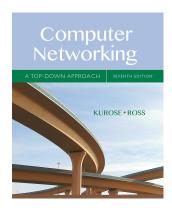
## Wireshark Lab: Ethernet & ARP **SOLUTION**

Supplement to *Computer Networking: A Top-Down Approach*, 7<sup>th</sup> ed., J.F. Kurose and K.W. Ross

© 2005-2016, J.F Kurose and K.W. Ross, All Rights Reserved



The solutions below are based on the trace file *ethernet--ethereal-trace-1* in the zip file <u>http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip</u>.

Shown below is the screen shot expanding the view of the Ethernet frame carrying the HTTP GET:

Ele Edit ýsev Go Casture Analyze Statistics belo         Image: Statistics Delo	_			eshark																<u>_ 0 ×</u>
Elker:           Expression Clar Apply            No         Time         Source         Destination         Protocal         Infe           1         0.000000         Net gear_61:8e:6d         LinksysG_45:90:a8         0x0800 IP           2         0.050606         LinksysG_45:90:a8         Net gear_61:8e:6d         0x0800 IP           3         0.050729         Net gear_61:8e:6d         0x0800 IP         0x0800 IP           4         0.055906         Net gear_61:8e:6d         0x0800 IP         0x0800 IP           5         0.128700         LinksysG_45:90:a8         Net gear_61:8e:6d         0x0800 IP           7         0.150302         LinksysG_45:90:a8         Net gear_61:8e:6d         0x0800 IP           9         0.213639         LinksysG_45:90:a8         Net gear_61:8e:6d         0x0800 IP           10         0.213749         LinksysG_45:90:a8         Net gear_61:8e:6d         0x0800 IP           12         0.231749         LinksysG_45:90:a8         Net gear_61:8e:6d         0x0800 IP           13         0.23145         Net gear_61:8e:6d         LinksysG_45:90:a8         0x0800 IP           14         0.231749         LinksysG_45:90:a8         Net gear_61:8e:6d         InksysG_45:90:a8		<u>E</u> dit	⊻iew		apture	<u>A</u> nalyze	Statistics	Help						_	_					
No.         Time         Source         Destination         Protocol         Info           1         0.000000         Netgear_61:8e:6d         LinksysG_45:90:a8         0x0800 IP           2         0.050606         LinksysG_45:90:a8         Netgear_61:8e:6d         0x0800 IP           4         0.055906         Netgear_61:8e:6d         LinksysG_45:90:a8         0x0800 IP           5         0.128700         LinksysG_45:90:a8         Netgear_61:8e:6d         0x0800 IP           5         0.128700         LinksysG_45:90:a8         Netgear_61:8e:6d         0x0800 IP           7         0.150302         LinksysG_45:90:a8         Netgear_61:8e:6d         0x0800 IP           9         0.213639         LinksysG_45:90:a8         Netgear_61:8e:6d         0x0800 IP           10         0.215724         LinksysG_45:90:a8         Netgear_61:8e:6d         0x0800 IP           12         0.231749         LinksysG_45:90:a8         Netgear_61:8e:6d         0x0800 IP           12         0.231749         LinksysG_45:90:a8         Netgear_61:8e:6d         0x0800 IP           13         0.232145         Netgear_61:8e:6d         LinksysG_45:90:a8         0x0800 IP           14         0.320470         Netgear_61:8e:6d         LinksysG_45:90:a		÷.	9				×	e <sup>g</sup>	8	এ	4	\$	¢)	Ŧ	⊻		3	÷	Θ	О,
<pre>1 0.000000 Netgear_61:8e:6d LinksysG_45:90:a8 0x0800 IP 2 0.050006 LinksysG_45:90:a8 Netgear_61:8e:6d 0x0800 IP 4 0.055906 Netgear_61:8e:6d LinksysG_45:90:a8 0x0800 IP 5 0.128700 LinksysG_45:90:a8 Netgear_61:8e:6d 0x0800 IP 7 0.150302 LinksysG_45:90:a8 Netgear_61:8e:6d 0x0800 IP 9 0.213639 LinksysG_45:90:a8 Netgear_61:8e:6d 0x0800 IP 10 0.215724 LinksysG_45:90:a8 Netgear_61:8e:6d 0x0800 IP 11 0.215724 LinksysG_45:90:a8 Netgear_61:8e:6d 0x0800 IP 12 0.231749 LinksysG_45:90:a8 Netgear_61:8e:6d 0x0800 IP 13 0.32245 Netgear_61:8e:6d LinksysG_45:90:a8 0x0800 IP 13 0.32245 Netgear_61:8e:6d LinksysG_45:90:a8 Netgear_61:8e:6d 0x0800 IP 14 0.320470 Netgear_61:8e:6d LinksysG_45:90:a8 0x0800 IP 13 0.332145 Netgear_61:8e:6d LinksysG_45:90:a8 0x0800 IP 14 0.320470 Netgear_61:8e:6d LinksysG_45:90:a8 0x0800 IP 14 0.320470 Netgear_61:8e:6d LinksysG_45:90:a8 0x0800 IP 14 0.320470 Netgear_61:8e:6d LinksysG_45:90:a8 0x0800 IP 15 0.403428 LinksysG_45:90:a8 Netgear_61:8e:6d 0x0800 IP 14 0.320470 Netgear_61:8e:6d LinksysG_45:90:a8 0x0800 IP 15 0.403428 LinksysG_45:90:a8 Netgear_61:8e:6d 0x0800 IP 14 0.320470 Netgear_61:8e:6d LinksysG_45:90:a8 0x0800 IP 15 0.403428 LinksysG_45:90:a8 Netgear_61:8e:6d 0x0800 IP 15 0.403428 LinksysG_45:90:a8 Netgear_61:8e:6d 0x0800 IP 16 9.393131 LinksysG_45:90:a8 0x0800 IP 17 0.579522 Netgear_61:8e:6d LinksysG_45:90:a8 0x0800 IP 19 9.392137 Netgear_61:8e:6d LinksysG_45:90:a8 0x0800 IP 19 0.389131 LinksysG_45:90:a8 (00:0c:41:45:90:a8) 0</pre>	<u>F</u> ilter:									·	Ē	pression	⊆	ear <u>A</u> p	oply					
2 0.050606 LinkSysG_45:90:a8 Netgeàr_61:8e:60 0x0800 IP 4 0.055906 Netgear_61:8e:60 LinkSysG_45:90:a8 0x0800 IP 5 0.128700 LinksysG_45:90:a8 Netgear_61:8e:60 0x0800 IP 7 0.150302 LinksysG_45:90:a8 Netgear_61:8e:60 0x0800 IP 9 0.213639 LinksysG_45:90:a8 Netgear_61:8e:60 0x0800 IP 10 0.215724 LinksysG_45:90:a8 Netgear_61:8e:60 0x0800 IP 11 0.215724 LinksysG_45:90:a8 Netgear_61:8e:60 0x0800 IP 12 0.231749 LinksysG_45:90:a8 Netgear_61:8e:60 0x0800 IP 13 0.32145 Netgear_61:8e:60 LinksysG_45:90:a8 0x0800 IP 15 0.403428 LinksysG_45:90:a8 Netgear_61:8e:60 0x0800 IP 16 0.423932 Netgear_61:8e:60 LinksysG_45:90:a8 0x0800 IP 18 3.833584 Netgear_61:8e:60 LinksysG_45:90:a8 0x0800 IP 18 3.83358 Netgear_61:8e:60 LinksysG_45:90:a8 0x0800 IP 19 9.392197 Netgear_61:8e:60 LinksysG_45:90:a8 0x0800 IP 19 9.392197 Netgear_61:8e:60 LinksysG_45:90:a8 0x0800 IP 19 9.392197 Netgear_61:8e:60 LinksysG_45:90:a8 0x0800 IP 19 0.389131 LinksysG_45:90:a8 Netgear_61:8e:60 0x0800 IP 19 0.389258 Netgear_61:8e:60 LinksysG_45:90:a8 0x0800 IP 10 0.389131 LinksysG_45:90:a8 (00:00:141:45:90:a8 0x0800 IP 10 0.389131 LinksysG_45:90:a8 (00:00:141:45:90:a8) 0	No													)						<u> </u>
<pre>5 0.128700 LinksysG_45:90:a8 Netgear_G1:8e:6d 0x0800 IP 6 0.134167 LinksysG_45:90:a8 Netgear_G1:8e:6d 0x0800 IP 7 0.150302 LinksysG_45:90:a8 Netgear_G1:8e:6d 0x0800 IP 8 0.150487 Netgear_G1:8e:6d LinksysG_45:90:a8 Netgear_G1:8e:6d 0x0800 IP 9 0.213639 LinksysG_45:90:a8 Netgear_G1:8e:6d 0x0800 IP 11 0.215724 LinksysG_45:90:a8 Netgear_G1:8e:6d 0x0800 IP 11 0.21574 LinksysG_45:90:a8 Netgear_G1:8e:6d 0x0800 IP 13 0.232145 Netgear_G1:8e:6d LinksysG_45:90:a8 0x0800 IP 14 0.320470 Netgear_G1:8e:6d LinksysG_45:90:a8 0x0800 IP 15 0.403428 LinksysG_45:90:a8 Netgear_G1:8e:6d 0x0800 IP 16 0.423932 Netgear_G1:8e:6d LinksysG_45:90:a8 0x0800 IP 17 0.579552 Netgear_G1:8e:6d LinksysG_45:90:a8 0x0800 IP 18 3.383584 Netgear_G1:8e:6d LinksysG_45:90:a8 0x0800 IP 19 9.392197 Netgear_G1:8e:6d LinksysG_45:90:a8 0x0800 IP 19 9.392197 Netgear_G1:8e:6d LinksysG_45:90:a8 0x0800 IP 12 0.1389131 LinksysG_45:90:a8 Netgear_G1:8e:6d 0x0800 IP 19 9.392197 Netgear_G1:8e:6d LinksysG_45:90:a8 0x0800 IP 20 10.389131 LinksysG_45:90:a8 Netgear_G1:8e:6d 0x0800 IP 21 10.389258 Netgear_G1:8e:6d LinksysG_45:90:a8 0x0800 IP 21 10.389258 Netgear_G1:8e:6d (00:09:5b:61:8e:6d), Dst: LinksysG_45:90:a8 (00:0c:41:45:90:a8) Address: LinksysG_45:90:a8 (00:0c:41:45:90:a8) Address: LinksysG_45:90:a8 (00:0c:41:45:90:a8) Address: LinksysG_45:90:a8 (00:0c:41:45:90:a8) 0</pre>		20	). 050 ). 050	606 729	Lin Net	KsysG_ gear_6	45:90:a8 1:8e:6d	Net Lin	geår_6: <sysg_4< td=""><td>1:8e:6 45:90:</td><td>id a8</td><td>0×080 0×080</td><td>0 IP 0 IP</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></sysg_4<>	1:8e:6 45:90:	id a8	0×080 0×080	0 IP 0 IP							
<pre>■ Ethernet II, Src: Netgear_61:8e:6d (00:09:5b:61:8e:6d), Dst: L1nksysG_45:90:a8 (00:0c:41:45:90:a8) ■ Destination: LinksysG_45:90:a8 (00:0c:41:45:90:a8) Address: LinksysG_45:90:a8 (00:0c:41:45:90:a8) 0 = IG bit: Individual address (unicast) 0</pre>		5 0 7 0 9 0 10 0 11 0 12 0 13 0 14 0 15 0 17 0 19 9 10 1 19 9 10 1 19 9 10 1 10 0 10	).128 ).134 ).150 ).213 ).215 ).215 ).231 ).232 ).232 ).232 ).403 ).423 ).423 ).423 ).320 ).423 ).320 ).320 ).320 ).383 ).392	700 167 302 487 639 724 947 749 145 470 428 932 522 584 197 9131	Lin Lin Lin Lin Lin Net Net Net Net	ksysG_ ksysG_ ksysG_ ksysG_ ksysG_ ksysG_ ksysG_ gear_6 ksysG_ gear_6 gear_6 ksysG_ gear_6 ksysG_ ksysG_	45:90:a8 45:90:a8 45:90:a8 45:90:a8 45:90:a8 1:8e:6d 1:8e:6d 1:8e:6d 1:8e:6d 1:8e:6d 1:8e:6d 1:8e:6d 1:8e:6d 1:8e:6d 1:8e:6d	Net(           Linl           Linl           Linl           Linl           Net(           Net(           Net(           Net(	gear_6 gear_6 gear_6 gear_6 gear_6 (sysG_4 (sysG_4 (sysG_4 (sysG_4 (sysG_4 (sysG_4 (sysG_4 (sysG_4 (sysG_4) (sy	L:8e:6 L:8e:6 L:8e:6 L:8e:6 L:8e:6 L:8e:6 L:8e:6 L:8e:6 45:90: L:8e:6 45:90: 45:90: 45:90: 45:90: 45:90: L:8e:6	id id id id a8 id a8 id a8 id a8 a8 a8 id a8 a8 a8 id a8 a8 a8 id a8 a8 a8 a8 a8 a8 a8 a8 a8 a8 a8 a8 a8	0x080 0x080 0x080 0x080 0x080 0x080 0x080 0x080 0x080 0x080 0x080 0x080 0x080 0x080 0x080 0x080 0x080	0 IP 0 IP 0 IP 0 IP 0 IP 0 IP 0 IP 0 IP							
<pre>■ Ethernet II, Src: Netgear_61:8e:6d (00:09:5b:61:8e:6d), Dst: L1nksysG_45:90:a8 (00:0c:41:45:90:a8) ■ Destination: LinksysG_45:90:a8 (00:0c:41:45:90:a8) Address: LinksysG_45:90:a8 (00:0c:41:45:90:a8) 0 = IG bit: Individual address (unicast) 0</pre>	<		4 (5	05 h.			For h			-12										
Address: LinksysG_45:90:a8 (00:0c:41:45:90:a8) 0 = IG bit: Individual address (unicast) 0 = LG bit: Globally unique address (factory default) □ Source: Netgear_61:8e:6d (00:09:5b:61:8e:6d) Address: Netgear_61:8e:6d (00:09:5b:61:8e:6d) 0 = IG bit: Individual address (unicast) 0											:6d)	, DST:	: ∟in	ksyso	5 <u>4</u> 5:	90:a8	(00:0	0⊂:41:	45:90	):a8)
	<ul> <li>□ Destination: LinksysG_45:90:a8 (00:0c:41:45:90:a8)         Address: LinksysG_45:90:a8 (00:0c:41:45:90:a8)        0</li></ul>																			
0000       00       0C       41       45       90       a8       000       95       b6       18       b6       08       001       45       00	0010 0020 0030 0040 0050 0060 0070	01 f5 68 74 33 0a	ec 8 0c 0 ff 3 61 7 68 6 2e 6 48 6	37 e9 07 f6 3a 9c 72 6b 55 72 58 74 5f 73	40 0( 00 5) 00 0( 2d 6) 65 6: 6d 6)	0 80 00 0 7a 74 0 47 49 1 61 62 1 6C 20 1 20 48	5 38 65 4 c4 58 5 54 20 2 73 2f d 6c 61 3 54 54	c0 a8 7d a6 2f 77 48 54 62 20 50 2f	3 02 91 5 27 90 7 69 72 4 54 50 9 66 69 51 26	80 7 50 1 65 7 2 65 7 2 65 6 2 6 6 6 31 0	7 8 3 5 5 d 5	@ hark- there 3.htm .Host	8 PZt . .GE 1 lab 9 al- 1 l н 1 : g а	Be X}.' /wi /HTT ab-f TTP/1 aia.c	w .P. res P-e ile .1.					

- *1.* What is the 48-bit Ethernet address of your computer? *The Ethernet address of my computer is* 00:09:5b:61:8e:6d
- 2. What is the 48-bit destination address in the Ethernet frame? 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.] *The destination address 00:0c:41:45:90:a8 is not the Ethernet address of gaia.cs.umass.edu. It is the address of my Linksys router, which is the link used to get off the subnet.*
- 3. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to? *The hex value for the 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 ths Ethernet frame will*

*be passed – is IP.* 

4. How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame? *The ASCII "G" appears 52 bytes from the start of the Ethernet frame. There are 14 B Ethernet frame, and then 20 bytes of IP header followed by 20 bytes of TCP header before the HTTP data is encountered.* 

Here is a screenshot of the Ethernet frame containing the HTTP OK response:

<mark>7 (</mark> Un	titleo	l) - Wi	reshark																		<u>_     ×</u>
Eile	Edit	⊻iew	<u>G</u> o <u>C</u>	apture	<u>A</u> nalyz	ze <u>S</u> ta	atistics	Help											 		
	<b>i</b>	e.		<b>M</b>			X	¢,			٩	\$	⇔	¢	Ŧ	⊉			P.	Θ,	Q,
<u>F</u> ilter:												▼ <u>E</u>	xpression	⊆	<u>l</u> ear ,	Apply					
No. +	1	lime -		Sour	rce			Des	tination				Protocol	Inf	fo						~
	2 ( 3 ( 4 ( 5 ( 6 (	).000 ).050 ).050 ).055 ).128 ).134	)606 )729 ;906 ;700 167	Lir Net Net Lir	:gear_ iksys6 :gear_ iksys6 iksys6	5_45: _61:8 _61:8 5_45: 5_45:	90:a8 e:6d e:6d 90:a8 90:a8	8 Net Lir Lir 8 Net 8 Net	nksys Igear Iksys Iksys Igear Igear	_61 G_4 G_4 _61 <mark>_61</mark>	:8e:0 5:90 5:90 :8e:0 :8e:0	6d :a8 :a8 6d 6d	0×080 0×080 0×080	0 IF 0 IF 0 IF 0 IF 0 IF							
	8 ( 9 ( 10 ( 11 ( 12 ( 13 ( 14 ( 15 ( 16 (	).150 ).213 ).215 ).215 ).231 ).231 ).232 ).232 ).320 ).320 ).403 ).403	9487 639 724 947 .749 145 9470 428 932	Net Lir Net Lir Net Lir Net	iksyso :gear_ iksyso :gear_ :gear_ :gear_ :gear_	_61:8 5_45: 5_45: 61:8 5_45: 61:8 61:8 5_45: 5_45: 61:8	e:6d 90:a8 90:a8 e:6d 90:a8 e:6d e:6d 90:a8 e:6d	Lir Net Lir Net Lir Lir Lir Lir	:gear, :gear, :gear, :gear, :ksys; :gear, :gear,	G_4 _61 _61 _61 _61 G_4 G_4 G_4 G_4	5:90 :8e:0 :8e:0 5:90 :8e:0 5:90 :8e:0 5:90	:a8 6d 6d :a8 6d :a8 6d :a8	0×080 0×080 0×080 0×080 0×080 0×080 0×080 0×080 0×080 0×080	0 IF 0 IF 0 IF 0 IF 0 IF 0 IF 0 IF							
	18 3 19 9 20 1		584	Net Net Lir	:gear_ :gear_ :gear_ :gear_ :gear_	_61:8 _61:8 5_45:	e:6d e:6d 90:a8	Lir Lir Net	:gear.	G_4 G_4 _61	5:90 5:90 :8e:0	:a8 :a8 6d		0 IF 0 IF 0 IF	) ) )						<u>۲</u>
	-		ols in T Se						).Oc.	A1 •	45.0	0.59	) Det	• NL	otao	on 61	.90.6	d Coc	 ih•e	1.04	• 6d)
<pre> ■ Ethernet II, Src: LinksysG_45:90:a8 (00:0c:41:45:90:a8), Dst: Netgear_61:8e:6d (00:09:5b:61:8e:6d)  Address: Netgear_61:8e:6d (00:09:5b:61:8e:6d) Address: Netgear_61:8e:6d (00:09:5b:61:8e:6d)0 = IG bit: Individual address (unicast)0</pre>																					
0000 0010 0020 0030 0040 0050 0060 0070 Etherne	01 02 19 30 2c 3a 65	5d 91 20 30 20 35 72	33 31 00 50 ae d0 20 4f 32 30 33 3a 3a 20	40 0 07 f 00 0 4b 0 20 4 34 3	0 48 d 0a a 75 5 20	06 a6 54 44 6e 47	41 45 da 4c 27 90 54 50 61 74 20 32 4d 54 68 65	80 7 7a 7 2f 3 65 3 30 3 0d 0	7 f5 4 c6 1 2e a 20 0 37 a 53	0c 1c 31 57 20 65	31 3 72 7	48 18 32 54 37 76 35	[а.1 .]31@ Р.  00 ок , 20 .:53:4 er: А 21 D: 21	.3. .}. .HT D Jun 5 G pac	.L.W '.zt TP/1 ate: 200 MT he/2	P. .12 Wed 717 Serv .0.5					

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? *The source address* 00:0c:41:45:90:a8 is neither the Ethernet address of gaia.cs.umass.edu nor the address of my computer. It is the address of my Linksys router, which is the link used to get onto my subnet.

- 6. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer? *The destination address 00:09:5b:61:8e:6d is the address of my computer*.
- 7. 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? *The hex value for the Frame type field is 0x0800. This value corresponds to the IP protocol (see also answer to 3. above).*
- 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? *The ASCII* "O" appears 52 bytes from the start of the Ethernet frame. Again, there are 14 bytes of Ethernet frame, and then 20 bytes of IP header followed by 20 bytes of TCP header before the HTTP data is encountered.



9. Write down the contents of your computer's ARP cache. What is the meaning of each column value? *The Internet Address column contains the IP address, the Physical Address column contains the MAC address, and the type indicates the protocol type.* 

*Here is a screenshot showing the ARP request message:* 

📶 ethernet-ethereal-trace-1 - Wireshark									
Eile Edit View Go Capture Analyze Statistics Help									
	Q ⇔ ∞ T ⊻ ≡ g Q Q 0								
Eilter:	▼ Expression <u>C</u> lear <u>Apply</u>								
No Time Source Destination	Protocol Info								
1 0.000000 AmbitMic_a9:3d:68 Broadcast	ARP who has 192.168.1.1? Tell 192.168.1.105								
2 0.001018 LinksysG_da:af:73 AmbitMic_a 3 0.001028 AmbitMic_a9:3d:68 LinksysG_d	a9:3d:68 ARP 192.168.1.1 is at 00:06:25:da:af:73								
4 2.962850 AmbitMic_a9:3d:68 LinksysG_d									
5 8.971488 AmbitMic_a9:3d:68 LinksysG_d	da:af:73 0x0800 IP								
6 13.542974 Telebit_73:8d:ce Broadcast 7 17.444423 AmbitMic_a9:3d:68 LinksysG_d									
8 17.465902 LinksysG_da:af:73 AmbitMic_a									
➡ Frame 1 (42 bytes on wire, 42 bytes captured)									
Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:	:a9:3d:68), Dst: Broadcast (ff:ff:ff:ff:ff)								
Destination: Broadcast (ff:ff:ff:ff:ff:ff)									
Address: Broadcast (ff:ff:ff:ff:ff:ff)									
1 IG bit: Group address (multicast/broadcast)									
	ocally administered address (this is NOT the factory default]								
□ Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)									
Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)									
= IG bit: Ir									
	lobally unique address (factory default)								
Type: ARP (0x0806) Address Resolution Protocol (request)									
Hardware type: Ethernet (0x0001)									
Protocol type: IP (0x0800)									
Hardware size: 6									
Protocol size: 4									
opcode: request (0x0001)									
sender MAC address: Amb1tM1<_a9:3d:68 (00:d0:59:a9:3d:68)									
Sender IP address: 192.168.1.105 (192.168.1.105)									
Target MAC address: 00:00:00_00:00:00 (00:00	0:00:00:00)								
Target IP address: 192.168.1.1 (192.168.1.1)	)								
4									
0000 ff ff ff ff ff ff 00 d0 59 a9 3d 68 08 06									
0010 08 00 06 04 00 01 00 d0 59 a9 3d 68 c0 a8	01 69 Yhi								
0020 00 00 00 00 00 00 c0 a8 01 01									
Ethernet (eth), 14 bytes	P: 17D: 17 M: 0								

- 11. 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? The hex value for the Ethernet Frame type field is 0x0806, for ARP.
- 12. Download the ARP specification from ftp://ftp.rfc-editor.org/innotes/std/std37.txt. A readable, detailed discussion of ARP is also at http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html.
  - a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin? *The ARP opcode field begins 20 bytes from the very beginning of the Ethernet 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? *The hex value for*

opcode field withing the ARP-payload of the request is 0x0001, for request.

- c) Does the ARP message contain the IP address of the sender? Yes, the ARP message containing the IP address 192.168.1.105 for the sender.
- *d)* Where in the ARP request does the "question" appear the Ethernet address of the machine whose corresponding IP address is being queried? *The field "Target MAC address" is set to 00:00:00:00:00:00 to question the machine whose corresponding IP address (192.168.1.1) is being queried.*

Here is the screenshot for the ARP	reply message:
------------------------------------	----------------

- 13. Now find the ARP reply that was sent in response to the ARP request.
  - *a)* How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin? *The ARP opcode field begins 20 bytes from the very beginning of the Ethernet 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? *The hex value for*

opcode field withing the ARP-payload of the request is 0x0002, for reply.

- 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 to the earlier ARP* request appears in the "Sender MAC address" field, which contains the Ethernet address 00:06:25:da:af:73 for the sender with IP address 192.168.1.1.
- 14. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message? *The hex value for the source address is 00:06:25:da:af:73 and for the destination is 00:d0:59:a9:3d:68*.
- 15. 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 indicated 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? 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.