Capture de trafic avec wireshark

Pour télécharger Wireshark	https://www.wireshark.org/download.html
Un tutoriel Wireshark	https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html
Exemples de fichiers de captures (pcap)	https://wiki.wireshark.org/SampleCaptures

1) Lancez une capture (gardez toutes les options par défaut).

2) Utilisez votre navigateur ou votre messagerie pour faire du trafic. Vous pouvez également faire un « ping » vers un site Internet. Vous devez voir apparaitre les trames capturées, dans le cas contraire « Choisissez une capture sur toutes les interfaces ».

3) Lister les protocoles relatifs aux trames capturés.

4) Choisir un ensemble de trames, pour lesquelles :

    a. Vous identifiez la pile protocolaire (protocoles encapsulés)
    b. Vous identifiez les tailles de ces trames

5) Identifiez pour différents protocoles (Ethernet, IP, TCP, UDP, HTTP) les octets correspondant à chacun des en-têtes de protocole, puis :
    a. Donnez la taille d'entête pour chaque protocole
    b. Schématisez l'entête de chaque protocole en décrivant chaque champ de l'entête (nom, taille et signification)