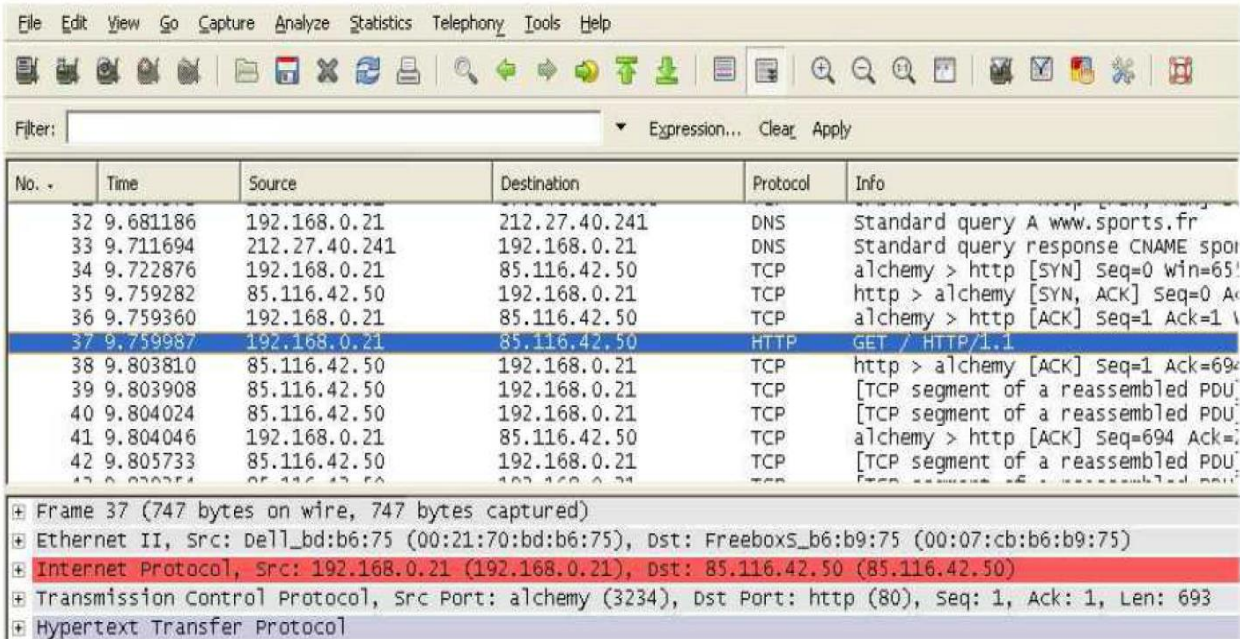


Contexte

Une entreprise a demandé à un administrateur réseau de chercher à savoir si un utilisateur salarié navigue sur des sites d'intérêt privé pendant son travail.

L'administrateur réseau utilise le logiciel libre Wireshark.



No. -	Time	Source	Destination	Protocol	Info
32	9.681186	192.168.0.21	212.27.40.241	DNS	Standard query A www.sports.fr
33	9.711694	212.27.40.241	192.168.0.21	DNS	Standard query response CNAME spor
34	9.722876	192.168.0.21	85.116.42.50	TCP	alchemy > http [SYN] Seq=0 win=65535
35	9.759282	85.116.42.50	192.168.0.21	TCP	http > alchemy [SYN, ACK] Seq=0 Ack=65535
36	9.759360	192.168.0.21	85.116.42.50	TCP	alchemy > http [ACK] Seq=1 Ack=1
37	9.759987	192.168.0.21	85.116.42.50	HTTP	GET / HTTP/1.1
38	9.803810	85.116.42.50	192.168.0.21	TCP	http > alchemy [ACK] Seq=1 Ack=694
39	9.803908	85.116.42.50	192.168.0.21	TCP	[TCP segment of a reassembled PDU]
40	9.804024	85.116.42.50	192.168.0.21	TCP	[TCP segment of a reassembled PDU]
41	9.804046	192.168.0.21	85.116.42.50	TCP	alchemy > http [ACK] Seq=694 Ack=
42	9.805733	85.116.42.50	192.168.0.21	TCP	[TCP segment of a reassembled PDU]

+ Frame 37 (747 bytes on wire, 747 bytes captured)
 + Ethernet II, Src: Dell_bd:b6:75 (00:21:70:bd:b6:75), Dst: FreeboxS_b6:b9:75 (00:07:cb:b6:b9:75)
 + Internet Protocol, Src: 192.168.0.21 (192.168.0.21), Dst: 85.116.42.50 (85.116.42.50)
 + Transmission Control Protocol, Src Port: alchemy (3234), Dst Port: http (80), Seq: 1, Ack: 1, Len: 693
 + Hypertext Transfer Protocol

Q1 : trouver sur quel site est allé l'utilisateur pendant son travail

Q2 : Quelle est l'adresse IP du serveur DNS ?

Analyse en détail de la trame 37 (en bas de l'image)

Q3 : En observant la trame 37, donner l'adresse MAC de la machine utilisée par le salarié

Q4 : donner l'adresse IP de la machine utilisée par le salarié

Q5 : Donner l'adresse IP de la machine hébergeant le site web visité