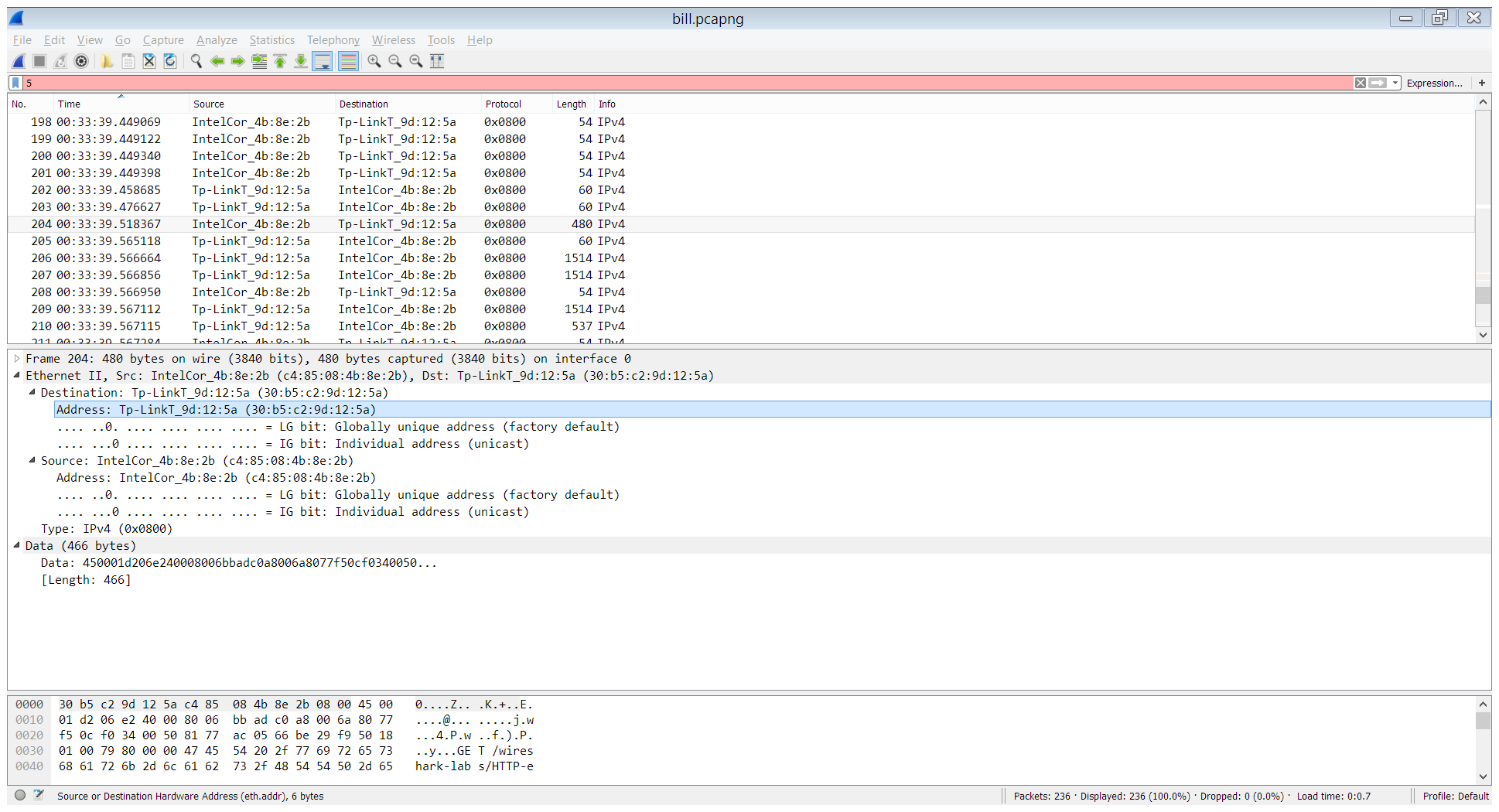
**Tevin Jeffrey**

**Wireshark Lab 7**

****

**1. What is the 48-bit Ethernet address of your computer?**

c4:85:08:4b:8e:2b

**2. What is the 48-bit destination address in the Ethernet frame?**

30:b5:c2:9d:12:5a

Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is no). What device has this as its Ethernet address? [Note: this is an important question, and one that students sometimes get wrong. Re-read pages 468-469 in the text and make sure you understand the answer here.]

That is the mac address of my home router.

**3. Give the hexadecimal value for the two-byte Frame type field. What do the bit(s) whose value is 1 mean within the flag field?**

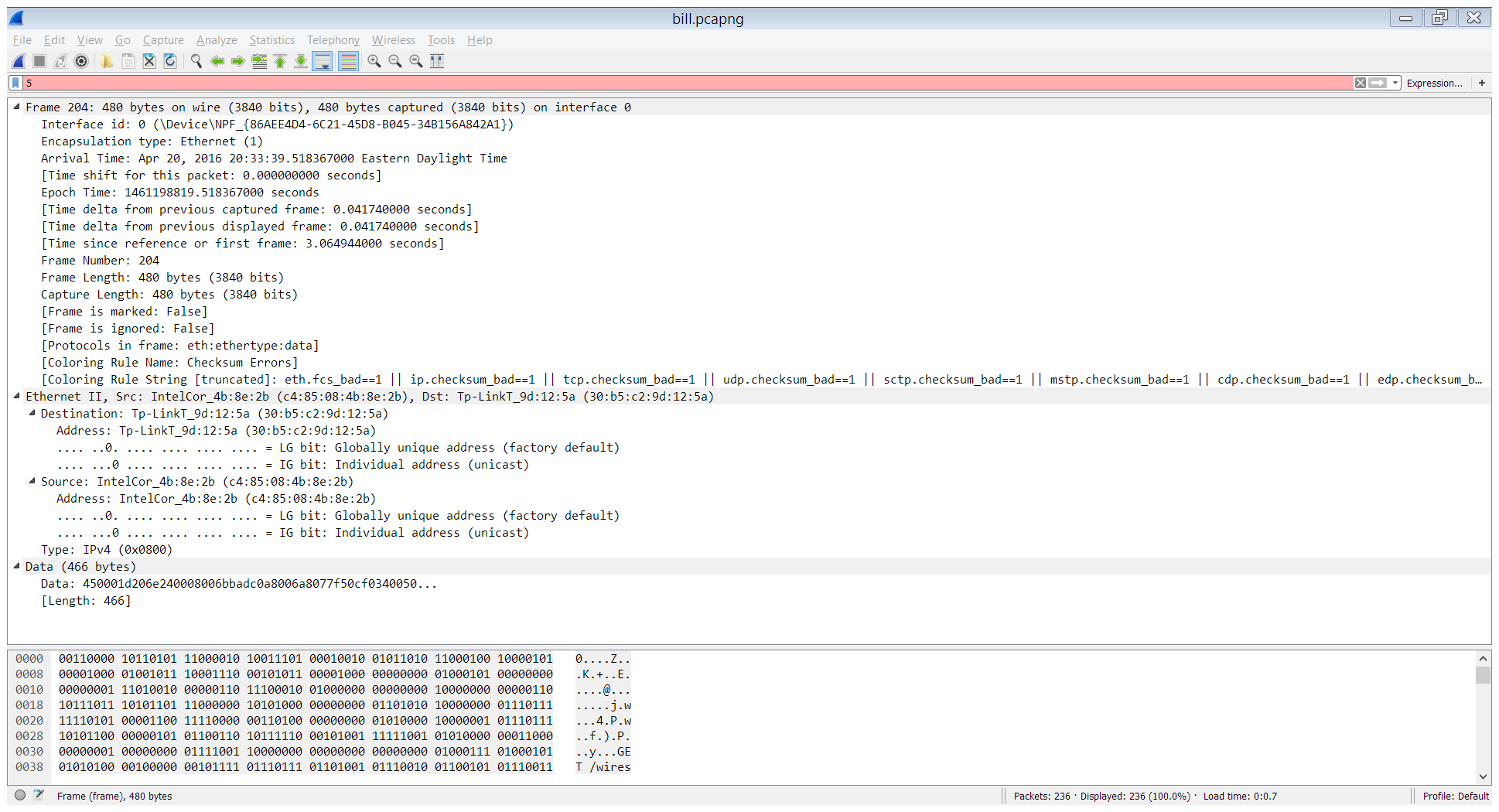
0x0800

It means internet protocol 4

**4. How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame?**

About 36 bytes from the start do I see the G in GET.

**5. What is the hexadecimal value of the CRC field in this Ethernet frame?**



I don’t see one.

**6. What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu (Hint: the answer is no).**

c4:85:08:4b:8e:2b, No

**What device has this as its Ethernet address?**

The network interface of on my PC.

**7. What is the destination address in the Ethernet frame?**

30:b5:c2:9d:12:5a

**Is this the Ethernet address of your computer?**

The network interface for my home router.

**8. Give the hexadecimal value for the two-byte Frame type field. What do the bit(s) whose value is 1 mean within the flag field?**

I don’t see one

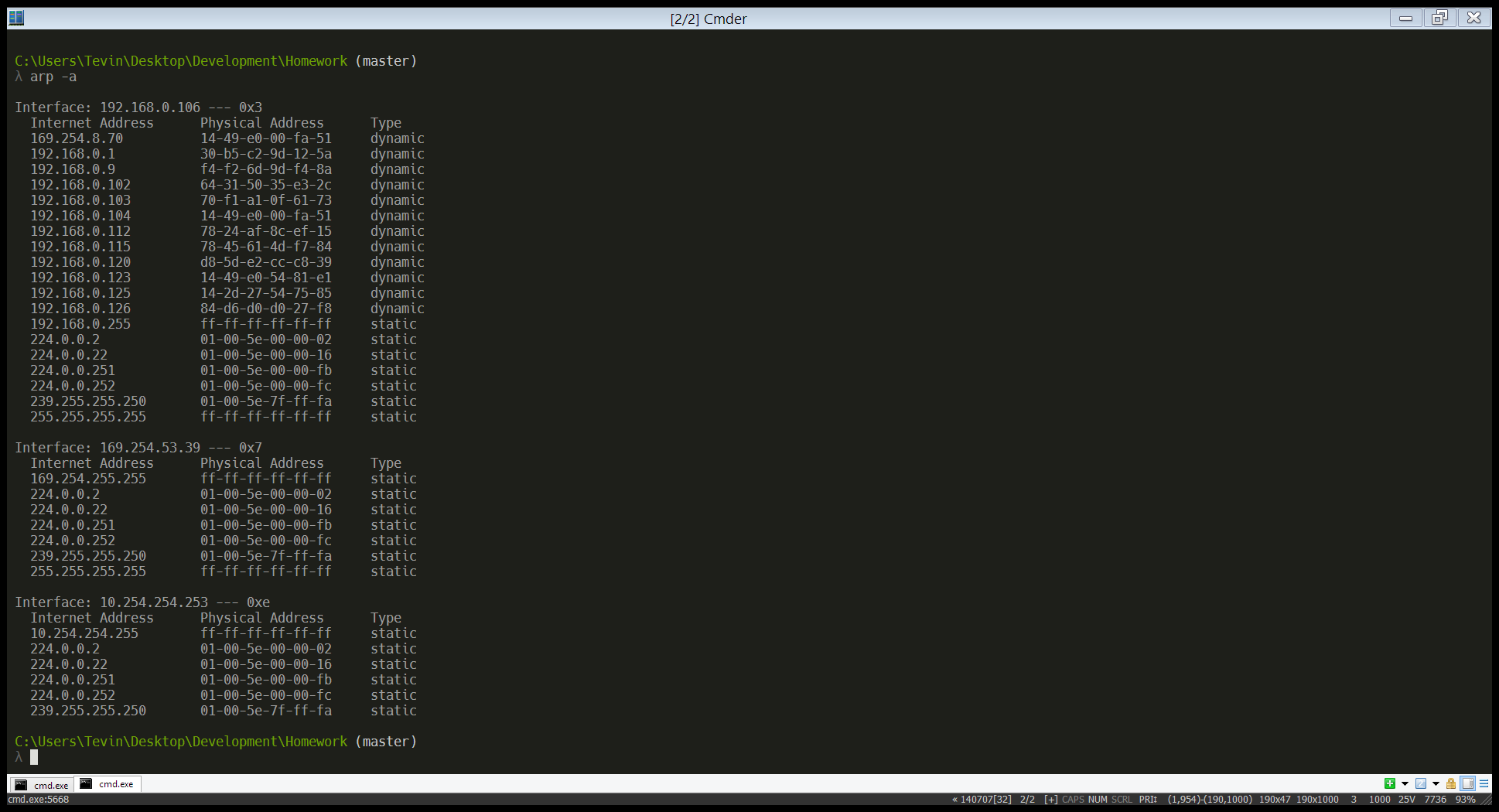
**9. How many bytes from the very start of the Ethernet frame does the ASCII “O” in “OK” (i.e., the HTTP response code) appear in the Ethernet frame?**

~46

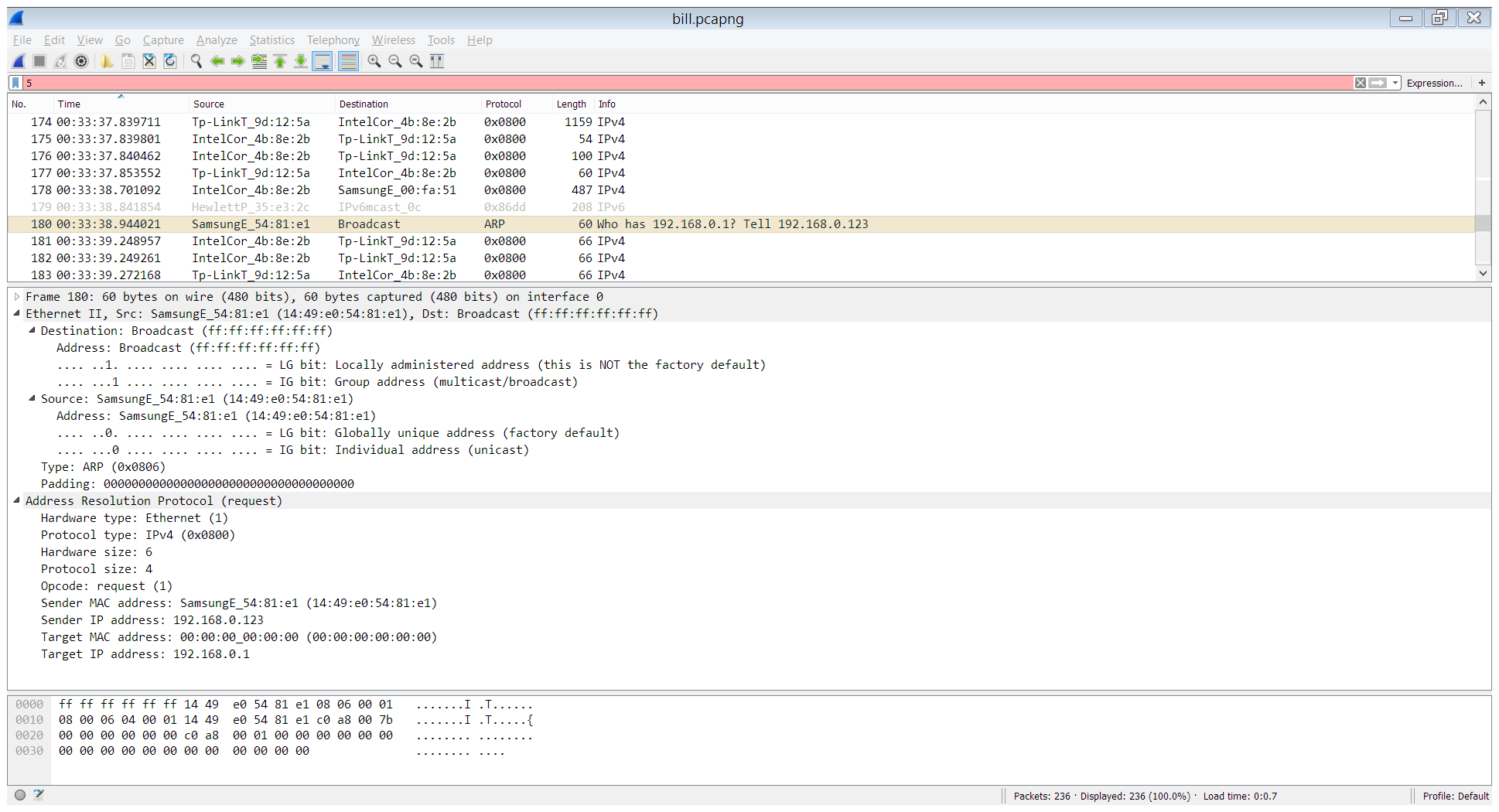
**10. What is the hexadecimal value of the CRC field in this Ethernet frame?**

There is none

**11. Write down the contents of your computer’s ARP cache. What is the meaning of each column value?**



The left colum is the IPv4 adress in the cache, the middle colum is the physical address of the interface for the machine with that ip adress and the far right is the whether physical address is bound to the internet adress dynamically or statically.



**12. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?**

Source: 14:49:e0:54:81:e1

Destination: ff:ff:ff:ff:ff:ff

**13. Give the hexadecimal value for the two-byte Ethernet Frame type field. What do the bit(s) whose value is 1 mean within the flag field?**

ARP

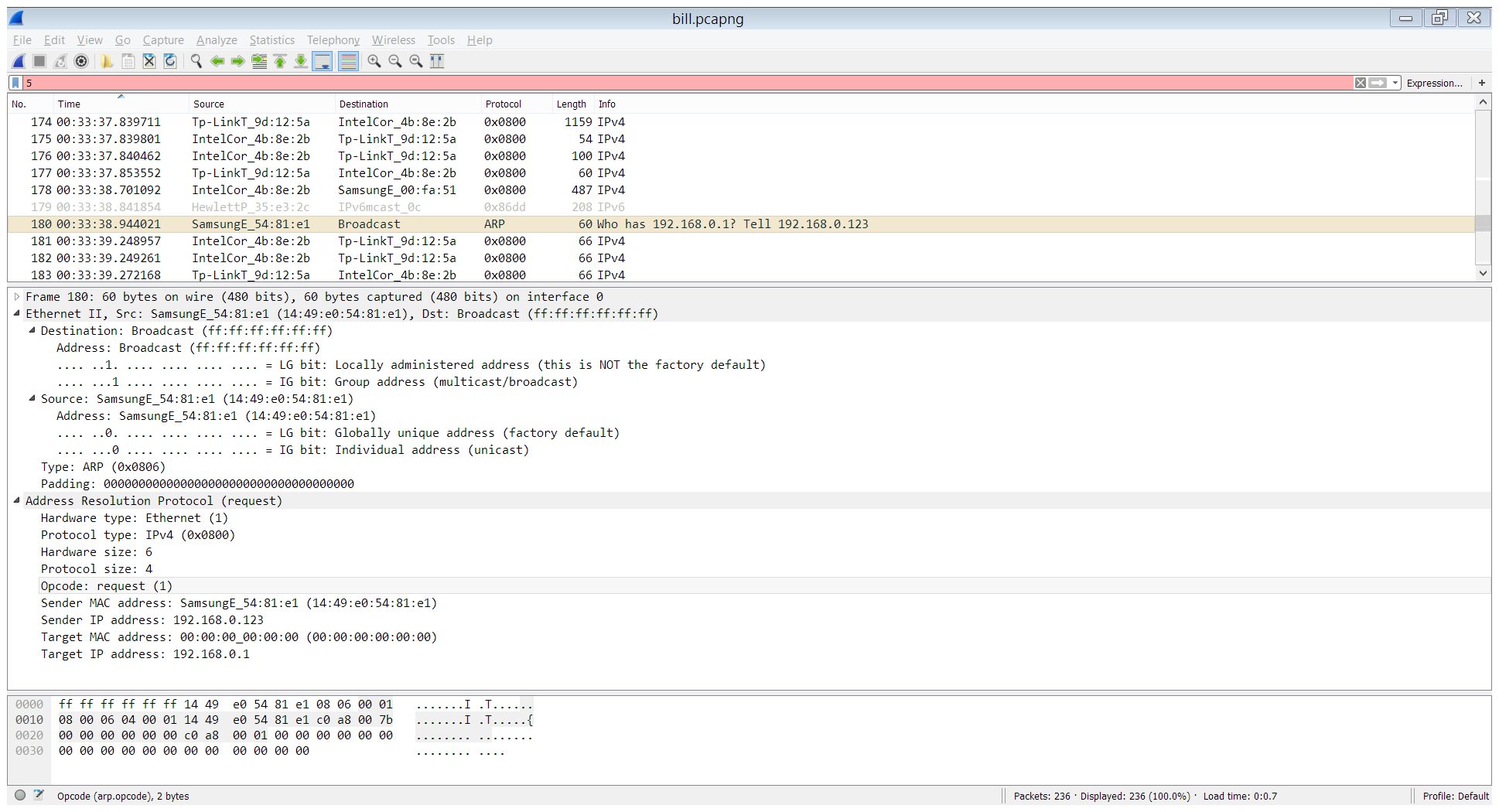
**14 a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?**

48 bytes

**b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made?**

1

**c) Does the ARP message contain the IP address of the sender?**



Yes.

**d) Where in the ARP request does the “question” appear – the Ethernet address of the machine whose corresponding IP address is being queried?**

The target MAC adress is empty while the target IP address is not. It’s fair to say the “querstion” is the ethernet address.

**15. a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?**

48 bytes

**b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made?**

2

**c) Where in the ARP message does the “answer” to the earlier ARP request appear – the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?**

The answer is in the Target MAC address field

**16. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?**

Src: SamsungE\_00:fa:51 (14:49:e0:00:fa:51)

Dst: IntelCor\_4b:8e:2b (c4:85:08:4b:8e:2b)

**17. Open the ethernet-ethereal-trace-1 trace file in http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip. The first and second ARP packets in this trace correspond to an ARP request sent by the computer running Wireshark, and the ARP reply sent to the computer running Wireshark by the computer with the ARP-requested Ethernet address. But there is yet another computer on this network, as indiated by packet 6 – another ARP request. Why is there no ARP reply (sent in response to the ARP request in packet 6) in the packet trace?**

It’s possible that this machine does not know the Ethernet addresses for the machine at that internet address.