In this lab we will use Wireshark to observe the DHCP process.

First, start Wireshark and select your active Network Interface

The Wireshark Network Analyzer	– 🗆 X
<u>File E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics Telephony <u>W</u> ireless <u>T</u> ools <u>H</u> elp	
◢ ■ ∅ ◉   _ 🗅 🖄 🖻   9 ⇔ ⇔ 🕾 🗿 🖢 🧮 🗮 🔍 9 € 9 ඞ	
Apply a display filter <ctrl-></ctrl->	Expression +
Welcome to Wireshark	
Open	
D:\Box Sync\OneDrive\cct\qqi\semester 1\datacomms\2016\assessments\groupa\GroupaCA1 v2.pcapng (244 KB)	^
D:\Box Sync\OneDrive\cct\qqi\semester 1\datacomms\2016\assessments\groupbCA1.pcapng (89 KB)	
D:\Box Sync\OneDrive\cct\qqi\semester 1\datacomms\2016\assessments\groupa\groupaCA1.pcapng (238 KB)	
D:\Box Sync\OneDrive\cct\qqi\semester 1\datacomms\2016\assessments\groupaCA1.pcapng (not found)	
C:\Users\lat1\Documents\groupbCA1.pcapng (not found)	
C:\Users\lat1\Documents\groupaCA1.pcapng (not found)	
C:\Users\latI\Documents\sample capture.pcapng (not found)	
C:\Users\tat \Ubecuments\sample capture.pcapng (not found)	~
	·
using this inter: A capture inter	
Wireless Network Connection^^	^
Addresses: fe80::c8b5:ae58:d730:33aa, 172:16:203:19 No capture filter Local Area Connection* 4 (*) USBRenn1	v
Learn	
User's Guide · Wiki · Questions and Answers · Mailing Lists	
You are running Wireshark 2.2.2 (v2.2.2-0-g775fb08). You receive automatic updates.	
Ready to load or capture No Packets	Profile: Default

In the next Window you should see traffic for that interface, including any broadcasts that your machine is receiving.

Capturing	from Wireless	Network Co	onnection							_		×
<u>File</u> Edit	View <u>G</u> o <u>C</u>	apture <u>A</u> r N PA O	nalyze <u>S</u> tatistics	。 Telephony	Wireless	Lools I	<u>H</u> elp					
			~~¥1		446	*#					Everession	1.4
Appiy a disp	lay filter <ctr< td=""><td>1-/&gt;</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>Expression</td><td>. T</td></ctr<>	1-/>									Expression	. T
No. Tin	ne	Source		Destination		Protocol	Length	Info				^
10.	000000	172.16.2	204.158	172.16.207.	255	NBNS	92	Name query NB MACBOOKAIR-6A8C	<00>			
2 0.	000334	fe80::42	2b8:37ff:fef	ff02::fb		MDNS	146	Standard query 0x0000 ANY And	roid-99.local,	"QM" que	estion AN	Y
30.	000524	te80::98	3†b:2b49:981…	tt02::tb		MDNS	74	Standard query response 0x000	90			
40.	000739	172.16.2	205.190	172.16.207.	255	UDP	50	2008->2008 Len=8				
50.	102045	1/2.16.4 f=004	205.190	1/2.16.20/.	255	MDNE	50	2007->2007 Len=8	ten local "		tion	
50.	102945	f-9009	200:3711:101	ff02fb		MDNE	94	Standard query 0x0000 PTR _TD	a	un ques	LION	
70.	103124	HonHaiPr	8h:0h:c1	Broadcast		APP	60	who has 172 16 200 12 Tell 17	72 16 204 168			
90	103670	Xirrus 6	_00.00.CI	Broadcast			60	Who has 172.10.200.1; Tell 17	72.10.204.100			
10.0.	103886	172.16.2	205.190	172.16.207.	255	UDP	50	2008->2008   en=8	2.10.204.201			
11 0.	104120	172.16.2	205.190	172.16.207.	255	UDP	50	2007→2007 Len=8				
12 0.	205212	Apple e	e2:ec	Broadcast		ARP	60	Gratuitous ARP for 172.16.204	.59 (Request)			
13 0.	205541	fe80::40	0c:379d:70ef	ff02::fb		MDNS	176	Standard guery 0x0000 PTR 00	000000-1801-57	98-567a-	f0bbb8224	2
14 0.	205697	172.16.2	202.144	172.16.207.	255	NBNS	92	Name guery NB WPAD<00>				
15 0.	206040	172.16.2	205.190	172.16.207.	255	UDP	50	2008→2008 Len=8				~
> Frame 1:	92 bytes o	n wire (7	'36 bits), 92	bytes captu	red (736	bits) or	n interf	ice 0				
> Ethernet	II, Src: H	onHaiPr_e	7:dd:6f (c0:1	.8:85:e7:dd:	6f), Dst:	Broadca	st (ff:	ff:ff:ff:ff:ff)				
> Internet	Protocol V	ersion 4,	Src: 172.16.	204.158, Ds	t: 172.16	.207.255	5					
> User Dat	agram Proto	col, Src	Port: 137, Ds	t Port: 137								
> NetBIOS	Name Servic	e										
aaaa ff f	* ** ** **	ff c0 18	85 e7 dd 6f	08 00 15 00			E					
0010 00 4	e 25 c4 00 0	00 80 11	20 1c ac 10	cc 9e ac 10	.N%							
0020 cf f	f 00 89 00	89 00 3a	b2 f5 ba 33	01 10 00 01		.:3						
0030 00 0	0 00 00 00 0	00 20 45	4e 45 42 45	44 45 43 45		E NEBED	DECE					
0040 50 4	5 50 45 4c 4	45 42 45	4a 46 43 43	4e 44 47 45	PEPELE	BE JFCC	IDGE					
0050 42 4	4 49 45 44 4	41 41 00	00 20 00 01		BDIEDA	A						
	1											
💛 🗷 Wire	eless Network Co	onnection: <l< td=""><td>ive capture in prog</td><td>ress&gt;</td><td></td><td></td><td></td><td>   Packets: 360 · Displa</td><td>yed: 360 (100.0%)</td><td></td><td>Profile: Def</td><td>ault <sub>i</sub></td></l<>	ive capture in prog	ress>				Packets: 360 · Displa	yed: 360 (100.0%)		Profile: Def	ault <sub>i</sub>

The traffic that we want to observe is small and we do not need to see all other traffic so we can apply a filter in wireshark.

In the filter box type *bootp* and press enter, this should remove a lot of unnecessary traffic from our view.

6	*Wir	reless	Network (	Conne	ction																									_		×	
<u>F</u> ile	Ec	dit	<u>V</u> iew <u>G</u> o	) <u>C</u> a	pture	<u>A</u> na	alyze	<u>S</u> tat	tistic	s T	Felep	hon <u>y</u>	W	ireless	s <u>T</u> e	ools	<u>H</u> el	р															
Ĺ		۵			G	9	<	• 🖻	1	J.			Ð	Θ	€																		
	pootp																												X	-) E	xpression.	.   +	
No.		Tir	me		Source	2				Des	tinati	on			P	rotoco	ol L	.ength	Info														٦
Г	872	22 87	7.246897		0.0.0	0.0				255	5.25	5.255	5.25	5	D	HCP		350	DHC	P Di	iscov	er	- Tr	ansa	ctior	n ID	0x8b	aa4f9o	с				
	876	54 88	8.371970	_	0.0.0	0.0				255	5.25	5.255	5.25	5	D	HCP		362	DHC	P Re	eques	t	- Tr	ansa	ctior	n ID	0x8b	aa4f9o	c				
	1082	27 12	29.64044	5	0.0.0	0.0				255	5.25	5.255	5.25	5	D	HCP		342	DHC	PR	eques	t	- Tr	ansa	ctior	n ID	0xa0	07e065	5				-
>	Fram	ie 87	22: 350	byte	s on	wire	e (28	00 b	its	), 3	50 b	ytes	са	ptur	ed (	2800	bit	s) or	n int	terf	ace	0											
2	Ethe	rnet	II, Sro	c: Mu	rataN	1a_68	3:bd:	11 (	f0::	27:6	5:68	3:bd:	11)	, Ds	t: B	roado	cast	(ff	ff:	ff:f	f:ff	:ff)	)										
3	Inte	rnet	: Protoco	ol Ve	rsion	14, Sec D	Src:	0.0 68	0.0.0	0, C + Pc	st:	255.	255	.255	. 255																		
5	Boot	stra	agram Fi op Protoc	col (	Disco	over)	)	00,	05			07																					
V																																	Т
000	00	ff f	f ff ff	ff f	f fØ	27	65 6	8 bd	11	08	00 4	5 00				eh.	E																7
00	.0	01 5	0 6e 83	00 0	0 40	11	0b 1	b 00	00	00	00 f	fff		.Pn.	@.																	- 1	
002	20	tf f ∧f o	+ 00 44	00 4	3 01	3c 00	40 0	7 01 0 00	01	06 00	00 8	b aa		D	.c.<	<b>@</b>	• • • •	•															
004	10	00 0	0 00 00	00 0	0 f0	27	65 6	8 bd	11	00	00 0	0 00				eh.		:															
00	60	00 0	0 00 00	00 0	0 00	00	00 00	0 00	00	00	00 0	00 00		• • • •		••••		•															
000	50 70	00 0 00 0	0 00 00	00 0	0 00 0 00	00 00	00 00	3 00 0 00	00	00 00	00 0	00 00 00 00		••••	••••	••••	• • • •	•															
008	30	00 0	0 00 00	00 0	0 00	00	00 00	0 00	00	00	00 0	00 00						:															
•	7	Boo	tstrap Prot	ocol: P	rotocol																		Packe	ets: 17	7960 ·	Displa	ayed: 3	(0.0%)	)	F	Profile: Def	fault	۳ :

Next we want to generate some DHCP traffic so minimise the Wireshark window, leaving the capture running.

Click START and type CMD, then right-click on the command prompt to RUN AS ADMINISTRATOR



Arrange the command prompt so you can see it and the live Wireshark capture in the background

bootp									Expressi	on   +
o.	Time	Source	Destination	Protocol	Length In	ō				
8722	87.246897	0.0.0.0	255.255.255.255	DHCP	350 DH	CP Discover	<ul> <li>Transaction</li> </ul>	ID 0x8baa4f9c		
8764	88.371970	0.0.0.0	255.255.255.255	DHCP	362 DH	CP Request	- Transaction	ID 0x8baa4f9c		
10827	129.640445	0.0.0.0	255.255.255.255	DHCP	342 DH	CP Request	- Transaction	ID 0xa007e065		
17965	286.099967	0.0.0.0	255.255.255.255	DHCP	343 DH	CP Request	- Transaction	ID 0x83d605a9		
18024	290.759692	0.0.0.0	255.255.255.255	DHCP	343 DH	CP Request	- Transaction	ID 0x83d605a9		
18053	295.626631	0.0.0.0	255.255.255.255	DHCP	343 DH	CP Request	- Transaction	ID 0x83d605a9		
18157	303.501884	0.0.0.0	255.255.255.255	DHCP	343 DH	CP Request	- Iransaction	1D 0x83d605a9		
18305	320.134343	0.0.0.0	255.255.255.255	DHCP	343 DH	CP Request	- Transaction	1D 0x3d83394		
18327	324.59/24/	0.0.0.0	255.255.255.255	DHCP	343 DH	CP Request	- Transaction	1D 0x3d83394		
						·				
F	Administrator: Co	ommand Prompt							 _	

In the command prompt type *ipconfig* /*release* and press ENTER.

Then type *ipconfig* /*renew* and press ENTER.

Return to the Wireshark capture and look for the Discover, Offer, Request, and Acknowledgement.

25626 478.707808	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover	- Transaction ID 0xf32c7ce2
25703 479.721248	172.16.200.1	172.16.203.19	DHCP	342 DHCP Offer	- Transaction ID 0xf32c7ce2
25704 479.721645	0.0.0	255.255.255.255	DHCP	349 DHCP Request	- Transaction ID 0xf32c7ce2
25710 479.834160	172.16.200.1	172.16.203.19	DHCP	342 DHCP ACK	- Transaction ID 0xf32c7ce2

Expand each one to view the details.

What is the Source MAC address of the Discover?

What is the Destination Port of the Offer?