Email Traffic Forensics

SMTP

Traffic files: https://github.com/frankwxu/digital-forensics-lab/tree/main/Illegal_Possession_Images/lab_files/smtp.pcap

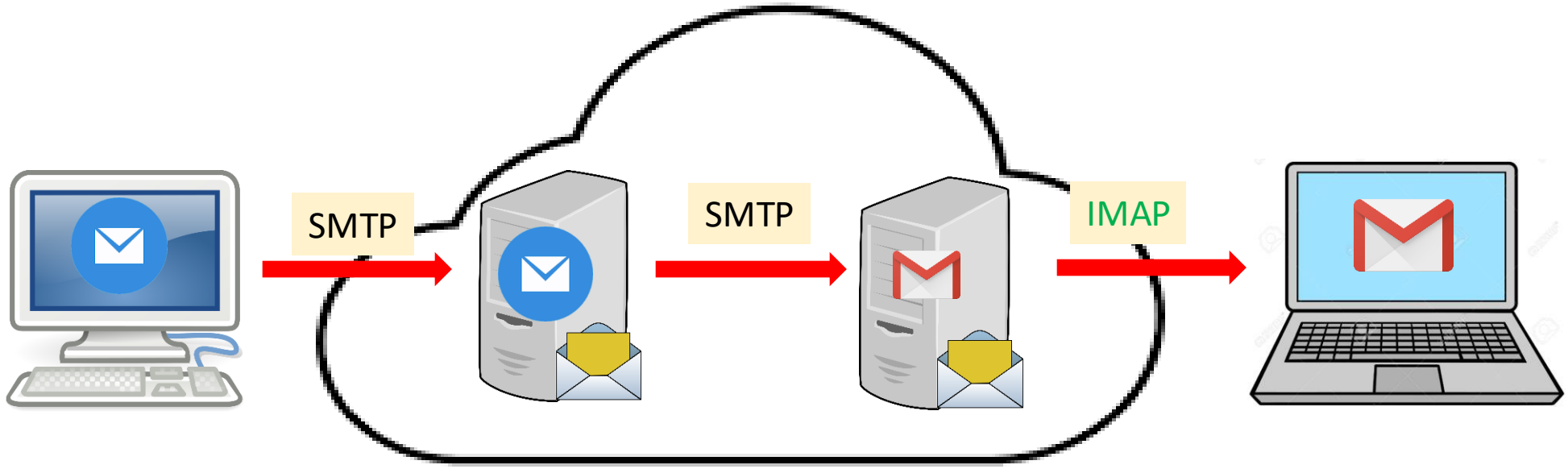
Overview

- Simple Mail Transfer Protocol
- Hands-on lab
  - A `.pcap` file contains MS Outlook email traffic
  - Assume the traffic is decreased

Simple Mail Transfer Protocol

Simple Mail Transfer Protocol (SMTP)

- It is a protocol used for sending and receiving email messages over the Internet.



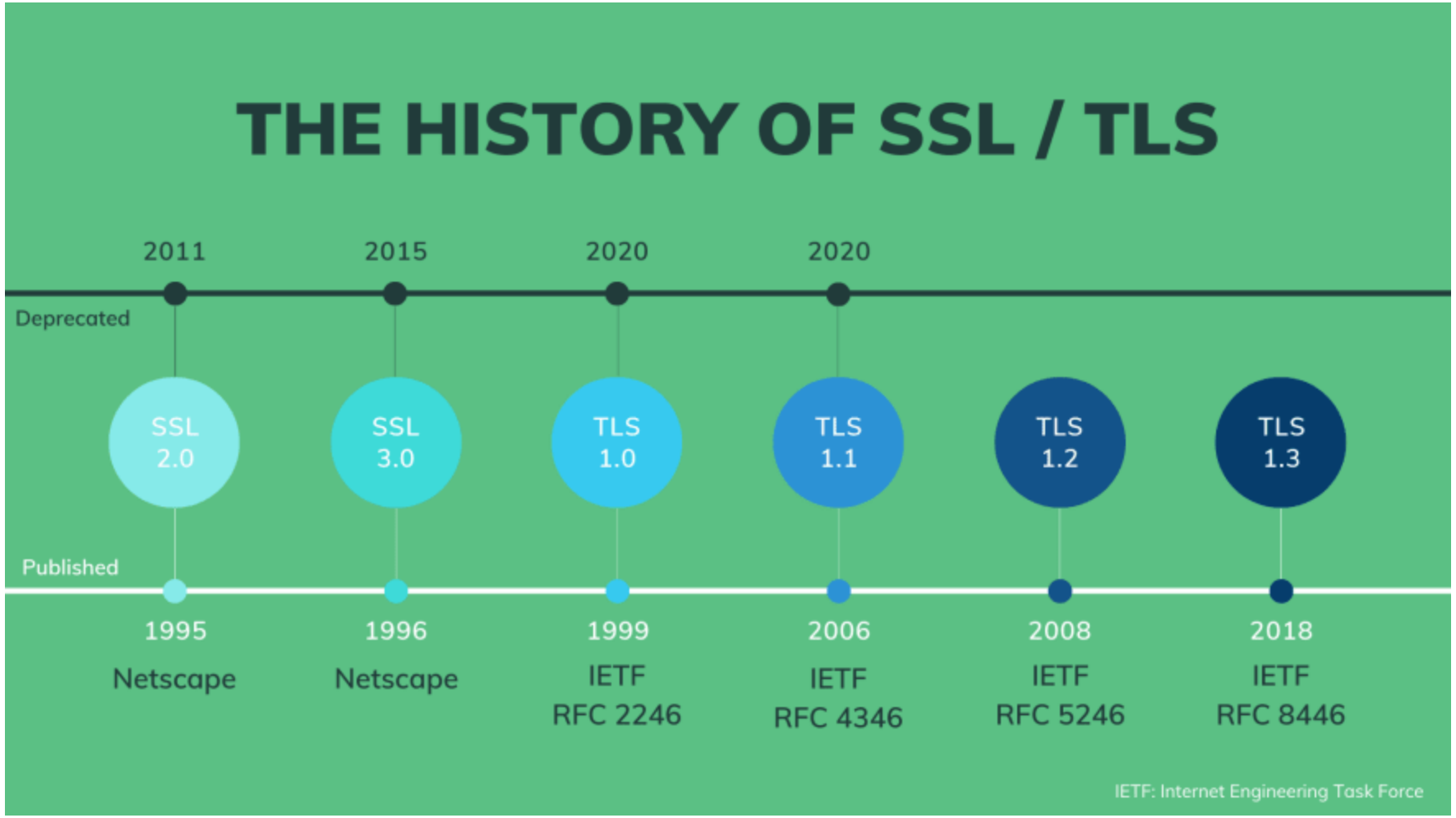
SMTP (Simple Mail Transfer Protocol): sending emails
IMAP (Internet Access Message Protocol): **download** emails

Simple Mail Transfer Protocol

- SMTP operates on port 25 by default, but other ports such as 587 and 465 may also be used.
- SMTP uses a set of commands and responses to transfer email messages between clients and servers.
- SMTP is a plain text protocol
  - data transmitted between clients and servers is not encrypted by default.
- SMTPS for secure email transmissions
  - SMTP over SSL/TLS
  - STARTTLS

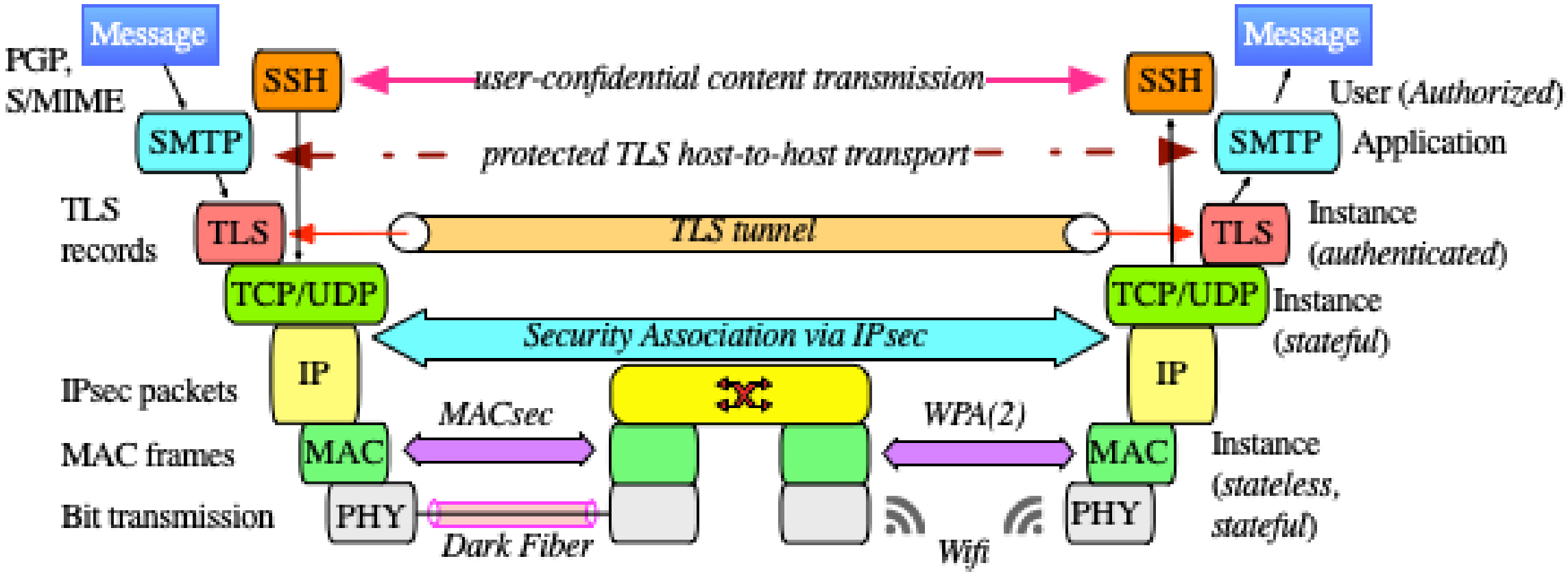
SSL/TLS

- SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are cryptographic protocols that provide secure communication over the internet.
  - SSL is the predecessor to TLS, and is no longer considered secure.
- Key security features
  - Authentication: SSL and TLS provide mechanisms for authenticating the identity of the client and server, so that both parties can be sure they are communicating with the intended party.
  - Data encryption: SSL and TLS encrypt data transmitted over the internet, so that it cannot be intercepted and read by unauthorized parties.
  - Data integrity: SSL and TLS ensure the integrity of data transmitted over the internet, so that it cannot be modified in transit without detection.



https://dev.to/techschoolguru/a-complete-overview-of-ssl-tls-and-its-cryptographic-system-36pd

SMTP is an application layer protocol

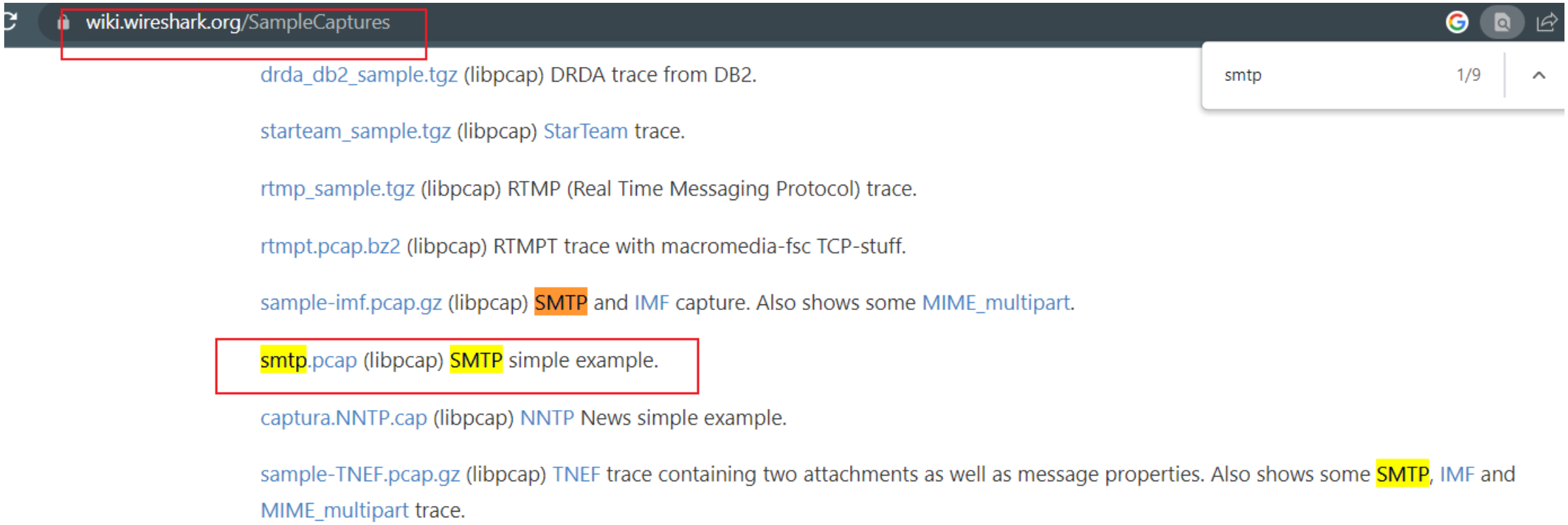


https://www.fehcom.de/qmail/smtptls.html

Hands-on Lab

Capture Emails traffic With Wireshark

Lab Files

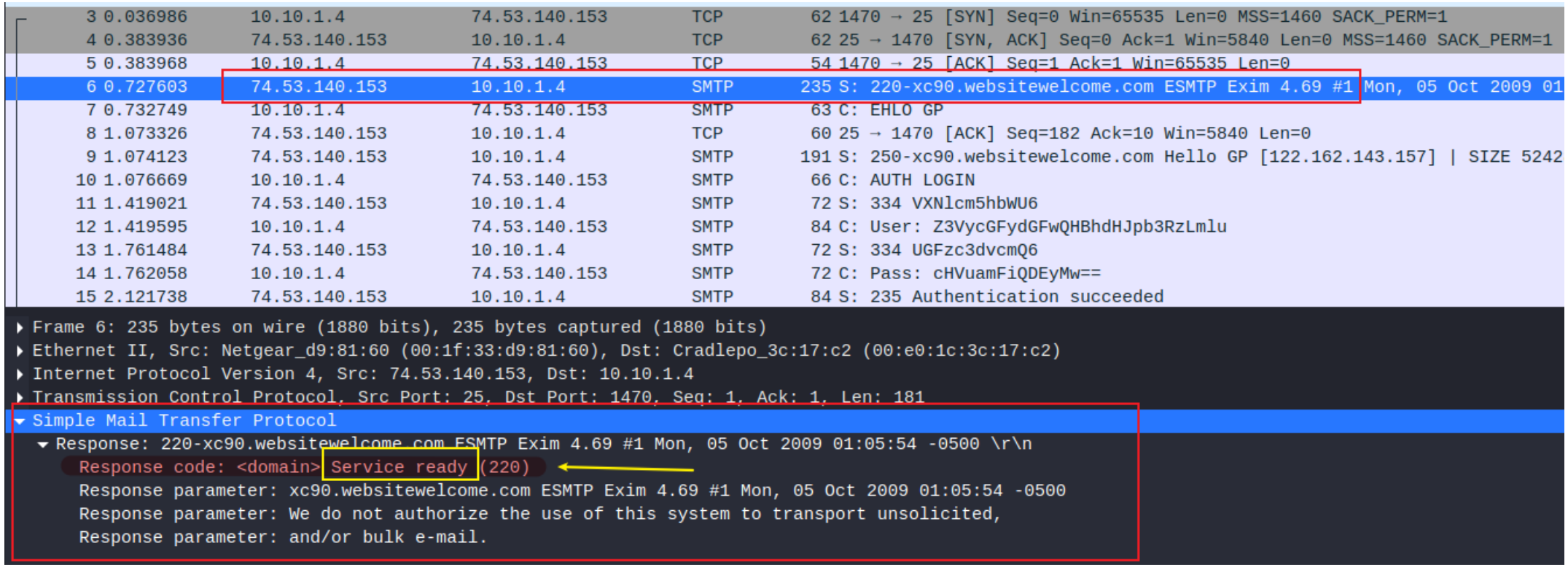


https://wiki.wireshark.org/SampleCaptures

Download smtp.pcap

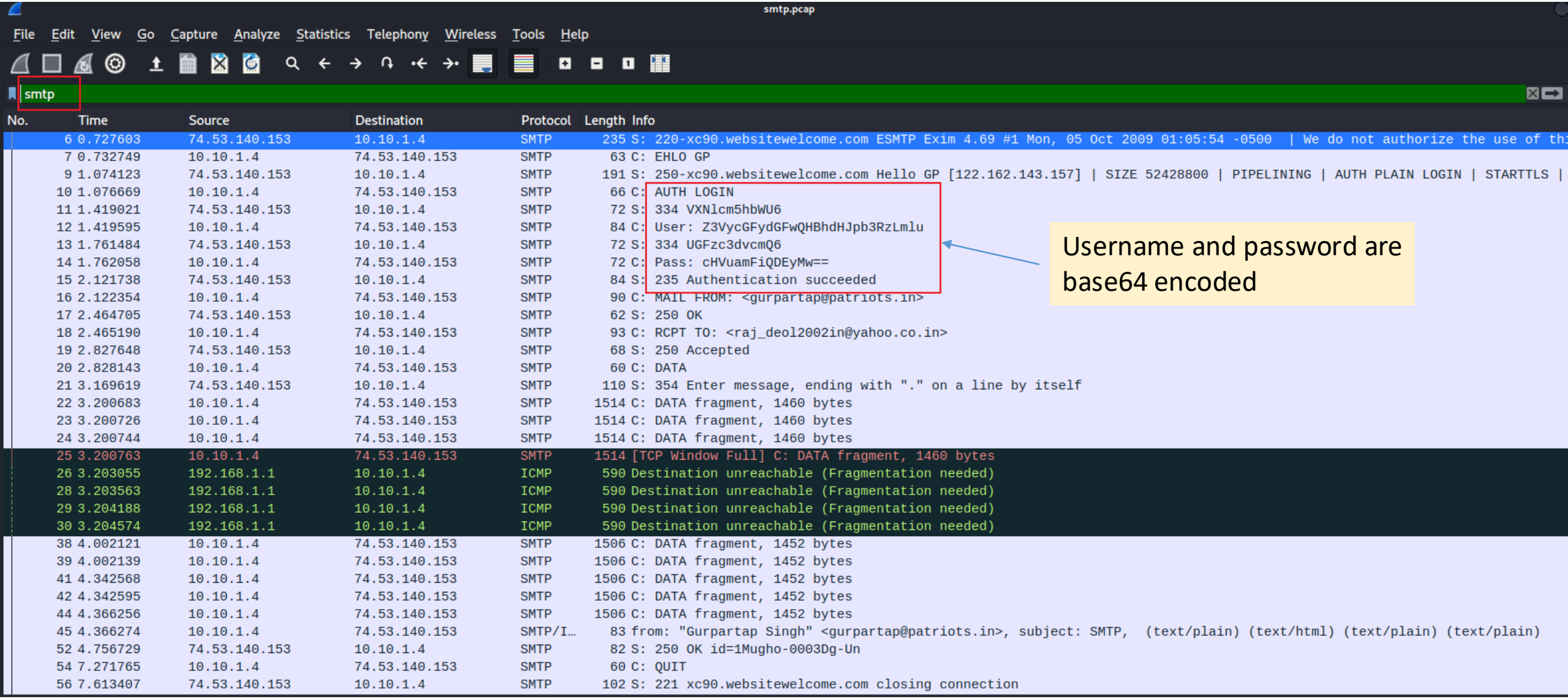
```
┌──(kali㉿kali)-[~/smtp]
└─$ wget https://wiki.wireshark.org/uploads/__moin_import__/attachments/SampleCaptures/smtp.pcap
--2023-03-10 14:58:08--  https://wiki.wireshark.org/uploads/__moin_import__/attachments/SampleCaptur
es/smtp.pcap
Resolving wiki.wireshark.org (wiki.wireshark.org)... 172.67.75.39, 104.26.10.240, 104.26.11.240, ...
Connecting to wiki.wireshark.org (wiki.wireshark.org)|172.67.75.39|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 27850 (27K) [application/octet-stream]
Saving to: ‘smtp.pcap’

smtp.pcap               100%[===================================>]  27.20K  --.-KB/s    in 0.004s

2023-03-10 14:58:08 (6.91 MB/s) - ‘smtp.pcap’ saved [27850/27850]
```

SMTP first response “service ready”



indicates that

- the device is running an SMTP server and is ready to receive email messages.
- additional information about the server and a warning that the server does not authorize the use of its system to send unsolicited or bulk emails.


smtp.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
smtp
No. Time Source Destination Protocol Length Info
6 0.727603 74.53.140.153 10.10.1.4 SMTP 235 S: 220-xc90.websitewelcome.com ESMTP Exim 4.69 #1 Mon, 05 Oct 2009 01:05:54 -0500 | We do not authorize the use of th
7 0.732749 10.10.1.4 74.53.140.153 SMTP 63 C: EHLO GP
9 1.074123 74.53.140.153 10.10.1.4 SMTP 191 S: 250-xc90.websitewelcome.com Hello GP [122.162.143.157] | SIZE 52428800 | PIPELINING | AUTH PLAIN LOGIN | STARTTLS |
10 1.076669 10.10.1.4 74.53.140.153 SMTP 66 C: AUTH LOGIN
11 1.419021 74.53.140.153 10.10.1.4 SMTP 72 S: 334 VXNlcm5hbWU6
12 1.419595 10.10.1.4 74.53.140.153 SMTP 84 C: User: Z3VycGFydGFwQHBhdHJpb3RzLmlu
13 1.761484 74.53.140.153 10.10.1.4 SMTP 72 S: 334 UGFzc3dvcmQ6
14 1.762058 10.10.1.4 74.53.140.153 SMTP 72 C: Pass: cHVuamFiQDEyMw==
15 2.121738 74.53.140.153 10.10.1.4 SMTP 84 S: 235 Authentication succeeded
16 2.122354 10.10.1.4 74.53.140.153 SMTP 90 C: MAIL FROM: <gurpartap@patriots.in>
17 2.464705 74.53.140.153 10.10.1.4 SMTP 62 S: 250 OK
18 2.465190 10.10.1.4 74.53.140.153 SMTP 93 C: RCPT TO: <raj_deol2002in@yahoo.co.in>
19 2.827648 74.53.140.153 10.10.1.4 SMTP 68 S: 250 Accepted
20 2.828143 10.10.1.4 74.53.140.153 SMTP 60 C: DATA
21 3.169619 74.53.140.153 10.10.1.4 SMTP 110 S: 354 Enter message, ending with "." on a line by itself
22 3.200683 10.10.1.4 74.53.140.153 SMTP 1514 C: DATA fragment, 1460 bytes
23 3.200726 10.10.1.4 74.53.140.153 SMTP 1514 C: DATA fragment, 1460 bytes
24 3.200744 10.10.1.4 74.53.140.153 SMTP 1514 C: DATA fragment, 1460 bytes
25 3.200763 10.10.1.4 74.53.140.153 SMTP 1514 [TCP Window Full] C: DATA fragment, 1460 bytes
26 3.203055 192.168.1.1 10.10.1.4 ICMP 590 Destination unreachable (Fragmentation needed)
28 3.203563 192.168.1.1 10.10.1.4 ICMP 590 Destination unreachable (Fragmentation needed)
29 3.204188 192.168.1.1 10.10.1.4 ICMP 590 Destination unreachable (Fragmentation needed)
30 3.204574 192.168.1.1 10.10.1.4 ICMP 590 Destination unreachable (Fragmentation needed)
38 4.002121 10.10.1.4 74.53.140.153 SMTP 1506 C: DATA fragment, 1452 bytes
39 4.002139 10.10.1.4 74.53.140.153 SMTP 1506 C: DATA fragment, 1452 bytes
41 4.342568 10.10.1.4 74.53.140.153 SMTP 1506 C: DATA fragment, 1452 bytes
42 4.342595 10.10.1.4 74.53.140.153 SMTP 1506 C: DATA fragment, 1452 bytes
44 4.366256 10.10.1.4 74.53.140.153 SMTP 1506 C: DATA fragment, 1452 bytes
45 4.366274 10.10.1.4 74.53.140.153 SMTP/I… 83 from: "Gurpartap Singh" <gurpartap@patriots.in>, subject: SMTP, (text/plain) (text/html) (text/plain) (text/plain)
52 4.756729 74.53.140.153 10.10.1.4 SMTP 82 S: 250 OK id=1Mugho-0003Dg-Un
54 7.271765 10.10.1.4 74.53.140.153 SMTP 60 C: QUIT
56 7.613407 74.53.140.153 10.10.1.4 SMTP 102 S: 221 xc90.websitewelcome.com closing connection
Username and password are base64 encoded

What is Base64 encoding

- Base64 encoding is a way to represent binary data in a text format.
- It is often used in email messages, HTML pages, and other types of text-based communication to transfer binary data such as images, audio files, or other types of non-text data.

Index	Binary	Char	Index	Binary	Char	Index	Binary	Char	Index	Binary	Char
0	000000	A	16	010000	Q	32	100000	g	48	110000	w
1	000001	B	17	010001	R	33	100001	h	49	110001	x
2	000010	C	18	010010	S	34	100010	i	50	110010	y
3	000011	D	19	010011	T	35	100011	j	51	110011	z
4	000100	E	20	010100	U	36	100100	k	52	110100	0
5	000101	F	21	010101	V	37	100101	l	53	110101	1
6	000110	G	22	010110	W	38	100110	m	54	110110	2
7	000111	H	23	010111	X	39	100111	n	55	110111	3
8	001000	I	24	011000	Y	40	101000	o	56	111000	4
9	001001	J	25	011001	Z	41	101001	p	57	111001	5
10	001010	K	26	011010	a	42	101010	q	58	111010	6
11	001011	L	27	011011	b	43	101011	r	59	111011	7
12	001100	M	28	011100	c	44	101100	s	60	111100	8
13	001101	N	29	011101	d	45	101101	t	61	111101	9
14	001110	O	30	011110	e	46	101110	u	62	111110	+
15	001111	P	31	011111	f	47	101111	v	63	111111	/

Conversion

Source	Text (ASCII)	M							a								n							
	Octets	77 (0x4d)							97 (0x61)								110 (0x6e)							
Bits		0	1	0	0	1	1	0	1	0	1	1	0	0	0	0	1	0	1	1	0	1	1	1	0
Base64 encoded	Sextets	19							22								5							46
	Character	T							W								F							u
	Octets	84 (0x54)							87 (0x57)								70 (0x46)							117 (0x75)

Source	Text (ASCII)	M							a															
	Octets	77 (0x4d)							97 (0x61)															
Bits		0	1	0	0	1	1	0	1	0	1	1	0	0	0	0	1	0	0						
Base64 encoded	Sextets	19							22								4			Padding				
	Character	T							W								E			=				
	Octets	84 (0x54)							87 (0x57)								69 (0x45)			61 (0x3D)				

Source	Text (ASCII)	M																					
	Octets	77 (0x4d)																					
Bits		0	1	0	0	1	1	0	1	0	0	0	0										
Base64 encoded	Sextets	19								16				Padding						Padding			
	Character	T								Q				=						=			
	Octets	84 (0x54)								81 (0x51)				61 (0x3D)						61 (0x3D)			

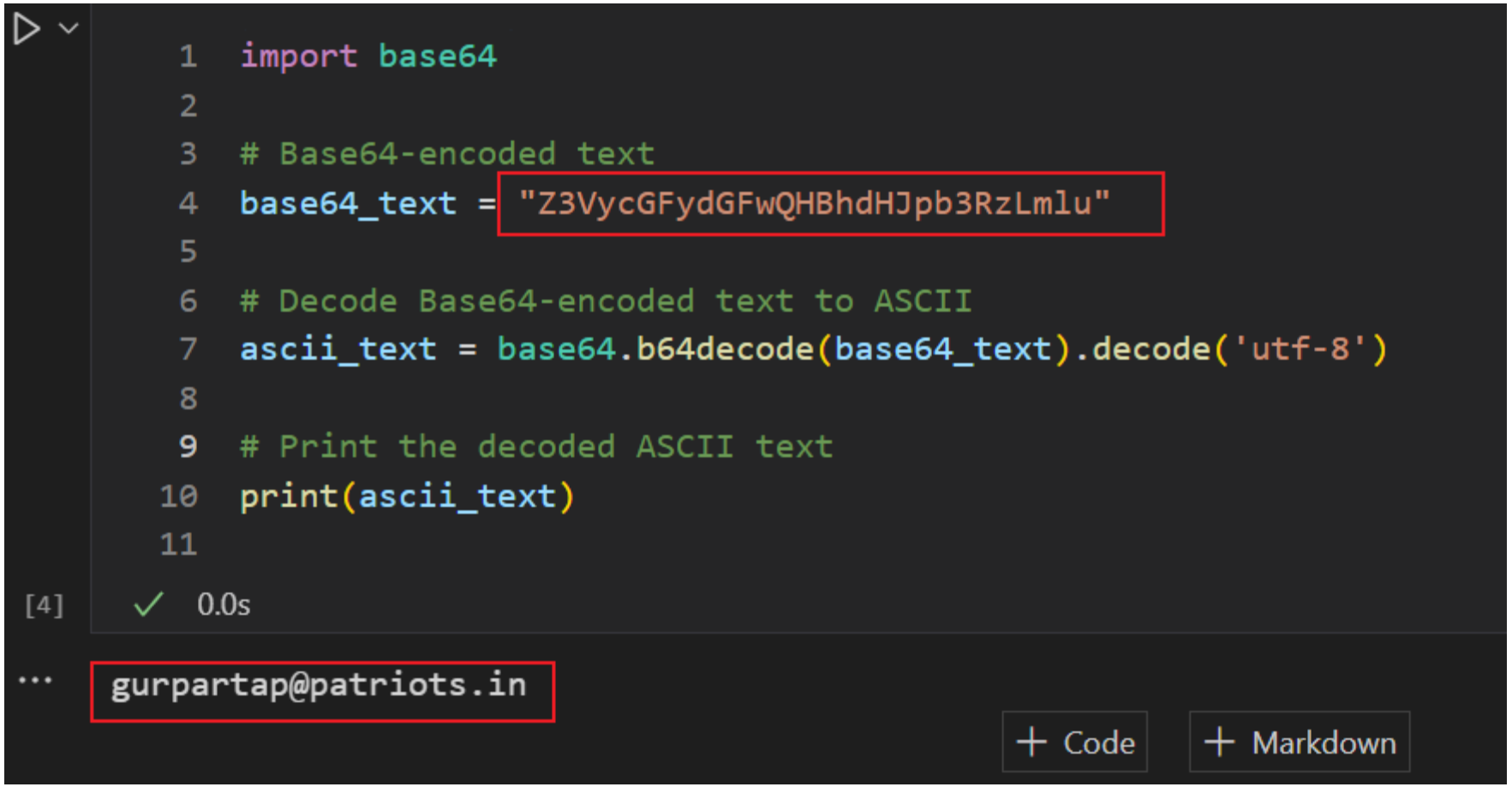
Decoding Based64 to text

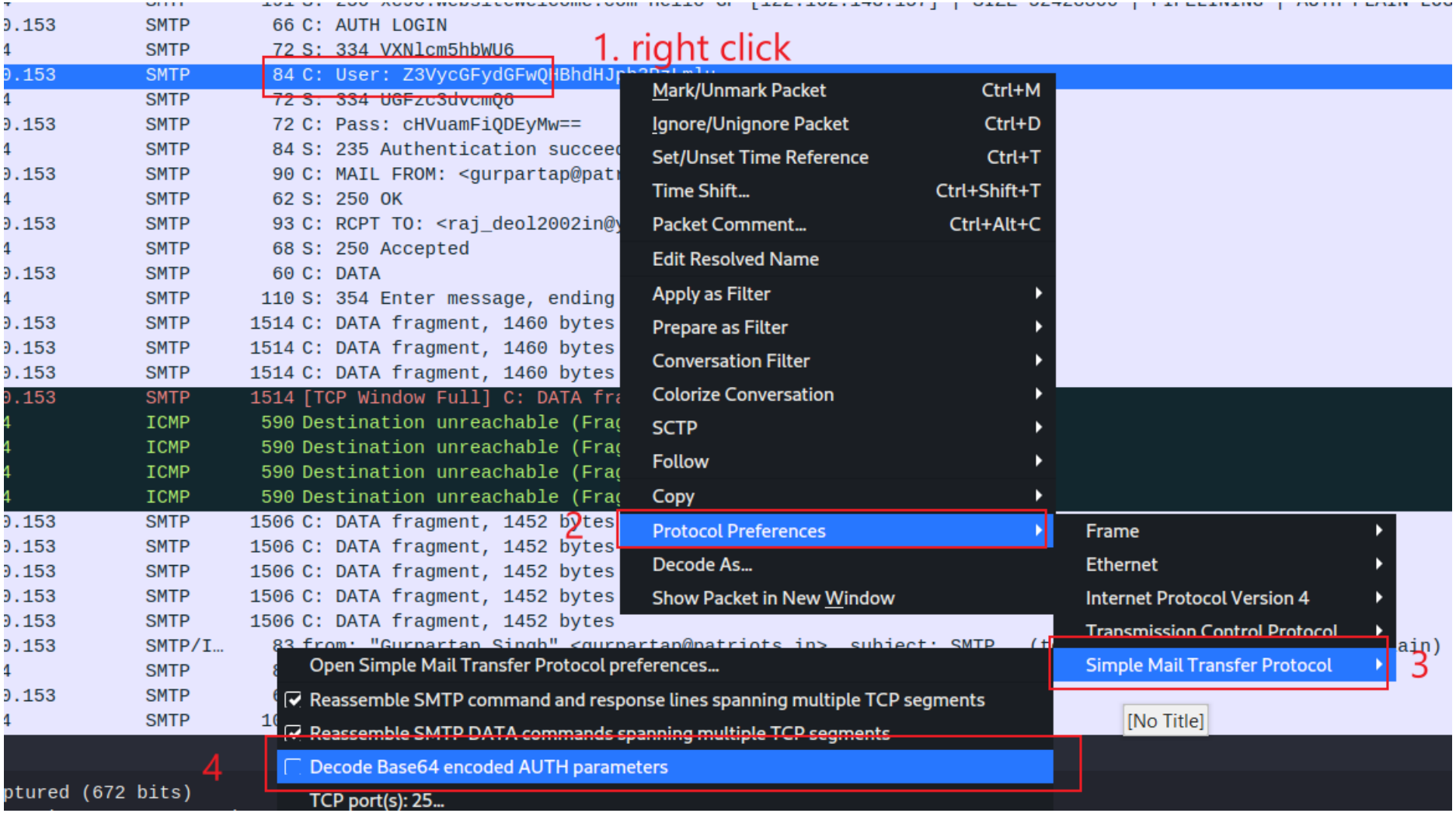
```
1  import base64
2
3  # Base64-encoded text
4  base64_text = "TWFu"
5
6  # Decode Base64-encoded text to ASCII
7  ascii_text = base64.b64decode(base64_text).decode('utf-8')
8
9  # Print the decoded ASCII text
10 print(ascii_text)
11
```

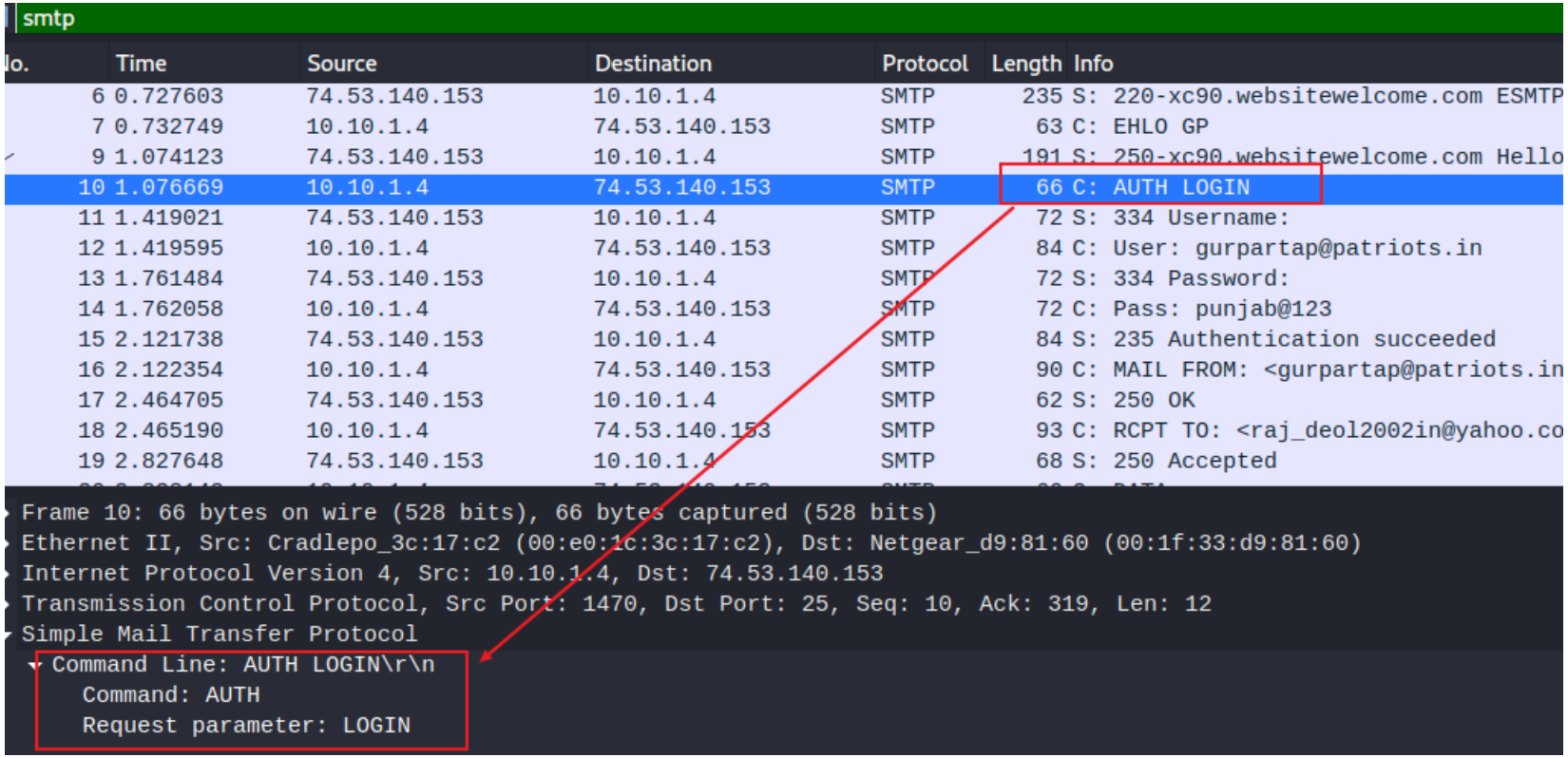
[8] ✓ 0.0s

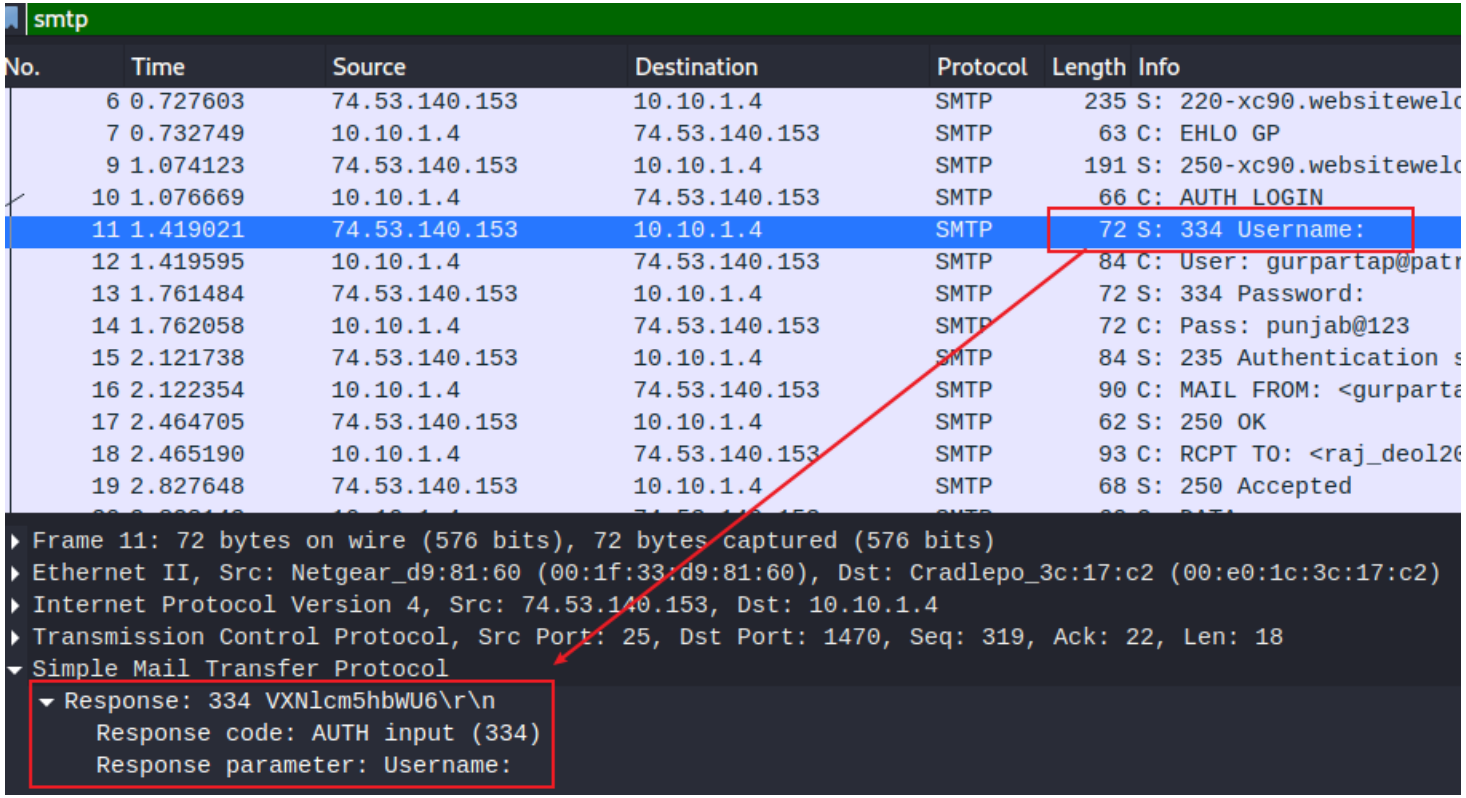
```
Man
```

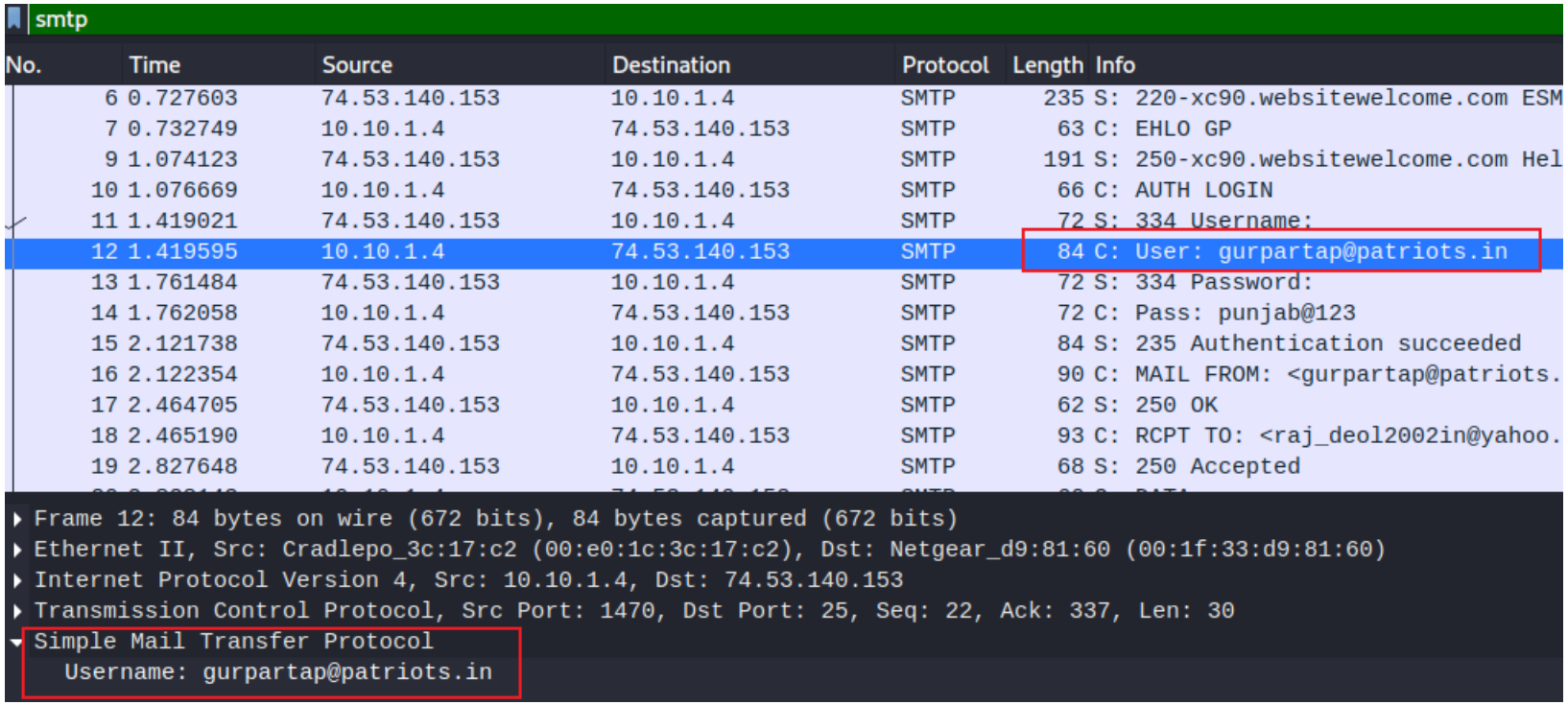
Decoding username




1. right click
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
2
Protocol Preferences
Decode As...
Show Packet in New Window
Frame
Ethernet
Internet Protocol Version 4
Transmission Control Protocol
Simple Mail Transfer Protocol
3
[No Title]
Open Simple Mail Transfer Protocol preferences...
Reassemble SMTP command and response lines spanning multiple TCP segments
Reassemble SMTP DATA commands spanning multiple TCP segments
Decode Base64 encoded AUTH parameters
4
TCP port(s): 25...
ptured (672 bits)


smtp
No. Time Source Destination Protocol Length Info
6 0.727603 74.53.140.153 10.10.1.4 SMTP 235 S: 220-xc90.websitewelcome.com ESMTP
7 0.732749 10.10.1.4 74.53.140.153 SMTP 63 C: EHLO GP
9 1.074123 74.53.140.153 10.10.1.4 SMTP 191 S: 250-xc90.websitewelcome.com Hello
10 1.076669 10.10.1.4 74.53.140.153 SMTP 66 C: AUTH LOGIN
11 1.419021 74.53.140.153 10.10.1.4 SMTP 72 S: 334 Username:
12 1.419595 10.10.1.4 74.53.140.153 SMTP 84 C: User: gurpartap@patriots.in
13 1.761484 74.53.140.153 10.10.1.4 SMTP 72 S: 334 Password:
14 1.762058 10.10.1.4 74.53.140.153 SMTP 72 C: Pass: punjab@123
15 2.121738 74.53.140.153 10.10.1.4 SMTP 84 S: 235 Authentication succeeded
16 2.122354 10.10.1.4 74.53.140.153 SMTP 90 C: MAIL FROM: <gurpartap@patriots.in
17 2.464705 74.53.140.153 10.10.1.4 SMTP 62 S: 250 OK
18 2.465190 10.10.1.4 74.53.140.153 SMTP 93 C: RCPT TO: <raj_deol2002in@yahoo.co
19 2.827648 74.53.140.153 10.10.1.4 SMTP 68 S: 250 Accepted
Frame 10: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: Cradlepo_3c:17:c2 (00:e0:1c:3c:17:c2), Dst: Netgear_d9:81:60 (00:1f:33:d9:81:60)
Internet Protocol Version 4, Src: 10.10.1.4, Dst: 74.53.140.153
Transmission Control Protocol, Src Port: 1470, Dst Port: 25, Seq: 10, Ack: 319, Len: 12
Simple Mail Transfer Protocol
Command Line: AUTH LOGIN\r\n
Command: AUTH
Request parameter: LOGIN


smtp
No. Time Source Destination Protocol Length Info
6 0.727603 74.53.140.153 10.10.1.4 SMTP 235 S: 220-xc90.websitewelc
7 0.732749 10.10.1.4 74.53.140.153 SMTP 63 C: EHLO GP
9 1.074123 74.53.140.153 10.10.1.4 SMTP 191 S: 250-xc90.websitewelc
10 1.076669 10.10.1.4 74.53.140.153 SMTP 66 C: AUTH LOGIN
11 1.419021 74.53.140.153 10.10.1.4 SMTP 72 S: 334 Username:
12 1.419595 10.10.1.4 74.53.140.153 SMTP 84 C: User: gurpartap@patr
13 1.761484 74.53.140.153 10.10.1.4 SMTP 72 S: 334 Password:
14 1.762058 10.10.1.4 74.53.140.153 SMTP 72 C: Pass: punjab@123
15 2.121738 74.53.140.153 10.10.1.4 SMTP 84 S: 235 Authentication s
16 2.122354 10.10.1.4 74.53.140.153 SMTP 90 C: MAIL FROM: <gurparta
17 2.464705 74.53.140.153 10.10.1.4 SMTP 62 S: 250 OK
18 2.465190 10.10.1.4 74.53.140.153 SMTP 93 C: RCPT TO: <raj_deol26
19 2.827648 74.53.140.153 10.10.1.4 SMTP 68 S: 250 Accepted
Frame 11: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)
Ethernet II, Src: Netgear_d9:81:60 (00:1f:33:d9:81:60), Dst: Cradlepo_3c:17:c2 (00:e0:1c:3c:17:c2)
Internet Protocol Version 4, Src: 74.53.140.153, Dst: 10.10.1.4
Transmission Control Protocol, Src Port: 25, Dst Port: 1470, Seq: 319, Ack: 22, Len: 18
Simple Mail Transfer Protocol
Response: 334 VXNlcm5hbWU6\r\n
Response code: AUTH input (334)
Response parameter: Username:


smtp
No. Time Source Destination Protocol Length Info
6 0.727603 74.53.140.153 10.10.1.4 SMTP 235 S: 220-xc90.websitewelcome.com ESM
7 0.732749 10.10.1.4 74.53.140.153 SMTP 63 C: EHLO GP
9 1.074123 74.53.140.153 10.10.1.4 SMTP 191 S: 250-xc90.websitewelcome.com Hel
10 1.076669 10.10.1.4 74.53.140.153 SMTP 66 C: AUTH LOGIN
11 1.419021 74.53.140.153 10.10.1.4 SMTP 72 S: 334 Username:
12 1.419595 10.10.1.4 74.53.140.153 SMTP 84 C: User: gurpartap@patriots.in
13 1.761484 74.53.140.153 10.10.1.4 SMTP 72 S: 334 Password:
14 1.762058 10.10.1.4 74.53.140.153 SMTP 72 C: Pass: punjab@123
15 2.121738 74.53.140.153 10.10.1.4 SMTP 84 S: 235 Authentication succeeded
16 2.122354 10.10.1.4 74.53.140.153 SMTP 90 C: MAIL FROM: <gurpartap@patriots.
17 2.464705 74.53.140.153 10.10.1.4 SMTP 62 S: 250 OK
18 2.465190 10.10.1.4 74.53.140.153 SMTP 93 C: RCPT TO: <raj_deol2002in@yahoo.
19 2.827648 74.53.140.153 10.10.1.4 SMTP 68 S: 250 Accepted
Frame 12: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)
Ethernet II, Src: Cradlepo_3c:17:c2 (00:e0:1c:3c:17:c2), Dst: Netgear_d9:81:60 (00:1f:33:d9:81:60)
Internet Protocol Version 4, Src: 10.10.1.4, Dst: 74.53.140.153
Transmission Control Protocol, Src Port: 1470, Dst Port: 25, Seq: 22, Ack: 337, Len: 30
Simple Mail Transfer Protocol
Username: gurpartap@patriots.in

	Time	Source	Destination	Protocol	Length	Info
6	0.727603	74.53.140.153	10.10.1.4	SMTP	235	S: 220-xc90.websitewelcome.com ESMTP Exim 4.69 #1 Mon, 05 Oct 200
7	0.732749	10.10.1.4	74.53.140.153	SMTP	63	C: EHLO GP
9	1.074123	74.53.140.153	10.10.1.4	SMTP	191	S: 250-xc90.websitewelcome.com Hello GP [122.162.143.157] | SIZE
10	1.076669	10.10.1.4	74.53.140.153	SMTP	66	C: AUTH LOGIN
11	1.419021	74.53.140.153	10.10.1.4	SMTP	72	S: 334 Username:
12	1.419595	10.10.1.4	74.53.140.153	SMTP	84	C: User: gurpartap@patriots.in
13	1.761484	74.53.140.153	10.10.1.4	SMTP	72	S: 334 Password:
14	1.762058	10.10.1.4	74.53.140.153	SMTP	72	C: Pass: punjab@123
15	2.121738	74.53.140.153	10.10.1.4	SMTP	84	S: 235 Authentication succeeded
16	2.122354	10.10.1.4	74.53.140.153	SMTP	90	C: MAIL FROM: <gurpartap@patriots.in>
17	2.464705	74.53.140.153	10.10.1.4	SMTP	62	S: 250 OK
18	2.465190	10.10.1.4	74.53.140.153	SMTP	93	C: RCPT TO: <raj_deol2002in@yahoo.co.in>
19	2.827648	74.53.140.153	10.10.1.4	SMTP	68	S: 250 Accepted
20	2.828143	10.10.1.4	74.53.140.153	SMTP	60	C: DATA
21	3.169619	74.53.140.153	10.10.1.4	SMTP	110	S: 354 Enter message, ending with "." on a line by itself
22	3.200683	10.10.1.4	74.53.140.153	SMTP	1514	C: DATA fragment, 1460 bytes
23	3.200726	10.10.1.4	74.53.140.153	SMTP	1514	C: DATA fragment, 1460 bytes
24	3.200744	10.10.1.4	74.53.140.153	SMTP	1514	C: DATA fragment, 1460 bytes
25	3.200763	10.10.1.4	74.53.140.153	SMTP	1514	[TCP Window Full] C: DATA fragment, 1460 bytes
26	3.203055	192.168.1.1	10.10.1.4	ICMP	590	Destination unreachable (Fragmentation needed)
28	3.203563	192.168.1.1	10.10.1.4	ICMP	590	Destination unreachable (Fragmentation needed)
29	3.204188	192.168.1.1	10.10.1.4	ICMP	590	Destination unreachable (Fragmentation needed)
30	3.204574	192.168.1.1	10.10.1.4	ICMP	590	Destination unreachable (Fragmentation needed)
38	4.002121	10.10.1.4	74.53.140.153	SMTP	1506	C: DATA fragment, 1452 bytes
39	4.002139	10.10.1.4	74.53.140.153	SMTP	1506	C: DATA fragment, 1452 bytes
41	4.342568	10.10.1.4	74.53.140.153	SMTP	1506	C: DATA fragment, 1452 bytes
42	4.342595	10.10.1.4	74.53.140.153	SMTP	1506	C: DATA fragment, 1452 bytes
44	4.366256	10.10.1.4	74.53.140.153	SMTP	1506	C: DATA fragment, 1452 bytes
45	4.366274	10.10.1.4	74.53.140.153	SMTP/I…	83	from: "Gurpartap Singh" <gurpartap@patriots.in>, subject: SMTP,

ignore them

Show email content (14 fragments, Wireshark reassemble them at 45)

No.	Time	Source	Destination	Protocol	Length	Info
40	4.342535	74.53.140.153	10.10.1.4	TCP	60	25 → 1470 [ACK] Seq=463 Ack=5959 Win=17424 Len=0
41	4.342568	10.10.1.4	74.53.140.153	SMTP	1506	C: DATA fragment, 1452 bytes
42	4.342595	10.10.1.4	74.53.140.153	SMTP	1506	C: DATA fragment, 1452 bytes
43	4.366241	74.53.140.153	10.10.1.4	TCP	60	[TCP ACKed unseen segment] 25 → 1470 [ACK] Seq=463 Ack=7411 Win=20328 Len=0
44	4.366256	10.10.1.4	74.53.140.153	SMTP	1506	C: DATA fragment, 1452 bytes
45	4.366274	10.10.1.4	74.53.140.153	SMTP/IMF	83	from: "Gurpartap Singh" <gurpartap@patriots.in>, subject: SMTP, (text/plain) (text/html) (text/plain)
46	4.389163	74.53.140.153	10.10.1.4	TCP	60	25 → 1470 [ACK] Seq=463 Ack=8863 Win=23232 Len=0
47	4.413523	74.53.140.153	10.10.1.4	TCP	60	25 → 1470 [ACK] Seq=463 Ack=10315 Win=26136 Len=0
48	4.708119	74.53.140.153	10.10.1.4	TCP	60	25 → 1470 [ACK] Seq=463 Ack=11767 Win=29040 Len=0
49	4.730686	74.53.140.153	10.10.1.4	TCP	60	25 → 1470 [ACK] Seq=463 Ack=13219 Win=31944 Len=0
50	4.754784	74.53.140.153	10.10.1.4	TCP	60	25 → 1470 [ACK] Seq=463 Ack=14671 Win=34848 Len=0
51	4.756231	74.53.140.153	10.10.1.4	TCP	60	25 → 1470 [ACK] Seq=463 Ack=14700 Win=34848 Len=0
52	4.756729	74.53.140.153	10.10.1.4	SMTP	82	S: 250 OK id=1Mugho-0003Dg-Un
53	4.895535	10.10.1.4	74.53.140.153	TCP	54	1470 → 25 [ACK] Seq=14700 Ack=491 Win=65045 Len=0

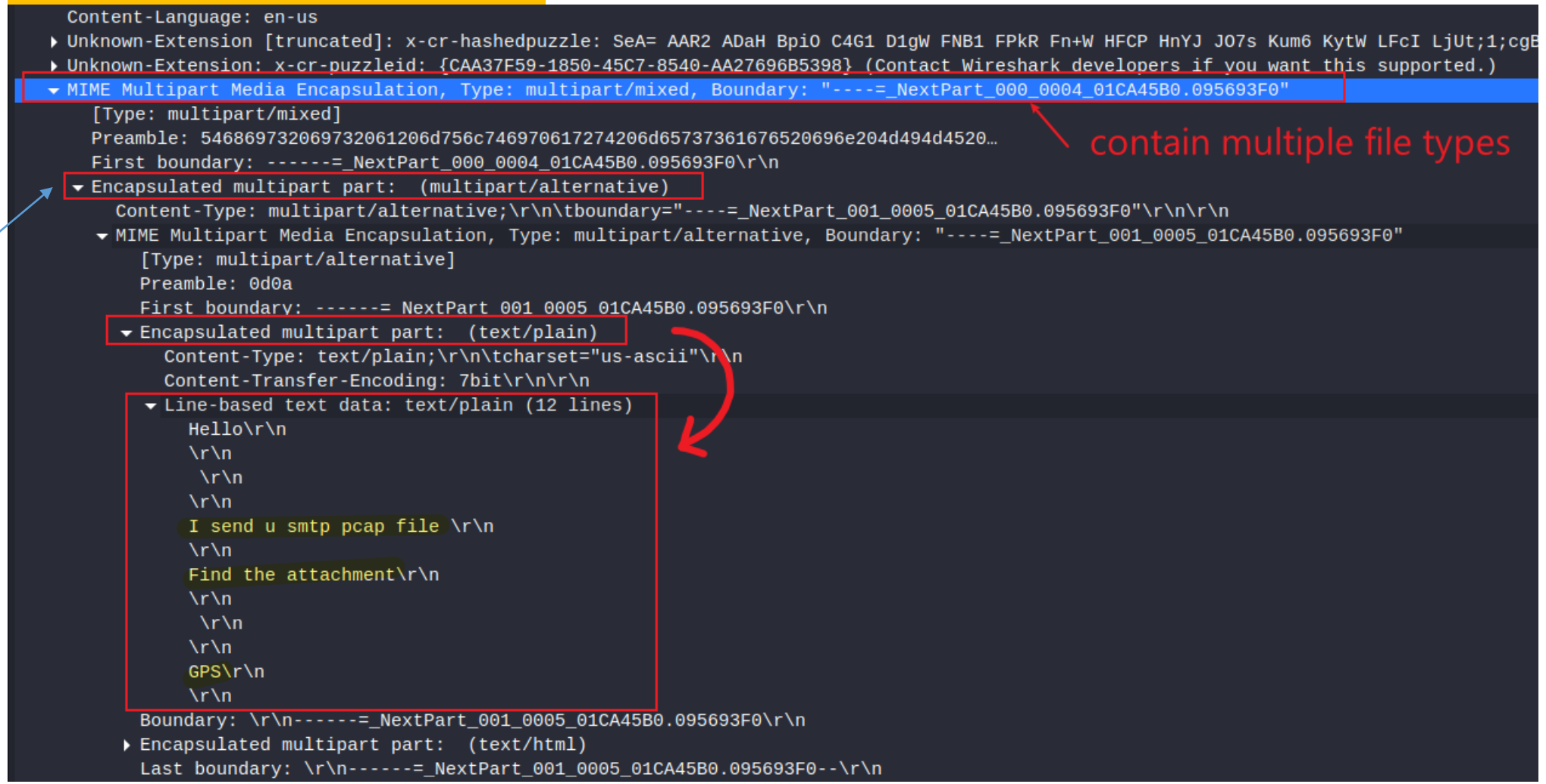
```
▸ Frame 45: 83 bytes on wire (664 bits), 83 bytes captured (664 bits)
▸ Ethernet II, Src: Cradlepo_3c:17:c2 (00:e0:1c:3c:17:c2), Dst: Netgear_d9:81:60 (00:1f:33:d9:81:60)
▸ Internet Protocol Version 4, Src: 10.10.1.4, Dst: 74.53.140.153
▸ Transmission Control Protocol, Src Port: 1470, Dst Port: 25, Seq: 14671, Ack: 463, Len: 29
▾ Simple Mail Transfer Protocol
    C: .
  ▸ [14 DATA fragments (15156 bytes): #22(1460), #23(1460), #24(1460), #25(1460), #26(508), #28(508), #29(508), #30(508), #38(1452), #39(1452), #41(1452), #42(1452), #44(1452), #45(24)]
▾ Internet Message Format
  ▸ From: "Gurpartap Singh" <gurpartap@patriots.in>, 1 item
  ▸ To: <raj_deol2002in@yahoo.co.in>, 1 item
    Subject: SMTP
    Date: Mon, 5 Oct 2009 11:36:07 +0530
    Message-ID: <000301ca4581$ef9e57f0$cedb07d0$@in>
    MIME-Version: 1.0
  ▸ Content-Type: multipart/mixed;\r\n\tboundary="----=_NextPart_000_0004_01CA45B0.095693F0"
    X-Mailer: Microsoft Office Outlook 12.0
    Thread-Index: AcpFgem9BvjjZEDeR1Kh8i+hUyVo0A==
    Content-Language: en-us
  ▸ Unknown-Extension [truncated]: x-cr-hashedpuzzle: SeA= AAR2 ADaH BpiO C4G1 D1gW FNB1 FPkR Fn+W HFCP HnYJ JO7s Kum6 KytW LFcI LjUt;1;cgBhAGoAXwBkAGUAbwBsADIAMAAwADIAaQBuAEAAeQBhAGgAbwB
  ▸ Unknown-Extension: x-cr-puzzleid: {CAA37F59-1850-45C7-8540-AA27696B5398} (Contact Wireshark developers if you want this supported.)
  ▸ MIME Multipart Media Encapsulation, Type: multipart/mixed, Boundary: "----=_NextPart_000_0004_01CA45B0.095693F0"
```

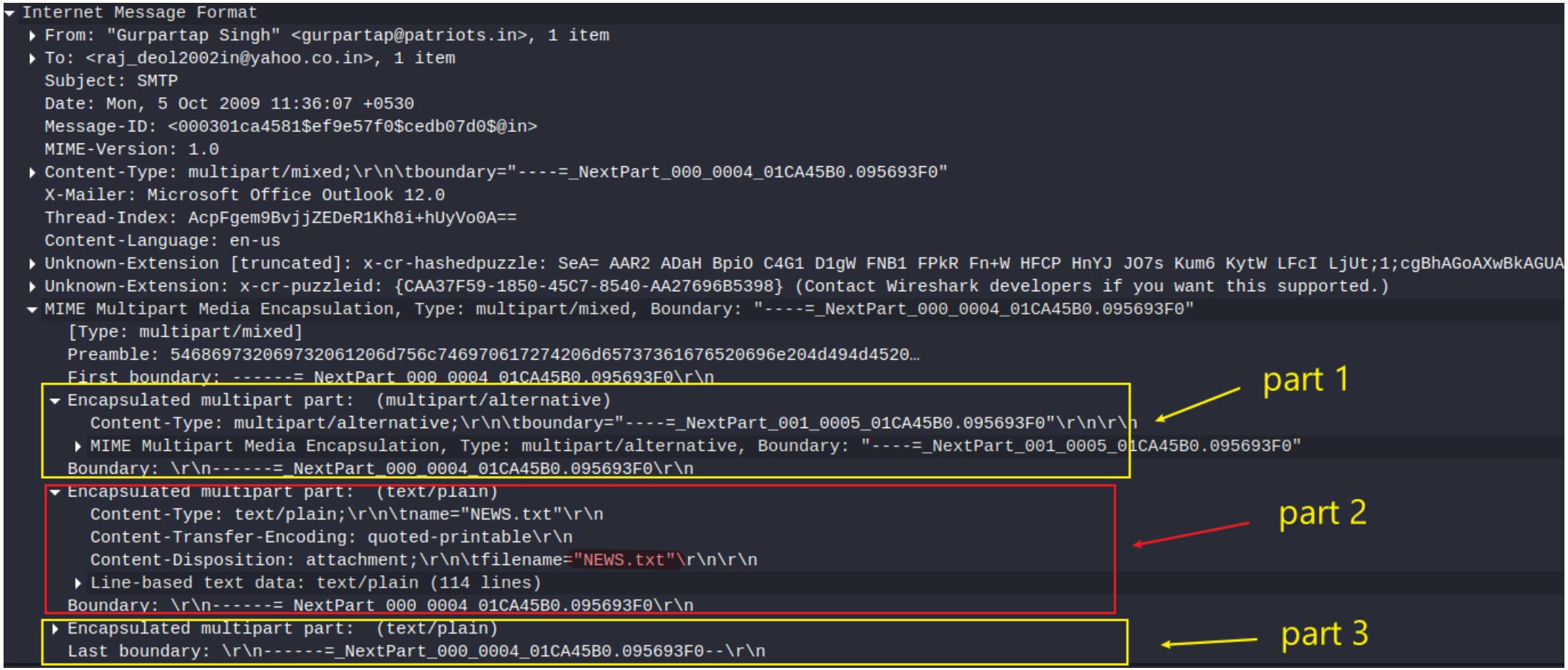
Email consists of 14 fragments

The whole email

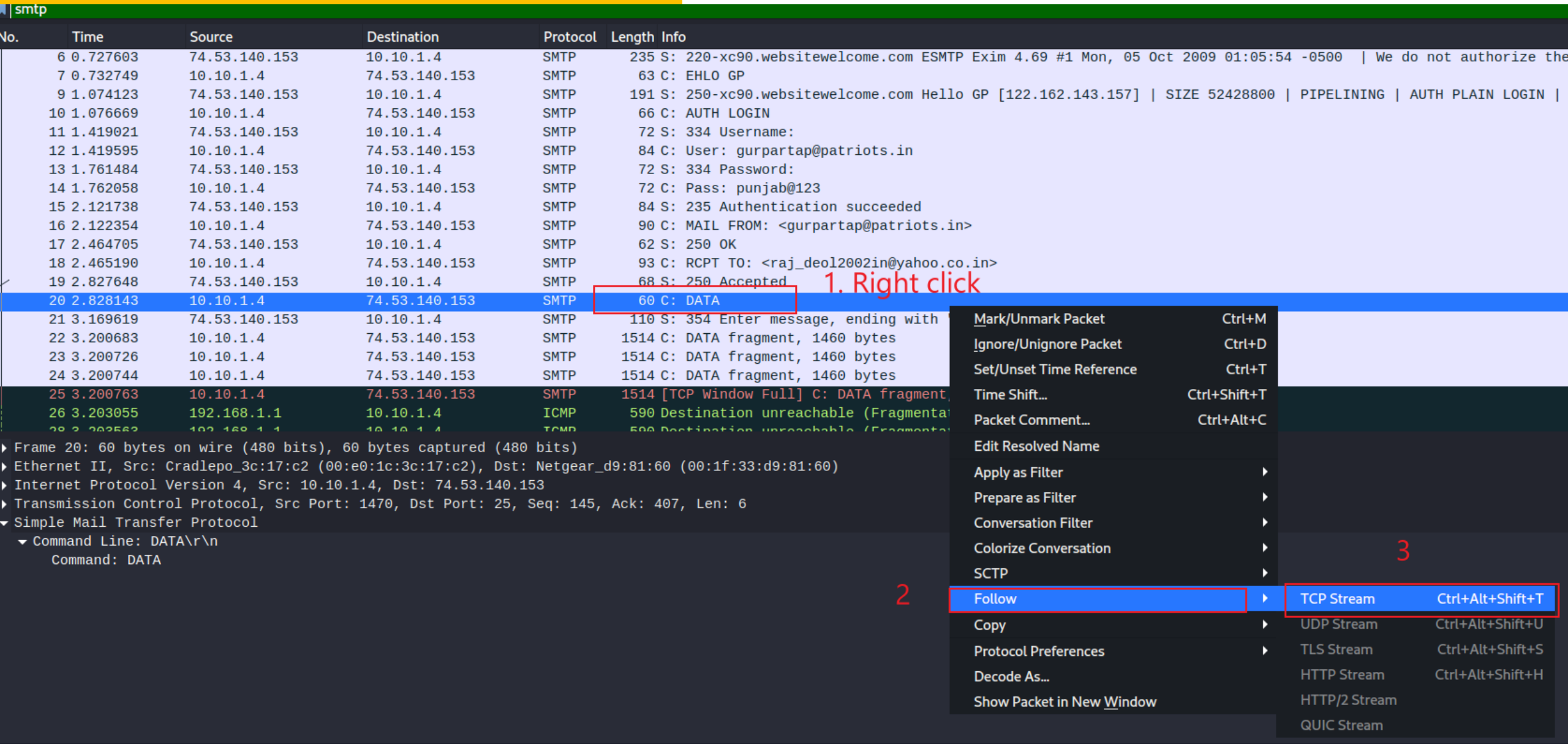
email client: office outlook 12.0

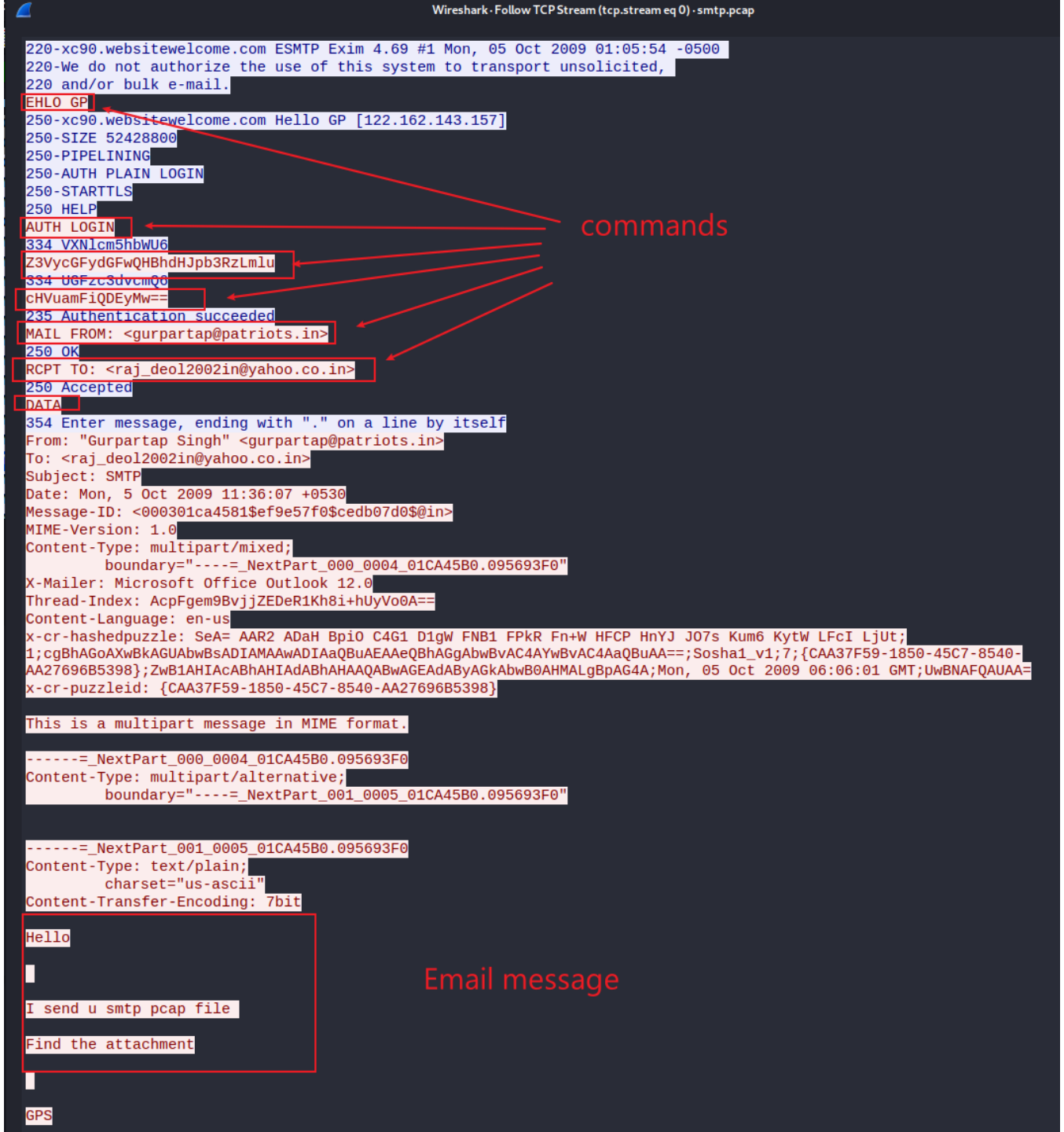
Show email content (text content)




Internet Message Format
From: "Gurpartap Singh" <gurpartap@patriots.in>, 1 item
To: <raj_deol2002in@yahoo.co.in>, 1 item
Subject: SMTP
Date: Mon, 5 Oct 2009 11:36:07 +0530
Message-ID: <000301ca4581$ef9e57f0$cedb07d0$@in>
MIME-Version: 1.0
Content-Type: multipart/mixed;\r\n\tboundary="----=_NextPart_000_0004_01CA45B0.095693F0"
X-Mailer: Microsoft Office Outlook 12.0
Thread-Index: AcpFgem9BvjjZEDeR1Kh8i+hUyVo0A==
Content-Language: en-us
Unknown-Extension [truncated]: x-cr-hashedpuzzle: SeA= AAR2 ADaH BpiO C4G1 D1gW FNB1 FPkR Fn+W HFCP HnYJ JO7s Kum6 KytW LFcI LjUt;1;cgBhAGoAXwBkAGUA
Unknown-Extension: x-cr-puzzleid: {CAA37F59-1850-45C7-8540-AA27696B5398} (Contact Wireshark developers if you want this supported.)
MIME Multipart Media Encapsulation, Type: multipart/mixed, Boundary: "----=_NextPart_000_0004_01CA45B0.095693F0"
[Type: multipart/mixed]
Preamble: 546869732069732061206d756c746970617274206d6573736167652065e204d494d4520…
First boundary: ------=_NextPart_000_0004_01CA45B0.095693F0\r\n
Encapsulated multipart part: (multipart/alternative)
Content-Type: multipart/alternative;\r\n\tboundary="----=_NextPart_001_0005_01CA45B0.095693F0"\r\n\r\n
MIME Multipart Media Encapsulation, Type: multipart/alternative, Boundary: "----=_NextPart_001_0005_01CA45B0.095693F0"
Boundary: \r\n------=_NextPart_000_0004_01CA45B0.095693F0\r\n
Encapsulated multipart part: (text/plain)
Content-Type: text/plain;\r\n\tname="NEWS.txt"\r\n
Content-Transfer-Encoding: quoted-printable\r\n
Content-Disposition: attachment;\r\n\tfilename="NEWS.txt"\r\n\r\n
Line-based text data: text/plain (114 lines)
Boundary: \r\n------=_NextPart_000_0004_01CA45B0.095693F0\r\n
Encapsulated multipart part: (text/plain)
Last boundary: \r\n------=_NextPart_000_0004_01CA45B0.095693F0--\r\n
part 1
part 2
part 3

Show email content (Alternative approach: follow TCP)




Wireshark · Follow TCP Stream (tcp.stream eq 0) · smtp.pcap
220-xc90.websitewelcome.com ESMTP Exim 4.69 #1 Mon, 05 Oct 2009 01:05:54 -0500
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
EHLO GP
250-xc90.websitewelcome.com Hello GP [122.162.143.157]
250-SIZE 52428800
250-PIPELINING
250-AUTH PLAIN LOGIN
250-STARTTLS
250 HELP
AUTH LOGIN
334 VXNlcm5hbWU6
Z3VycGFydGFwQHBhdHJpb3RzLmlu
334 UGFzc3dvcmQ6
cHVuamFiQDEyMw==
235 Authentication succeeded
MAIL FROM: <gurpartap@patriots.in>
250 OK
RCPT TO: <raj_deol2002in@yahoo.co.in>
250 Accepted
DATA
354 Enter message, ending with "." on a line by itself
From: "Gurpartap Singh" <gurpartap@patriots.in>
To: <raj_deol2002in@yahoo.co.in>
Subject: SMTP
Date: Mon, 5 Oct 2009 11:36:07 +0530
Message-ID: <000301ca4581$ef9e57f0$cedb07d0$@in>
MIME-Version: 1.0
Content-Type: multipart/mixed;
boundary="----=_NextPart_000_0004_01CA45B0.095693F0"
X-Mailer: Microsoft Office Outlook 12.0
Thread-Index: AcpFgem9BvjjZEDeR1Kh8i+hUyVo0A==
Content-Language: en-us
x-cr-hashedpuzzle: SeA= AAR2 ADaH BpiO C4G1 D1gW FNB1 FPkR Fn+W HFCP HnYJ JO7s Kum6 KytW LFcI LjUt;
1;cgBhAGoAXwBkAGUAbwBsADIAMAAwADIAaQBuAEAAeQBhAGgAbwBvAC4AYwBvAC4AaQBuAA==;Sosha1_v1;7;{CAA37F59-1850-45C7-8540-
AA27696B5398};ZwB1AHIAcABhAHIAdABhAHAAQABwAGEAdAByAGkAbwB0AHMALgBpAG4A;Mon, 05 Oct 2009 06:06:01 GMT;UwBNAFQAUAA=
x-cr-puzzleid: {CAA37F59-1850-45C7-8540-AA27696B5398}
This is a multipart message in MIME format.
------=_NextPart_000_0004_01CA45B0.095693F0
Content-Type: multipart/alternative;
boundary="----=_NextPart_001_0005_01CA45B0.095693F0"
------=_NextPart_001_0005_01CA45B0.095693F0
Content-Type: text/plain;
charset="us-ascii"
Content-Transfer-Encoding: 7bit
Hello
I send u smtp pcap file
Find the attachment
GPS
commands
Email message

Questions you need to answer

- When did it happen?
  - the timestamps email
- The email client
  - outlook
- The content of the email
  - multiple parts
- What was the approach?
  - ports (sender and receiver)
  - IP addresses (sender and receiver)
  - Mac addresses (sender and receiver)

Extra credits

- Sniff SMTP traffic