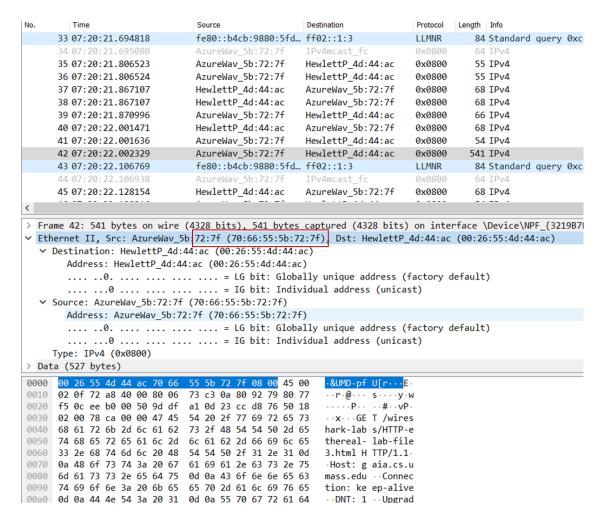




1/ What is the 48-bit Ethernet address of your computer?

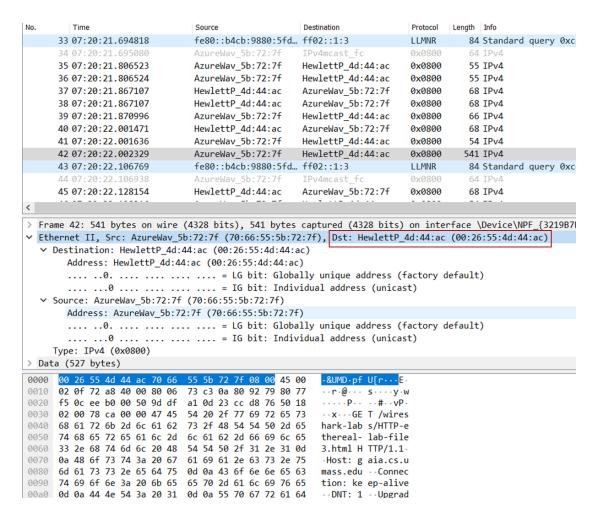
Answer: The 48-bit Ethernet address of my computer is 70:66:55:5b:72:7f



2/ What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? What device has this as its Ethernet address?

Answer: The 48-bit destination address in the Ethernet frame is 00:26:55:4d:44:ac. This is not the address of gaia.cs.umass.edu. This is the address of the router that my computer has to go through in order to reach the destination.





3/ Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

Answer: The hexadecimal value for the two-byte frame type field is 0x0800. This corresponds to the IP protocol (the frame type filed indicates that the nest layer above IP – the layer to which the payload of the Ethernet frame will connect to IP.



No.	Time					S	ource	9					De	stinat	ion				Protocol	Ler	ngth	Info		
	33 07:	20:21.	6948	18		f	e80	::b	4cb	:98	80:	5fd	ff	02:	1:3				LLMNR		84	Standard	query	0xc
	34 07:	20:21.	69508	80		Α	zur	eWa	v_5	b:7	2:7	f	IF	v4m	ast_f	fc		(0x0800		64	IPv4		
	35 07:	20:21.	8065	23		Α	zur	eWa	v_5	b:7	2:7	f	Нє	ewlet	ttP_4	d:4	4:ac	(0800x6		55	IPv4		
	36 07:	20:21.	8065	24		Α	zur	eWa	v_5	b:7	2:7	f	Не	ewlet	tP_4	d:4	4:ac	(0800x6		55	IPv4		
	37 07:	20:21.	8671	27		Н	ewl	ettl	P_4	d:4	4:a	С	Az	zurel	lav_5t	b:7	2:7f	(0800x6		68	IPv4		
	38 07:	20:21.	8671	27		Н	ewl	ett	P_4	d:4	4:a	С	Az	zurel	lav_5b	b:7	2:7f	(0800x6		68	IPv4		
	39 07:	20:21.	87099	96		Α	zur	eWa	v_5	b:7	2:7	f	Нє	ewlet	ttP_4	d:4	4:ac	(0800x6		66	IPv4		
	40 07:	20:22.	0014	71		Н	ewl	ett	P_4	d:4	4:a	С	Az	zurel	lav_5Ł	b:7	2:7f	(0800x6		68	IPv4		
	41 07:	20:22.	0016	36		Α	zur	eWa	v_5	b:7	2:7	f	Нє	ewlet	ttP_4	d:4	4:ac	(0800x6		54	IPv4		
	42 07:	20:22.	0023	29		Α	zur	eWa	v_5	b:7	2:7	f	Не	ewlet	ttP_4	d:4	4:ac	(080x6		541	IPv4		
	43 07:	20:22.	1067	59		f	e80	::b	4cb	:98	80:	5fd	ff	02:	1:3				LLMNR		84	Standard	query	0xc
	44 07:	20:22.	1069	38		Α	zur	eWa	v_5	b:7	2:7	f	IF	v4m	cast_f	fc		(0x0800		64	IPv4		
	45 07:	20:22.	1281	54		Н	ewl	ettl	P_4	d:4	4:a	С	Az	zurel	lav_5Ł	b:7	2:7f	(0800x6		68	IPv4		
<									_	_	-													
\ Fno.	ma 12.	E // 1 h.	.+			/42	าด เ		- \	E 4	1 h				ad //	1220	0 6:+-	- \ .			'	Davis ca\ NE	יר (ססי	10071
						_						_						_				\Device\NF 5:55:4d:44		19871
	Destina				_										DSC.	пеи	wiettr	_40	1.44.aC	. (6)	0.20).	+.ac)	
,		ess: H			_																			
				_			•						•	, un	iaua	94d	lnace	(fa	ctory	dofa	1+	1		
		0																-	-	ucia	ult	,		
	Source:												viu	uai	auui C	33	(unite	asc	,					
,		ess: A				_						-	7f)											
														v un	ique	add	lress	(fa	ctory	defa	u1+)		
		0																-	_	acro		,		
-	Type: I							_	10	UI	j 1		. v I u	uuı	uuui C		(unite	usc	,					
	a (527	•																						
0000	00 26			c 70	66	55	5h	72	7.5	ag	aa	15	aa		LIMD - r	ı.	J[r···	c .						
0010	02 Of						c3										5 V							
0020	f5 0c						0d								_		# · · v							
0030	02 00						20										Γ/wir							
0040	68 61					73											s/HTTP							
0050	74 68	65 72	65 6	1 60	2d	6c	61	62	2d	66	69	6c	65	th	ereal	-]	lab-fi	ile						
0060	33 2e	68 74	6d 6	c 20	48	54	54	50	2f	31	2e	31	0d	3.	html	Η٦	ΓΤΡ/1.	1-						
	0a 48															_	aia.cs							
0080																	Conn							
0090	74 69																ep-ali							
00a0	0d 0a	44 4e	54 3	a 20	31	Ød	0a	55	70	67	72	61	64		DNT:	1 .	· · Upgr	ad						

4/ How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame?

Answer: The ASCII "G" appears 54 bytes from the start of the Ethernet frame.

- The ethernet frame (first 14 bytes containing destination address, source address, and frame type)
- The IP header (20 bytes)
- The TCP header (20 bytes)

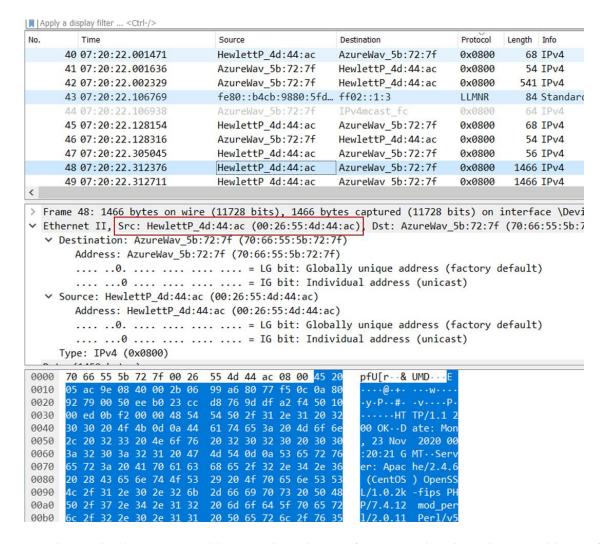


	F1 11 F033		
0000	00 26 55 4d 44 ac 70 66 55 5	5b 72 7f 08 00 <mark>45 00</mark>	-&UMD-pf U[r··· <mark>E·</mark>
0010	02 0f 72 a8 40 00 80 06 73 (3 0a 80 92 79 80 77	r.@ sy.w
0020	f5 0c ee b0 00 50 9d df a1 0	0d 23 cc d8 76 50 18	P#vP.
0030	02 00 78 ca 00 00 47 45 54 2	20 2f 77 69 72 65 73	xGE T /wires
0040	68 61 72 6b 2d 6c 61 62 73 2	2f 48 54 54 50 2d 65	hark-lab s/HTTP-e
0050	74 68 65 72 65 61 6c 2d 6c 6	51 62 2d 66 69 6c 65	thereal- lab-file
0060	33 2e 68 74 6d 6c 20 48 54 5	54 50 2f 31 2e 31 0d	3.html H TTP/1.1.
0070	0a 48 6f 73 74 3a 20 67 61 6	59 61 2e 63 73 2e 75	·Host: g aia.cs.u
0080	6d 61 73 73 2e 65 64 75 Ød (a 43 6f 6e 6e 65 63	mass.edu ··Connec
0090	74 69 6f 6e 3a 20 6b 65 65 3	70 2d 61 6c 69 76 65	tion: ke ep-alive
00a0	0d 0a 44 4e 54 3a 20 31 0d (0a 55 70 67 72 61 64	DNT: 1Upgrad
00b0	65 2d 49 6e 73 65 63 75 72 6	55 2d 52 65 71 75 65	e-Insecu re-Reque
00c0	73 74 73 3a 20 31 0d 0a 55 3	73 65 72 2d 41 67 65	sts: 1 User-Age
00d0	6e 74 3a 20 4d 6f 7a 69 6c (5c 61 2f 35 2e 30 20	nt: Mozi lla/5.0
00e0	28 57 69 6e 64 6f 77 73 20 4	le 54 20 31 30 2e 30	(Windows NT 10.0
00f0	3b 20 57 69 6e 36 34 3b 20 3	78 36 34 29 20 41 70	; Win64; x64) Ap
0100	70 6c 65 57 65 62 4b 69 74 2	2f 35 33 37 2e 33 36	pleWebKi t/537.36
0110	20 28 4b 48 54 4d 4c 2c 20 6	5c 69 6b 65 20 47 65	(KHTML, like Ge
0120	63 6b 6f 29 20 43 68 72 6f 6	5d 65 2f 38 36 2e 30	cko) Chr ome/86.0
0130	2e 34 32 34 30 2e 31 39 38 2	20 53 61 66 61 72 69	.4240.19 8 Safari

5/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). What device has this as its Ethernet address?

Answer: The value of the Ethernet source address is 00:26:55:4d:44:ac, this is not the address of my computer or gaia.cs.umass.edu. This is once again the address of the router that has recieved the ok message and forwarded it to my computer.





6/ What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?

Answer: The destination address is 70:66:55:5b:72:7f. This is the address This is the address of my computer.



```
47 07:20:22.305045 HewlettP_4d:44:ac AzureWav_5b:72:7f
                                                                        0x0800
                                                                                   56 IPv4
      0x0800
                                                                                 1466 IPv4
      49 07:20:22.312711
                               HewlettP 4d:44:ac AzureWav 5b:72:7f
                                                                        0x0800
                                                                                 1466 IPv4
> Frame 48: 1466 bytes on wire (11728 bits), 1466 bytes captured (11728 bits) on interface \Device\NPF_{32:
Ethernet II, Src: HewlettP_4d:44:ac (00:26:55:4d:44:ac), Dst: AzureWav_5b:72:7f (70:66:55:5b:72:7f)
  v Destination: AzureWav_5b:72:7f (70:66:55:5b:72:7f)
       Address: AzureWav_5b:72:7f (70:66:55:5b:72:7f)
       .....0. .... = LG bit: Globally unique address (factory default)
       .... = IG bit: Individual address (unicast)
  Source: HewlettP_4d:44:ac (00:26:55:4d:44:ac)
       Address: HewlettP_4d:44:ac (00:26:55:4d:44:ac)
       .... .0. .... = LG bit: Globally unique address (factory default)
       .... ...0 .... = IG bit: Individual address (unicast)
     Type: IPv4 (0x0800)
0000 70 66 55 5b 72 7f 00 26 55 4d 44 ac 08 00 45 20
                                                       pfU[r..& UMD...
0010
      05 ac 9e 08 40 00 2b 06 99 a6 80 77 f5 0c 0a 80
      92 79 00 50 ee b0 23 cc d8 76 9d df a2 f4 50 10
00 ed 0b f2 00 00 48 54 54 50 2f 31 2e 31 20 32
                                                         .....HT TP/1.1 2
      30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 4d 6f 6e
9949
                                                        00 OK..D ate: Mor
      2c 20 32 33 20 4e 6f 76 20 32 30 32 30 20 30 30
0050
                                                         23 Nov 2020 06
      3a 32 30 3a 32 31 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36
                                                         20:21 G MT - Ser
9969
0070
                                                         r: Apac he/2.4.
      20 28 43 65 6e 74 4f 53 29 20 4f 70 65 6e 53 5
           31 2e 30 2e 32 6b 2d 66 69 70 73 20 50 48
                                                        L/1.0.2k -fips P
P/7.4.12 mod_pe
           37 2e 34 2e 31 32 20 6d 6f 64 5f 70 65 72
00a0
aaha
            32 2e 30 2e 31 31
                              20 50 65 72 6c 2f
                                                         /2.0.11 Perl/v
            36 2e 33 0d 0a 4c
                              61 73 74 2d 4d 6f 64
```

7/ Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

Answer: The hex value of this field is 0x0800. This corresponds to the IP protocol.

```
47 07:20:22.305045
                                   HewlettP 4d:44:ac
                                                          AzureWav 5b:72:7f
                                                                                  0x0800
                                                                                               56 IPv4
                                   HewlettP_4d:44:ac AzureWav_5b:72:7f
      48 07:20:22.312376
                                                                                  0x0800
                                                                                            1466 IPv4
      49 07:20:22.312711
                                   HewlettP 4d:44:ac AzureWav 5b:72:7f
                                                                                            1466 IPv4
                                                                                  0x0800
> Frame 48: 1466 bytes on wire (11728 bits), 1466 bytes captured (11728 bits) on interface \Device\NPF_{32:
Ethernet II, Src: HewlettP_4d:44:ac (00:26:55:4d:44:ac), Dst: AzureWav_5b:72:7f (70:66:55:5b:72:7f)
  v Destination: AzureWav_5b:72:7f (70:66:55:5b:72:7f)
        Address: AzureWav_5b:72:7f (70:66:55:5b:72:7f)
        .... .0. .... = LG bit: Globally unique address (factory default)
        .... = IG bit: Individual address (unicast)
  Source: HewlettP 4d:44:ac (00:26:55:4d:44:ac)
        Address: HewlettP_4d:44:ac (00:26:55:4d:44:ac)
        .....0. .... = LG bit: Globally unique address (factory default)
                            = IG bit: Individual address (unicast)
     Type: IPv4 (0x0800)
      70 66 55 5b 72 7f 00 26 55 4d 44 ac 08 00 45 20
      05 ac 9e 08 40 00 2b 06 99 a6 80 77 f5 0c 0a 80
0010
      92 79 00 50 ee b0 23 cc d8 76 9d df a2 f4 50 10
00 ed 0b f2 00 00 48 54  54 50 2f 31 2e 31 20 32
0020
      30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 4d 6f 6e
                                                               00 OK··D ate: Mor
0040
      2c 20 32 33 20 4e 6f 76   20 32 30 32 30 20 30 30
3a 32 30 3a 32 31 20 47   4d 54 0d 0a 53 65 72 76
0050
                                                                23 Nov 2020 00
      65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 3
0070
                                                                er: Apac he/2.4.
      20 28 43 65 6e 74 4f 53  29 20 4f 70 65 6e 53 53
4c 2f 31 2e 30 2e 32 6b  2d 66 69 70 73 20 50 48
0080
                                                                (CentOS ) OpenS
                                                                /1.0.2k -fips PH
0090
      6c 2f 37 2e 34 2e 31 32 20 6d 6f 64 5f 70 65 72
6c 2f 32 2e 30 2e 31 31 20 50 65 72 6c 2f 76 35
2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69
                                                               P/7.4.12 mod per
00a0
                                                               1/2.0.11 Perl/v
00b0
```



8/ 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?

Answer: There are 67 bytes before the "O" (or "O" appears as the 68th byte). These bytes include the ethernet frame, the IP header, the TCP header, and some HTTP preamble text.

```
0000
      70 66 55 5b 72 7f 00 26
                                55 4d 44 ac 08 00 45 20
                                                           pfU[r··& UMD···E
0010
      05 ac 9e 08 40 00 2b 06
                                99 a6 80 77 f5 0c 0a 80
                                                            · · · · · @ · + · · · · · w · · · ·
                                                           ·v-P--#-
0020
      92 79 00 50 ee b0 23 cc
                                d8 76 9d df a2 f4 50 10
      00 ed 0b f2 00 00 48 54
                                54 50 2f
0030
                                         31 2e 31 20 32
                                                            .....HT TP/1.1
0040
      30 30 20 4f 4b 0d 0a 44
                                61 74 65 3a 20 4d 6f 6e
                                                           00 OK⋅⋅D ate: Mor
0050
      2c 20 32 33 20 4e 6f 76
                                20 32 30 32 30 20 30 30
                                                             23 Nov
      3a 32 30 3a 32 31 20 47
                                4d 54 0d 0a 53 65 72 76
0060
                                                            :20:21 G MT - Serv
      65 72 3a 20 41 70 61 63
                                68 65 2f 32 2e 34 2e 36
0070
                                                           er: Apac he/2.4.6
      20 28 43 65 6e 74 4f 53
                                29 20 4f 70 65 6e 53 53
0080
                                                            (CentOS ) OpenSS
0090
      4c 2f 31 2e 30 2e 32 6b
                                2d 66 69 70 73 20 50 48
                                                           L/1.0.2k -fips PH
00a0
      50 2f 37 2e 34 2e 31 32
                                20 6d 6f 64 5f
                                               70 65
                                                           P/7.4.12
                                                                     mod_per
00b0
      6c 2f 32 2e 30 2e 31 31
                                20 50 65
                                         72 6c 2f
                                                   76 35
                                                           1/2.0.11
                                                                     Perl/v
      2e 31 36 2e 33 0d 0a 4c
                                61 73 74 2d 4d 6f 64 69
00c0
                                                            .16.3⋅⋅L ast-Modi
      66 69 65 64 3a 20 53 75
                                6e 2c 20 32 32 20 4e 6f
00d0
                                                           fied: Su n, 22 No
      76 20 32 30 32 30 20 30
                                36 3a 35 39 3a 30 31 20
                                                            v 2020 0 6:59:01
00e0
                                67 3a 20 22 31 31 39 34
00f0
      47 4d 54 0d 0a 45 54 61
                                                            GMT⋅⋅ETa g: "1194
0100
      2d 35 62 34 61 63 39 63
                                63 35 66 63 37 39 22 0d
                                                            -5b4ac9c c5fc79"
0110
      0a 41 63 63 65 70 74 2d
                                52 61 6e 67 65 73 3a 20
                                                            ·Accept- Ranges:
      62 79 74 65 73 0d 0a 43
                                6f 6e 74 65 6e 74 2d 4c
0120
                                                            bytes∙∙C ontent-I
```

9/Write down the contents of your computer's ARP cache. What is the meaning of each column value?

Answer: The columns show the internet address (IPv4) and the physical address (Ethernet). The last column shows whether the IPv4 address is dynamic or static.

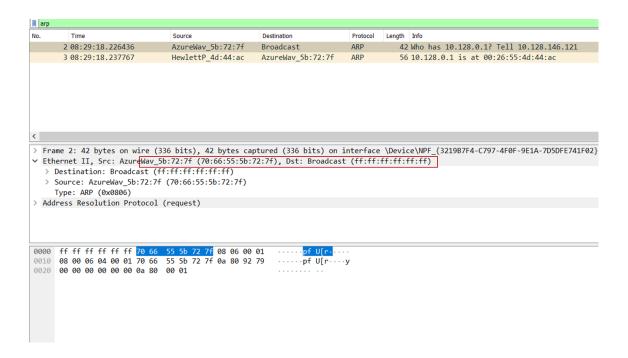


```
C:\Users\Admin>arp -a
Interface: 10.128.146.121 --- 0x5
 Internet Address Physical Address
                                             Type
 10.128.0.1
                       00-26-55-4d-44-ac
                                             dynamic
 10.128.255.255
                       ff-ff-ff-ff-ff
                                             static
 224.0.0.22
                       01-00-5e-00-00-16
                                             static
 224.0.0.251
224.0.0.252
                       01-00-5e-00-00-fb
                                             static
                       01-00-5e-00-00-fc
                                             static
 239.255.255.250
                       01-00-5e-7f-ff-fa
                                             static
 255.255.255.255
                       ff-ff-ff-ff-ff
                                             static
 iterface: 192.1.
Internet Address
Interface: 192.168.56.1 --- 0x8
                       Physical Address
                                             Type
                       ff-ff-ff-ff-ff
                                             static
 224.0.0.22
                      01-00-5e-00-00-16
                                             static
                    01-00-5e-00-00-16
01-00-5e-00-00-fb
 224.0.0.251
224.0.0.252
                                             static
                       01-00-5e-00-00-fc
                                             static
 239.255.255.250
                       01-00-5e-7f-ff-fa
                                             static
Interface: 169.254.168.189 --- 0xe
 Internet Address
                       Physical Address
                                             Type
 169.254.255.255
                       ff-ff-ff-ff-ff
                                             static
 224.0.0.22
                       01-00-5e-00-00-16
                                             static
 224.0.0.251
                      01-00-5e-00-00-fb
                                             static
                       01-00-5e-00-00-fc
 224.0.0.252
                                             static
                       01-00-5e-7f-ff-fa
 239.255.255.250
                                             static
                       ff-ff-ff-ff-ff
 255.255.255.255
                                             static
```

10/ What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?

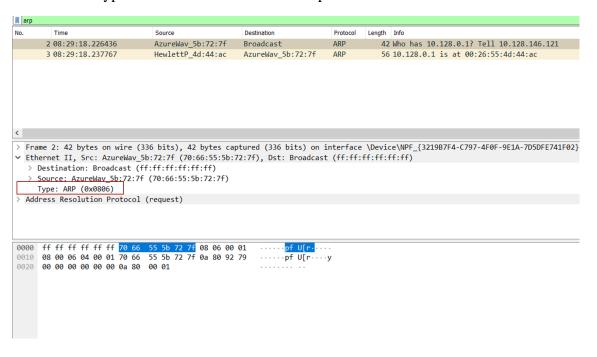
Answer: The source address is (70:66:55:5b:72:7f), the destination address is (ff:ff:ff:ff:ff). The source address is the Ethernet address of my computer and the destination address is broadcast.





11/ Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?

Answer: The type value is 0x0806 which corresponds to ARP.





12/

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

Answer: The opcode field starts 20 bytes from the beginning of the frame.

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?

Answer: The opcode has a hex value of 0x0001, which is for request.

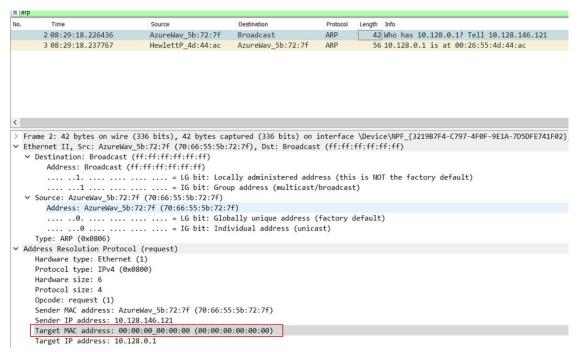
c/Does the ARP message contain the IP address of the sender?

Answer: The ARP message contains the IP address 10.128.0.1

	No.	Time	Source	Destination	Protocol	Length Info
3 08:29:18.237767 HewlettP_4d:44:ac AzureWav_5b:72:7f ARP 56 10.128.0.1 is at 00:26:		2 08:29:18.226436	AzureWav_5b:72:7f	Broadcast	ARP	42 Who has 10.128.0.1? Tell 10.128.146.1
		3 08:29:18.237767	HewlettP 4d:44:ac	AzureWav 5b:72:7f	ARP	56 10.128.0.1 is at 00:26:55:4d:44:ac

d/Where in the ARP request does the "question" appear – the Ethernet address of the machine whose corresponding IP address is being queried?

Answer: The "question" is in the field Target MAC address, which is set to :00:00:00:00:00





13/

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

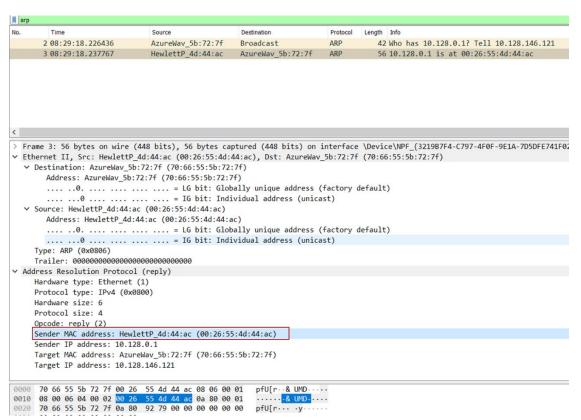
Answer: The opcode field begins 20 bytes from the beginning of the frame.

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?

Answer: The hex value for opcode field withing the ARP-payload of the request is 0x0002, for reply message.

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?

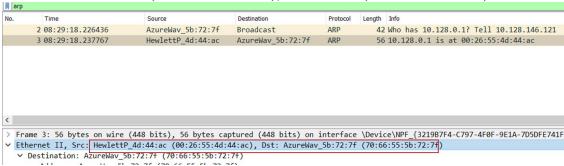
Answer: The answer to the earlier ARP request appears in the "Sender MAC address" field, which contains the Ethernet address 00:26:55:4d:dd:ac for the sender with IP address 10.128.0.1





14/ What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?

Answer: The source is (00:26:55:4d:44:ac), Destination (70:66:55:5b:72:7f)



15/

Answer: There is no reply in this trace, because we are not at the machine that sent the request. The ARP request is broadcast, but the ARP reply is sent back directly to the sender's Ethernet address.