Actividad 3: Configuración y auditoria forense de computadores en red

Datos del estudiante

Nombre y apellidos	Antonio López García
Fecha de entrega	11/1272023
Fecha límite de entrega	**12/12/2023**

Respuesta a las tareas

PARTE 1: CONFIGURACIÓN DE UN ENTORNO DE COMPUTADORES EN RED (4 PUNTOS)

1.- (4 puntos) Especifique, mediante una tabla, las direcciones IP asignadas a cada nodo de la red siguiendo el ejemplo de la tabla inferior:

Dispositivo	ETD /ETCD	Dirección IP	Máscara de red	Puerta de enlace

	Dispositivo	ETD /ETCD	Dirección IP	Máscara de red	Puerta de enlace
192.168.1.0/24	PC1	ETD	192.168.1.10	255.255.255.0	192.168.1.1
192.168.1.0/24	PC2	ETD	192.168.1.11	255.255.255.0	192.168.1.1
192.168.1.0/24	IMP1	ETD	192.168.1.12	255.255.255.0	192.168.1.1
192.168.1.0/24	HOST	ETD	192.168.1.13	255.255.255.0	192.168.1.1
	SWITCH1	ETCD			
	ROUTER	ETCD	192.168.1.1	255.255.255.0	
	ROUTER	ETCD	192.168.12.1	255.255.255.0	
	SWITCH2	ETCD			
	ACCESSPOINT	ETCD			
192.168.12.0/24	PC3	ETD	192.168.12.10	255.255.255.0	192.168.12.1
192.168.12.0/24	PC4	ETD	192.168.12.11	255.255.255.0	192.168.12.1
192.168.12.0/24	PC5	ETD	192.168.12.12	255.255.255.0	192.168.12.1
192.168.12.0/24	IMP2	ETD	192.168.12.13	255.255.255.0	192.168.12.1
192.168.12.0/24	PORTATIL1	ETD	192.168.12.14	255.255.255.0	192.168.12.1
192.168.12.0/24	PORTATIL2	ETD	192.168.12.15	255.255.255.0	192.168.12.1

192.168.12.0/24	IMP3	ETD	192.168.12.16	255.255.255.0	192.168.12.1
192.168.12.0/24	WEBCAM	ETD	192.168.12.17	255.255.255.0	192.168.12.1

PARTE 2: ANÁLISIS FORENSE DE UN ENTORNO EN RED (6 PUNTOS)

1.- (1 punto) Describa básicamente el archivo que el cliente nos ha suministrado reportando los siguientes datos (*Propiedades del archivo de captura*):

Fecha y hora de la captura:	2023-01-13 13:15:40
Duración de la captura:	00:05:22

Archivo

Nombre:	/media/tonilogar/67151cdc-c7cd-4700-85e0-b5ca7ecefdc2/tonilogar/Documentos/trabajos/carlemany/redes/thirdWeek/test/capturaAuditada.pcapng
Longitud:	61 MB
Hash (SHA256):	2103f42a8b791508b9bb0928630e4021deb237f387aa628ab2d668b880fae5ce
Hash (RIPEMD160):	93c735dcaf54615d47a52489b982fa28eed050e9
Hash (SHA1):	07f2c53d2748f50af327b7e19eabb0133ec60fc9
Formato:	Wireshark/... - pcapng
Encapsulado:	Ethernet

Intervalo

Primer paquete:	2023-01-13 13:15:40
Último paquete:	2023-01-13 13:21:03
Transcurrido:	00:05:22

Captura

Hardware:	Intel(R) Core(TM) i5-3210M CPU @ 2.50GHz (with SSE4.2)
SO:	64-bit Windows 10 (22H2), build 19045
Aplicación:	Dumpcap (Wireshark) 4.0.2 (v4.0.2-0-g415456d13370)

Interfaces

Interfaz	Paquetes perdidos	Filtro de captura	Tipo de enlace	Packet size limit (snaplen)
Wi-Fi	0 (0.0%)	ninguno	Ethernet	262144 bytes

Estadísticas

Medida	Capturado	Mostrado	Marcado
Paquetes	59109	59109 (100.0%)	—
Espacio de tiempo, s	322.555	322.555	—
Promedio pps	183.3	183.3	—
Promedio de tamaño de paquete, B	1006	1006	—
Bytes	59473704	59473704 (100.0%)	0
Promedio de bytes/s	184 k	184 k	—
Promedio de bits/s	1.475 k	1.475 k	—

Interfaz utilizada:	Wi-Fi
Nº de paquetes capturados:	59109
KB capturados:	59473704 Bytes

2.- (3 puntos) Análisis de las fuentes:

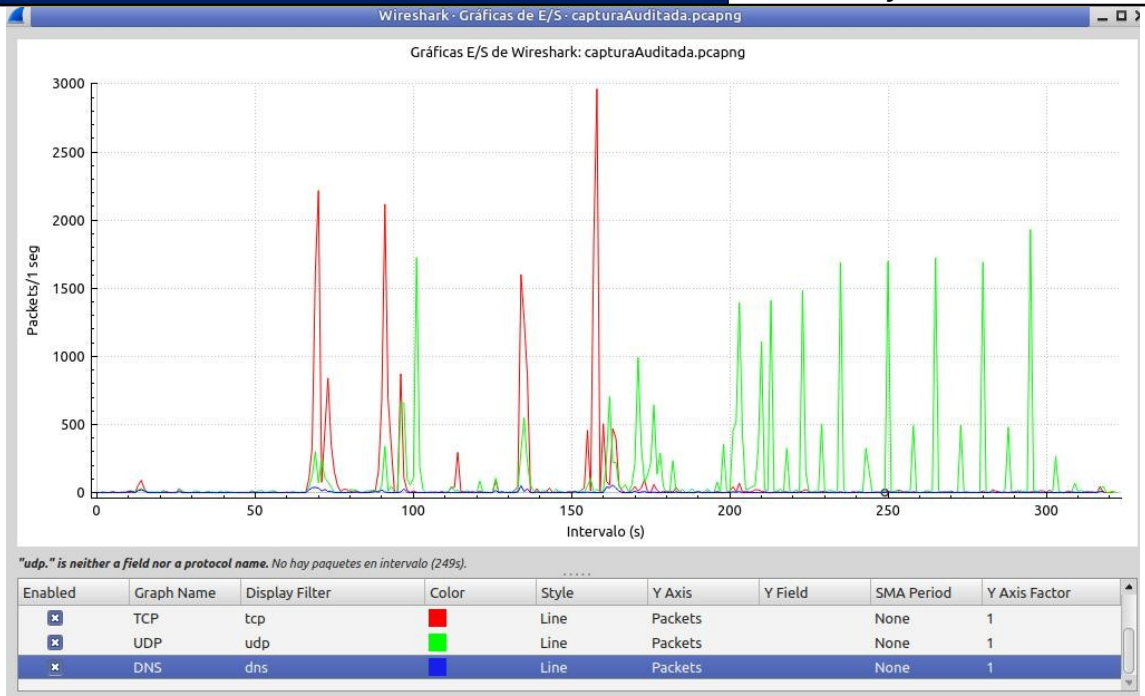
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Pack	Rx Bytes	Co
192.168.0.1	332	199106	260	145191	72	53915	
192.168.0.2	238	99749	238	99749	0	0	
192.168.0.20	21	4575	21	4575	0	0	
192.168.0.22	2	505	2	505	0	0	
192.168.0.25	61	19263	61	19263	0	0	
192.168.0.26	31	5735	31	5735	0	0	
192.168.0.27	32	5984	32	5984	0	0	
192.168.0.30	55087	58766774	10056	2495381	45031	56271393	
192.168.0.31	72	21750	72	21750	0	0	
192.168.0.47	1	243	1	243	0	0	
192.168.0.72	90	25285	90	25285	0	0	
192.168.0.80	13	2835	13	2835	0	0	
192.168.0.102	73	21915	73	21915	0	0	
192.168.0.106	101	26035	101	26035	0	0	
192.168.0.108	6	3584	6	3584	0	0	
192.168.0.109	7	1512	7	1512	0	0	
192.168.0.113	19	7450	19	7450	0	0	
192.168.0.114	8	1736	8	1736	0	0	
192.168.0.116	29	8227	29	8227	0	0	
192.168.0.118	25	20325	25	20325	0	0	
192.168.0.119	13	2860	13	2860	0	0	
192.168.0.121	12	2592	12	2592	0	0	
192.168.0.122	12	2592	12	2592	0	0	
192.168.0.255	23	5346	0	0	23	5346	

a)(*Puntos finales*) ¿Cuántas direcciones IP del mismo segmento de red del equipo que realizó la captura (192.168.0.30) han sido "origen" o "destino" en la comunicación registrada?

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
▼ Packet Lengths	59109	1006,17	42	1514	0,1833	100%	12,8500	70,210
0-19	0	-	-	-	0,0000	0,00%	-	-
20-39	0	-	-	-	0,0000	0,00%	-	-
40-79	10979	65,54	42	79	0,0340	18,57%	0,8900	223,889
80-159	2575	105,50	80	159	0,0080	4,36%	0,3600	91,282
160-319	2017	228,30	160	319	0,0063	3,41%	0,2100	162,184
320-639	1772	464,60	320	639	0,0055	3,00%	0,5800	158,865
640-1279	1930	1027,66	640	1279	0,0060	3,27%	1,2500	135,211
1280-2559	39836	1386,07	1280	1514	0,1235	67,39%	12,3700	70,210
2560-5119	0	-	-	-	0,0000	0,00%	-	-
5120 and greater	0	-	-	-	0,0000	0,00%	-	-

b)(*Conversaciones*) ¿Con cuántas direcciones IP diferentes se ha mantenido comunicación desde el equipo que realizó la captura (192.168.0.30) durante la escucha?

Nº total de equipos de destino:	131
Bytes totales enviados:	2465901 Bytes



Tasa de transferencia media (Bits/s A→B):	11.855,06 bits por segundo
Máxima velocidad de transferencia registrada:	273488.8433463066 Bits/s

a) **c)(*Longitudes de paquete*) ¿Cuáles son los tres rangos de longitudes de paquetes más utilizados por las PDUs en la captura analizada?**

1280-2559, 40-79, 80-159

3.- (2 puntos) Representa una gráfica de líneas que incluya el tráfico de paquetes de los protocolos DNS, TCP y UDP en tres series de datos diferentes, con una escala de intervalo temporal de 1 segundo (*Gráficas de E/S*):

a)Capturar la imagen de la gráfica y pegarla en este informe.

b)¿Qué protocolo de transporte es el más utilizado en la comunicación capturada?

UDP es el más utilizado, hay más número de picos altos en el protocolo UDP "verde".

c)¿El uso de dichos protocolos de transporte es homogéneo durante toda la captura?

No es homogéneo, los tres protocolos muestran una gráfica con picos altos y bajos en diferentes espacios de tiempo. Para ser homogéneo, la gráfica tendría que representar en espacios de tiempo similares picos y valles de la misma altura.

d)¿Observas alguna relación entre el tráfico de paquetes DNS y UDP?

No le veo relación. Los datos de UDP son mucho más grandes que los del DNS.
Los dos protocolos operan en capas diferentes del modelo OSI.
UDP pertenece a la capa trasporte y el protocolo DNS pertenece a la capa aplicación.