

Triển khai giao thức POP3, SMTP

Họ tên: Nguyễn Văn Mạnh

Lớp: AT12C

Email: nguyenmanh0397@gmail.com

Nội dung bài thực hành

- I. Mô hình mạng
- II. Cài đặt môi trường
- III. Thực hành gửi, nhận mail với pop3 và smtp không mã hóa. Chặn bắt gói tin.
- IV. Thực hành gửi, nhận mail với pop3 và smtp dùng ssl/tls để mã hóa. Chặn bắt gói tin.

I. Mô hình mạng

Windows7



10.1.65.100

Mailserver(windowserver2012)

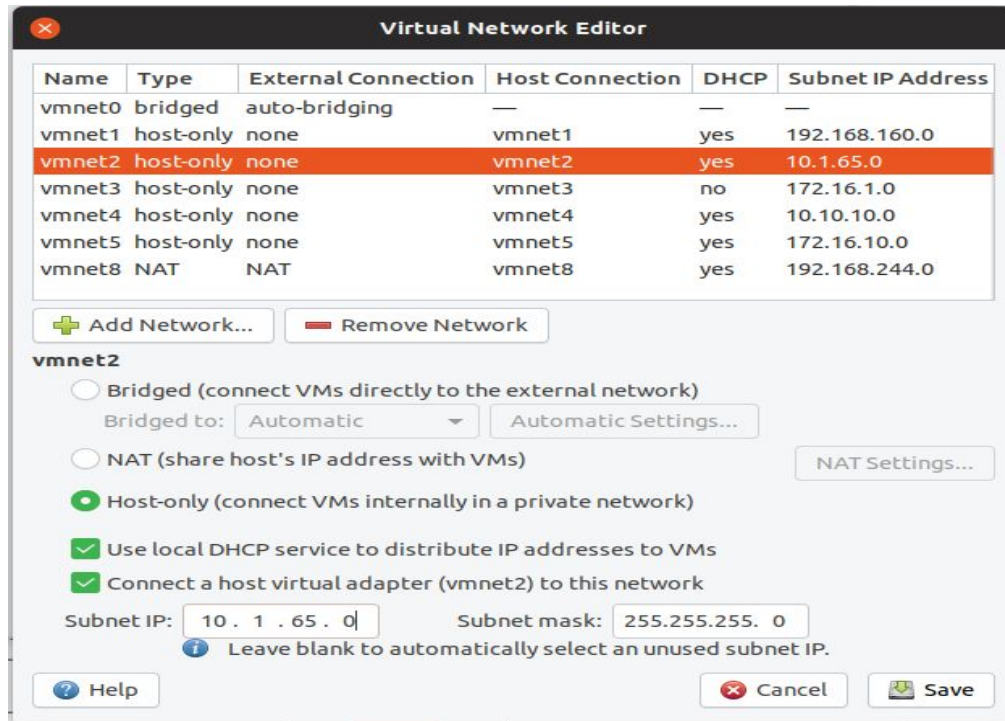


10.1.65.1



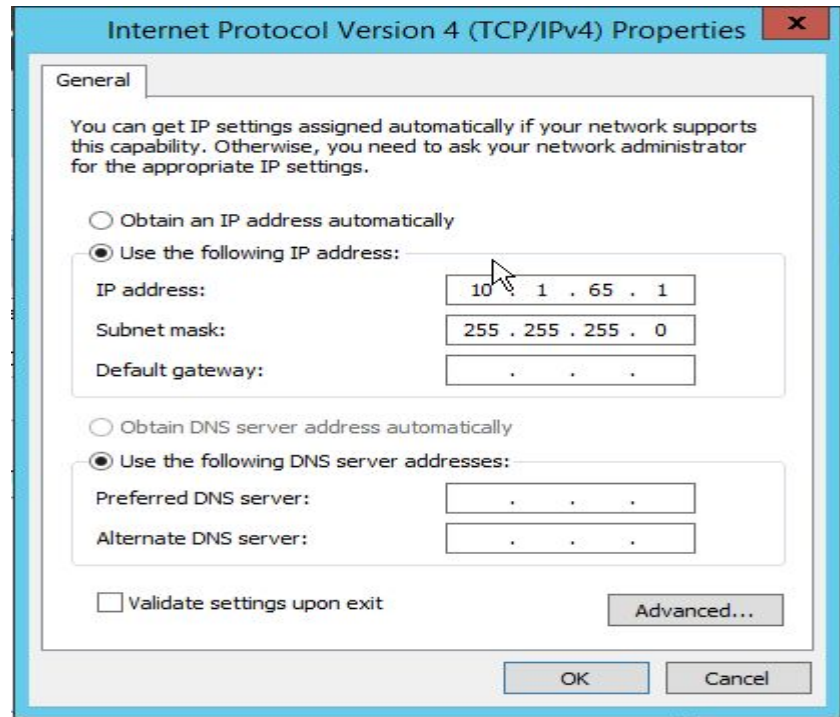
II. Cài đặt môi trường

- Cấu hình vmnet1 với :
 - subnetip: 10.1.65.0
 - subnet mask: 255.255.255.0



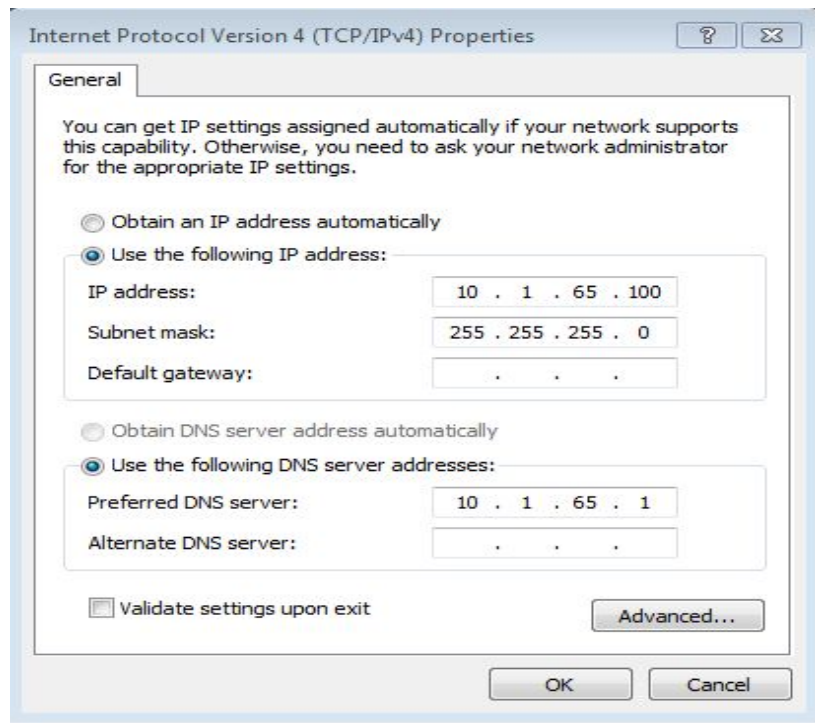
II. Cài đặt môi trường

- Đặt địa chỉ ip tĩnh cho mail server:
 - ip: 10.1.65.1
 - subnet mask: 255.255.255.0



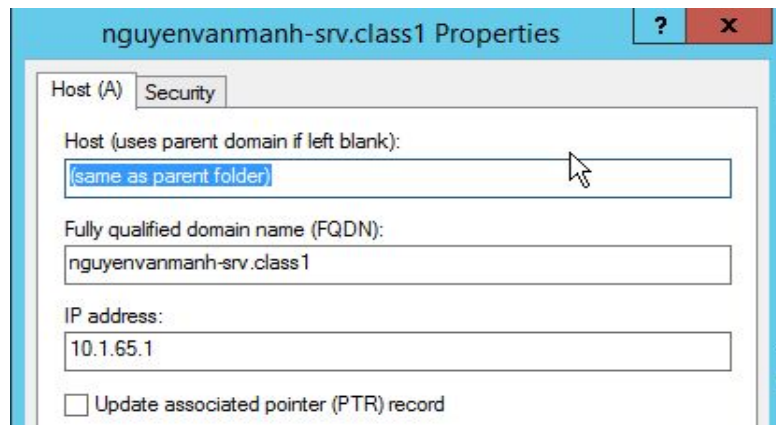
II. Cài đặt môi trường

- Cài đặt địa chỉ ip tĩnh cho client:
 - ip: 10.1.65.100
 - subnet mask: 255.255.255.0
 - DNS server: 10.1.65.1



II. Cài đặt môi trường

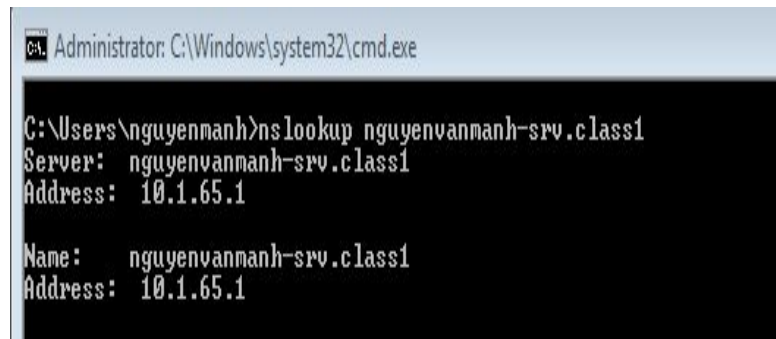
- Trên server thêm bản ghi DNS để phân giải tên miền
 - Domain: nguyenvanmanh-srv.class1
 - Ip phân giải: 10.1.65.1
- Chuyển sang máy window 7 chạy nslookup để chắc chắn rằng đã server đã phân giải được tên miền.



The screenshot shows the 'nguyenvanmanh-srv.class1 Properties' dialog box with the 'Security' tab selected. The 'Host (A)' section contains the following fields:

- Host (uses parent domain if left blank):
- Fully qualified domain name (FQDN):
- IP address:

At the bottom, there is an unchecked checkbox labeled 'Update associated pointer (PTR) record'.

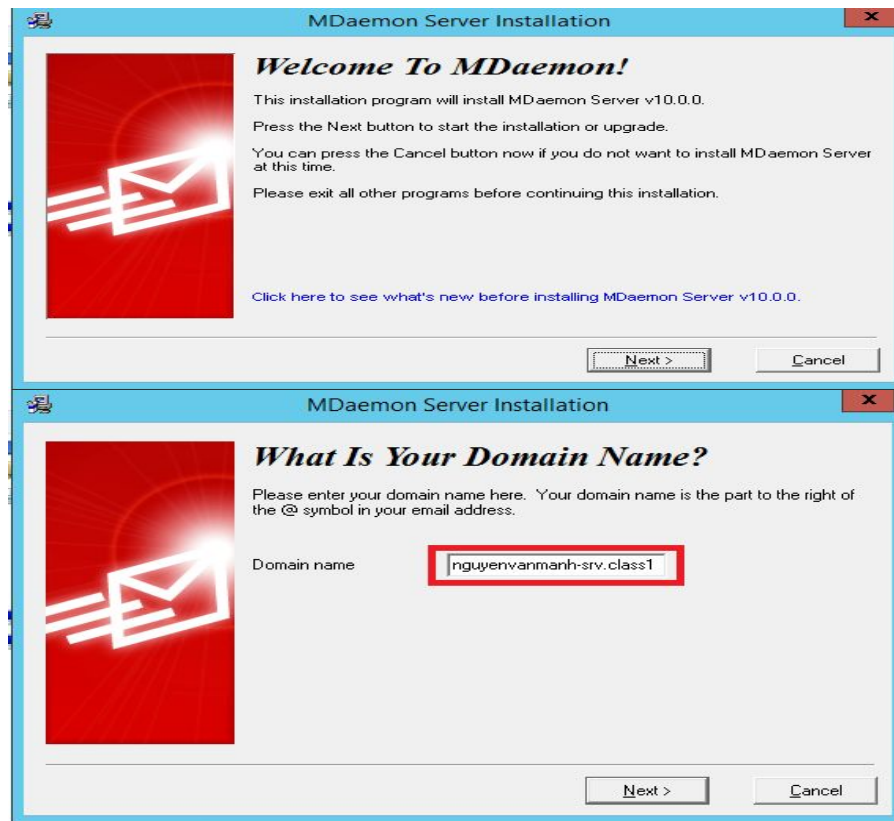


```
C:\Users\nguyenmanh>nslookup nguyenvanmanh-srv.class1
Server: nguyenvanmanh-srv.class1
Address: 10.1.65.1

Name: nguyenvanmanh-srv.class1
Address: 10.1.65.1
```

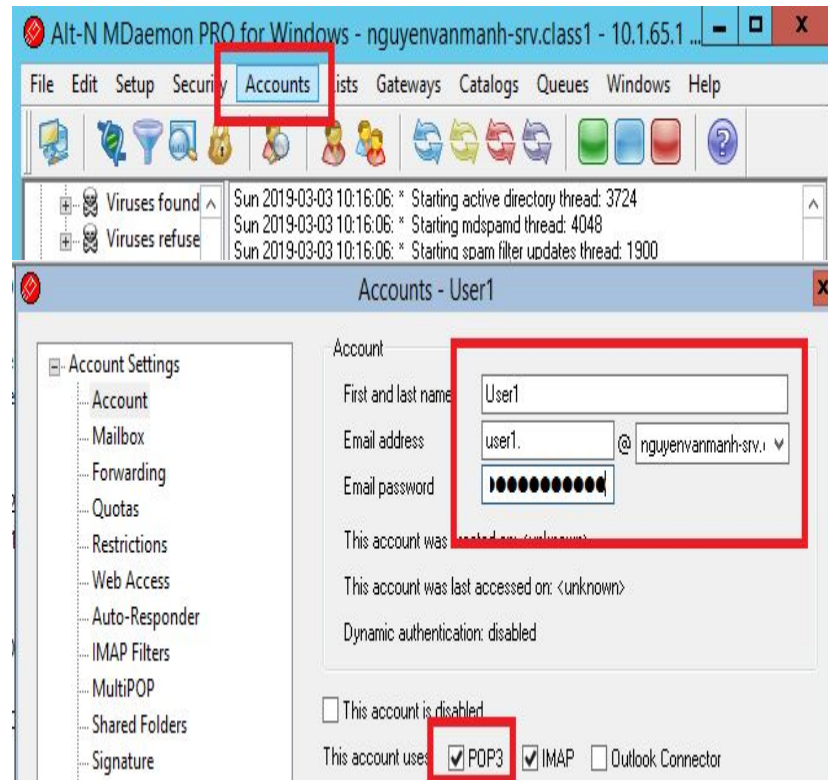
II. Cài đặt môi trường

- Trên máy window 2012 cài đặt MDdeamon để làm mail server:
 - Điền domain name.



II. Cài đặt môi trường

- Trên MDdaemon tạo 2 tài khoản:
 - User1:
user1@nguyenvanmanh-srv@class1
 - User2:
user2@nguyenvanmanh-srv@class1



II. Cài đặt môi trường

- Trên window 7 cài đặt Thunderbird



II. Cài đặt môi trường

- Đăng nhập 2 tài khoản đã tạo vào thunderbird

Mail Account Setup

Your name: Your name, as shown to others

Email address: ⚠ Double-check this email address!

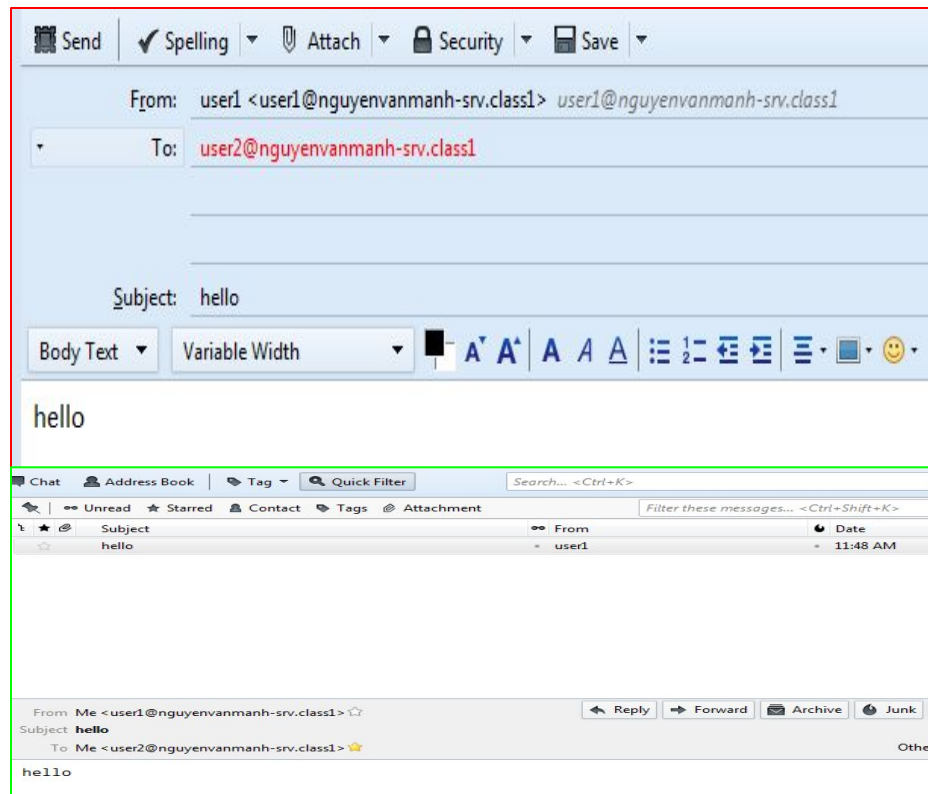
Password:

☒ Remember password



III. Gửi mail và chặn bắt (không mã hóa)

- Dùng user1 gửi một tin nhắn tới user2:
 - Tiêu đề: **hello**
 - Tin nhắn: **hello**
- Vào user2 bấm **get messages** để lấy mail về và đã nhận được mail từ user1.
 - Tiêu đề: **hello**
 - Tin nhắn: **hello**



III. Gửi mail và chặn bắt (không mã hóa)

Trên wireshark chúng ta chặn bắt gói tin SMTP

The image shows a Wireshark packet capture of SMTP traffic. The top pane displays a list of packets. Packet 5 is selected, showing its details in the middle pane and its raw data in hexadecimal and ASCII in the bottom pane.

No.	Time	Source	Destination	Protocol	Length	Info
5...	3121.2286...	10.1.65.100	10.1.65.1	SMTP	60	C: DATA
5...	3121.2300...	10.1.65.1	10.1.65.100	SMTP	94	S: 354 Enter mail, end with <CRLF>.<CRLF>
5...	3121.2312...	10.1.65.100	10.1.65.1	SMTP	450	C: DATA fragment, 396 bytes
5...	3121.2315...	10.1.65.100	10.1.65.1	SMTP IMF	57	from: user1 <user1@nguyenvanmanh-srv.class1>, subject: hello, (text/plain)
5...	3121.2352...	10.1.65.1	10.1.65.100	SMTP	133	S: 250 Ok, message saved <Message-ID: 5C7B5CB6.8010602@nguyenvanmanh-srv.class1>
5...	3121.2361...	10.1.65.100	10.1.65.1	SMTP	60	C: QUIT
5...	3121.2458...	10.1.65.1	10.1.65.100	SMTP	80	S: 221 See ya in cyberspace
6...	3552.4651...	10.1.65.1	10.1.65.100	SMTP	142	S: 220 nguyenvanmanh-srv.class1 ESMTP MSA MDAemon 10.0.0; Sun, 03 Mar 2019 11:56...
6...	3552.4658...	10.1.65.100	10.1.65.1	SMTP	74	C: EHLO [10.1.65.100]
6...	3552.4821...	10.1.65.1	10.1.65.100	SMTP	125	S: 250-nguyenvanmanh-srv.class1 Hello [10.1.65.100], pleased to meet you
6...	3552.6894...	10.1.65.1	10.1.65.100	SMTP	121	S: 250-AUTH=LOGIN 250-AUTH LOGIN CRAM-MD5 250-8BITMIME 250 SIZE 0
6...	3559.3719...	10.1.65.100	10.1.65.1	SMTP	69	C: AUTH CRAM-MD5
6...	3559.3725...	10.1.65.1	10.1.65.100	SMTP	148	S: 334 PE1EQUVNT04tRjIwMTkwMzAzMTE1Ni5BQTU2MjIxNjZNRDAwMTJAbmd1ewVudmFubWFuaC1zc...
6...	3559.3731...	10.1.65.100	10.1.65.1	SMTP	108	C: dXNlcjEgZDE3ZTk0MDE0NTBiOGNjOTg1Y2UwMjBmMDhlY2E5NzI=
6...	3559.3734...	10.1.65.1	10.1.65.100	SMTP	85	S: 235 Authentication successful

Message-ID: <5C7B5CB6.8010602@nguyenvanmanh-srv.class1>
Date: Sun, 03 Mar 2019 11:48:54 +0700

- From: user1 <user1@nguyenvanmanh-srv.class1>, 1 item
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:31.0) Gecko/20100101 Thunderbird/31.5.0
MIME-Version: 1.0
- To: user2@nguyenvanmanh-srv.class1, 1 item
Subject: hello
- Content-Type: text/plain; charset=utf-8; format=flowed
Content-Transfer-Encoding: 7bit

Line-based text data: text/plain (1 lines)

0000 00 0c 29 0b 43 9f 00 0c 29 e2 df 10 08 00 45 00 ..).C...)....E
0010 00 2b 06 a0 40 00 80 06 5d c6 0a 01 41 64 0a 01 .+..@...]...Ad..
0020 41 01 c0 36 02 4b fa 1c 94 b6 39 29 20 29 50 18 A..6.K...9)P..
0030 00 fe 35 b0 00 00 2e 0d 0a ..5.....

Frame (57 bytes) Reassembled SMTP (396 bytes)

wireshark_vmnet2_20190303105654_rJhzS6.pcapng Packets: 6110 · Displayed: 78 (1.3%) Profile: Default

III. Gửi mail và chặn bắt (không mã hóa)

Trên wireshark chúng ta chặn bắt gói tin POP

pop

No.	Time	Source	Destination	Protocol	Length	Info
4...	2784.7425...	10.1.65.1	10.1.65.100	POP	83	S: +OK Capability list follows
4...	2784.9444...	10.1.65.1	10.1.65.100	POP IMF	74	TOP , USER , UIDL , .
4...	2784.9475...	10.1.65.100	10.1.65.1	POP	66	C: USER user1
4...	2784.9482...	10.1.65.1	10.1.65.100	POP	76	S: +OK user1... User ok
4...	2784.9523...	10.1.65.100	10.1.65.1	POP	73	C: PASS Manh18031997
4...	2784.9561...	10.1.65.1	10.1.65.100	POP	132	S: +OK user1@nguyenvanmanh-srv.class1's mailbox has 0 total messages (0 octets)
4...	2784.9577...	10.1.65.100	10.1.65.1	POP	60	C: QUIT
4...	2784.9580...	10.1.65.1	10.1.65.100	POP	155	S: +OK user1@nguyenvanmanh-srv.class1 nguyenvanmanh-srv.class1 POP3 Server signi...
4...	2864.1996...	10.1.65.1	10.1.65.100	POP	174	S: +OK nguyenvanmanh-srv.class1 POP3 MDAemon 10.0.0 ready <MDAEMON-F201903031144...
4...	2864.2075...	10.1.65.100	10.1.65.1	POP	60	C: CAPA
4...	2864.2077...	10.1.65.100	10.1.65.1	POP	60	C: QUIT
4...	2864.2193...	10.1.65.1	10.1.65.100	POP	174	S: +OK nguyenvanmanh-srv.class1 POP3 MDAemon 10.0.0 ready <MDAEMON-F201903031144...
4...	2864.2197...	10.1.65.100	10.1.65.1	POP	60	C: CAPA
4...	2864.2201...	10.1.65.100	10.1.65.1	POP	60	C: QUIT
4...	2864.2524...	10.1.65.1	10.1.65.100	POP	83	S: +OK Capability list follows
4...	2864.2617...	10.1.65.1	10.1.65.100	POP	83	S: +OK Capability list follows

▶ Frame 4583: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
▶ Ethernet II, Src: Vmware_e2:df:10 (00:0c:29:e2:df:10), Dst: Vmware_0b:43:9f (00:0c:29:0b:43:9f)
▶ Internet Protocol Version 4, Src: 10.1.65.100, Dst: 10.1.65.1
▶ Transmission Control Protocol, Src Port: 49192, Dst Port: 110, Seq: 25, Ack: 221, Len: 19
▼ Post Office Protocol
 ▼ PASS Manh18031997\r\n
 Request command: PASS
 Request parameter: Manh18031997

0000 00 0c 29 0b 43 9f 00 0c 29 e2 df 10 08 00 45 00 ..).C...)....E.
0010 00 3b 05 3f 40 00 80 06 5f 17 0a 01 41 64 0a 01 .;?@... _...Ad..
0020 41 01 c0 28 00 6e 6f 7a 6e 94 8f e6 c1 6e 50 18 A..(.noz n....nP.
0030 00 ff b5 2f 00 00 50 41 53 53 20 4d 61 6e 68 31 .../..PA SS Manh1
0040 38 30 33 31 39 39 37 0d 0a 8031997..

wireshark vmnet2 20190303105654 rJhzS6.pcapng Packets: 5983 · Displayed: 81 (1.4%) Profile: Default

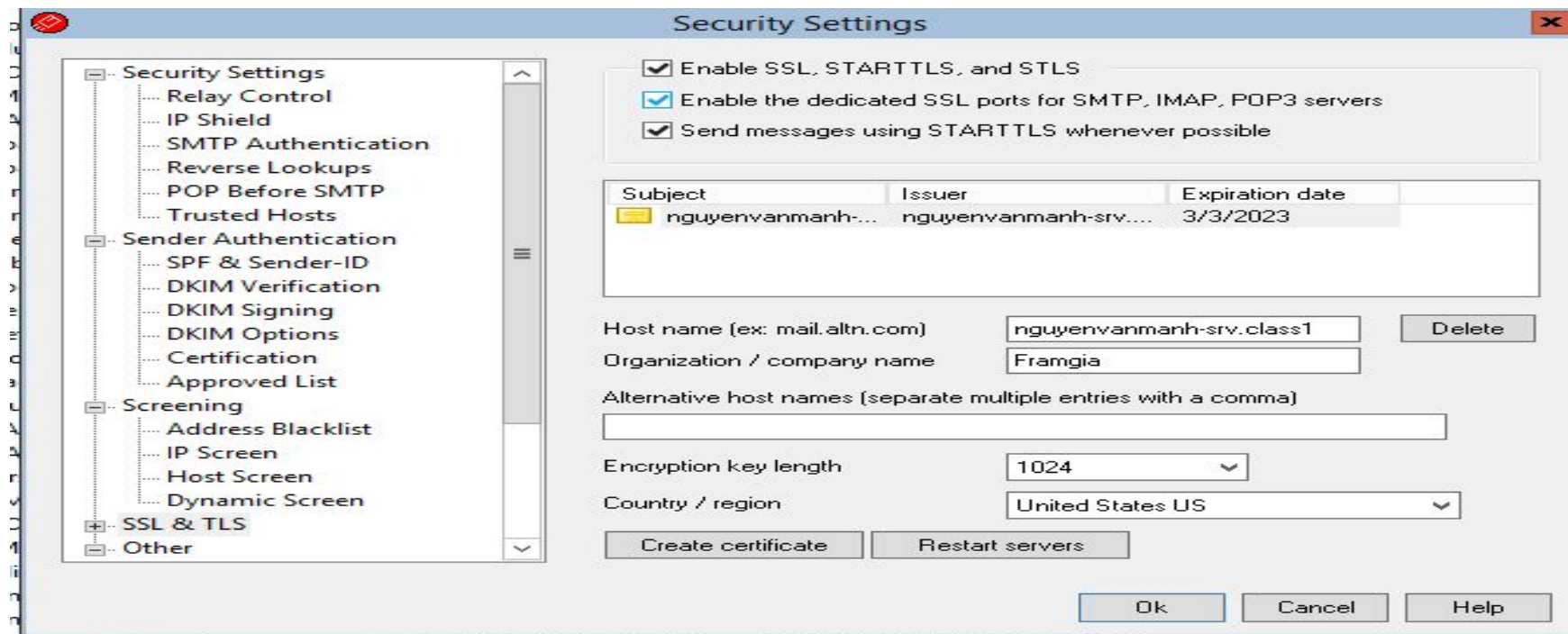
III. Gửi mail và chặn bắt (không mã hóa)

Dữ liệu được truyền đang ở dạng rõ (không mã hóa)

```
▶ Unknown-Extension: X-Authenticated-Sender: user1@nguyenvanmanh-srv.class1 (Contact Wireshark developers if you want this supported.)
▶ Unknown-Extension: X-Rcpt-To: user2@nguyenvanmanh-srv.class1 (Contact Wireshark developers if you want this supported.)
▶ Unknown-Extension: X-MDRcpt-To: user2@nguyenvanmanh-srv.class1 (Contact Wireshark developers if you want this supported.)
▶ Unknown-Extension: X-MDRemoteIP: 10.1.65.100 (Contact Wireshark developers if you want this supported.)
▶ Unknown-Extension: X-Return-Path: user1@nguyenvanmanh-srv.class1 (Contact Wireshark developers if you want this supported.)
▶ Unknown-Extension: X-Envelope-From: user1@nguyenvanmanh-srv.class1 (Contact Wireshark developers if you want this supported.)
▶ Unknown-Extension: X-MDaemon-Deliver-To: user2@nguyenvanmanh-srv.class1 (Contact Wireshark developers if you want this supported.)
Message-ID: <5C7B5CB6.8010602@nguyenvanmanh-srv.class1>
Date: Sun, 03 Mar 2019 11:48:54 +0700
▶ From: user1 <user1@nguyenvanmanh-srv.class1>, 1 item
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:31.0) Gecko/20100101 Thunderbird/31.5.0
MIME-Version: 1.0
▶ To: user2@nguyenvanmanh-srv.class1, 1 item
Subject: hello
▶ Content-Type: text/plain; charset=utf-8; format=flowed
Content-Transfer-Encoding: 7bit
▼ Line-based text data: text/plain (3 lines)
hello\r\n
\r\n
.\r\n
```

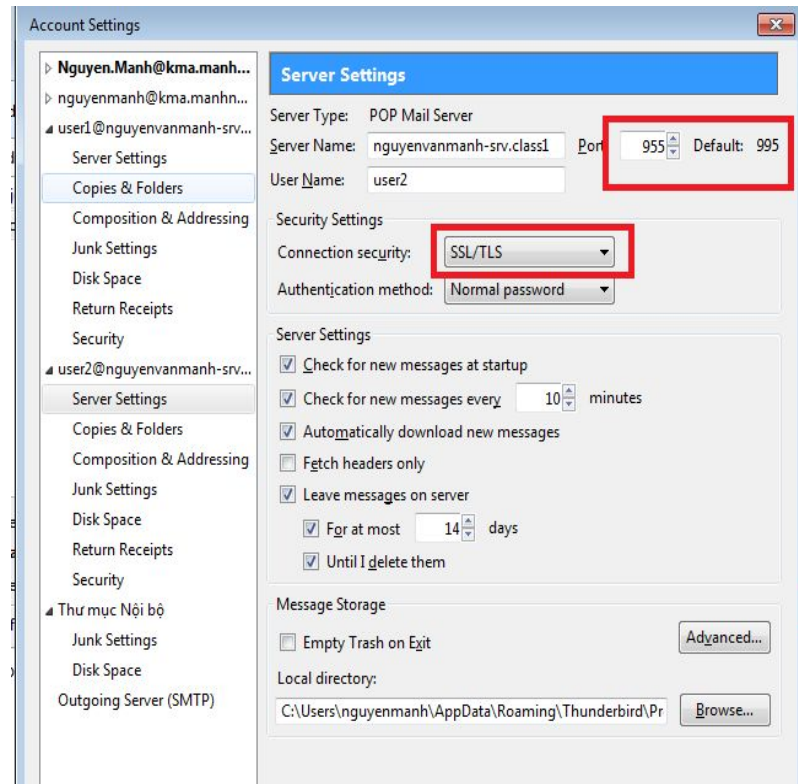
IV. Gửi mail và chặn bắt (mã hóa)

Vào MDdeamon cài đặt để có thể mã hóa được dữ liệu với SSL/TLS



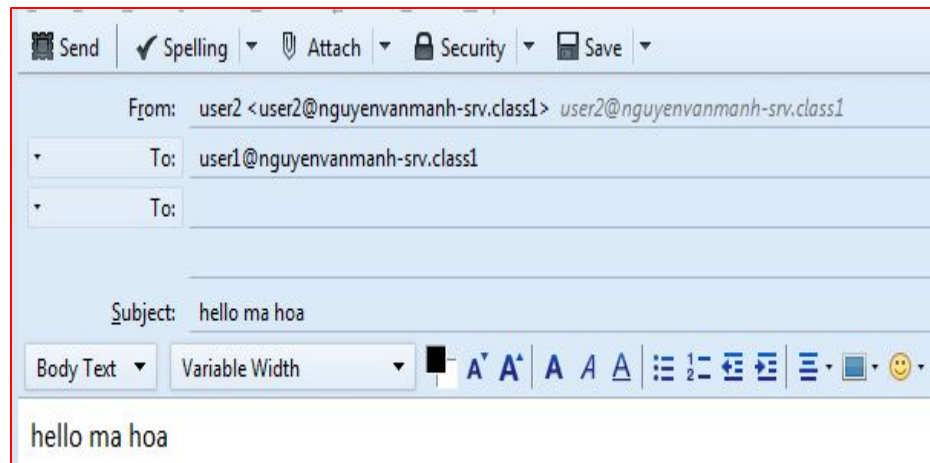
IV. Gửi mail và chặn bắt (mã hóa)

- Trên Thunderbird thực hiện cài đặt lại 2 tài khoản user1, user1:
 - Đặt lại cổng server thành 995
 - Chọn connection security: SSL/TLS

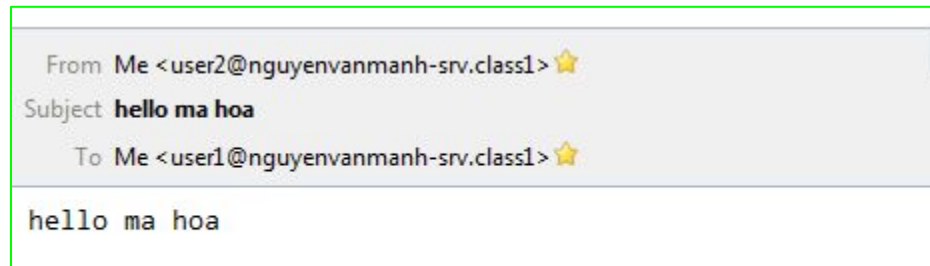


IV. Gửi mail và chặn bắt (mã hóa)

- Dùng user2 gửi một tin nhắn tới user1:
 - Tiêu đề: **hello ma hoa**
 - Tin nhắn: **hello ma hoa**
- Vào user1 bấm **get messages** để lấy mail về và đã nhận được mail từ user2.
 - Tiêu đề: **hello ma hoa**
 - Tin nhắn: **hello ma hoa**



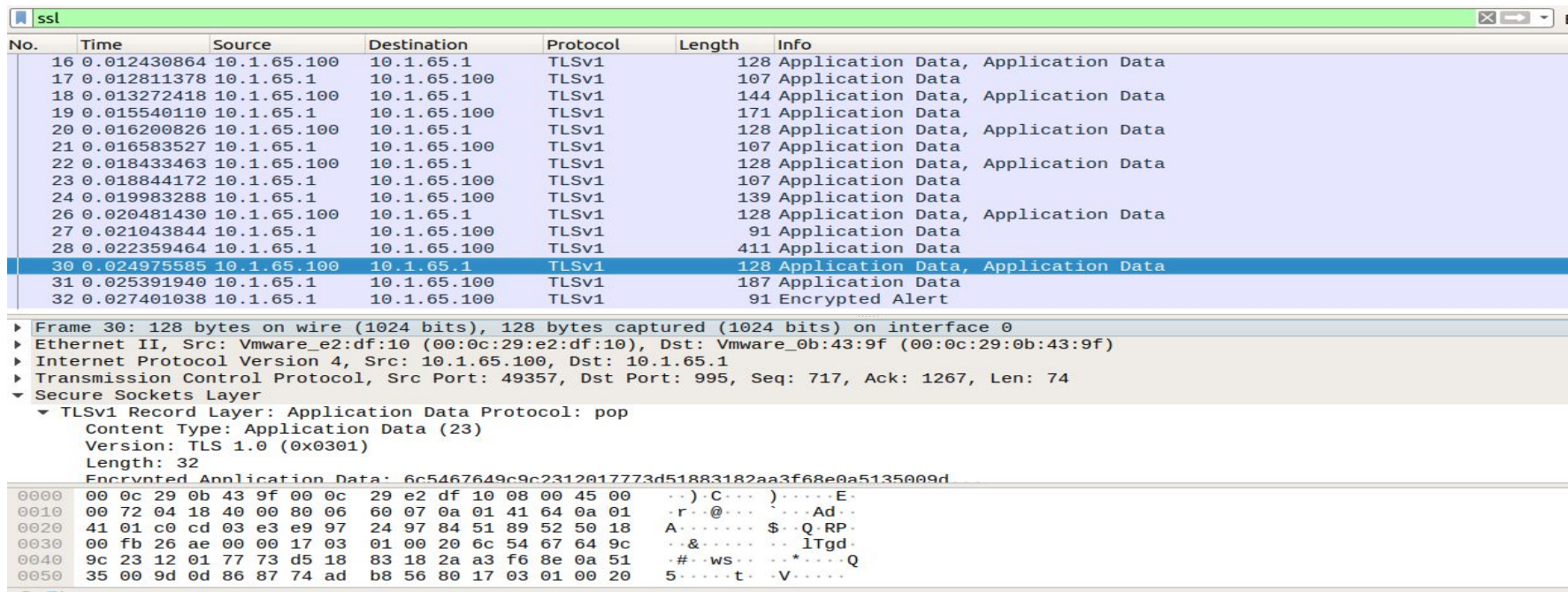
A screenshot of an email composition window. The window has a light blue header bar with icons for Send, Spelling, Attach, Security, and Save. Below the header, the 'From' field is set to 'user2 <user2@nguyenvanmanh-srv.class1> user2@nguyenvanmanh-srv.class1'. The 'To' field is set to 'user1@nguyenvanmanh-srv.class1'. The 'Subject' field is set to 'hello ma hoa'. The 'Body Text' dropdown is set to 'Variable Width'. The body of the email contains the text 'hello ma hoa'.



A screenshot of an email received in a user interface. The email header shows 'From Me <user2@nguyenvanmanh-srv.class1>' with a yellow star icon. The 'Subject' is 'hello ma hoa'. The 'To' is 'Me <user1@nguyenvanmanh-srv.class1>' with a yellow star icon. The body of the email contains the text 'hello ma hoa'.

IV. Gửi mail và chặn bắt (mã hóa)

Trên wireshark bây giờ chúng ta chuyển qua chặn bắt SSL/TLS



ssl

No.	Time	Source	Destination	Protocol	Length	Info
16	0.012430864	10.1.65.100	10.1.65.1	TLSv1	128	Application Data, Application Data
17	0.012811378	10.1.65.1	10.1.65.100	TLSv1	107	Application Data
18	0.013272418	10.1.65.100	10.1.65.1	TLSv1	144	Application Data, Application Data
19	0.015540110	10.1.65.1	10.1.65.100	TLSv1	171	Application Data
20	0.016200826	10.1.65.100	10.1.65.1	TLSv1	128	Application Data, Application Data
21	0.016583527	10.1.65.1	10.1.65.100	TLSv1	107	Application Data
22	0.018433463	10.1.65.100	10.1.65.1	TLSv1	128	Application Data, Application Data
23	0.018844172	10.1.65.1	10.1.65.100	TLSv1	107	Application Data
24	0.019983288	10.1.65.1	10.1.65.100	TLSv1	139	Application Data
26	0.020481430	10.1.65.100	10.1.65.1	TLSv1	128	Application Data, Application Data
27	0.021043844	10.1.65.1	10.1.65.100	TLSv1	91	Application Data
28	0.022359464	10.1.65.1	10.1.65.100	TLSv1	411	Application Data
30	0.024975585	10.1.65.100	10.1.65.1	TLSv1	128	Application Data, Application Data
31	0.025391940	10.1.65.1	10.1.65.100	TLSv1	187	Application Data
32	0.027401038	10.1.65.1	10.1.65.100	TLSv1	91	Encrypted Alert

Frame 30: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits) on interface 0

Ethernet II, Src: Vmware_e2:df:10 (00:0c:29:e2:df:10), Dst: Vmware_0b:43:9f (00:0c:29:0b:43:9f)

Internet Protocol Version 4, Src: 10.1.65.100, Dst: 10.1.65.1

Transmission Control Protocol, Src Port: 49357, Dst Port: 995, Seq: 717, Ack: 1267, Len: 74

Secure Sockets Layer

TLSv1 Record Layer: Application Data Protocol: pop

Content Type: Application Data (23)

Version: TLS 1.0 (0x0301)

Length: 32

Encrypted Application Data: 6c5467649c9c2312017773d51883182aa3f68e0a5135009d

0000 00 0c 29 0b 43 9f 00 0c 29 e2 df 10 08 00 45 00 ..).C...).....E..

0010 00 72 04 18 40 00 80 06 60 07 0a 01 41 64 0a 01 ..r..@... ..Ad..

0020 41 01 c0 cd 03 e3 e9 97 24 97 84 51 89 52 50 18 A.....\$.Q.RP..

0030 00 fb 26 ae 00 00 17 03 01 00 20 6c 54 67 64 9c ..&..... lTgd..

0040 9c 23 12 01 77 73 d5 18 83 18 2a a3 f6 8e 0a 51 ..#..ws...*.....Q

0050 35 00 9d 0d 86 87 74 ad b8 56 80 17 03 01 00 20 5.....t..V.....

IV. Gửi mail và chặn bắt (mã hóa)

Tất cả dữ liệu đã được mã hóa.

- ▶ Frame 30: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits) on interface 0
- ▶ Ethernet II, Src: Vmware_e2:df:10 (00:0c:29:e2:df:10), Dst: Vmware_0b:43:9f (00:0c:29:0b:43:9f)
- ▶ Internet Protocol Version 4, Src: 10.1.65.100, Dst: 10.1.65.1
- ▶ Transmission Control Protocol, Src Port: 49357, Dst Port: 995, Seq: 717, Ack: 1267, Len: 74
- ▼ Secure Sockets Layer
 - ▼ TLSv1 Record Layer: Application Data Protocol: pop
 - Content Type: Application Data (23)
 - Version: TLS 1.0 (0x0301)
 - Length: 32
 - Encrypted Application Data: 6c5467649c9c2312017773d51883182aa3f68e0a5135009d...
 - ▼ TLSv1 Record Layer: Application Data Protocol: pop
 - Content Type: Application Data (23)
 - Version: TLS 1.0 (0x0301)
 - Length: 32
 - Encrypted Application Data: b0242f4d72012cc9051d1126e50ad18a2a739e89d3a5a810...