

Journées des inspecteurs et inspectrices en charge des enseignements de SNT et NSI



11h00 - 11h45

Exemple de travaux pratiques pour
l'apprentissage des réseaux

UNE ACTIVITÉ RÉSEAUX ET CYBERSÉCURITÉ...

Mohammed GRIMEJ

Professeur d'informatique

Lycée Descartes, 4 Boulevard Copernic - 77420 CHAMPS-SUR-MARNE

mohammed.grimej@ac-creteil.fr

Contenu de la présentation

- **Une activité d'apprentissage de la notion de protocole**
 - Analyse d'une trame HTTP
 - Interception d'un mot de passe
- **Prolongements possibles**

- **Retour d'expérience**
 - Actions proposées aux élèves
 - Projets
 - Cybersécurité
 - Intelligence artificielle
 - Égalité
 - Découverte, Immersion, visites,
 - Rencontres, ouverture
 - Infrastructure utilisée en NSI
 - Filles-Garçons

Une activité d'apprentissage de la notion de protocole ...

Contenus des programmes étudiés

- **Interactions entre l'homme et la machine sur le Web**
 - Modalités de l'interaction entre l'homme et la machine
 - **Interaction avec l'utilisateur dans une page Web**
 - Interaction client-serveur. Requêtes HTTP, réponses du serveur
 - Formulaire d'une page Web
- **Architectures matérielles, systèmes d'exploitation et réseaux**
 - **Transmission de données dans un réseau - Protocoles de communication**
 - Protocoles TCP/IP (*Adressage MAC, IP*)
 - Encapsulation
- **Sécurisation des communications**

Première

Terminale

Analyse d'une trame HTTP

Une activité pour l'apprentissage des protocoles ...

| Contenus | Capacités attendues | Commentaires |
|---|--|--|
| Modalités de l'interaction entre l'homme et la machine Événements | Identifier les différents composants graphiques permettant d'interagir avec une application Web. Identifier les événements que les fonctions associées aux différents composants graphiques sont capables de traiter. | Il s'agit d'examiner le code HTML d'une page comprenant des composants graphiques et de distinguer ce qui relève de la description des composants graphiques en HTML de leur comportement (réaction aux événements) programmé par exemple en JavaScript. |
| Interaction avec l'utilisateur dans une page Web | Analyser et modifier les méthodes exécutées lors d'un clic sur un bouton d'une page Web. | |
| Interaction client-serveur. Requêtes HTTP, réponses du serveur | Distinguer ce qui est exécuté sur le client ou sur le serveur et dans quel ordre. Distinguer ce qui est mémorisé dans le client et retransmis au serveur. Reconnaître quand et pourquoi la transmission est chiffrée. | Il s'agit de faire le lien avec ce qui a été vu en classe de seconde et d'expliquer comment on peut passer des paramètres à un site grâce au protocole HTTP. |
| Formulaire d'une page Web | Analyser le fonctionnement d'un formulaire simple. Distinguer les transmissions de paramètres par les requêtes POST ou GET. | Discuter les deux types de requêtes selon le type des valeurs à transmettre et/ou leur confidentialité. |
| Transmission de données dans un réseau Protocoles de communication Architecture d'un réseau | Mettre en évidence l'intérêt du découpage des données en paquets et de leur encapsulation. Dérouter le fonctionnement d'un protocole simple de récupération de perte de paquets (bit alterné). Simuler ou mettre en œuvre un réseau. | Le protocole peut être expliqué et simulé en mode débranché. Le lien est fait avec ce qui a été vu en classe de seconde sur le protocole TCP/IP. Le rôle des différents constituants du réseau local de l'établissement est présenté. |



Zoom pour une lecture aisée

Programme NSI

Première

Interactions entre l'homme et la machine sur le Web

Terminale

Architectures matérielles, systèmes d'exploitation et réseaux

| | | |
|--|---|--|
| Transmission de données dans un réseau | Mettre en évidence l'intérêt du découpage des données en paquets et de leur encapsulation. | Le protocole peut être expliqué et simulé en mode débranché. |
| Protocoles de communication | Dérouler le fonctionnement d'un protocole simple de récupération de perte de paquets (bit alterné). | Le lien est fait avec ce qui a été vu en classe de seconde sur le protocole TCP/IP. |
| Architecture d'un réseau | Simuler ou mettre en œuvre un réseau. | Le rôle des différents constituants du réseau local de l'établissement est présenté. |

Première

Architectures matérielles et systèmes d'exploitation

| Contenus | Capacités attendues | Commentaires |
|---|--|--|
| Modalités de l'interaction entre l'homme et la machine Événements | Identifier les différents composants graphiques permettant d'interagir avec une application Web. Identifier les événements que les fonctions associées aux différents composants graphiques sont capables de traiter. | Il s'agit d'examiner le code HTML d'une page comprenant des composants graphiques et de distinguer ce qui relève de la description des composants graphiques en HTML de leur comportement (réaction aux événements) programmé par exemple en JavaScript. |
| Interaction avec l'utilisateur dans une page Web | Analyser et modifier les méthodes exécutées lors d'un clic sur un bouton d'une page Web. | |
| Interaction client-serveur. Requêtes HTTP, réponses du serveur | Distinguer ce qui est exécuté sur le client ou sur le serveur et dans quel ordre. Distinguer ce qui est mémorisé dans le client et retransmis au serveur. Reconnaître quand et pourquoi la transmission est chiffrée. | Il s'agit de faire le lien avec ce qui a été vu en classe de seconde et d'expliquer comment on peut passer des paramètres à un site grâce au protocole HTTP. |
| Formulaire d'une page Web | Analyser le fonctionnement d'un formulaire simple. Distinguer les transmissions de paramètres par les requêtes POST ou GET. | Discuter les deux types de requêtes selon le type des valeurs à transmettre et/ou leur confidentialité. |
| Transmission de données dans un réseau Protocoles de communication Architecture d'un réseau | Mettre en évidence l'intérêt du découpage des données en paquets et de leur encapsulation. Dérouler le fonctionnement d'un protocole simple de récupération de perte de paquets (bit alterné). Simuler ou mettre en œuvre un réseau. | Le protocole peut être expliqué et simulé en mode débranché. Le lien est fait avec ce qui a été vu en classe de seconde sur le protocole TCP/IP. Le rôle des différents constituants du réseau local de l'établissement est présenté. |

Une activité d'apprentissage de la notion de protocole ...

objectifs et capacités

- Mettre en évidence le découpage des données en **paquets** et leur **encapsulation**.
- Analyser le fonctionnement d'un formulaire simple.
- *Analyser les méthodes exécutées lors d'un clic sur un bouton d'une page Web.*
- Reconnaître quand et pourquoi la transmission est **chiffrée**.
- *Identifier les différents composants graphiques permettant d'interagir avec une application Web.*
- Mettre en lien le modèle **TCP/IP**, les couches réseaux et **protocoles**
- Illustrer concrètement le **rôle d'un protocole** (HTTP)



Analyse d'une trame HTTP
Une activité pour l'apprentissage des protocoles ...

Guide de démonstration avec HTTP

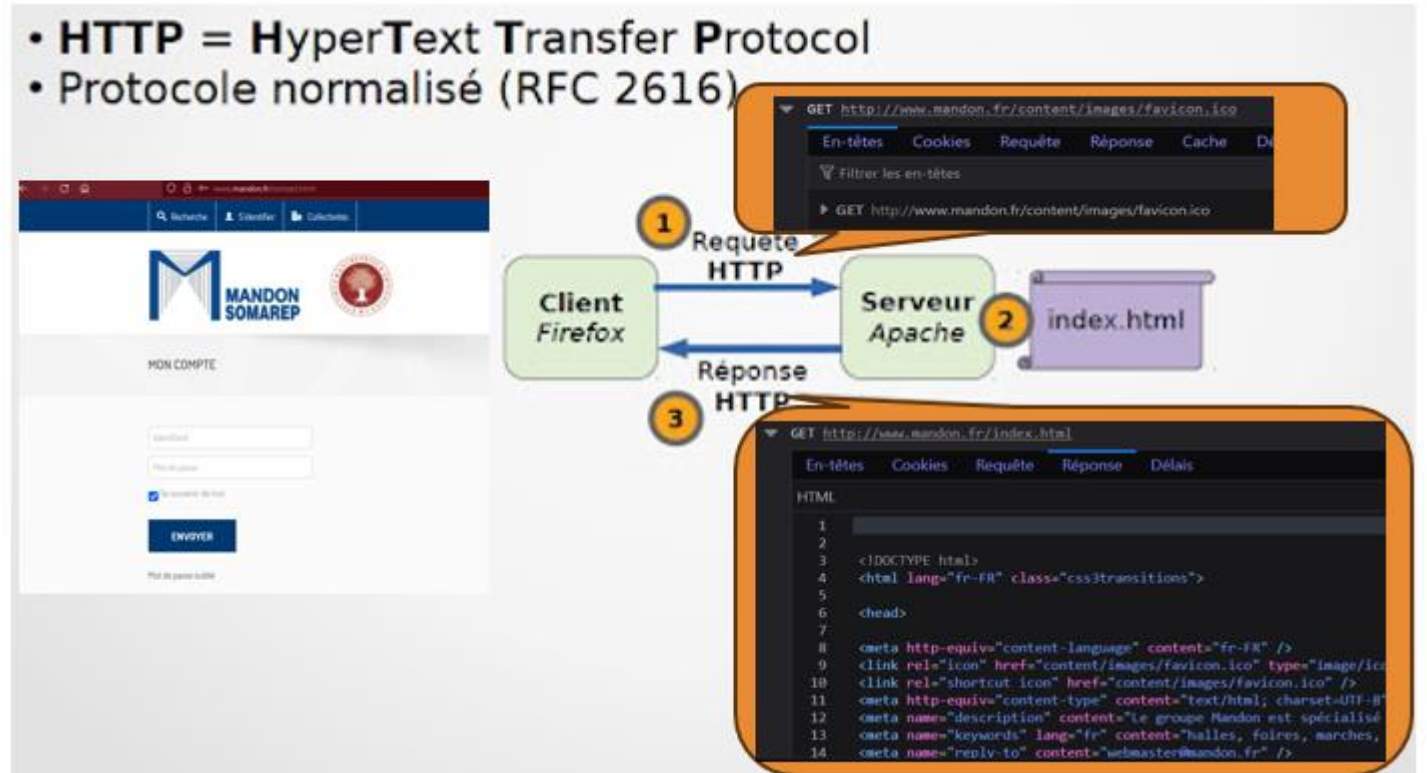
- Contextualisation : Pourquoi le choix du site (le site cible, qui est encore en HTTP)
- Rappels des notions :
 - Protocole HTTP, Requête, client-serveur
 - Protocoles TCP/IP
 - Encapsulation
- Ordre des actions et architecture de la démonstration
 - Aller sur le site via son URL et le protocole HTTP
 - Besoin de trouver l'adresse IP du serveur (utilisation de la commande ping)
 - Lancement du logiciel Wireshark en mode administrateur
 - Prise en main de l'outil, rôle des différentes fenêtres, les filtres, les expressions, IPV4, IPV6...
 - Utilisation de l'inspecteur de code du navigateur (Firefox ou autre)
 - Repérer les champs
 - Repérer la bonne trame
 - Naviguer dans la trame et repérer les éléments des protocoles
 - Identifier la donnée d'application recherchée (donnée de formulaire)
 - Trouver le mot de passe

Requête HTTP dans un dialogue client-serveur ...

Rôle de HTTP

- HyperText Transfert Protocol

Les messages envoyés par le client (généralement un navigateur web) sont appelés des *requêtes* et les messages renvoyés par le serveur sont appelés *réponses*.



Analyse d'une trame HTTP

Une activité pour l'apprentissage des réseaux ...

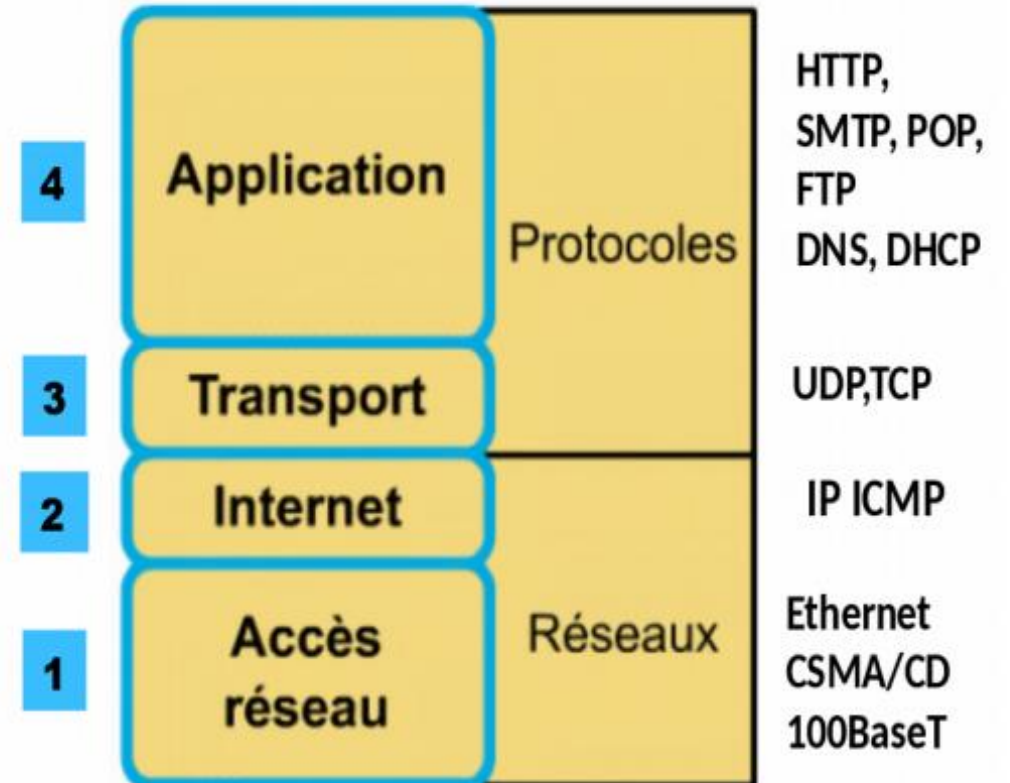
Requête HTTP dans un dialogue client-serveur ...

Du navigateur Web (client) au un serveur Web...et vice-versa

- Protocoles TCP/IP

HTTP un protocole de la couche application dont les données transitent via TCP

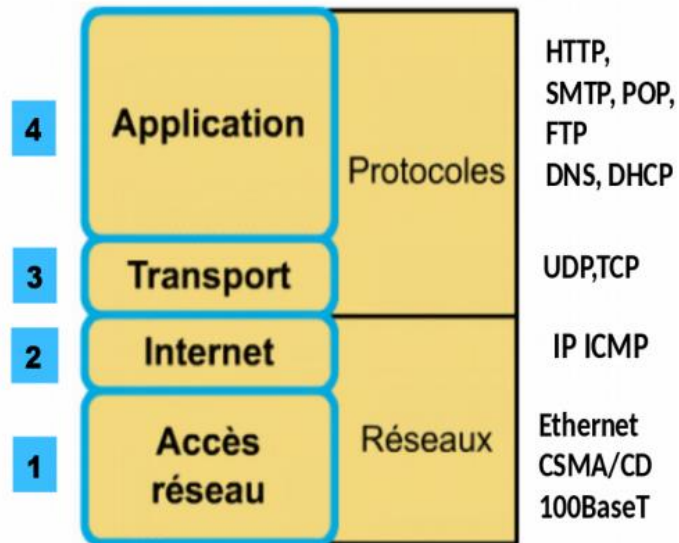
... ou bien à travers une connexion TCP chiffrée avec TLS
Deviens alors *HTTP over TLS*



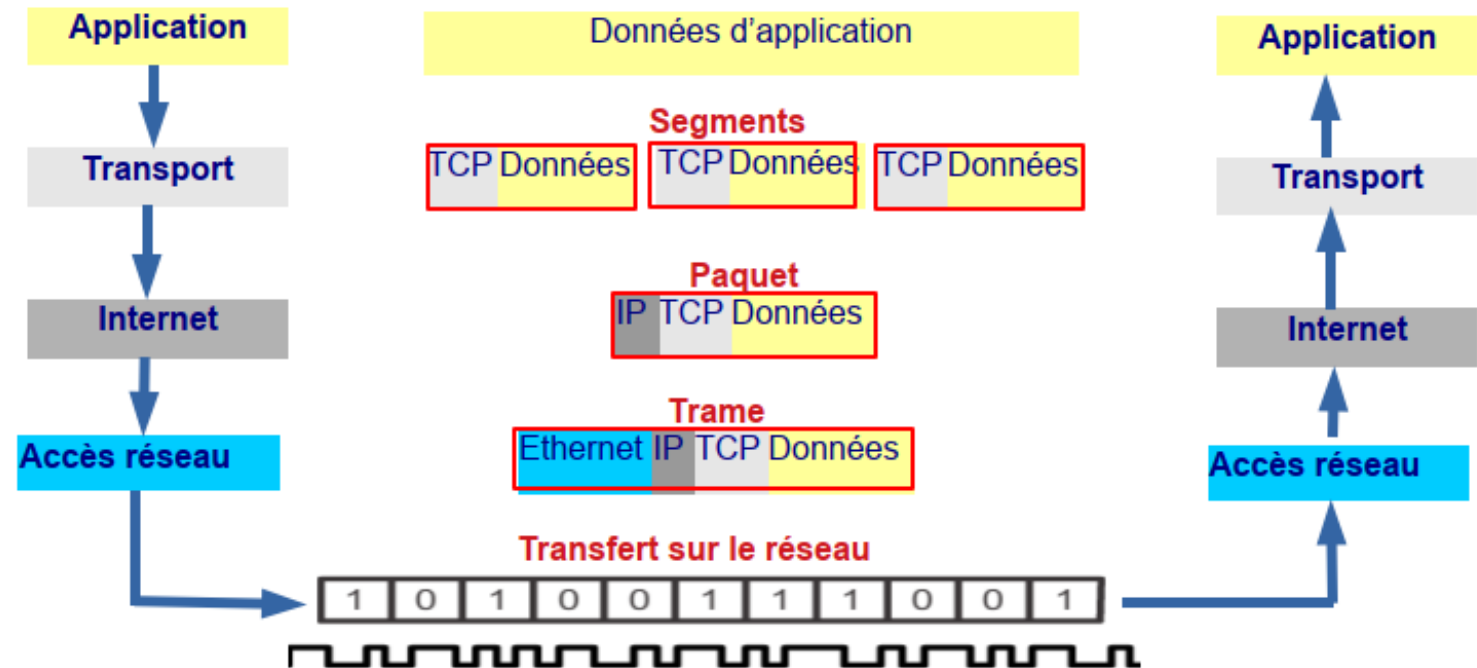
Requête HTTP dans un dialogue client-serveur ...

Du navigateur Web (client) au un serveur Web...et vice-versa

- L'encapsulation



Récapitulatif : encapsulation/dés-encapsulation



Démonstration

Analyse d'une trame HTTP

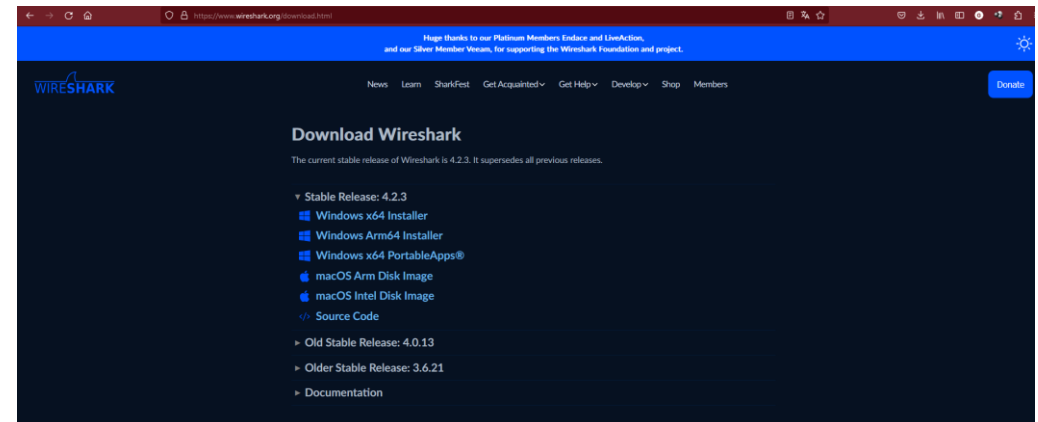
- Un ordinateur : celui-ci
- Un site web *réel* avec une page de connexion en HTTP : [HTTP://www.mandon.fr](http://www.mandon.fr)
- Un accès internet
- Un logiciel analyseur de paquets (analyseur de trames) : Wireshark
 - Logiciel libre, Open source
 - Analyse de trames complète et outillée

Prise en main de ...



- Logiciel libre, Open source
- Prise en main de l'outil Wireshark
 - Lancement d'une capture
 - Le rôle des différentes fenêtres,
 - Les filtres, les expressions,
 - IPV4, IPV6...

Site officiel - Téléchargement- Documentation



Analyse d'une trame HTTP
Une activité pour l'apprentissage des réseaux ...



Interception des données d'un formulaire

Le bon filtre aide beaucoup

The screenshot shows the Wireshark interface with a filter applied: `ip.dst==213.215.54.222 && http`. The packet list pane displays several HTTP requests, with the last one (No. 287605) selected. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The Hypertext Transfer Protocol section is expanded to show the HTML Form URL Encoded data, which contains the following form items:

- Form item: "act" = "login"
- Form item: "login" = "jeudi"
- Form item: "password" = "matin"
- Form item: "submit" = "Envoyer"
- Form item: "rememberme" = "forever"
- Form item: "redirect_to" = "/"

The packet bytes pane shows the raw data of the selected packet, with the following hex and ASCII representation:

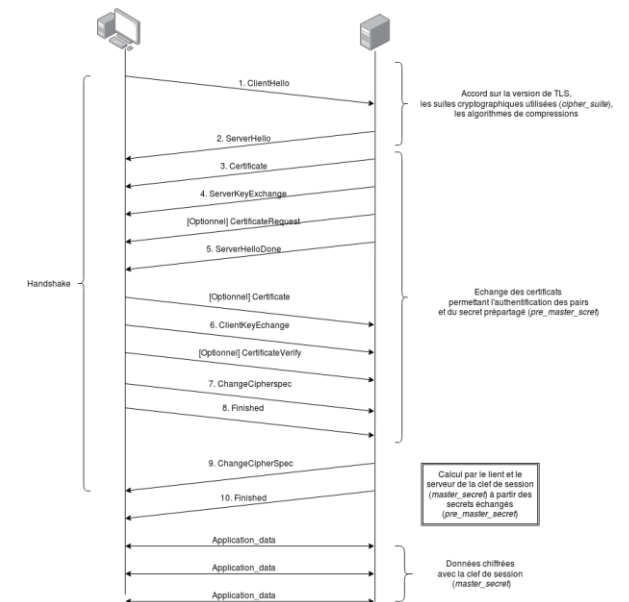
```
0230 61 62 6c 65 64 3d 64 65 63 6c 69 6e 65 64 3b 20      abled=de clined;
0240 50 48 50 53 45 53 53 49 44 3d 62 6c 73 6a 6a 70      PHPSESSI D=blsjjp
0250 33 73 34 39 33 72 35 64 74 6e 67 6b 75 71 35 30      3s493r5d tngkuq50
0260 6f 30 36 31 0d 0a 55 70 67 72 61 64 65 2d 49 6e      o061··Up grade-In
0270 73 65 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a      secure-R equests:
0280 20 31 0d 0a 0d 0a 61 63 74 3d 6c 6f 67 69 6e 26      1····ac t=login&
0290 6c 6f 67 69 6e 3d 6a 65 75 64 69 26 70 61 73 73      login=je udi&pass
02a0 77 6f 72 64 3d 6d 61 74 69 6e 26 73 75 62 6d 69      word=mat in&submi
02b0 74 3d 45 6e 76 6f 79 65 72 26 72 65 6d 65 6d 62      t=Envoye r&rememb
02c0 65 72 6d 65 3d 66 6f 72 65 76 65 72 26 72 65 64      erme=for ever&red
02d0 69 72 65 63 74 5f 74 6f 3d 25 32 46                irect to =%2F
```

...et HTTPS



- L'HyperText Transfer Protocol Secure (HTTPS, littéralement « protocole de transfert hypertextuel sécurisé ») est la combinaison du HTTP avec une couche de chiffrement TLS
- Programme NSI Terminale

| | | |
|---|---|---|
| <p>Sécurisation des communications.</p> | <p>Décrire les principes de chiffrement symétrique (clef partagée) et asymétrique (avec clef privée/clef publique). Décrire l'échange d'une clef symétrique en utilisant un protocole asymétrique pour sécuriser une communication HTTPS.</p> | <p>Les protocoles symétriques et asymétriques peuvent être illustrés en mode débranché, éventuellement avec description d'un chiffrement particulier. La négociation de la méthode de chiffrement du protocole SSL (<i>Secure Sockets Layer</i>) n'est pas abordée.</p> |
|---|---|---|



Questionnement

- Quelle remarque à propos de l'URL de ce site web ent.iledefrance.fr?
 - Le site Web utilise HTTPS et il y a un verrouSaisir `tcp.port==443` (ip.dst== « @IP di site ») comme filtre, puis cliquez sur **Apply**
Naviguer parmi les différents messages HTTPS, puis sélectionnez un message **Application Data**
- Par quoi la section HTTP précédente a-t-elle été remplacée ?
 - Après la section TCP, il y a maintenant une section Secure Sockets Layer (SSL/TLS 1.3) au lieu de HTTP.Cliquer sur **Encrypted Application Data**.
- Les données d'application sont-elles en texte clair ou dans un format lisible ?
 - Non. La charge utile des données est chiffrée à l'aide du protocole TLSv1.3 et ne peut pas être visualisée.
- Quels sont les avantages d'utiliser HTTPS plutôt que HTTP ?
 - Lors de l'utilisation de HTTPS, la charge utile de données d'un message est cryptée et ne peut être visualisée que par les appareils qui font partie de la conversation cryptée.
- Tous les sites web qui utilisent le protocole HTTPS sont-ils considérés comme sécurisés ?
 - Non, car les sites Web malveillants peuvent utiliser HTTPS pour apparaître légitimes tout en continuant à capturer les données et les connexions des utilisateurs.

tcp.port==443 && ip.dst==164.132.92.230

| No. | Time | Source | Destination | Protocol | Length | Text item | Info |
|--------|-------------|--------------|----------------|----------|--------|-----------|------------------|
| 16825 | 256.463343 | 192.168.1.86 | 164.132.92.230 | TLSv1.3 | 1345 | ✓ | Client Hello |
| 124257 | 4364.324362 | 192.168.1.86 | 164.132.92.230 | TLSv1.3 | 1245 | ✓ | Application Data |
| 63641 | 1231.580410 | 192.168.1.86 | 164.132.92.230 | TLSv1.3 | 1110 | ✓ | Application Data |
| 16846 | 256.620425 | 192.168.1.86 | 164.132.92.230 | TLSv1.3 | 1110 | ✓ | Application Data |
| 87436 | 2557.087492 | 192.168.1.86 | 164.132.92.230 | TLSv1.3 | 1081 | ✓ | Application Data |
| 479 | 16.280099 | 192.168.1.86 | 164.132.92.230 | TLSv1.3 | 1054 | ✓ | Application Data |
| 19946 | 357.949744 | 192.168.1.86 | 164.132.92.230 | TLSv1.3 | 802 | ✓ | Application Data |
| 18435 | 285.569724 | 192.168.1.86 | 164.132.92.230 | TLSv1.3 | 801 | ✓ | Application Data |
| 124247 | 4364.309942 | 192.168.1.86 | 164.132.92.230 | TLSv1.3 | 726 | ✓ | Client Hello |
| 87426 | 2557.071335 | 192.168.1.86 | 164.132.92.230 | TLSv1.3 | 726 | ✓ | Client Hello |
| 63619 | 1231.498402 | 192.168.1.86 | 164.132.92.230 | TLSv1.3 | 726 | ✓ | Client Hello |
| 469 | 16.263027 | 192.168.1.86 | 164.132.92.230 | TLSv1.3 | 726 | ✓ | Client Hello |

Démonstration avec HTTPS

```
> Frame 63641: 1110 bytes on wire (8880 bits), 1110 bytes captured (8880 bits) on interface \Device\NPF_{A4E274F3-C087-4488-9B1D-3179C1E4139A}, id 0
> Ethernet II, Src: Chongqin_14:39:f5 (1c:bf:c0:14:39:f5), Dst: FreeboxS_32:d4:fb (70:fc:8f:32:d4:fb)
> Internet Protocol Version 4, Src: 192.168.1.86, Dst: 164.132.92.230
> Transmission Control Protocol, Src Port: 53084, Dst Port: 443, Seq: 954, Ack: 5274, Len: 1056
▼ Transport Layer Security
  ▼ TLSv1.3 Record Layer: Application Data Protocol: http-over-tls
    Opaque Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 1051
    Encrypted Application Data: 1a47449f3a7f228ad4516289762a151d2b5620117b380d245def54da843b2698c84a3629...
    [Application Data Protocol: http-over-tls]
```

```
0030 01 fe b8 a5 00 00 17 03 03 04 1b 1a 47 44 9f 3a .....GD::
0040 7f 22 8a d4 51 62 89 76 2a 15 1d 2b 56 20 11 7b .."..Qb.v *..+V .{
0050 38 0d 24 5d ef 54 da 84 3b 26 98 c8 4a 36 29 14 8.$].T.. ;&..J6).
0060 54 4b 74 93 6f 7b 8b 35 b0 22 ed 4d c9 2f 28 07 Tkt.o{.5 ."M./(.
0070 12 39 c8 c8 3e b8 ad f7 b6 81 92 51 dd 54 5a 18 .9.>... ..Q.TZ.
0080 ec 07 a0 46 34 65 56 ed 53 70 d9 b3 ce e8 3e 4f ...F4eV. Sp...>0
0090 63 11 14 d3 f8 4c 3c 0e 39 ee 1c 23 a5 76 c7 15 c...L<. 9..#..v..
00a0 59 88 f3 e8 2a 89 ec 28 b8 a9 ff b7 52 56 51 d2 Y...*( ...RVQ.
00b0 09 5c f9 54 fb 01 be 2a a1 4a 83 80 6a e0 37 37 .\T...* .J..j.77
00c0 80 80 33 12 b3 f1 63 ff a1 ef d1 56 4e 86 89 cc ..3...c. ...VN...
00d0 8a 02 77 b9 1b 1e 56 de e6 93 39 e1 37 87 2f b9 ..w...V. ..9.7./.
00e0 d3 43 71 55 9a 8a 2b db e4 92 76 b5 0a fe ff f7 .CqU...+ ..v.....
00f0 a0 17 21 b9 3b cf 0b 96 f2 30 d5 41 51 9f ac d4 ..!.;... .0.AQ...
0100 72 9c bd a1 b4 b4 18 0a b8 b4 0b a0 33 b0 78 c8 r..... ..3.x.
0110 59 9f e8 28 9d 7e fe 5a 85 4f 5f 4e 3b 78 9e a9 Y..(~... .0_N;x..
0120 bd 44 a1 b0 64 a5 cf 03 2d ba e3 d3 fb bb d5 01 .D.d... ..
0130 87 5a 42 8e 12 f9 65 c4 73 f5 55 29 72 64 19 6f .ZB...e. s.U)rd.o
0140 ad c7 25 00 db cb dd 28 4c f7 9c 59 b7 6d 4b fc ..%....( L.Y.mK.
0150 8b 41 4f 5b df 0f d8 2d 96 74 28 e8 3b 28 e8 7b .AO[.... .t(;({
0160 2b 00 be 7f c3 97 c3 d3 da db 88 e8 c4 82 84 7b +..... ..{
0170 a1 34 52 df cf b4 9a 9c 9b 1a 45 06 ff 98 0f 34 .4R..... ..E....4
```

...Utilité de la segmentation

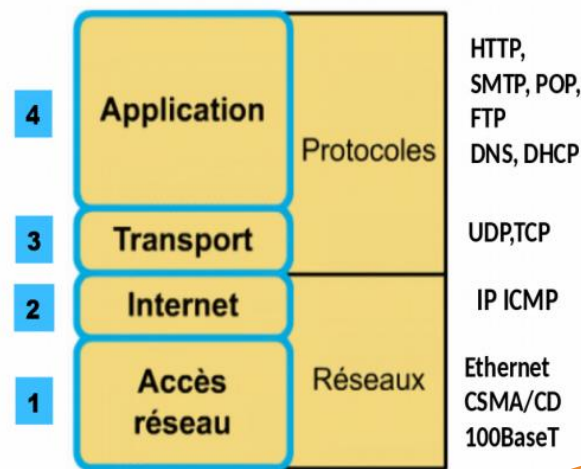
| | | |
|--|---|--|
| Transmission de données dans un réseau | Mettre en évidence l'intérêt du découpage des données en paquets et de leur encapsulation. | Le protocole peut être expliqué et simulé en mode débranché. |
| Protocoles de communication | Dérouler le fonctionnement d'un protocole simple de récupération de perte de paquets (bit alterné). | Le lien est fait avec ce qui a été vu en classe de seconde sur le protocole TCP/IP. |
| Architecture d'un réseau | Simuler ou mettre en œuvre un réseau. | Le rôle des différents constituants du réseau local de l'établissement est présenté. |

- 1. Gestion de la taille des données** : Les applications génèrent souvent des données de tailles diverses, et la segmentation permet de découper ces données en segments de taille gérable.
- 2. Fiabilité de la transmission** : La segmentation permet de réduire les risques de perte de données lors de la transmission.
- 3. Contrôle de flux** : La segmentation aide à réguler le flux de données à travers le réseau. Les segments sont envoyés et reçus à un rythme contrôlé.
- 4. Contrôle de la congestion** : La segmentation contribue à éviter la congestion du réseau en ajustant la quantité de données envoyées en fonction de l'état du réseau.
- 5. Traitement efficace des erreurs** : La segmentation permet également un traitement efficace des erreurs. En cas de problème avec un segment particulier, seuls les segments concernés doivent être renvoyés, plutôt que de devoir retransmettre l'ensemble du message, ce qui réduit la charge sur le réseau.

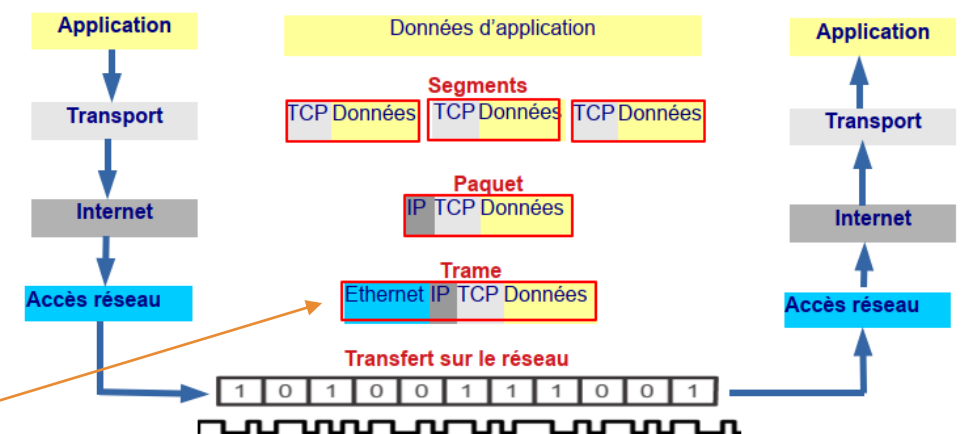
Pour résumer

La segmentation dans la couche de transport offre une méthode efficace pour gérer et contrôler la transmission des données sur un réseau, en garantissant la **fiabilité**, le **contrôle de flux** et la **résistance à la congestion** ainsi que le **traitement efficace des erreurs**, tout en optimisant l'utilisation des ressources disponibles.

Les applications génèrent souvent des données de tailles diverses, et la segmentation permet de découper ces données en segments de taille gérable.
1518 octets max par trame Ethernet

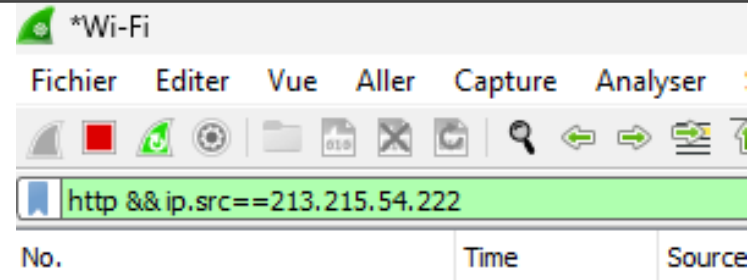


Récapitulatif : encapsulation/dés-encapsulation



Démonstration autour d'une communication HTTP fragmentée

1. Lancer la capture
2. Filtrer pour isoler les trames recherchées
3. Générer du flux avec le site (aller sur des pages riches)
4. Repérer une trame HTTP avec de la data (une image)



5. La sectionner

| No. | Time | Source |
|--------|-------------|-----------------------------------|
| 216528 | 7723.435137 | 213.215.54.222 |
| | | 192.168.1.86 |
| | | HTTP |
| | | 559 ✓ |
| | | HTTP/1.1 200 OK (JPEG JFIF image) |


```
> Frame 216528: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface \Device\NPF_{A4E274F3-C087-4488-981D-3179C1E4139A}, id 0
> Ethernet II, Src: FreeboxS_32:d4:fb (70:fc:8f:32:d4:fb), Dst: Chongqin_14:39:f5 (1c:bf:c0:14:39:f5)
> Internet Protocol Version 4, Src: 213.215.54.222, Dst: 192.168.1.86
> Transmission Control Protocol, Src Port: 80, Dst Port: 53963, Seq: 15621, Ack: 476, Len: 505
> [12 Reassembled TCP Segments (16125 bytes): #216489(1420), #216490(1420), #216492(1420), #216494(1420), #216496(1420), #216497(1420), #216499(1420), #216500(1420), #216502(1420), #216508(1420), #216527(1420), #216528(505)]
> Hypertext Transfer Protocol
> JPEG File Interchange Format
```

200 - Tout va bien, le serveur a été en mesure de satisfaire la requête (document trouvé)

Décortiquer une trame de rassemblement

```
> Frame 216528: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface \Device\NPF_{A4E274F3-C087-4488-9B1D-3179C1E4139A}, id 0
> Ethernet II, Src: FreeboxS_32:d4:fb (70:fc:8f:32:d4:fb), Dst: Chongqin_14:39:f5 (1c:bf:c0:14:39:f5)
> Internet Protocol Version 4, Src: 213.215.54.222, Dst: 192.168.1.86
> Transmission Control Protocol, Src Port: 80, Dst Port: 53963, Seq: 15621, Ack: 476, Len: 505
> [12 Reassembled TCP Segments (16125 bytes): #216489(1420), #216490(1420), #216492(1420), #216494(1420), #216496(1420), #216497(1420), #216499(1420), #216500(1420), #216502(1420), #216508(1420), #216527(1420), #216528(505)]
> Hypertext Transfer Protocol
> JPEG File Interchange Format
```

12 segments TCP ont été rassemblés au niveau applicatif pour reconstituer l'image

```
> Frame 216528: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) o
> Ethernet II, Src: FreeboxS_32:d4:fb (70:fc:8f:32:d4:fb), Dst: Chongqin_14:39:
> Internet Protocol Version 4, Src: 213.215.54.222, Dst: 192.168.1.86
> Transmission Control Protocol, Src Port: 80, Dst Port: 53963, Seq: 15621, Ack
> [12 Reassembled TCP Segments (16125 bytes): #216489(1420), #216490(1420), #21
> Hypertext Transfer Protocol
> JPEG File Interchange Format
```

```
0000 1c bf c0 14 39 f5 70 fc 8f 32 d4 fb 08 00 45 00  ...9 p 2...E
0010 02 21 cd 94 40 00 38 06 a4 8e d5 d7 36 de c0 a8  !..@.8....6...
0020 01 56 00 50 d2 cb e8 d8 6e e4 73 52 01 77 50 18  .V.P...n.sR.wP...
0030 00 7b e6 36 00 00 3d cf 07 e7 8d 41 b3 eb 75 1d  .{.6... ..A.u...
0040 e4 50 37 cd e6 14 ad 66 cc b8 9f ef 48 bf ce 0f  .P7...f...H...
0050 cf 11 3b 3a bf 51 de 45 3e f9 9c c2 b0 99 af 2c  .;:Q.E>.....
0060 f8 55 62 7f 38 3f 3c 0f e1 f7 1d 47 79 14 fb e6  .Ub-8?<...Gy...
0070 73 0b b4 cd 79 65 76 f4 ac 4f e7 37 f9 e1 be 1f  s...yev...0.7...
0080 71 d4 77 91 4b 7c ce 61 75 f2 a7 2c ff 00 6b 43  q.w.K|a u...kC
0090 fe 7b 7f 9e 1b dc 2e 3a 8e f2 29 6f 99 cc 20 84  .{.....}o...
00a0 cf 67 9c 9f eb 16 11 1b f9 b4 49 9b 20 dd 09 47  .g.....I...G
00b0 da f6 48 85 14 93 c5 53 1a 3b cb ee a1 cf fb 3f  .H...S ;.....?
00c0 8e 1c 10 62 97 3f 55 cc 4f 90 11 26 b5 25 89 f1  .-b?U.0.&.%...
00d0 c1 c6 4f 8a da f7 b4 b6 ab 5b a6 ab 2a 61 ea 3a  .0.....[...*a:
00e0 f5 ec 2d 2d 74 11 1f 2f f0 90 14 81 d7 d5 7c cb  .-t.../.....|
00f0 7d 9e b3 21 24 37 3e 38 3c 0e a4 81 54 97 b6 b4  }.!$7>8 <...T...
0100 5b f4 d5 e7 d5 30 9d 52 f9 cd c2 5a e8 88 f9 38  [. ...0.R ...Z...8
0110 79 24 05 2e 7e aa f9 54 f2 73 aa e1 3f 56 61 ee  y$. ...T s...?Va
0120 20 b8 de 97 25 21 20 03 df 38 8d a6 ae 5d 58 ac  .%!. .8...]X
0130 28 dd 08 86 11 10 72 6f 2d 25 4f 15 3e 7e aa b9  (. ...ro -X0>...>
```

Frame (559 bytes) Reassembled TCP (16125 bytes) De-chunked entity body (15728 bytes)

```
216577 7723.493071 213.215.54.222 192.168.1.86
216579 7723.496046 213.215.54.222 192.168.1.86
> Frame 216528: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface
> Ethernet II, Src: FreeboxS_32:d4:fb (70:fc:8f:32:d4:fb), Dst: Chongqin_14:39:f5 (1c:bf:c
> Internet Protocol Version 4, Src: 213.215.54.222, Dst: 192.168.1.86
> Transmission Control Protocol, Src Port: 80, Dst Port: 53963, Seq: 15621, Ack: 476, Len:
> [12 Reassembled TCP Segments (16125 bytes): #216489(1420), #216490(1420), #216492(1420),
[Frame: 216489, payload: 0-1419 (1420 bytes)]
[Frame: 216490, payload: 1420-2839 (1420 bytes)]
[Frame: 216492, payload: 2840-4259 (1420 bytes)]
[Frame: 216494, payload: 4260-5679 (1420 bytes)]
[Frame: 216496, payload: 5680-7099 (1420 bytes)]
[Frame: 216497, payload: 7100-8519 (1420 bytes)]
[Frame: 216499, payload: 8520-9939 (1420 bytes)]
[Frame: 216500, payload: 9940-11359 (1420 bytes)]
[Frame: 216502, payload: 11360-12779 (1420 bytes)]
[Frame: 216508, payload: 12780-14199 (1420 bytes)]
[Frame: 216527, payload: 14200-15619 (1420 bytes)]
[Frame: 216528, payload: 15620-16124 (505 bytes)]
[Segment count: 12]
[Reassembled TCP length: 16125]
```

```
0000 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d HTTP/1.1 200 OK
0010 0a 44 61 74 65 3a 20 57 65 64 2c 20 32 30 20 4d .Data: Wed, 20 M
```

Chaque segment correspond à une trame atteignable, Wireshark nous les indique par des liens cliquables

On fait les comptes

- > Frame 216528: 559 bytes on wire (4472 bits), 559 bytes captured
- > Ethernet II, Src: FreeboxS_32:d4:fb (70:fc:8f:32:d4:fb), Dst: C
- > Internet Protocol Version 4, Src: 213.215.54.222, Dst: 192.168.1.86
- > Transmission Control Protocol, Src Port: 80, Dst Port: 53963, Seq: 216528, Len: 559
- ✓ [12 Reassembled TCP Segments (16125 bytes): #216489(1420), #216490(1420), #216492(1420), #216494(1420), #216496(1420), #216497(1420), #216499(1420), #216500(1420), #216502(1420), #216508(1420), #216527(1420), #216528(505)]
 - [Frame: 216489, payload: 0-1419 (1420 bytes)]
 - [Frame: 216490, payload: 1420-2839 (1420 bytes)]
 - [Frame: 216492, payload: 2840-4259 (1420 bytes)]
 - [Frame: 216494, payload: 4260-5679 (1420 bytes)]
 - [Frame: 216496, payload: 5680-7099 (1420 bytes)]
 - [Frame: 216497, payload: 7100-8519 (1420 bytes)]
 - [Frame: 216499, payload: 8520-9939 (1420 bytes)]
 - [Frame: 216500, payload: 9940-11359 (1420 bytes)]
 - [Frame: 216502, payload: 11360-12779 (1420 bytes)]
 - [Frame: 216508, payload: 12780-14199 (1420 bytes)]
 - [Frame: 216527, payload: 14200-15619 (1420 bytes)]
 - [Frame: 216528, payload: 15620-16124 (505 bytes)]
- [Segment count: 12]
- [Reassembled TCP length: 16125]

| No. | Time | Source | Destination |
|--------|-------------|----------------|--------------|
| 216483 | 7723.374551 | 213.215.54.222 | 192.168.1.86 |
| 216486 | 7723.377836 | 213.215.54.222 | 192.168.1.86 |
| 216489 | 7723.380863 | 213.215.54.222 | 192.168.1.86 |
| 216490 | 7723.383847 | 213.215.54.222 | 192.168.1.86 |
| 216492 | 7723.386846 | 213.215.54.222 | 192.168.1.86 |
| 216494 | 7723.389850 | 213.215.54.222 | 192.168.1.86 |
| 216496 | 7723.392708 | 213.215.54.222 | 192.168.1.86 |
| 216497 | 7723.395792 | 213.215.54.222 | 192.168.1.86 |
| 216499 | 7723.398716 | 213.215.54.222 | 192.168.1.86 |
| 216500 | 7723.406323 | 213.215.54.222 | 192.168.1.86 |
| 216502 | 7723.406669 | 213.215.54.222 | 192.168.1.86 |
| 216508 | 7723.408303 | 213.215.54.222 | 192.168.1.86 |
| 216511 | 7723.410577 | 213.215.54.222 | 192.168.1.86 |
| 216513 | 7723.413679 | 213.215.54.222 | 192.168.1.86 |
| 216515 | 7723.416556 | 213.215.54.222 | 192.168.1.86 |
| 216517 | 7723.419892 | 213.215.54.222 | 192.168.1.86 |
| 216519 | 7723.422441 | 213.215.54.222 | 192.168.1.86 |
| 216521 | 7723.425362 | 213.215.54.222 | 192.168.1.86 |
| 216523 | 7723.428618 | 213.215.54.222 | 192.168.1.86 |
| 216527 | 7723.433483 | 213.215.54.222 | 192.168.1.86 |

- > Frame 216527: 1474 bytes on wire (11792 bits), 1474 bytes captured (11792 bits) on interface eth0
- > Ethernet II, Src: FreeboxS_32:d4:fb (70:fc:8f:32:d4:fb), Dst: Chongqin_14:39:f5
- > Internet Protocol Version 4, Src: 213.215.54.222, Dst: 192.168.1.86
- > Transmission Control Protocol, Src Port: 80, Dst Port: 53963, Seq: 14201, Ack: 53963, Len: 1474

```
0000 1c bf c0 14 39 f5 70 fc 8f 32 d4 fb 08 00 45 00  ....9 p...2...E.
0010 05 b4 cd 93 40 00 38 06 a0 fc d5 d7 36 de c0 a8  ....@ 8...6...
0020 01 56 00 50 d2 cb e8 d8 69 58 73 52 01 77 50 10  .V.P....iXsR.wP.
0030 00 7b ea 8e 00 00 de 45 51 c5 b3 7a 8d ff 00 62  .{-...E Q-z...b
0040 fc 95 40 ed 8a 7c 67 61 cd ac ba fc 67 87 4b cc  .@..|ga...g.K.
0050 3d 38 8c 08 57 c0 93 74 5c 41 de d3 50 eb 3c f8  =8.W.t \A.P.<.
0060 24 cb 8d 9e c7 62 6b 00 23 93 50 94 ec 93 35 f8  $....bk.#P...5.
0070 94 44 fe f5 7f e9 c0 3f c4 76 df dd e5 fc ab 7f  .D...?..v.....
0080 1a a1 fd de 4b 41 67 25 e5 24 55 ff 00 54 47 e5  ...KAg%.$U.TG.
0090 f3 15 5f c5 71 cc bb 6a 5c ff 00 98 e5 cf fc 42  ...q..j \.....B
00a0 bf 5c ab 29 94 b2 c0 aa 68 a4 44 b7 8f aa 1b fd  .\.....h.D.....
00b0 f8 17 c4 6e 3f cc 77 9a 8f be d6 eb bb cd 57 93  .n?..w.....W.
00c0 49 a4 31 5b a4 43 66 99 0c 59 98 b2 16 4a 77 76  .I-1[.Cf...Y...Jwv
00d0 d5 74 b2 da 28 e9 5b 6d cc 49 83 d3 b8 a8 ea 35  .t..([m.I.....5
00e0 1e 5e f9 6e 18 e9 1e 25 01 f7 95 b1 01 88 e7 da  .^n...%.....
00f0 50 fc af 58 a0 4e 06 62 bb 01 be fb ad 59 72 42  .P.X.N.b...YrB
0100 44 6c 18 27 6c 4e 80 21 22 7b 4a c8 df a6 2d 6d  .D.'lN!' "{J...m
0110 0b 4a d4 e5 c1 c7 0c 4c 62 33 19 02 7f dc 81 4a  .J.....L b3...J
0120 f9 ee c8 b9 d2 ae 8e 65 cb e0 f4 86 3d 1e 62 eb  ....e...=..b.
0130 2f b9 19 a4 18 e1 67 9c 65 c1 6c 91 a5 d9 16 ca  ./...g.e.l....
0140 63 7b d9 11 3c 76 5c 57 f8 7d 72 01 c6 20 80 7e  c{...<v\W }r...w
0150 63 90 22 73 f2 29 1b cf f5 28 4f 3c 50 b8 12 0e  c"'.s)...(O<P...
0160 23 65 ea 83 d5 be 6c 2a 30 ae 93 3c 70 6d 54 79  #e...l* 0<pmTy
0170 b5 28 22 ec 89 e1 f0 c4 db b1 eb 62 01 dc 4e 93  .("...l...b.N.
0180 9c 4e 12 79 6a a0 6e c7 6a b2 de 77 a3 93 ed c6  .N.yj.n.j.w...
0190 69 b9 2e c8 78 d4 5a 6d a6 54 b5 88 eb bb c3 bf  .i..x.Zm.T.....
01a0 cd dd a3 df ae dd 3a 60 47 64 55 00 b8 96 86 8e  ....:..GdU.....
01b0 67 4d 32 ef cc 79 ea 97 bc 37 b5 5a 9d 98 a1 c2  .gM2.y...7.Z...
01c0 9e 90 e4 9b 82 a8 28 66 f0 8a ab 41 af 57 0c 09  ....(f...A.W...
```

Changer les filtres pour afficher les trames du protocole TCP

On fait les comptes en détail

- Trame étudiée : numéro 216527
 - Charge utile vue précédemment au niveau applicatif : 1420 Octets
- Taille de la trame brute : 1474 octets
 - En-tête Ethernet : 14 octets
 - En-tête IP : 20 octets
 - En-tête TCP : 20 octets
- Des calculs simples ...
- $1420 + 14 + 20 + 14 = ?$
 - 1474

$$1420 + 20 + 20 + 14 =$$

1474

```
> Frame 216527: 1474 bytes on wire (11792 bits), 1474 bytes captured (11792 bits) on interface 0
> Ethernet II, Src: FreeboxS_32:d4:fb (70:fc:8f:32:d4:fb), Dst: Chongqin_14:39:f5 (08:00:00:14:39:f5)
> Internet Protocol Version 4, Src: 213.215.54.222, Dst: 192.168.1.86
> Transmission Control Protocol, Src Port: 80, Dst Port: 53963, Seq: 14201, Ack: 14201, Win: 0, Len: 0
```

```
> Frame 216527: 1474 bytes on wire (11792 bits), 1474 bytes captured (11792 bits) on interface 0
> Ethernet II, Src: FreeboxS_32:d4:fb (70:fc:8f:32:d4:fb), Dst: Chongqin_14:39:f5 (08:00:00:14:39:f5)
> Internet Protocol Version 4, Src: 213.215.54.222, Dst: 192.168.1.86
> Transmission Control Protocol, Src Port: 80, Dst Port: 53963, Seq: 14201, Ack: 14201, Win: 0, Len: 0
```

```
0000  1c bf c0 14 39 f5 70 fc 8f 32 d4 fb 08 00 45 00  .
0010  05 b4 cd 93 40 00 38 06 a0 fc d5 d7 36 de c0 a8  .
0020  01 56 00 50 d2 cb e8 d8 69 58 73 52 01 77 50 10  .
0030  00 7b ea 8e 00 00 de 45 51 c5 b3 7a 8d ff 00 62  .
```

```
> Frame 216527: 1474 bytes on wire (11792 bits), 1474 bytes captured (11792 bits) on interface 0
> Ethernet II, Src: FreeboxS_32:d4:fb (70:fc:8f:32:d4:fb), Dst: Chongqin_14:39:f5 (08:00:00:14:39:f5)
> Internet Protocol Version 4, Src: 213.215.54.222, Dst: 192.168.1.86
> Transmission Control Protocol, Src Port: 80, Dst Port: 53963, Seq: 14201, Ack: 14201, Win: 0, Len: 0
```

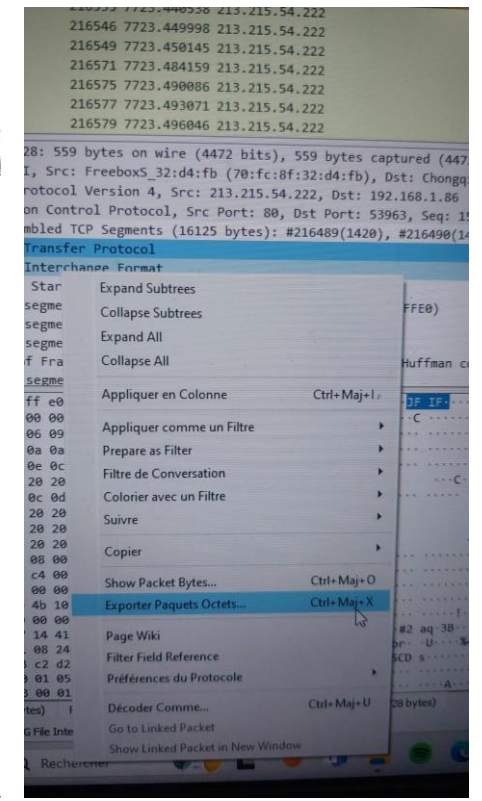
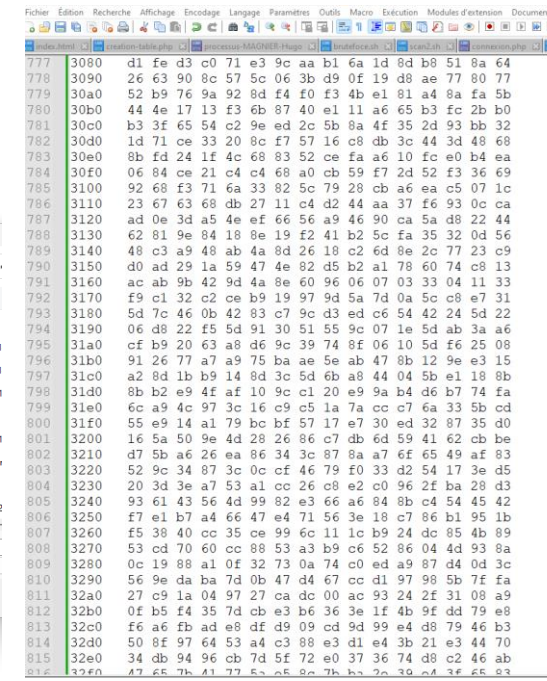
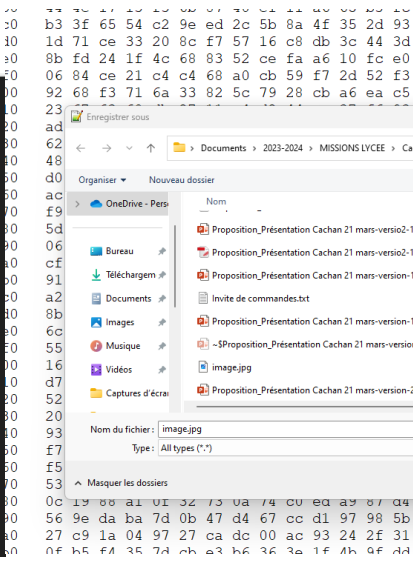
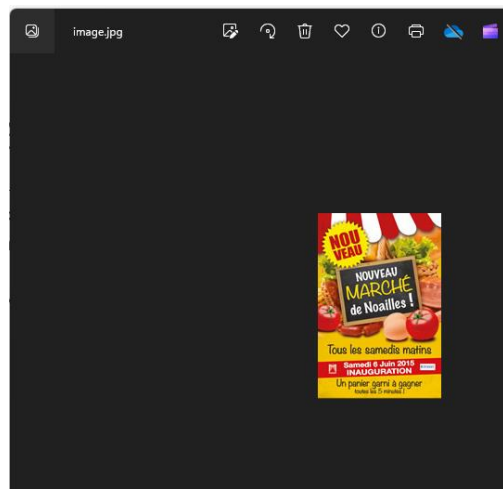
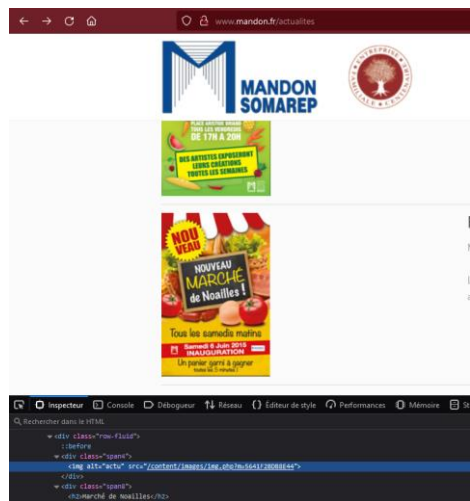
```
0020  01 56 00 50 d2 cb e8 d8 69 58 73 52 01 77 50 10  .V.P... iXsR.wP.
0030  00 7b ea 8e 00 00 de 45 51 c5 b3 7a 8d ff 00 62  .{....E Q..z...b
0040  fc 95 40 ed 8a 7c 67 61 cd ac ba fc 67 87 4b cc  .@...|ga ...g.K.
```

```
> Frame 216527: 1474 bytes on wire (11792 bits), 1474 bytes captured (11792 bits) on interface 0
> Ethernet II, Src: FreeboxS_32:d4:fb (70:fc:8f:32:d4:fb), Dst: Chongqin_14:39:f5 (08:00:00:14:39:f5)
> Internet Protocol Version 4, Src: 213.215.54.222, Dst: 192.168.1.86
> Transmission Control Protocol, Src Port: 80, Dst Port: 53963, Seq: 14201, Ack: 14201, Win: 0, Len: 0
```

```
[Bytes sent since last PUSH flag: 15620]
TCP payload (1420 bytes)
[Reassembled PDU in frame: 216528]
TCP segment data (1420 bytes)
0030  00 7b ea 8e 00 00 de 45 51 c5 b3 7a 8d ff 00 62  .{....E Q..z...b
0040  fc 95 40 ed 8a 7c 67 61 cd ac ba fc 67 87 4b cc  .@...|ga ...g.K.
0050  3d 38 8c 08 57 c0 93 74 5c 41 de d3 50 eb 3c f8  =8.W.t \A.P.<
0060  24 cb 8d 9e c7 62 6b 00 23 93 50 94 ec 93 35 f8  $....bk.#.P...5.
0070  94 44 fe f5 7f e9 c0 3f c4 76 df dd e5 fc ab 7f  .D....? .v.....
0080  1a a1 fd de 4b 41 67 25 e5 24 55 ff 00 54 47 e5  ...KAg% .$.TG.
0090  f3 15 5f c5 71 cc bb 6a 5c ff 00 98 e5 cf fc 42  ._.q..j \.....B
00a0  bf 5c ab 29 94 b2 c0 aa 68 a4 44 b7 8f aa 1b fd  .\.)....h.D....
00b0  f8 17 c4 6e 3f cc 77 9a 8f be d6 eb bb cd 57 93  ...n?.w. ....W.
00c0  49 a4 31 5b a4 43 66 99 0c 59 98 b2 16 4a 77 76  I-1[.Cf..Y...Jwv
00d0  d5 74 b2 da 28 e9 5b 6d cc 49 83 d3 b8 a8 ea 35  .t.../m .T.....5
```

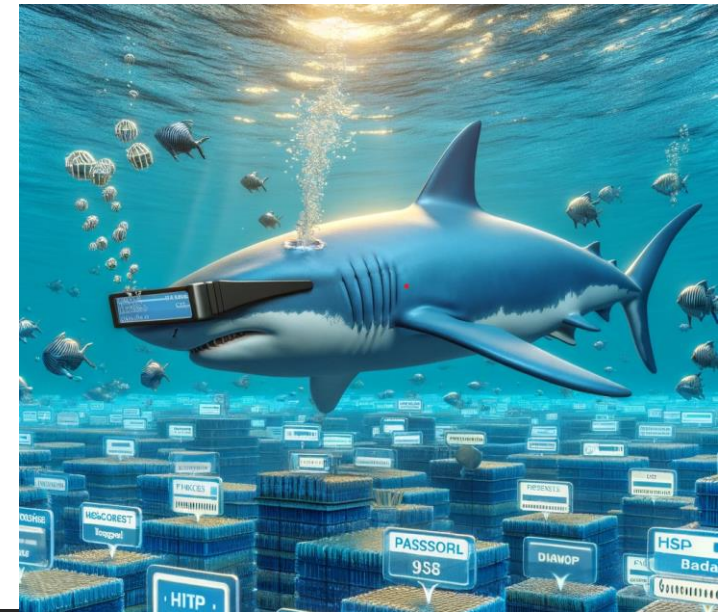
Pour aller plus loin : Reconstituer la donnée

- Exporter le paquet d'octets
- Le coller dans un éditeur hexadécimal (Notepad++)
- Enregistrer ce fichier au format image
- Essayer d'ouvrir l'image et la retrouver sur le site



Bilan

- Cette activité est adaptée à la classe de première et de terminale
 - Première : Pédagogie démonstrative
 - Terminale : pédagogie active
 - *Seconde : Thèmes Internet et Web supposés maîtrisés*
 - *Certains suivent, une première couche, pédagogie démonstrative*
 - *Des élèves de seconde de l'atelier cybersécurité reproduisent la capture*
- Prolongements possibles
 - L'importance démontrée du chiffrement : **HTTPS...**(avec le certificat)
 - *Dans le même style : Analyse d'une trame FTP, SFTP*
 - Autres protocoles réseau : Trame DHCP...



Contenu de la présentation

- Une activité réseaux *et cybersécurité* (25 mn)
 - Analyse d'une trame HTTP
 - Interception d'un mot de passe
- Prolongements possibles (5 mn)

■ Retour d'expérience

- Actions proposées aux élèves
 - Projets
 - Cybersécurité
 - Intelligence artificielle
 - Égalité
 - Découverte, Immersion, visites,
 - Rencontres, ouverture
- Infrastructure utilisée en NSI
- Filles-Garçons

Actions proposées aux élèves

Culture

Egalité
Startup
Entreprises
Cybersécurité
Intelligence Artificielle

- Culture Cybersécurité (Toutes les classes)
 - Hack@Descartes : *Un atelier nouveau?* CDSG
 - 2022-2023 : Démarrage
 - 2023-2024 : Décollage
 - Passe ton Hack d'abord :
 - 2023 : Expérience
 - 2024 : 10^{ème} et 15^{ème}
 - Rootme
- Culture IA :
 - Teens in AI (deux hackathons)
- Nouveaux projets : élèves de SNT et NSI
 - Réseau de capteurs environnementaux,
 - Python, Web, accès distant, données météo

Nombreuses actions

- Découverte des métiers de l'informatique
- Immersion en écoles Post Lycée
- Visite d'entreprises
- Rencontres avec des Rôles Modèles
- **Ouverture bidirectionnelle sur l'extérieur**
- **L'importance du réseau**
- **Marketing pédagogique**

Actions proposées aux élèves

Projets

Egalité
Startup
Entreprises
Cybersécurité
Intelligence Artificielle

- VoteToMusic
 - Playlist collaborative
- Startups@Descartes (Incubateurs Agoranov, Willa)
 - 2021 : Startup Jexplore - Mon métier n'existe pas encore, Imaginer les [métiers à Horizon 2050](#).
 - 2022 : Startup Equilys - Egalité professionnelle. Outils d'aide à l'[écriture inclusive](#) d'offres d'emploi
 - 2023 : Startup Tackle - Outil de sensibilisation et de lutte contre Les [RPS](#) (milieu scolaire et entreprise)

Retour d'expérience

Vers une mixité ?

- Bac 2021
 - 16 élèves
 - 12,5% de filles (2F+14G)
 - Bac 2022
 - 17 élèves
 - 17,6% de filles (3F+14G)
 - Bac 2023
 - 22,3% de filles (4F+14G)
 - Bac 2024
 - 22,3% de filles (4F+14G)
 - Conjecture : Asymptote 25 % ?
- Bac 2021
 - Mathématiques (+MathExp)
 - 3 ES, 1 HGGSP
 - Bac 2022
 - Mathématiques (+MathExp)
 - 2 ES, 1 HGGSP, LLCER
 - Bac 2023
 - Mathématiques (+MathExp)
 - 1 ES, 1 HGGSP, 1 LLCER
 - Bac 2024
 - Mathématiques (+MathExp)
 - 1 ES, 1 LLCER
 - Conjecture : duo Mathématiques – NSI ?

Retour d'expérience

Outils et moyens utilisés

- Premières NSI
 - 2 chariots mobiles : 32 ordinateurs portables (reformatées Linux)
 - Dotation région pour NSI
- Terminales NSI
 - 20 ordinateurs portables prêtés à l'année aux terminales (Gagné dans un le prix régional Lycée'Up)
 - Reformatés Linux chaque année par les élèves (Clé USB, Bios-UEFI, ISO ubuntu...)
- Contact continu avec les élèves
 - ENT, Google forms, strawpoll, Whatsapp ...
 - Association des anciens élèves du lycée créée grâce aux élèves de NSI 2021
- Marketing Pédagogique

Merci

Temps d'échange

