 4, Src: 192.168.100.36, Dst: 128.119.245.12

IP: 0x00000000 = Version: 4

- 0x00000000 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x0000 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 536
- Identification: 0x5636 (22878)
- Flags: 0x0000
  - 0x0000 = Reserved bit: Not set
  - 0x0000 = Don't Fragment: Not set
  - 0x0000 = More Fragments: Not set
  - 0x0000 = Fragment Offset: 1480
- Time to Live: 255
- Protocol: TCP (6)
- Header Checksum: 0xc8b4 [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 192.168.100.36
- Destination Address: 128.119.245.12

Protocol: TCP (6)

Sequence Number: 1480712082

Window Size: 0

Checksum: 0xc8b4

Urgent Pointer: 0

Options: 0x00000000

Frame 7439 (534 bytes) Reassembled IPV4 (580 bytes)

Protocol (6, proto, 1, byte(s))

Packets: 13875 - Displayed: 13875 (100.0%) - Dropped: 0 (0.0%)

Profile: Default

**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 there more fragments? How can you tell?**

Podemos ver que não é o primeiro fragmento pois o offset é de 1480, porém este é o último pois não foram setados novos fragmentos após teste.

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

Os campos que se alteraram entre o primeiro e segundo fragmento são: total length, flags, fragment offset, and checksum.

