

Protokol E-mail

Nama Penulis

inungf@ymail.com

<http://inungandthenotes.blogspot.com>

Lisensi Dokumen:

Copyright © 2003-20013 IlmuKomputer.Com

Seluruh dokumen di IlmuKomputer.Com dapat digunakan, dimodifikasi dan disebarkan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak menghapus atau merubah atribut penulis dan pernyataan copyright yang disertakan dalam setiap dokumen. Tidak diperbolehkan melakukan penulisan ulang, kecuali mendapatkan ijin terlebih dahulu dari IlmuKomputer.Com.

E-mail merupakan salah satu media elektronik yang digunakan untuk mengirim pesan dari suatu alamat ke alamat yang lain. Dalam pengiriman e-mail ini diperlukan suatu protokol yang menyertai pengiriman suatu pesan tersebut. Diantaranya adalah SMTP, POP3, dan IMAP. Dari ketiga protokol-protokol tersebut memiliki peran masing-masing dalam proses pengiriman suatu e-mail. Berikut penjelasan singkat dari ketiga protokol e-mail tersebut.

SMTP (Simple Mail Transfer Protocol) merupakan salah satu protokol email yang umum digunakan untuk pengiriman email di Internet. Protokol ini dipergunakan untuk mengirimkan data dari komputer pengirim ke server email tujuan.

POP3 (Post Office Protocol version 3) adalah protokol email yang digunakan untuk mengambil email dari server (pull email). Protokol POP3 ditujukan agar ada yang menyimpan email untuk sementara sampai email tersebut diambil oleh penerimanya di komputernya.

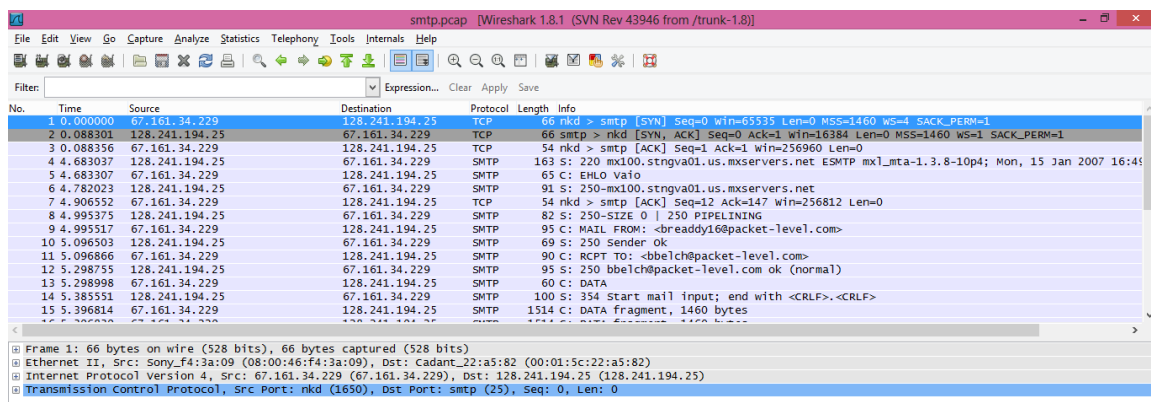
IMAP (Internet Message Access Protocol) adalah protokol standar untuk mengakses atau mengambil email dari server. IMAP memungkinkan pengguna memilih pesan email yang akan diambil, membuat folder di server, mencari email tertentu, maupun menghapus email yang ada. Ini lebih baik daripada POP (Post Office Protocol) yang hanya memperbolehkan kita mengambil/download semua pesan yang ada tanpa terkecuali. Dengan IMAP terjadi komunikasi dua arah, sehingga terjadi sinkronisasi data. Sedangkan POP yang hanya satu arah, yaitu

download saja dari email server ke komputer atau perangkat anda yang sudah terpasang email client.

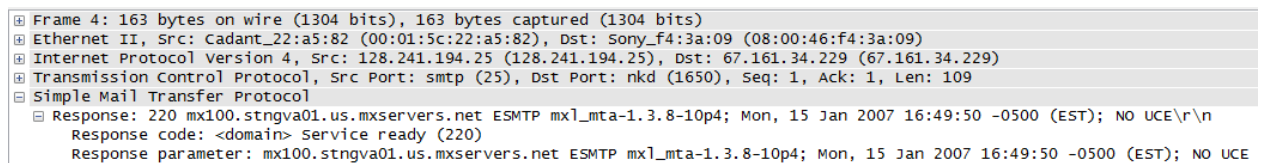
Dari ketiga protokol di atas kita dapat melakukan monitoring tentang lalu lalang protokol ketika sedang melakukan kirim, membuka, ataupun mengunduh email. Dengan menggunakan aplikasi wireshark, protokol tersebut mampu tercapture dengan baik. Dan tentunya harus menggunakan koneksi internet sehingga *interface* yang akan dicapture bisa menampilkan protokol-protokol tersebut.

Berikut contoh protokol email yang tercapture oleh wireshark.

1. SMTP



Sebelum melakukan pengiriman ke suatu alamat email. Client diharuskan membuat koneksi dengan server agar koneksi tersebut *established*, ini merupakan salah satu ciri dari koneksi menggunakan TCP yang *connection-oriented*. Koneksi dari client dan server diketahui dari frame 1 sampai 3. Lalu pada frame ke-4 diketahui keterangan sebagai berikut.



Yang menunjukkan bahwa server telah siap untuk melakukan pengiriman. Berlanjut pada frame berikutnya yang tercapture adalah alamat email pengirim yaitu sebagai berikut.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	67.161.34.229	128.241.194.25	TCP	66	nkd > smtp [SYN] Seq=0 win=65535 Len=0 MSS=1460 WS=4 SACK_PERM=1
2	0.088301	128.241.194.25	67.161.34.229	TCP	66	smtp > nkd [SYN, ACK] Seq=0 Ack=1 win=16384 Len=0 MSS=1460 WS=1 SACK_PERM=1
3	0.088356	67.161.34.229	128.241.194.25	TCP	54	nkd > smtp [ACK] Seq=1 Ack=1 win=256960 Len=0
4	4.683037	128.241.194.25	67.161.34.229	SMTP	163	S: 220 mx100.stngva01.us.mxservers.net ESMTP mx1_mta-1.3.8-10p4; Mon, 15 Jan 2007 16:45
5	4.683307	67.161.34.229	128.241.194.25	SMTP	65	C: EHLO vaio
6	4.782023	128.241.194.25	67.161.34.229	SMTP	91	S: 250-mx100.stngva01.us.mxservers.net
7	4.906552	67.161.34.229	128.241.194.25	TCP	54	nkd > smtp [ACK] Seq=12 Ack=147 win=256812 Len=0
8	4.995375	128.241.194.25	67.161.34.229	SMTP	82	S: 250-SIZE 0 250 PIPELINING
9	4.995517	67.161.34.229	128.241.194.25	SMTP	95	C: MAIL FROM: <bready16@packet-level.com>
10	5.096503	128.241.194.25	67.161.34.229	SMTP	69	S: 250 Sender ok
11	5.096866	67.161.34.229	128.241.194.25	SMTP	90	C: RCPT TO: <bbelch@packet-level.com>
12	5.298755	128.241.194.25	67.161.34.229	SMTP	95	S: 250 bbelch@packet-level.com ok (normal)
13	5.298998	67.161.34.229	128.241.194.25	SMTP	60	C: DATA
14	5.385551	128.241.194.25	67.161.34.229	SMTP	100	S: 354 Start mail input; end with <CRLF>.<CRLF>
15	5.396814	67.161.34.229	128.241.194.25	SMTP	1514	C: DATA Fragment, 1460 bytes

Frame 9: 95 bytes on wire (760 bits), 95 bytes captured (760 bits)
 Ethernet II, Src: Sony_F4:3a:09 (08:00:46:F4:3a:09), Dst: Cadant_22:a5:82 (00:01:5c:22:a5:82)
 Internet Protocol Version 4, Src: 67.161.34.229 (67.161.34.229), Dst: 128.241.194.25 (128.241.194.25)
 Transmission Control Protocol, Src Port: nkd (1650), Dst Port: smtp (25), Seq: 12, Ack: 175, Len: 41
 Simple Mail Transfer Protocol
 Command Line: MAIL FROM: <bready16@packet-level.com>\r\n
 Command: MAIL
 Request parameter: FROM: <bready16@packet-level.com>

Karena pada frame sebelumnya server telah siap, maka ketika pengirim mengirim suatu email server akan menunjukkan bahwa *Request mail action okay*,

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	67.161.34.229	128.241.194.25	TCP	66	nkd > smtp [SYN] Seq=0 win=65535 Len=0 MSS=1460 WS=4 SACK_PERM=1
2	0.088301	128.241.194.25	67.161.34.229	TCP	66	smtp > nkd [SYN, ACK] Seq=0 Ack=1 win=16384 Len=0 MSS=1460 WS=1 SACK_PERM=1
3	0.088356	67.161.34.229	128.241.194.25	TCP	54	nkd > smtp [ACK] Seq=1 Ack=1 win=256960 Len=0
4	4.683037	128.241.194.25	67.161.34.229	SMTP	163	S: 220 mx100.stngva01.us.mxservers.net ESMTP mx1_mta-1.3.8-10p4; Mon, 15 Jan 2007 16:45
5	4.683307	67.161.34.229	128.241.194.25	SMTP	65	C: EHLO vaio
6	4.782023	128.241.194.25	67.161.34.229	SMTP	91	S: 250-mx100.stngva01.us.mxservers.net
7	4.906552	67.161.34.229	128.241.194.25	TCP	54	nkd > smtp [ACK] Seq=12 Ack=147 win=256812 Len=0
8	4.995375	128.241.194.25	67.161.34.229	SMTP	82	S: 250-SIZE 0 250 PIPELINING
9	4.995517	67.161.34.229	128.241.194.25	SMTP	95	C: MAIL FROM: <bready16@packet-level.com>
10	5.096503	128.241.194.25	67.161.34.229	SMTP	69	S: 250 Sender ok
11	5.096866	67.161.34.229	128.241.194.25	SMTP	90	C: RCPT TO: <bbelch@packet-level.com>
12	5.298755	128.241.194.25	67.161.34.229	SMTP	95	S: 250 bbelch@packet-level.com ok (normal)
13	5.298998	67.161.34.229	128.241.194.25	SMTP	60	C: DATA
14	5.385551	128.241.194.25	67.161.34.229	SMTP	100	S: 354 Start mail input; end with <CRLF>.<CRLF>
15	5.396814	67.161.34.229	128.241.194.25	SMTP	1514	C: DATA Fragment, 1460 bytes

Frame 10: 69 bytes on wire (552 bits), 69 bytes captured (552 bits)
 Ethernet II, Src: Cadant_22:a5:82 (00:01:5c:22:a5:82), Dst: Sony_F4:3a:09 (08:00:46:F4:3a:09)
 Internet Protocol Version 4, Src: 128.241.194.25 (128.241.194.25), Dst: 67.161.34.229 (67.161.34.229)
 Transmission Control Protocol, Src Port: smtp (25), Dst Port: nkd (1650), Seq: 175, Ack: 53, Len: 15
 Simple Mail Transfer Protocol
 Response: 250 Sender ok\r\n
 Response code: Requested mail action okay, completed (250)
 Response parameter: Sender ok

Protokol pada frame berikutnya yang tercapture adalah alamat email yang dituju.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	67.161.34.229	128.241.194.25	TCP	66	nkd > smtp [SYN] Seq=0 win=65535 Len=0 MSS=1460 WS=4 SACK_PERM=1
2	0.088301	128.241.194.25	67.161.34.229	TCP	66	smtp > nkd [SYN, ACK] Seq=0 Ack=1 win=16384 Len=0 MSS=1460 WS=1 SACK_PERM=1
3	0.088356	67.161.34.229	128.241.194.25	TCP	54	nkd > smtp [ACK] Seq=1 Ack=1 win=256960 Len=0
4	4.683037	128.241.194.25	67.161.34.229	SMTP	163	S: 220 mx100.stngva01.us.mxservers.net ESMTP mx1_mta-1.3.8-10p4; Mon, 15 Jan 2007 16:45
5	4.683307	67.161.34.229	128.241.194.25	SMTP	65	C: EHLO vaio
6	4.782023	128.241.194.25	67.161.34.229	SMTP	91	S: 250-mx100.stngva01.us.mxservers.net
7	4.906552	67.161.34.229	128.241.194.25	TCP	54	nkd > smtp [ACK] Seq=12 Ack=147 win=256812 Len=0
8	4.995375	128.241.194.25	67.161.34.229	SMTP	82	S: 250-SIZE 0 250 PIPELINING
9	4.995517	67.161.34.229	128.241.194.25	SMTP	95	C: MAIL FROM: <bready16@packet-level.com>
10	5.096503	128.241.194.25	67.161.34.229	SMTP	69	S: 250 Sender ok
11	5.096866	67.161.34.229	128.241.194.25	SMTP	90	C: RCPT TO: <bbelch@packet-level.com>
12	5.298755	128.241.194.25	67.161.34.229	SMTP	95	S: 250 bbelch@packet-level.com ok (normal)
13	5.298998	67.161.34.229	128.241.194.25	SMTP	60	C: DATA
14	5.385551	128.241.194.25	67.161.34.229	SMTP	100	S: 354 Start mail input; end with <CRLF>.<CRLF>
15	5.396814	67.161.34.229	128.241.194.25	SMTP	1514	C: DATA Fragment, 1460 bytes

Frame 11: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
 Ethernet II, Src: Sony_F4:3a:09 (08:00:46:F4:3a:09), Dst: Cadant_22:a5:82 (00:01:5c:22:a5:82)
 Internet Protocol Version 4, Src: 67.161.34.229 (67.161.34.229), Dst: 128.241.194.25 (128.241.194.25)
 Transmission Control Protocol, Src Port: nkd (1650), Dst Port: smtp (25), Seq: 53, Ack: 190, Len: 36
 Simple Mail Transfer Protocol
 Command Line: RCPT TO: <bbelch@packet-level.com>\r\n
 Command: RCPT
 Request parameter: TO: <bbelch@packet-level.com>

Pada frame 11, server yang telah menerima permintaan email mengirim balik dengan *Request mail action okay*. Berikut adalah form yang berisi pengirim dan penerima.

No.	Time	Source	Destination	Protocol	Length	Info
14	5.383531	128.241.194.25	67.161.34.229	SMTP	100	S: 394 Start mail input; end with <CRLF>.<CRLF>
15	5.396814	67.161.34.229	128.241.194.25	SMTP	1514	C: DATA fragment, 1460 bytes
16	5.396839	67.161.34.229	128.241.194.25	SMTP	1514	C: DATA fragment, 1460 bytes
17	5.396852	67.161.34.229	128.241.194.25	SMTP	1476	C: DATA fragment, 1422 bytes
18	5.496652	128.241.194.25	67.161.34.229	TCP	60	smtp > nkd [ACK] Seq=277 Ack=3015 Win=65535 Len=0
19	5.496674	67.161.34.229	128.241.194.25	IMF	59	From: "Brian Readdy16" <bready16@packet-level.com>, subject: Test email,
20	5.500820	128.241.194.25	67.161.34.229	TCP	60	smtp > nkd [ACK] Seq=277 Ack=4437 Win=64113 Len=0
21	5.718332	128.241.194.25	67.161.34.229	TCP	60	smtp > nkd [ACK] Seq=277 Ack=4442 Win=64108 Len=0
22	5.360434	128.241.194.25	67.161.34.229	SMTP	102	S: 250 0-0484658135 Message accepted for delivery
23	6.511697	67.161.34.229	128.241.194.25	TCP	54	nkd > smtp [ACK] Seq=4442 Ack=325 Win=256636 Len=0
24	8.870299	67.161.34.229	128.241.194.25	SMTP	60	C: QUIT
25	8.870419	67.161.34.229	128.241.194.25	TCP	54	nkd > smtp [FIN, ACK] Seq=4448 Ack=325 Win=256636 Len=0
26	8.958082	128.241.194.25	67.161.34.229	SMTP	128	S: 221 mx100.stngva01.us.mxservers.net service closing transmission channel
27	8.958126	67.161.34.229	128.241.194.25	TCP	54	nkd > smtp [RST, ACK] Seq=4449 Ack=399 Win=0 Len=0
28	8.959077	128.241.194.25	67.161.34.229	TCP	60	smtp > nkd [FIN, ACK] Seq=399 Ack=4448 Win=64102 Len=0
29	8.959097	67.161.34.229	128.241.194.25	TCP	54	nkd > smtp [RST] Seq=4448 Win=0 Len=0

C: .
 [3 DATA fragments (4342 bytes): #15(1460), #16(1460), #17(1422)]
 Internet Message Format
 From: "Brian Readdy16" <bready16@packet-level.com>, 1 item
 To: "Barnel Belch" <bbelch@packet-level.com>, 1 item
 Subject: Test email
 Date: Mon, 15 Jan 2007 13:55:23 -0800
 Message-ID: <006d01c738ef5e44a9905e522a143@hq.wmbnet>
 MIME-Version: 1.0
 Content-Type: multipart/alternative;\r\n\r\nboundary="-----_NextPart_000_006E_01C738AC.D7216990"
 X-Mailer: Microsoft Office Outlook 11
 Thread-Index: Acc479ph2gILPVD6gq1KnNrF3RphpQ==
 X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.3028\r\n
 The multipart dissector could not find the required boundary parameter.
 Data (3866 bytes)

Setelah email terkirim ke alamat yang dituju, pengirim mengirimkan paket yang berisi *Quit* yang menandakan proses telah selesai.

No.	Time	Source	Destination	Protocol	Length	Info
24	8.870299	67.161.34.229	128.241.194.25	SMTP	60	C: QUIT
25	8.870419	67.161.34.229	128.241.194.25	TCP	54	nkd > smtp [FIN, ACK] Seq=4448 Ack=325 Win=256636 Len=0
26	8.958082	128.241.194.25	67.161.34.229	SMTP	128	S: 221 mx100.stngva01.us.mxservers.net service closing transmission channel
27	8.958126	67.161.34.229	128.241.194.25	TCP	54	nkd > smtp [RST, ACK] Seq=4449 Ack=399 Win=0 Len=0
28	8.959077	128.241.194.25	67.161.34.229	TCP	60	smtp > nkd [FIN, ACK] Seq=399 Ack=4448 Win=64102 Len=0
29	8.959097	67.161.34.229	128.241.194.25	TCP	54	nkd > smtp [RST] Seq=4448 Win=0 Len=0
30	8.963616	128.241.194.25	67.161.34.229	TCP	60	smtp > nkd [ACK] Seq=400 Ack=4449 Win=64102 Len=0
31	8.963628	67.161.34.229	128.241.194.25	TCP	54	nkd > smtp [RST] Seq=4449 Win=0 Len=0

Frame 24: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
 Ethernet II, Src: Sony_F4:3a:09 (08:00:46:F4:3a:09), Dst: cadant_22:a5:82 (00:01:5c:22:a5:82)
 Internet Protocol Version 4, Src: 67.161.34.229 (67.161.34.229), Dst: 128.241.194.25 (128.241.194.25)
 Transmission Control Protocol, Src Port: nkd (1650), Dst Port: smtp (25), Seq: 4442, Ack: 325, Len: 6
 Simple Mail Transfer Protocol
 Command Line: QUIT\r\n
 Command: QUIT

2. POP3

No.	Time	Source	Destination	Protocol	Length	Info
1	0.900000	67.161.34.229	128.241.194.25	TCP	66	isis-ambc > pop3 [SYN] Seq=0 Win=65525 Len=0 MSS=1460 WS=4 SACK_PERM=1
2	0.086899	128.241.194.25	67.161.34.229	TCP	66	pop3 > isis-ambc [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 WS=1 SACK_PERM=1
3	0.086943	67.161.34.229	128.241.194.25	TCP	54	isis-ambc > pop3 [ACK] Seq=1 Ack=1 Win=256960 Len=0
4	4.680620	128.241.194.25	67.161.34.229	POP	103	S: +OK POP3 [128.241.194.25] v2000.70 server ready
5	4.681007	67.161.34.229	128.241.194.25	POP	70	C: USER rgantrey1
6	4.770897	128.241.194.25	67.161.34.229	POP	95	S: +OK user name accepted, password please
7	4.771077	67.161.34.229	128.241.194.25	POP	69	C: PASS abcdefgh
8	4.886065	128.241.194.25	67.161.34.229	POP	84	S: +OK Mailbox open, 1 messages
9	4.886357	67.161.34.229	128.241.194.25	POP	60	C: STAT
10	4.978243	128.241.194.25	67.161.34.229	POP	67	S: +OK 1 11110 ainul
11	4.978520	67.161.34.229	128.241.194.25	POP	60	C: UIDL
12	5.071986	128.241.194.25	67.161.34.229	POP	108	S: +OK Unique-ID listing follows
13	5.072202	67.161.34.229	128.241.194.25	POP	60	C: LIST
14	5.166592	128.241.194.25	67.161.34.229	POP	100	S: +OK Mailbox scan listing follows
15	5.168841	67.161.34.229	128.241.194.25	POP	62	C: RETR 1

Frame 2: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)

Sama dengan protokol sebelumnya, POP3 juga menggunakan jasa TCP sebagai *transport protocol*, oleh karena itu koneksi antara client dan server harus tetap *established* dengan membentuk *three ways handshaking* terlebih dahulu seperti pada frame 1 sampai 3.

Protokol POP3 sering digunakan untuk *sniffing* password dari suatu *social media*. Dari frame ketiga menunjukkan bahwa server telah siap melakukan koneksi dengan *client* melalui protokol POP.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	67.161.34.229	128.241.194.25	TCP	66	isis-ambc > pop3 [SYN] Seq=0 win=65535 Len=0 MSS=1460 WS=4 SACK_PERM=1
2	0.086899	128.241.194.25	67.161.34.229	TCP	66	pop3 > isis-ambc [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 WS=1 SACK_PERM=1
3	0.086943	67.161.34.229	128.241.194.25	TCP	54	isis-ambc > pop3 [ACK] Seq=1 Ack=1 Win=256960 Len=0
4	4.680620	128.241.194.25	67.161.34.229	POP	103	S: +OK POP3 [128.241.194.25] v2000.70 server ready
5	4.681007	67.161.34.229	128.241.194.25	POP	70	C: USER rgantrey1
6	4.770897	128.241.194.25	67.161.34.229	POP	95	S: +OK user name accepted, password please
7	4.771077	67.161.34.229	128.241.194.25	POP	69	C: PASS abcdefgh
8	4.886065	128.241.194.25	67.161.34.229	POP	84	S: +OK Mailbox open, 1 messages
9	4.886357	67.161.34.229	128.241.194.25	POP	60	C: STAT
10	4.978243	128.241.194.25	67.161.34.229	POP	67	S: +OK 1 11110
11	4.978520	67.161.34.229	128.241.194.25	POP	60	C: UIDL
12	5.071986	128.241.194.25	67.161.34.229	POP	108	S: +OK Unique-ID listing follows
13	5.072202	67.161.34.229	128.241.194.25	POP	60	C: LIST
14	5.166592	128.241.194.25	67.161.34.229	POP	100	S: +OK Mailbox scan listing follows
15	5.168841	67.161.34.229	128.241.194.25	POP	62	C: RETR 1

Frame 5: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
 Ethernet II, Src: Sony_F4:3a:09 (08:00:46:F4:3a:09), Dst: cadant_22:a5:82 (00:01:5c:22:a5:82)
 Internet Protocol Version 4, Src: 67.161.34.229 (67.161.34.229), Dst: 128.241.194.25 (128.241.194.25)
 Transmission Control Protocol, Src Port: isis-ambc (1643), Dst Port: pop3 (110), Seq: 1, Ack: 50, Len: 16
 Post office Protocol
 USER rgantrey1\r\n
 Request command: USER
 Request parameter: rgantrey1

Pada frame kelima client diharuskan mengisi USER yang isinya “rgantrey1”, karena USER telah disetujui oleh server maka server melanjutkan permintaan PASS.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	67.161.34.229	128.241.194.25	TCP	66	isis-ambc > pop3 [SYN] Seq=0 win=65535 Len=0 MSS=1460 WS=4 SACK_PERM=1
2	0.086899	128.241.194.25	67.161.34.229	TCP	66	pop3 > isis-ambc [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 WS=1 SACK_PERM=1
3	0.086943	67.161.34.229	128.241.194.25	TCP	54	isis-ambc > pop3 [ACK] Seq=1 Ack=1 Win=256960 Len=0
4	4.680620	128.241.194.25	67.161.34.229	POP	103	S: +OK POP3 [128.241.194.25] v2000.70 server ready
5	4.681007	67.161.34.229	128.241.194.25	POP	70	C: USER rgantrey1
6	4.770897	128.241.194.25	67.161.34.229	POP	95	S: +OK user name accepted, password please
7	4.771077	67.161.34.229	128.241.194.25	POP	69	C: PASS abcdefgh
8	4.886065	128.241.194.25	67.161.34.229	POP	84	S: +OK Mailbox open, 1 messages
9	4.886357	67.161.34.229	128.241.194.25	POP	60	C: STAT
10	4.978243	128.241.194.25	67.161.34.229	POP	67	S: +OK 1 11110
11	4.978520	67.161.34.229	128.241.194.25	POP	60	C: UIDL
12	5.071986	128.241.194.25	67.161.34.229	POP	108	S: +OK Unique-ID listing follows
13	5.072202	67.161.34.229	128.241.194.25	POP	60	C: LIST
14	5.166592	128.241.194.25	67.161.34.229	POP	100	S: +OK Mailbox scan listing follows
15	5.168841	67.161.34.229	128.241.194.25	POP	62	C: RETR 1

Frame 7: 69 bytes on wire (552 bits), 69 bytes captured (552 bits)
 Ethernet II, Src: Sony_F4:3a:09 (08:00:46:F4:3a:09), Dst: cadant_22:a5:82 (00:01:5c:22:a5:82)
 Internet Protocol Version 4, Src: 67.161.34.229 (67.161.34.229), Dst: 128.241.194.25 (128.241.194.25)
 Transmission Control Protocol, Src Port: isis-ambc (1643), Dst Port: pop3 (110), Seq: 17, Ack: 91, Len: 15
 Post office Protocol
 PASS abcdefgh\r\n
 Request command: PASS
 Request parameter: abcdefgh

Pada frame ketujuh client mengisi PASS dengan “abcdefgh”. Dengan segera server membuka Mailbox yang dimiliki oleh USER tadi.

3. IMAP

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	127.0.0.1	127.0.0.1	TCP	54	griffin > imap [SYN] Seq=0 win=32768 Len=0
2	0.000058	127.0.0.1	127.0.0.1	TCP	54	imap > griffin [SYN, ACK] Seq=0 Ack=1 win=32768 Len=0
3	0.000068	127.0.0.1	127.0.0.1	TCP	54	griffin > imap [ACK] Seq=1 Ack=1 win=32768 Len=0
4	0.000107	127.0.0.1	127.0.0.1	IMAP	190	Response: * OK [CAPABILITY IMAP4REV1 LOGIN-REFERRALS STARTTLS LOGINDISABLED] tequila IM
5	0.000118	127.0.0.1	127.0.0.1	TCP	54	griffin > imap [ACK] Seq=1 Ack=137 win=32768 Len=0
6	0.000161	127.0.0.1	127.0.0.1	IMAP	82	Request: A0001 LOGIN fred flinstone
7	0.000172	127.0.0.1	127.0.0.1	TCP	54	imap > griffin [ACK] Seq=137 Ack=29 win=32768 Len=0
8	0.000202	127.0.0.1	127.0.0.1	IMAP	80	Response: A0001 OK LOGIN completed
9	0.000213	127.0.0.1	127.0.0.1	TCP	54	griffin > imap [ACK] Seq=29 Ack=163 win=32768 Len=0
10	0.000251	127.0.0.1	127.0.0.1	IMAP	79	Request: A0002 SELECT my-mailbox
11	0.000262	127.0.0.1	127.0.0.1	TCP	54	imap > griffin [ACK] Seq=163 Ack=54 win=32768 Len=0
12	0.000364	127.0.0.1	127.0.0.1	TCP	349	Response: * 172 EXISTS
13	0.000375	127.0.0.1	127.0.0.1	TCP	54	griffin > imap [ACK] Seq=54 Ack=458 win=32768 Len=0
14	0.000432	127.0.0.1	127.0.0.1	IMAP	77	Request: A0011 FETCH 2:4 FLAGS
15	0.000444	127.0.0.1	127.0.0.1	TCP	54	imap > griffin [ACK] Seq=458 Ack=77 win=32768 Len=0

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
 Ethernet II, Src: woonsang_04:05:06 (01:02:03:04:05:06), Dst: 06:05:04:03:02:01 (06:05:04:03:02:01)
 Internet Protocol Version 4, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)
 Transmission Control Protocol, Src Port: griffin (2458), Dst Port: imap (143), Seq: 0, Len: 0

Sama dengan protokol sebelumnya, POP3 juga menggunakan jasa TCP sebagai *transport protocol*, oleh karena itu koneksi antara client dan server harus tetap *established* dengan membentuk *three ways handshaking* terlebih dahulu seperti pada frame 1 sampai 3.

Dari protokol di atas diketahui bahwa client bernama “fred flinstone”. Tiap client melakukan koneksi dengan server, client mengirimkan ACK untuk menjaga kestabilan koneksi antara mail server dengan mail client. Pada frame 8 mail client telah berhasil masuk untuk melakukan

remote ke mail server.

No.	Time	Source	Destination	Protocol	Length	Info
8	0.000202	127.0.0.1	127.0.0.1	IMAP	80	Response: A0001 OK LOGIN completed
9	0.000213	127.0.0.1	127.0.0.1	TCP	54	griffin > imap [ACK] Seq=29 Ack=163 win=32768 Len=0
10	0.000251	127.0.0.1	127.0.0.1	IMAP	79	Request: A0002 SELECT my-mailbox
11	0.000262	127.0.0.1	127.0.0.1	TCP	54	imap > griffin [ACK] Seq=163 Ack=54 win=32768 Len=0
12	0.000364	127.0.0.1	127.0.0.1	IMAP	349	Response: * 172 EXISTS
13	0.000375	127.0.0.1	127.0.0.1	TCP	54	griffin > imap [ACK] Seq=54 Ack=458 win=32768 Len=0
14	0.000432	127.0.0.1	127.0.0.1	IMAP	77	Request: A0011 FETCH 2:4 FLAGS
15	0.000444	127.0.0.1	127.0.0.1	TCP	54	imap > griffin [ACK] Seq=458 Ack=77 win=32768 Len=0
16	0.000478	127.0.0.1	127.0.0.1	IMAP	149	Response: * 2 FLAGS (\Noselect)
17	0.000489	127.0.0.1	127.0.0.1	TCP	54	griffin > imap [ACK] Seq=77 Ack=553 win=32768 Len=0
18	0.000516	127.0.0.1	127.0.0.1	IMAP	68	Request: A9999 LOGOUT
19	0.000527	127.0.0.1	127.0.0.1	TCP	54	imap > griffin [ACK] Seq=553 Ack=91 win=32768 Len=0
20	0.000555	127.0.0.1	127.0.0.1	IMAP	117	Response: * BYE IMAP4rev1 Server logging out
21	0.000566	127.0.0.1	127.0.0.1	TCP	54	griffin > imap [ACK] Seq=91 Ack=616 win=32768 Len=0
22	0.000580	127.0.0.1	127.0.0.1	TCP	54	griffin > imap [RST] Seq=91 win=32768 Len=0

Frame 18: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)
 Ethernet II, Src: woonsang_04:05:06 (01:02:03:04:05:06), Dst: 06:05:04:03:02:01 (06:05:04:03:02:01)
 Internet Protocol Version 4, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)
 Transmission Control Protocol, Src Port: griffin (2458), Dst Port: imap (143), Seq: 77, Ack: 553, Len: 14
 Internet Message Access Protocol
 Line: A9999 LOGOUT\r\n
 Request Tag: A9999
 Request: LOGOUT

Pada frame 18 mail client melakukan *logout* dari meremote mail server. Dilanjutkan dengan *logging out* koneksi dengan mail server.

No.	Time	Source	Destination	Protocol	Length	Info
8	0.000202	127.0.0.1	127.0.0.1	IMAP	80	Response: A0001 OK LOGIN completed
9	0.000213	127.0.0.1	127.0.0.1	TCP	54	griffin > imap [ACK] Seq=29 Ack=163 win=32768 Len=0
10	0.000251	127.0.0.1	127.0.0.1	IMAP	79	Request: A0002 SELECT my-mailbox
11	0.000262	127.0.0.1	127.0.0.1	TCP	54	imap > griffin [ACK] Seq=163 Ack=54 win=32768 Len=0
12	0.000364	127.0.0.1	127.0.0.1	IMAP	349	Response: * 172 EXISTS
13	0.000375	127.0.0.1	127.0.0.1	TCP	54	griffin > imap [ACK] Seq=54 Ack=458 win=32768 Len=0
14	0.000432	127.0.0.1	127.0.0.1	IMAP	77	Request: A0011 FETCH 2:4 FLAGS
15	0.000444	127.0.0.1	127.0.0.1	TCP	54	imap > griffin [ACK] Seq=458 Ack=77 win=32768 Len=0
16	0.000478	127.0.0.1	127.0.0.1	IMAP	149	Response: * 2 FLAGS (\Noselect)
17	0.000489	127.0.0.1	127.0.0.1	TCP	54	griffin > imap [ACK] Seq=77 Ack=553 win=32768 Len=0
18	0.000516	127.0.0.1	127.0.0.1	IMAP	68	Request: A9999 LOGOUT
19	0.000527	127.0.0.1	127.0.0.1	TCP	54	imap > griffin [ACK] Seq=553 Ack=91 win=32768 Len=0
20	0.000555	127.0.0.1	127.0.0.1	IMAP	117	Response: * BYE IMAP4rev1 Server logging out
21	0.000566	127.0.0.1	127.0.0.1	TCP	54	griffin > imap [ACK] Seq=91 Ack=616 win=32768 Len=0
22	0.000580	127.0.0.1	127.0.0.1	TCP	54	griffin > imap [RST] Seq=91 win=32768 Len=0

Frame 20: 117 bytes on wire (936 bits), 117 bytes captured (936 bits)
 Ethernet II, Src: 06:05:04:03:02:01 (06:05:04:03:02:01), Dst: woonsang_04:05:06 (01:02:03:04:05:06)
 Internet Protocol Version 4, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)
 Transmission Control Protocol, Src Port: imap (143), Dst Port: griffin (2458), Seq: 553, Ack: 91, Len: 63
 Internet Message Access Protocol
 Line: * BYE IMAP4rev1 Server logging out\r\n
 Response Tag: *
 Response: BYE IMAP4rev1 Server logging out
 Line: A9999 OK LOGOUT completed\r\n
 Response Tag: A9999
 Response: OK LOGOUT completed

Dari ketiga protokol yang telah tercapture di atas dapat disimpulkan bahwa protokol-protokol tersebut menggunakan TCP sebagai *transport protocol*. Setiap aktivitas LOGIN pada IMAP dan POP3 tercapture nama dari USER.

Biografi Penulis



Biografi Penulis

Ainul Fuad Farhan. Mahasiswa Politeknik Negeri Semarang Jurusan Teknik Elektro, Prodi D4 Telekomunikasi. Alumni SMA N 1 JUWANA tahun 2010.

Contact Person :

Blog : <http://inungandthenotes.blogspot.com>

Facebook : lukazkazx@yahoo.com

Twitter : @inungf