|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  |  | | --- | --- | --- | | |  | | --- | | **Travaux pratiques**  **TP1.**  **Etude des couches OSI.**  **a)** Lancez une capture (gardez toutes les options par défaut).  **b)** Utilisez votre navigateur ou votre messagerie pour faire du trafic. Vous devez voir apparaitre les trames capturées, dans le cas contraire sélectionnez une autre interface.  **c)** Quels protocoles voyez-vous apparaitre dans la fenêtre du haut ?  **d)** Sélectionnez les successivement les différentes trames capturées, toutes les couches du modèle OSI sont-elles représentées dans la fenêtre du milieu ? Expliquez.  **e)** Quelle est la taille des trames capturées ?  **f)** Choisissez une trame dans laquelle le protocole HTTP est présent (il faut pour cela que vous génériez du trafic avec votre navigateur). Sélectionnez ensuite dans la fenêtre du milieu les différents protocoles présent dans cette trame (Ethernet, IP, TCP, HTTP). Les octets correspondant à chacun des en-têtes de protocole doivent apparaitre en surligné dans la fenêtre du bas. Combien d’octets obtenez-vous pour chaque protocole ? Retrouvez en additionnant le total indiqué sur la première ligne de la fenêtre du milieu.    **g)** Dans quel ordre les octets sont-ils capturés par l’analyseur ? En d’autres termes, à quelle couche correspondent les premiers octets de la trame ? Comment sont encapsulées les données HTTP pour au final constituer une trame circulant sur le réseau ? | |  | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | http://prive.iutenligne.net/11jsG5Kljum6LIB5/informatique/reseaux/lohier/reseaux_fondamentaux/styles/images/pixel-trans.gif | | | | | | | | | | | | | | | | | | | http://prive.iutenligne.net/11jsG5Kljum6LIB5/informatique/reseaux/lohier/reseaux_fondamentaux/styles/images/pixel-trans.gif |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | http://prive.iutenligne.net/11jsG5Kljum6LIB5/informatique/reseaux/lohier/reseaux_fondamentaux/styles/images/pixel-trans.gif | | | | | | | | | | | | | | | | | | | http://prive.iutenligne.net/11jsG5Kljum6LIB5/informatique/reseaux/lohier/reseaux_fondamentaux/styles/images/pixel-trans.gif |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | | |
| |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | http://prive.iutenligne.net/11jsG5Kljum6LIB5/informatique/reseaux/lohier/reseaux_fondamentaux/styles/images/pixel-trans.gif | | | | | | | | | | | | | | | | | | | http://prive.iutenligne.net/11jsG5Kljum6LIB5/informatique/reseaux/lohier/reseaux_fondamentaux/styles/images/pixel-trans.gif |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |

|  |  |  |
| --- | --- | --- |
| |  | | --- | | **TP2**  **Analyse des protocoles TCP-IP**  Analyse de la commande ping.   * Quel protocole de niveau réseau est utilisé par la commande Ping ? * Effectuez un ping vers votre passerelle. Utilisez un filtre d’affichage permettant de visualiser uniquement les trames correspondant à une commande ping. Analysez les trames visualisées. Combien trouvez-vous de trames ? A quoi correspondent-elles. Quels sont les protocoles présents dans une trame ping ? * Quels sont les codes ICMP permettant de déterminer la nature du message ICMP (*Echo Request* ou *Echo Reply*). * A quoi correspondent les données (« Data ») ICMP ?   Analyse de la commande Tracert   * Lancez une capture. Effectuez une commande **tracert** sur un serveur web de votre choix.  Quel protocole de niveau réseau est utilisé par la commande tracert ? Utilisez un filtre d’affichage permettant de visualiser uniquement les trames correspondant à une commande tracert. * Observez les champs TTL des trames émises par votre machine et le champ Type des trames reçues. A partir de ces observations, expliquez le fonctionnement de la commande tracert.   Analyse du protocole IP   * Lancez une capture dans laquelle le protocole IP est présent (vous pouvez utiliser un filtre d’affichage pour isoler certaines trames). * Quelles sont les couches OSI présentes dans les trames relevées ? * Quelle est la version de IP ? * Quelle est la taille l’en-tête IP ? * Le paquet IP est –il fragmenté ? Justifiez votre réponse. * Quelle est la valeur du champ TTL de l’en-tête IP ? Justifiez votre réponse. * Quel est le protocole de niveau supérieur ? Par quelle valeur est-il identifié ? * Pouvez-vous retrouver les valeurs hexadécimales des adresses IP source et destination ?   Analyse d’une connexion TCP.   * Lancez une capture. Connectez-vous à un site web quelconque, puis déconnectez-vous. Analysez la connexion TCP à l’aide de filtres d’affichage. * Combien y-a-t-il de segments d’ouverture et de fermeture de la connexion ? Quelles sont les valeurs des « flags » pour ces segments ? Quels sont les numéros de port utilisés. Justifiez votre réponse. * Vérifiez l’évolution des numéros de séquence et des numéros d’acquittements pour deux trames successives en réponse l’une à l’autre. Vous pouvez pour cela vous aider d’un schéma. * Wireshark possède un outil nommé, *Follow TCP stream* (menu Statistics/Flow Graph/TCP Flow). Vous pouvez ainsi visualiser l’enchainement des segments avec les du numéro de séquence et d’acquittement pour toute la session TCP. | |  | |
| |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | http://prive.iutenligne.net/11jsG5Kljum6LIB5/informatique/reseaux/lohier/reseaux_fondamentaux/styles/images/pixel-trans.gif | | | | | | | | | | | | | | | | | | | http://prive.iutenligne.net/11jsG5Kljum6LIB5/informatique/reseaux/lohier/reseaux_fondamentaux/styles/images/pixel-trans.gif |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |