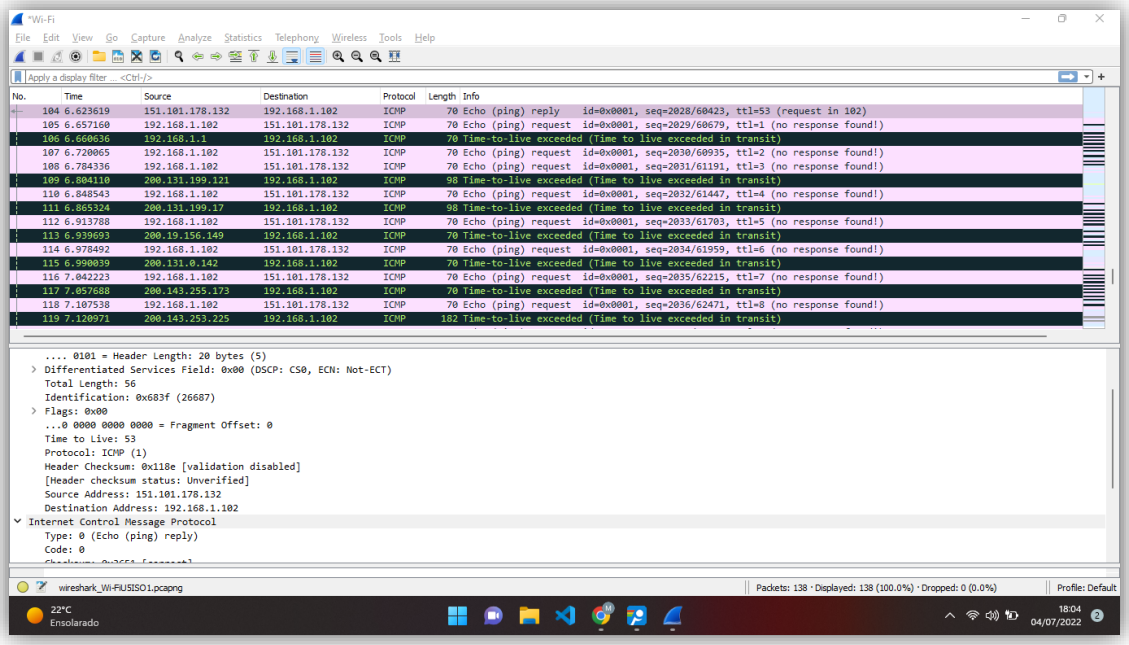
GSI023 – Redes de Computadores

Wireshark Lab - IP

Murielly Oliveira Nascimento – 11921BSI222 – murielly.nascimento@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?**



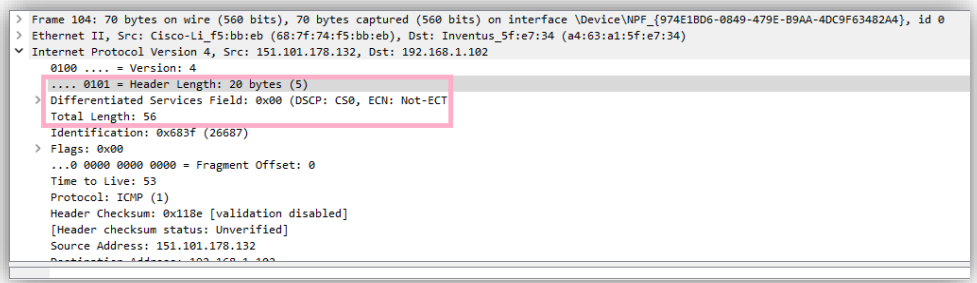
O endereço IP é 151. 101.178.132

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

Dentro do header, o valor do protocolo da camada superior é ICMP (0x01).

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.**

Há 20 bytes no IP header, e 56 bytes de comprimento no total, o que resulta em 36 bytes de payload do IP datagram.



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

O fragment offset é de 0, logo os pacotes de dados não foram fragmentados.

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?**

Identificação, Tempo de Duração e a soma do Header sempre mudam.

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

Os campos que permanecem constantes entre IP datagrams são:

- Version, no caso, IPv4
- Header length
- Source IP
- Destination IP
- Differentiated Services
- Upper Layer Protocol

Os campos que devem permanecer constantes são:

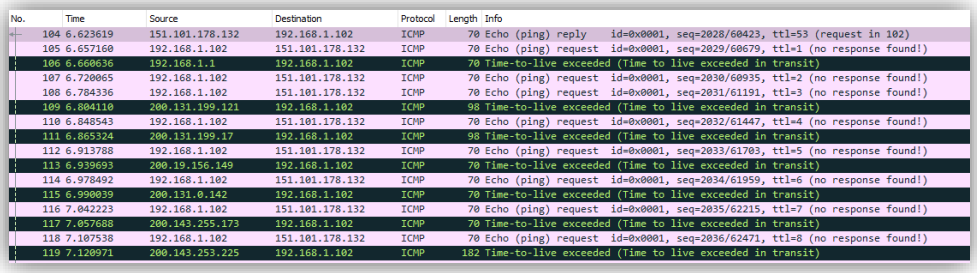
- Version
- Header Length
- Source IP
- Destination IP
- Differentiated Services
- Upper Layer Protocol

Os campos que devem mudar:

- Identification
- Time to live
- Header checksum

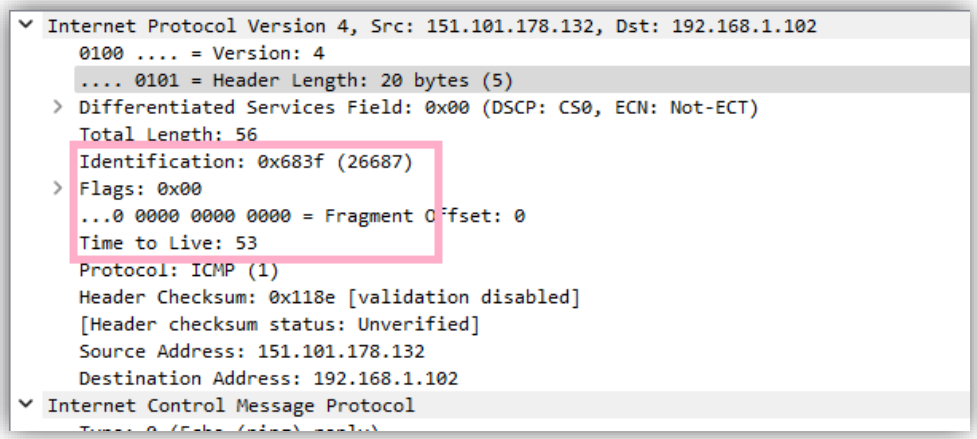
7. **Describe the pattern you see in the values in the Identification field of the IP datagram**

O padrão é que os campos de identificação do cabeçalho IP sejam incrementados a cada Solicitação de eco ICMP (ping).



No.	Time	Source	Destination	Protocol	Length	Info
104	6.623619	151.101.178.132	192.168.1.102	ICMP	70	Echo (ping) reply id=0x0001, seq=2028/60423, ttl=53 (request in 102)
105	6.657160	192.168.1.102	151.101.178.132	ICMP	70	Echo (ping) request id=0x0001, seq=2029/60679, ttl=1 (no response found!)
106	6.660636	192.168.1.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
107	6.720065	192.168.1.102	151.101.178.132	ICMP	70	Echo (ping) request id=0x0001, seq=2030/60935, ttl=2 (no response found!)
108	6.784336	192.168.1.102	151.101.178.132	ICMP	70	Echo (ping) request id=0x0001, seq=2031/61191, ttl=3 (no response found!)
109	6.804110	200.131.199.121	192.168.1.102	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
110	6.848543	192.168.1.102	151.101.178.132	ICMP	70	Echo (ping) request id=0x0001, seq=2032/61447, ttl=4 (no response found!)
111	6.865324	200.131.199.17	192.168.1.102	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
112	6.913788	192.168.1.102	151.101.178.132	ICMP	70	Echo (ping) request id=0x0001, seq=2033/61703, ttl=5 (no response found!)
113	6.939693	200.19.156.149	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
114	6.978492	192.168.1.102	151.101.178.132	ICMP	70	Echo (ping) request id=0x0001, seq=2034/61959, ttl=6 (no response found!)
115	6.990039	200.131.0.142	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
116	7.042223	192.168.1.102	151.101.178.132	ICMP	70	Echo (ping) request id=0x0001, seq=2035/62215, ttl=7 (no response found!)
117	7.057688	200.143.255.173	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
118	7.107538	192.168.1.102	151.101.178.132	ICMP	70	Echo (ping) request id=0x0001, seq=2036/62471, ttl=8 (no response found!)
119	7.120971	200.143.253.225	192.168.1.102	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)

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



Identificação: 26687

TTL: 53

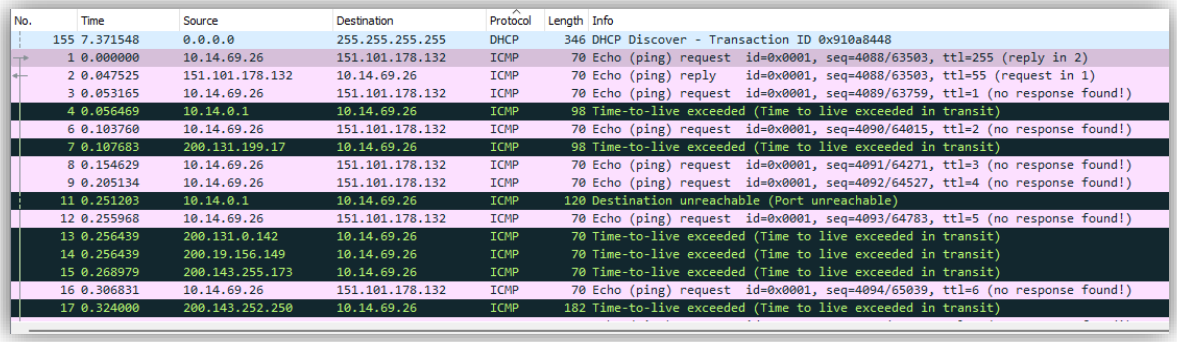
9. **Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?**

O campo de identificação muda para todas as respostas ICMP TTL excedidas porque o campo de identificação é um valor único. Quando dois ou mais IPs datagramas têm o mesmo valor de identificação, então isso significa que esses IP datagramas são fragmentos de um único datagrama IP grande. O campo TTL permanece inalterado porque o TTL para o primeiro roteador de salto é sempre o mesmo.

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?**

Sim, este pacote foi fragmentado em mais de um datagrama IP.

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?**



No.	Time	Source	Destination	Protocol	Length	Info
155	7.371548	0.0.0.0	255.255.255.255	DHCP	346	DHCP Discover - Transaction ID 0x910a8448
1	0.000000	10.14.69.26	151.101.178.132	ICMP	70	Echo (ping) request id=0x0001, seq=4088/63503, ttl=255 (reply in 2)
2	0.047525	151.101.178.132	10.14.69.26	ICMP	70	Echo (ping) reply id=0x0001, seq=4088/63503, ttl=55 (request in 1)
3	0.053165	10.14.69.26	151.101.178.132	ICMP	70	Echo (ping) request id=0x0001, seq=4089/63759, ttl=1 (no response found!)
4	0.056469	10.14.0.1	10.14.69.26	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
6	0.103760	10.14.69.26	151.101.178.132	ICMP	70	Echo (ping) request id=0x0001, seq=4090/64015, ttl=2 (no response found!)
7	0.107683	200.131.199.17	10.14.69.26	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
8	0.154629	10.14.69.26	151.101.178.132	ICMP	70	Echo (ping) request id=0x0001, seq=4091/64271, ttl=3 (no response found!)
9	0.205134	10.14.69.26	151.101.178.132	ICMP	70	Echo (ping) request id=0x0001, seq=4092/64527, ttl=4 (no response found!)
11	0.251203	10.14.0.1	10.14.69.26	ICMP	120	Destination unreachable (Port unreachable)
12	0.255968	10.14.69.26	151.101.178.132	ICMP	70	Echo (ping) request id=0x0001, seq=4093/64783, ttl=5 (no response found!)
13	0.256439	200.131.0.142	10.14.69.26	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
14	0.256439	200.19.156.149	10.14.69.26	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
15	0.268979	200.143.255.173	10.14.69.26	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
16	0.306831	10.14.69.26	151.101.178.132	ICMP	70	Echo (ping) request id=0x0001, seq=4094/65039, ttl=6 (no response found!)
17	0.324000	200.143.252.250	10.14.69.26	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)

O bit Flags para mais fragmentos é definido, indicando que o datagrama foi fragmentado. Como o deslocamento do fragmento é 0, sabemos que este é o primeiro fragmento. Este primeiro datagrama tem um comprimento total de 1500, incluindo o cabeçalho.

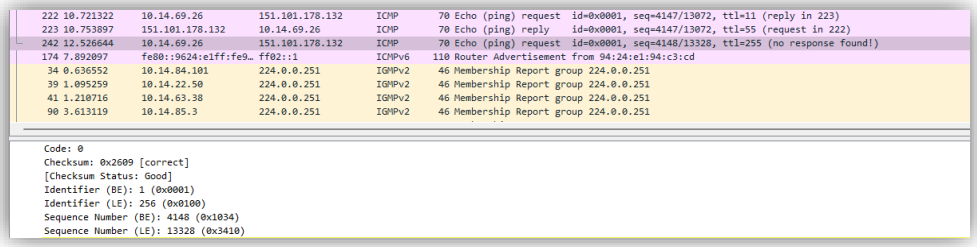
12. **Print out the second fragment of the fragmented IP datagram. What information in the IP header indicates that this is not the first datagram fragment? Are the more fragments? How can you tell?**

Determinamos isso pelo fragment offset é diferente de 0. E que é o último fragmento já que não há mais fragments flag setados.

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

Os campos do header que mudaram entre os fragmentos são: comprimento total, fragment offset e checksum.

14. **How many fragments were created from the original datagram?**



Depois de modificado para 3500, há a criação de 3 pacotes do datagram original.

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

Os campos de cabeçalho IP que mudaram entre todos os pacotes são: deslocamento do fragmento e soma de verificação. Entre os dois primeiros pacotes e o último pacote, vemos uma mudança no comprimento total e também nos sinalizadores. Os dois primeiros pacotes têm um comprimento total de 1500, com o bit de mais fragmentos definido como 1, e o último pacote tem um comprimento total de 540, com o bit de mais fragmentos definido como 0.