Harcèlement à Nitroba

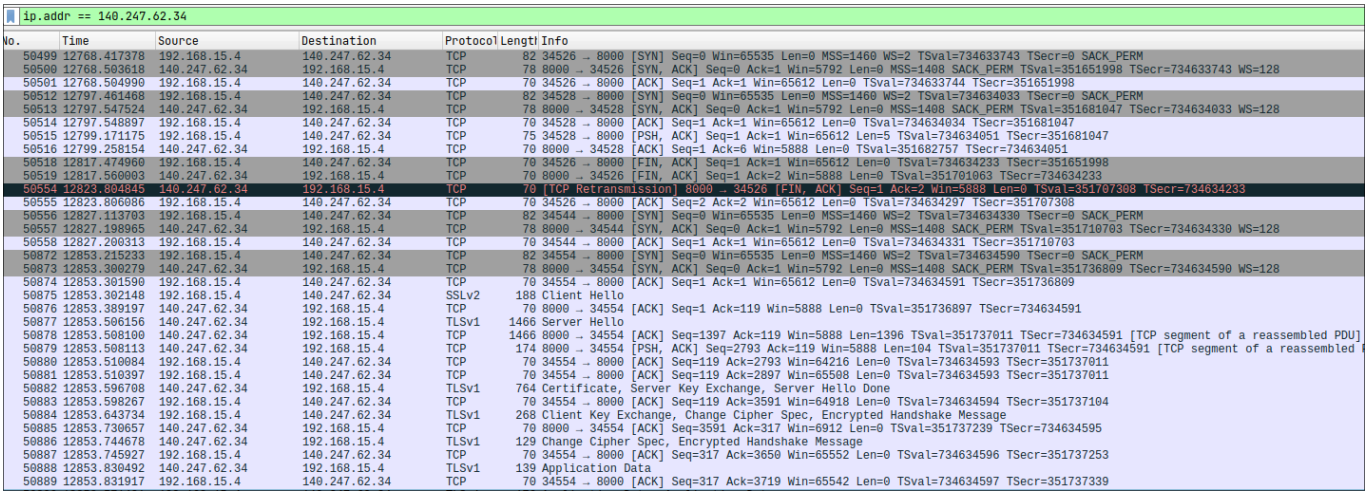
L'objectif de ce TP est de trouver qui envoie des mails offensif à l'enseignante Lily Tuckrige.

Afin de résoudre ce problème je vais suivre les étapes suivantes:

1. Établir la carte du réseau de la chambre des étudiants à Nitroba.
2. Trouver qui a envoyer le mail à lilytuckrige@yahoo.com
3. Identifier l'autre connexion TCP qui appartient à l'attaquant.
4. Trouver des informations dans l'une de ces connexions TCP afin d'identifier l'attaquant.

1. Établir la carte du réseau de la chambre des étudiants à Nitroba

On verifie avec l'IP trouver dans l'en-tête du mail Yahoo dans quels trame elle apparait:



ip.addr == 140.247.62.34

No.	Time	Source	Destination	Protocol	Length	Info
50499	12768.417378	192.168.15.4	140.247.62.34	TCP	82	34526 → 8000 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2 TSval=734633743 TSecr=0 SACK_PERM
50500	12768.503618	140.247.62.34	192.168.15.4	TCP	78	8000 → 34526 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1408 SACK_PERM TSval=351651998 TSecr=734633743 WS=128
50501	12768.504990	192.168.15.4	140.247.62.34	TCP	70	34526 → 8000 [ACK] Seq=1 Ack=1 Win=65612 Len=0 TSval=734633744 TSecr=351651998
50512	12797.461468	192.168.15.4	140.247.62.34	TCP	82	34528 → 8000 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2 TSval=734634033 TSecr=0 SACK_PERM
50513	12797.547524	140.247.62.34	192.168.15.4	TCP	78	8000 → 34528 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1408 SACK_PERM TSval=351681047 TSecr=734634033 WS=128
50514	12797.548897	192.168.15.4	140.247.62.34	TCP	70	34528 → 8000 [ACK] Seq=1 Ack=1 Win=65612 Len=0 TSval=734634034 TSecr=351681047
50515	12799.171175	192.168.15.4	140.247.62.34	TCP	75	34528 → 8000 [PSH, ACK] Seq=1 Ack=1 Win=65612 Len=5 TSval=734634051 TSecr=351681047
50516	12799.258154	140.247.62.34	192.168.15.4	TCP	70	8000 → 34528 [ACK] Seq=1 Ack=6 Win=5888 Len=0 TSval=351682757 TSecr=734634051
50518	12817.474960	192.168.15.4	140.247.62.34	TCP	70	34526 → 8000 [FIN, ACK] Seq=1 Ack=1 Win=65612 Len=0 TSval=734634233 TSecr=351651998
50519	12817.560003	140.247.62.34	192.168.15.4	TCP	70	8000 → 34526 [FIN, ACK] Seq=1 Ack=2 Win=5888 Len=0 TSval=351701063 TSecr=734634233
50554	12823.804845	140.247.62.34	192.168.15.4	TCP	70	[TCP Retransmission] 8000 → 34526 [FIN, ACK] Seq=1 Ack=2 Win=5888 Len=0 TSval=351707308 TSecr=734634233
50555	12823.806086	192.168.15.4	140.247.62.34	TCP	70	34526 → 8000 [ACK] Seq=2 Ack=2 Win=65612 Len=0 TSval=734634297 TSecr=351707308
50556	12827.113703	192.168.15.4	140.247.62.34	TCP	82	34544 → 8000 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2 TSval=734634330 TSecr=0 SACK_PERM
50557	12827.198965	140.247.62.34	192.168.15.4	TCP	78	8000 → 34544 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1408 SACK_PERM TSval=351710703 TSecr=734634330 WS=128
50558	12827.200313	192.168.15.4	140.247.62.34	TCP	70	34544 → 8000 [ACK] Seq=1 Ack=1 Win=65612 Len=0 TSval=734634331 TSecr=351710703
50872	12853.215233	192.168.15.4	140.247.62.34	TCP	82	34554 → 8000 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2 TSval=734634590 TSecr=0 SACK_PERM
50873	12853.300279	140.247.62.34	192.168.15.4	TCP	78	8000 → 34554 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1408 SACK_PERM TSval=351736809 TSecr=734634590 WS=128
50874	12853.301590	192.168.15.4	140.247.62.34	TCP	70	34554 → 8000 [ACK] Seq=1 Ack=1 Win=65612 Len=0 TSval=734634591 TSecr=351736809
50875	12853.302148	192.168.15.4	140.247.62.34	SSLv2	188	Client Hello
50876	12853.389197	140.247.62.34	192.168.15.4	TCP	70	8000 → 34554 [ACK] Seq=1 Ack=119 Win=5888 Len=0 TSval=351736897 TSecr=734634591
50877	12853.506156	140.247.62.34	192.168.15.4	TLSv1	1466	Server Hello
50878	12853.508100	140.247.62.34	192.168.15.4	TCP	1466	8000 → 34554 [ACK] Seq=1397 Ack=119 Win=5888 Len=1396 TSval=351737011 TSecr=734634591 [TCP segment of a reassembled PDU]
50879	12853.508113	140.247.62.34	192.168.15.4	TCP	174	8000 → 34554 [PSH, ACK] Seq=2793 Ack=119 Win=5888 Len=104 TSval=351737011 TSecr=734634591 [TCP segment of a reassembled
50880	12853.510084	192.168.15.4	140.247.62.34	TCP	70	34554 → 8000 [ACK] Seq=119 Ack=2793 Win=64216 Len=0 TSval=734634593 TSecr=351737011
50881	12853.510397	192.168.15.4	140.247.62.34	TCP	70	34554 → 8000 [ACK] Seq=119 Ack=2897 Win=65508 Len=0 TSval=734634593 TSecr=351737011
50882	12853.596708	140.247.62.34	192.168.15.4	TLSv1	764	Certificate, Server Key Exchange, Server Hello Done
50883	12853.598267	192.168.15.4	140.247.62.34	TCP	70	34554 → 8000 [ACK] Seq=119 Ack=3591 Win=64918 Len=0 TSval=734634594 TSecr=351737104
50884	12853.643734	192.168.15.4	140.247.62.34	TLSv1	268	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
50885	12853.730657	140.247.62.34	192.168.15.4	TCP	70	8000 → 34554 [ACK] Seq=3591 Ack=317 Win=6912 Len=0 TSval=351737239 TSecr=734634595
50886	12853.744678	140.247.62.34	192.168.15.4	TLSv1	129	Change Cipher Spec, Encrypted Handshake Message
50887	12853.745927	192.168.15.4	140.247.62.34	TCP	70	34554 → 8000 [ACK] Seq=317 Ack=3650 Win=65552 Len=0 TSval=734634596 TSecr=351737253
50888	12853.830492	140.247.62.34	192.168.15.4	TLSv1	139	Application Data
50889	12853.831917	192.168.15.4	140.247.62.34	TCP	70	34554 → 8000 [ACK] Seq=317 Ack=3719 Win=65542 Len=0 TSval=734634597 TSecr=351737339

On remarque que cette IP n'apparait que dans des échanges avec l'IP local 192.168.15.4 qui est surement l'IP local de l'attaquant.

On peut vérifier dans l'onglet Statistiques > Point de terminaisons toutes les adresses IP qui apparaissent dans cette capture avec le nombre de paquets qu'elles ont envoyés:

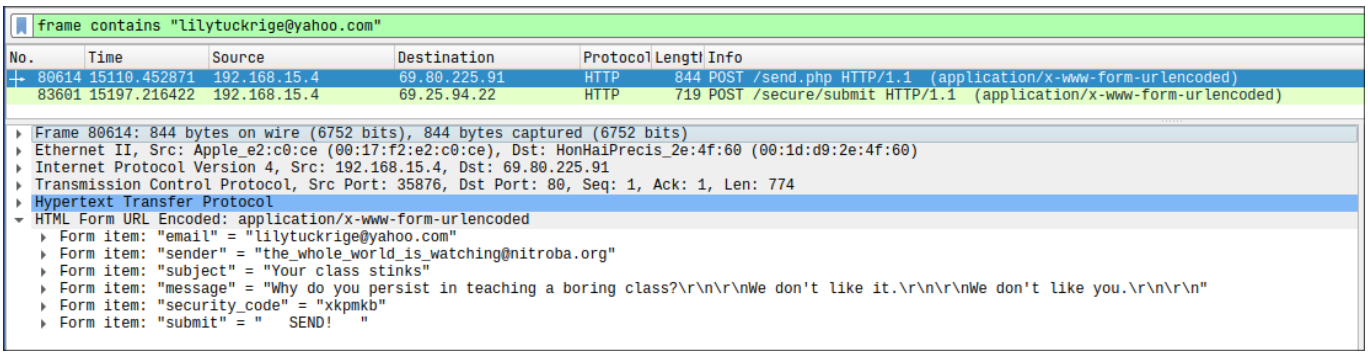
Ethernet · 17 | IPv4 · 443 | IPv6

Adresse	Paquets	Octets
192.168.15.1	2 154	795 ko
192.168.15.2	6	536 octets
192.168.15.4	73 197	45 Mo
192.168.15.5	14	2 ko
192.168.15.7	3	192 octets
192.168.15.8	6	600 octets
192.168.15.255	1	70 octets

Il y a donc 5 machines connectés sur le réseau (192.168.15.1 est la gateway) mais on remarque que l'IP trouvé précedemment à envoyé beaucoup plus de paquets que les autres (73 197).

2. Trouver qui a envoyer le mail à lilytuckrige@yahoo.com

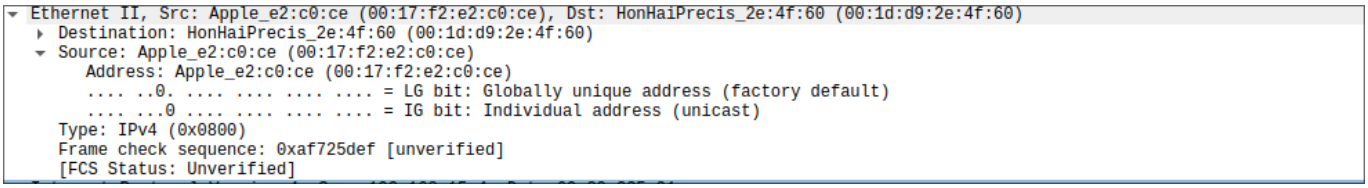
On vient chercher dans les flux http qui à envoyé un mail à Lily pour ce faire j'utilise le filtre `frame contains "lilytuckrige@yahoo.com"` pour trouver dans les flux http l'email correspondant.



On trouve bien un mail, provenant de l'IP 192.168.15.4 comme trouvé ci-dessus. On peut voir dans le champ "HTML Form URL Encoded" l'email d'envoie qui est: `the_whole_world_is_watching@nitroba.org`

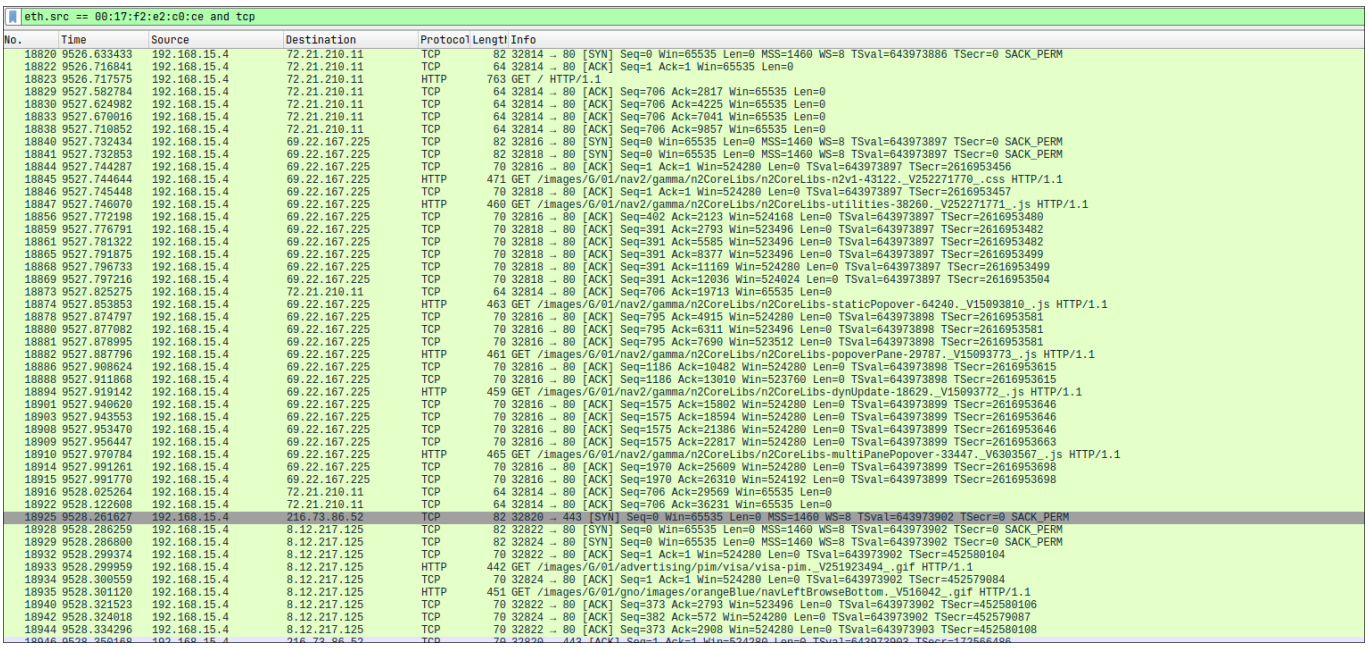
Cet email ne nous aide pas beaucoup car il ne nous donne pas de réel identité sur l'attaquant.

En revanche, j'ai pu trouver des informations sur l'adresse MAC de l'attaquant dans l'en-tête ethernet.

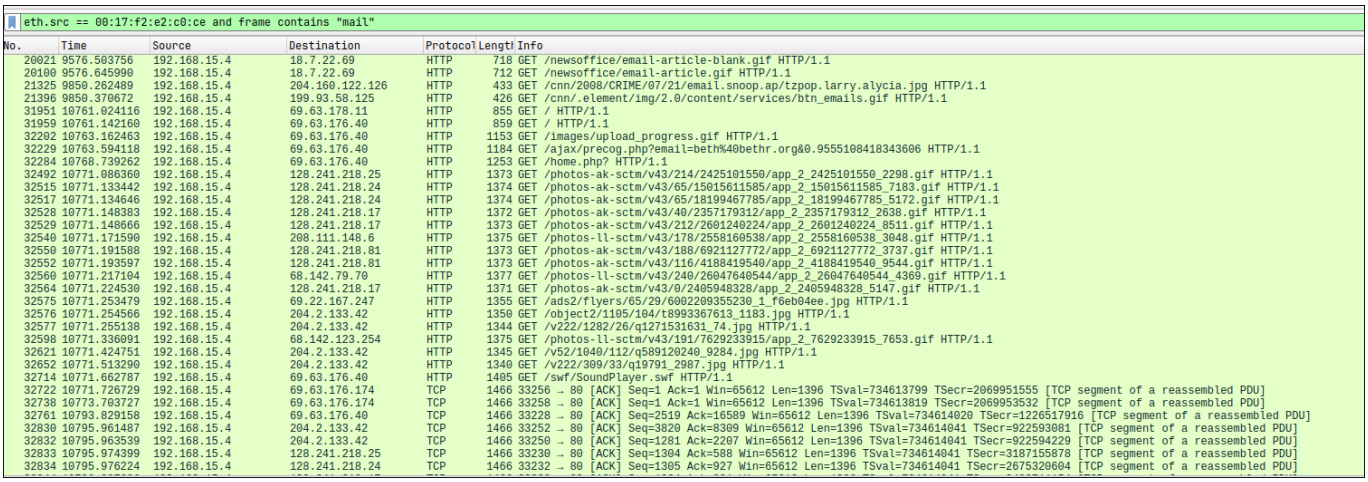


L'adresse MAC de l'attaquant est 00:17:f2:e2:c0:ce, c'est une machine Apple qui est utilisé.

3. Identifier l'autre connexion TCP qui appartient à l'attaquant



L'attaquant a de nombreuses connexions TCP qui lui appartiennent cependant on peut rechercher uniquement celles qui sont relatives à des mails avec le filtre suivant: `frame contains "mail"`

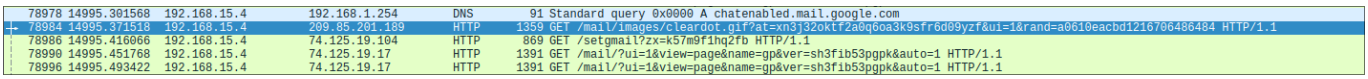


Il y a encore beaucoup de connexions TCP contenant du mail dans de l'HTTP.

4. Trouver des informations dans l'une de ces connexions TCP afin d'identifier l'attaquant

En naviguant dans les connexions HTTP, je remarque également les requêtes DNS passé par l'attaquant et particulièrement une requête vers **mail.google.com** relative à l'utilisation de gmail.

Je vois de nombreux échanges suite à la requête DNS, mais je remarque avec le nombre important de requête sur "mail/html/load.html" qu'il s'agit de la page de chargement de gmail (avant d'arriver sur la boite mail), je n'ai pas trouvé de formulaire de connexion dans les trames suivantes. Cela peut signifier que l'utilisateur est deja connecté, il y a peut-être son adresse email stocké dans un cookie. Je continue de descendre dans les trames et je remarque une autre requêtes DNS vers les serveurs de mail de google mais cette fois-ci sur **chatenabled.mail.google.com** je penses que c'est la requête envoyé une fois le chargement terminé.



En analysant le flux HTTP des trames suivant la requête DNS, je trouve un cookie nommé **gmailchat** qui contient une adresse mail:

L'adresse email est: jcoachj@gmail.com

On regardant la liste des élèves fournie, un élève semble correspondre à cet email.

```
Chemistry 109 class list:

Teacher: Lily Tuckrige

Students:
    Amy Smith
    Burt Greedom
    Tuck Gorge
    Ava Book
    Johnny Coach
    Jeremy Ledvkin
    Nancy Colburne
    Tamara Perkins
    Esther Pringle
    Asar Misrad
    Jenny Kant
```

L'étudiant qui a envoyé tout ces mails à Lily Tuckrige est **Johnny Coach** dont l'email est jcoachj@gmail.com.