TP4

# Accès distant aux boîtes aux lettres avec IMAP

Liste des commandes IMAP : <https://tools.ietf.org/html/rfc3501>

Format d’une commande IMAP : . COMMAND paramètres

* créer une connexion interactive sécurisée avec le serveur IMAP : openssl s\_client -connect webmail.grenoble-inp.org:993
* se connecter sur sa boite mail : . LOGIN prenom.nom@grenoble-inp.org mdp
* se déconnecter : . LOGOUT
* nombre de messages dans la boite mail (nb de récents, de non-vus, …) : . SELECT inbox
* lire le contenu d’un message : . FETCH numero\_du\_mail BODY[TEXT] (Attention le mail numéro 1 est le plus ancien)
* lire l’entête d’un message : . FETCH numero\_du\_mail BODY[HEADER]
* supprimer un mail : . STORE numero\_du\_mail +FLAGS (\Deleted) (Attention à bien avoir fait toutes les commandes avant !)

Cette commande supprime de la boîte mais pas du serveur.

Pour supprimer du serveur : . CLOSE (supprime tous les messages avec le flag \Deleted)

* créer un dossier : . CREATE nom\_du\_dossier
* déplacer un message dans un dossier : . COPY numero\_du\_mail nom\_du\_dossier
* se “mettre” dans un dossier : . SELECT nom\_du\_dossier
* marquer un mail comme lu : . STORE numero\_du\_mail +FLAGS (\Seen) (Attention à bien être dans le dossier dans lequel se trouve le mail pour lui mettre le flag Seen)

# Transfert de courrier électronique avec SMTP

Liste des commandes SMTP : <https://tools.ietf.org/html/rfc2821>

Open classroom : <https://openclassrooms.com/courses/comprendre-la-messagerie-electronique/envoyer-un-mail-avec-smtp>

* Trouvez les serveurs de messagerie associés au nom de domaine grenoble-inp.org en utilisant une requête DNS : dig MX grenoble-inp.org
* Port par défaut qu’utilise un serveur SMTP : 25
* Créer une connexion interactive non sécurisée entre sa machine et un des serveurs de messagerie de grenoble-inp.org : telnet adresse\_ip\_hote 25 (l’adresse\_ip\_hote a été prise dans une de celles de la réponse à la requête précédente / 25 est le numéro du port)
* Saluer le serveur : helo nom\_serveur (Attention helo avec un seul L ! / le nom du serveur est obtenu dans la requête précédente)
* Envoyer un mail :
  + MAIL FROM:<[james.bond@grenoble-inp.org](mailto:james.bond@grenoble-inp.org)>
  + RCPT TO:<[nom.prenom@grenoble-inp.org](mailto:nom.prenom@grenoble-inp.org)>
  + DATA

Subject: objet\_du\_mail (cette ligne est optionnelle, si on ne la complète pas, on envoie juste un mail sans objet)

contenu du message

* + . (le “.” indique la fin du contenu du message)
  + QUIT
* Avec une capture Wireshark on remarque que la communication n’est pas du tout sécurisée car tout est visible dans les paquets Wireshark
* Pour ouvrir une session sécurisée : openssl s\_client -starttls smtp -connect adress\_ip\_hote:numero\_du\_port puis reprendre la procédure helo, etc
* STRATTLS : 3 requêtes non chiffrées dont “helo”, ne fonctionne pas avec grenoble-inp.org car certificat nécessaire

*→ openssl s\_client -starttls smtp -connect <hôte>:<port>*

# Sécurisation des échanges de bout en bout avec S/MIME

* Obtention d’un trousseau de clés : suivre la procédure décrite dans la partie 1.3.1 du sujet (Attention : pour sauvegarder le certificat il faut faire Backup si vous êtes en anglais sur votre ordi :p)
* Mise en place des certificats utilisateur et échanges sécurisés :
  + Pour importer le trousseau dans ThunderBird : aller dans ThunderBird, clic droit sur la messagerie, puis paramètres....