

# **Laboratoire de Technologies de e-commerce et mobile**

Application Mail Agent

Groupe B32: Cyril RUSSE

# 1 Introduction

Projet pour maîtriser les concepts et techniques de messagerie électronique.

Ce projet est censé simuler la communication entre un client et un fournisseur. Mon projet permet donc l'envoi de mail depuis une adresse gmail avec un mot de passe d'application. Dans mon cas, ce sera donc depuis l'adresse `cyril.russe@gmail.com` j'ai moyen de définir dans mon code l'adresse de l'expéditeur dont on veut recevoir des mails dans la mailbox.

L'application est une interface graphique en JavaFX constituée d'un système de 2 pages. La première correspondant à la gestion d'input pour envoyer un mail avec une pièce jointe type fichier classique (pdf/txt/...) et une image. La seconde permet de lister les mails dans la boîte de réception dont l'expéditeur est l'adresse définie comme "fournisseur". Il est ensuite possible d'afficher le contenu des mails et les en-têtes.

## 2 Analyse des échanges réseaux avec Wireshark

### 2.1 Envoi email

On peut observer sur la figure ci-dessous l'utilisation du protocole TCP, SMTP et TLS. TCP prouve l'utilisation d'une connexion entre client/serveur. On observe la technique habituelle de connexion correspondant à une demande de connexion, suivi d'un acknowledgement du serveur et enfin un autre ACK en réponse au serveur du client. SMTP correspond également au protocole utilisé pour l'envoi de message. Et on a bien sur TLS qui est un protocole requis pour SMTP qui correspond au port qu'on utilise : 587. Dans le détail des échanges, on perçoit aussi la demande d'accès au serveur `smtp.gmail.com`.

No.	Time	Source	Destination	Protocol	Length	Info
2126	12.611700	10.222.12.69	142.251.5.108	TCP	66	64204 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2127	12.637836	142.251.5.108	10.222.12.69	TCP	66	587 → 64204 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1386 SACK_PERM WS=256
2128	12.637942	10.222.12.69	142.251.5.108	TCP	54	64204 → 587 [ACK] Seq=1 Ack=1 Win=131584 Len=0
2288	13.741152	142.251.5.108	10.222.12.69	SMTP	140	S: 220 smtp.gmail.com ESMTP g38-20020a05600c4ca600b004078d71be9csm1488492wmp.13 - gsmt
2294	13.781674	10.222.12.69	142.251.5.108	TCP	54	64204 → 587 [ACK] Seq=1 Ack=87 Win=131584 Len=0
3130	18.272610	10.222.12.69	142.251.5.108	SMTP	76	C: EHLO DESKTOP-8NBCOHO
3131	18.301668	142.251.5.108	10.222.12.69	TCP	56	587 → 64204 [ACK] Seq=87 Ack=23 Win=65536 Len=0
3132	18.303572	142.251.5.108	10.222.12.69	SMTP	225	S: 250-smtp.gmail.com at your service, [193.190.123.168]   SIZE 35882577   8BITMIME   ST
3133	18.304002	10.222.12.69	142.251.5.108	SMTP	64	C: STARTTLS
3148	18.333638	142.251.5.108	10.222.12.69	SMTP	84	S: 220 2.0.0 Ready to start TLS
3149	18.337635	10.222.12.69	142.251.5.108	TLSv1.3	807	Client Hello
3150	18.368124	142.251.5.108	10.222.12.69	TLSv1.3	273	Server Hello, Change Cipher Spec, Application Data
3151	18.369402	10.222.12.69	142.251.5.108	TLSv1.3	60	Change Cipher Spec
3152	18.399179	142.251.5.108	10.222.12.69	TCP	56	587 → 64204 [ACK] Seq=507 Ack=792 Win=67072 Len=0
3153	18.399221	10.222.12.69	142.251.5.108	TLSv1.3	204	Application Data, Application Data
3154	18.424187	142.251.5.108	10.222.12.69	TCP	56	587 → 64204 [ACK] Seq=507 Ack=942 Win=68608 Len=0
3155	18.424187	142.251.5.108	10.222.12.69	TLSv1.3	844	Application Data, Application Data
3156	18.425216	10.222.12.69	142.251.5.108	TLSv1.3	104	Application Data
3182	18.449921	142.251.5.108	10.222.12.69	TLSv1.3	94	Application Data

> Frame 2126: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF\_{A6C8BE7...}

> Ethernet II, Src: IntelCor\_9d:f8:b9 (e4:42:a6:9d:f8:b9), Dst: Fortinet\_09:00:20 (00:09:0f:09:00:20)

> Internet Protocol Version 4, Src: 10.222.12.69, Dst: 142.251.5.108

> Transmission Control Protocol, Src Port: 64204, Dst Port: 587, Seq: 0, Len: 0

0000	00 09 0f 09 00 20 e4 42	a6 9d f8 b9 08 00 45 00	...
0010	00 34 02 29 40 00 80 06	4d 11 0a de 0c 45 8e fb	...
0020	05 6c fa cc 02 4b 99 09	9c 66 00 00 00 00 02	...
0030	fa f0 96 0d 00 00 02 04	05 b4 01 03 03 08 01 01	...
0040	04 02		...

Figure 1: Screenshot des échanges dans wireshark sur le port 587

## 2.2 Reception mails correspondant à une demande imap

De même que pour l'envoi, on utilise le protocole TCP et TLS. Et on peut entrevoir l'interrogation du seueur imap.gmail.com .

tcp.port == 993					
Time	Source	Destination	Protocol	Length	Info
2078 11.421798	10.222.12.69	142.250.27.108	TCP	66	64147 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2079 11.440311	142.250.27.108	10.222.12.69	TCP	66	993 → 64147 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1386 SACK_PERM WS=256
2080 11.440394	10.222.12.69	142.250.27.108	TCP	54	64147 → 993 [ACK] Seq=1 Ack=1 Win=131584 Len=0
2210 12.094868	10.222.12.69	142.250.27.108	TLSv1.3	505	Client Hello
2211 12.114537	142.250.27.108	10.222.12.69	TCP	56	993 → 64147 [ACK] Seq=1 Ack=452 Win=66816 Len=0
2212 12.114537	142.250.27.108	10.222.12.69	TLSv1.3	1448	Server Hello, Change Cipher Spec
2213 12.114537	142.250.27.108	10.222.12.69	TCP	1448	993 → 64147 [PSH, ACK] Seq=1387 Ack=452 Win=66816 Len=1386 [TCP segment of a reassembled PDU]
2214 12.114537	142.250.27.108	10.222.12.69	TCP	1448	993 → 64147 [ACK] Seq=2773 Ack=452 Win=66816 Len=1386 [TCP segment of a reassembled PDU]
2215 12.114537	142.250.27.108	10.222.12.69	TLSv1.3	191	Application Data
2216 12.114622	10.222.12.69	142.250.27.108	TCP	54	64147 → 993 [ACK] Seq=452 Ack=4296 Win=131584 Len=0
2217 12.132751	10.222.12.69	142.250.27.108	TLSv1.3	60	Change Cipher Spec
2218 12.157538	142.250.27.108	10.222.12.69	TCP	56	993 → 64147 [ACK] Seq=4296 Ack=458 Win=66816 Len=0
2275 12.306796	10.222.12.69	142.250.27.108	TLSv1.3	144	Application Data
2276 12.325626	142.250.27.108	10.222.12.69	TCP	56	993 → 64147 [ACK] Seq=4296 Ack=548 Win=66816 Len=0
2277 12.328919	142.250.27.108	10.222.12.69	TLSv1.3	689	Application Data, Application Data
2278 12.334255	10.222.12.69	142.250.27.108	TLSv1.3	107	Application Data
2279 12.355999	142.250.27.108	10.222.12.69	TLSv1.3	282	Application Data
2280 12.363281	10.222.12.69	142.250.27.108	TLSv1.3	115	Application Data
2281 12.385223	142.250.27.108	10.222.12.69	TLSv1.3	80	Application Data

Version: TLS 1.2 (0x0303)  
Random: 527cec14c96f51e8b7728e26c6428c2742c2184d3c62aabfa64e5c3b9596960a  
Session ID Length: 32  
Session ID: 3bb2db1dd1c0099404133952fa7b7da912b96a90caf695d2c01bdd540c7a0828  
Cipher Suites Length: 74  
Cipher Suites (37 suites)  
Compression Methods Length: 1  
Compression Methods (1 method)  
Extensions Length: 295  
Extensions: server\_name (len=19)  
Type: server\_name (0)  
Length: 19  
Server Name Indication extension  
Server Name list length: 17  
Server Name Type: host\_name (0)  
Server Name length: 14  
Server Name: imap.gmail.com  
Extension: status\_request (len=5)  
Type: status\_request (5)

00a0 c0 24 c0 28 c0 23 c0 27 00 6b 00 6a 00 67 00 40 -\$(#.' k j g @  
00b0 c0 0a c0 14 c0 09 c0 13 00 39 00 38 00 33 00 32 ..... 9 8 3 2  
00c0 00 9d 00 9c 00 3d 00 3c 00 35 00 2f 00 ff 01 00 .....< 5 / .....  
00d0 01 27 00 00 00 13 00 11 00 00 0e 69 6d 61 70 2e .....imap.  
00e0 67 6d 61 69 6c 2e 63 6f 6d 00 05 00 05 01 00 00 .....gmail.co m .....  
00f0 00 00 00 0a 00 16 00 14 00 1d 00 17 00 18 00 19 .....  
0100 00 1e 01 00 01 01 01 02 01 03 01 04 00 0b 00 02 .....  
0110 01 00 00 11 00 09 00 07 02 00 04 00 00 00 00 00 .....# .....& \$ .....  
0120 17 00 00 00 23 00 00 00 0d 00 26 00 24 04 03 05 .....  
0130 03 06 03 08 07 08 08 08 04 08 05 08 06 08 09 08 .....  
0140 0a 08 0b 04 01 05 01 06 01 04 02 03 02 01 02 .....  
0150 02 00 2b 00 05 04 03 04 03 03 00 2d 00 02 01 01 .....+ .....  
0160 00 32 00 26 00 24 04 03 05 03 06 03 08 07 08 08 .....2 & \$ .....  
0170 08 04 08 05 08 06 08 09 08 0a 08 0b 04 01 05 01 .....  
0180 06 01 04 02 02 03 02 01 02 02 00 33 00 6b 00 69 .....: 3 k i  
0190 00 1d 00 20 37 96 9b 28 0b 8a 60 b5 c9 eb 78 cd .....7 ( ' ' ' ' x  
01a0 9f 4c f9 18 63 60 0e fb ee 95 e5 67 26 85 63 08 .....L ' ' ' ' ' g & c  
01b0 73 4b 6b 0b 00 17 00 41 04 47 89 e6 03 fc ae f8 .....sKk .....A iG .....  
01c0 ca c0 89 42 b2 a2 32 58 e0 44 cd 99 a2 da 4f f5 .....B . 2X .D . . . . 0  
01d0 16 25 99 2a f8 98 f0 0a a8 8e 3f a7 24 8e 5b fe .....% . . . . . ? \$ . [ .  
01e0 50 3a 40 cf 19 88 e1 01 40 cc ee 9b 95 5a b7 cd .....@ .....@ .....Z .

Figure 2: Screenshot des échanges dans wireshark sur le port 993