## ACTIVIDAD 7 – MONITORIZACIÓN DEL TRÁFICO EN REDES – TEMA 2 – SAD

## a) Descarga e instala Wireshark y realiza filtrado de servicios de red para monitorizar sólo el tráfico deseado.

Instalamos Wireshark y nos encontramos en la pantalla principal donde elegimos del menú Capture y Options



Ahora nos aparece esta pantalla donde vamos a dejarlo por defecto como viene en la instalación, y le damos a start

Wireshark: Capture Options											
Capture											
Interface: Loca	ıl	▼ VM	ware	Virtual Etherne	t Adap	ter: \Device\NPF_{4FAFB8D7-87A7-4					
IP address: fe80	::794f:e	8ce:43d9:1	92d,	192.168.0.1							
Link-layer head	er type	: Ethernet	Wireless Settings								
Capture pac	kets in	promiscuo	Remote Settings								
Capture pac	kets in	pcap-ng f	Buffer size: 1 megabyte(s)								
<u>L</u> imit each p	acket t	<b>0</b> 65535	······								
Capture Filter:			Compile BPF								
Capture File(s)			Display Options								
File:			se	Update list of packets in real time							
🔲 Use <u>m</u> ultiple	files										
Vext file eve	ry	1	* *	megabyte(s)	-	<u>A</u> utomatic scrolling in live capture					
Next file eve	ry	1	*	minute(s)	-	Hide capture info dialog					
Ring buffer	with	2	A V	files							
Stop capture	e after	1	A V	file(s)		Name Resolution					
Stop Capture				Enable <u>M</u> AC name resolution							
🔲 after	1	4	pac	:ket(s)		Enable network name resolution					
🔲 after	1	A V	me	egabyte(s)	-	<u> </u>					
🔲 after	1	Å	minute(s)			Enable transport name resolution					
Help						<u>Start</u> <u>C</u> ancel					

En el menú, elegimos Analyze y vamos a elegir Display Filter, esto es para elegir que queremos que nos enseñe, vamos a elegir solo por IP

📶 Wiresha	rk: Display Filter - Profile: Default									
Edit	Display Filter									
New	Ethernet address 00:08:15:00:08:15									
	Ethernet type 0x0806 (ARP)									
	Ethernet broadcast									
	No ARP									
	IP only									
	IP address 192.168.0.1									
	IP address isn't 192.168.0.1, don't use != for this!									
	IPX only									
Delete	TCP only									
	UDP only									
	UDP port isn't 53 (not DNS), don't use != for this!									
Properties										
Filter name: IP only										
Filter string: ip Expression										
<u>H</u> elp	<u>QK</u> <u>Apply</u> <u>Cancel</u>									

Y empiezan a enviarse paquetes dependiendo del tráfico que nosotros tengamos en la red

Description	IP	Packets	Packets/s	Stop			
Microsoft	fe80::e528:6ba5:c962:566	2130	14	Start Options Details			
Realtek PCIe FE Family Controller	fe80::9ce4:aed4:69f5:5312	0	0	Start Options Details			
🜁 VMware Virtual Ethernet Adapter	fe80::794f:e8ce:43d9:192d	13	0	Start Options Details			
🜁 VMware Virtual Ethernet Adapter	fe80::3cc0:470:3866:6030	13	0	Start Options Details			

Aquí nos aparece el tráfico de paquetes y nos lo muestra solamente por ip como pedimos al configurarlo anteriormente

<b>N</b>	/Mwan	e Virtual	Ethern	et Ada	pter	[Wires	hark 1	.6.6 (	SVN F	Rev 41	.803 f	from	/trun	k-1.6)]						X	
Eile	<u>E</u> dit	View	Go	<u>C</u> aptu	e <u>A</u>	nalyze	<u>S</u> tat	istics	Tele	phon	уŢ	ools	Inte	ernals <u>H</u>	lelp						
		94 斛			. 3	چ ک	8	0	、 🔶	\$	4	Ŧ	⊉			<b>€</b> Q @	. 🖭	×.	¥ 🍕	6	»
Filt	er: ip												•	Expression	on	Clear App	ly				
No.		Time		Source	2				estin	ation				Protoco	ol Ler	ngth Info					
		70.60	9500	192.	168.	0.1			239.	255.	255	. 25		SSDP		167 M-SE	ARCH		TP/1.	1	
	11	70.61	1558	192.	168.	0.1			239.	255.	255	.25	)	SSDP		165 M-SE	ARCH	* нт	TP/1.:	1	
	13	73.61	0460	192.	168.	0.1			239.	255.	255	. 25(	)	SSDP		167 M-SE	ARCH	* нт	ТР/1.:	1	
	15	73.61	3053	192.	168.	0.1			239.	255.	255	.25	)	SSDP		165 M-SE	ARCH	* нт	TP/1.:	1	
	17	76.61	1476	192.	168.	0.1		1.1	239.	255.	255	.25	)	SSDP		167 M-SE	ARCH	* нт	ТР/1.:	1	
	19	76.61	3779	192.	168.	0.1			239.	255.	255	.25	)	SSDP		165 M-SE	ARCH	* нт	TP/1.:	1	
																	1				
< □								1	Л	_							]				-
E F	rame	9:1	67 by	rtes (	on w	ire (	1336	5 bi	ts),	167	by	tes	cap	otured	(133	6 bits)					-
÷ E	ther	net I	I, Sr	C: VI	nware	e_c0:	00:0	)1 (	00:5	0:56	;c0	:00	:01)	), Dst:	IPV	4mcast_7	t:ff:	fa (	01:00	:5e:	
E I	Inter	net P	rotoc	01 V	ersio	on 4,	Sro	:: 1	92.1	68.0	).1	(19	2.16	58.0.1)	, DS	t: 239.2	55.25	5.25	0 (239	9.25	
. ⊕ L	Jser	Datag	ram P	roto	:01,	Snc	Port	:: 6	2894	(62	894	), I	Dst	Port:	ssdp	(1900)					-
	lvner	text .	Trans	ter (	prote	ncól															
										_											
000	0 0	1 00 5	je 7f	fff	a 00	50	56	c0 (	0 01	1 08	00	45	00	^.	P	VE	•				
001	0 0	0 99 ( F fa f	JI 6/	00 0	0 01	11	4d	ca (	10 al	5 00 d 52	45	eT 41	52		· • · ·	M M-SEA					Ξ
003	0 4	3 48 2	20 2a	20 4	8 54	54	50	2f	31 20	e 31	0d	0a	48	СН *	нтт	P/1.1.	H				
004	0 6	F 73 7	'4 3a	32 3	3 39	2e	32	35	35 20	e 32	35	35	2e	ost:	239.	255.255					-
005	0 2	> > = =	20.25	21 2	0.20	20	04	0- 1	() E/	1 2 -	75	77	60	250+	1000	CTION	<u>.</u>			_	
	File: "C	:\Users\	LALES	AppDa	ta\Loc	al\Ten	np	Pack	ets: 19	9 Disp	layed	1:6 N	larked	d: 0 Dropp	ped: 0	Profile: De	fault				

## b) Descarga e instala Kismet o Network Stumbler para redes inalámbricas y realiza filtrados de red para monitorizar sólo el tráfico deseado.

Nos descargamos Network Stumbler, donde nos va a detectar las redes inalámbricas y el tráfico deseado.



Cuando ya lo tenemos ya instalado nos aparece la pantalla principal que es la que figura a continuación, aunque a la derecha deberían de aparecer las redes inalámbricas que haya reconocido, pero vemos que no reconoce ninguna, ya que la tarjeta de nuestro portátil no es compatible.



## MARÍA ÁNGELES PEÑASCO SÁNCHEZ – ACTIVIDAD 7 – TEMA 2 – SAD