# **BAB IV**

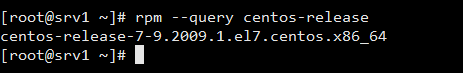
# **HASIL DAN PEMBAHASAN**

Bab ini memuat tentang pembahasan dan instalasi, konfigurasi mail server*,* serta Analisa dan hasil uji coba.

## **Hasil Instalasi Dan Konfigurasi**

Pada tahap hasil dan implementasi ini terdiri dari dua bagian yaitu hasil instalasi dan konfigurasi *server* dan hasil konfigurasi *client* (Hanif 2018).

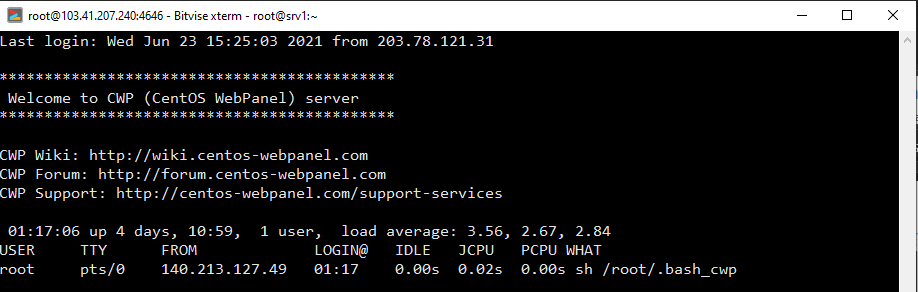
### **Hasil Instalasi Dan Konfigurasi *Server***

Tahap instalasi dan konfigurasi server berisikan instalasi CentOS Web Panel, konfigurasi DNS server, dan konfigurasi Mail server. Server yang digunakan pada penelitian ini adalah Virtual Private Server yang telah di sewa pada salah satu penyedia jasa layanan VPS, Alamat IP VPS yang diberikan oleh penyedia jasa layanan VPS adalah 103.41.207.240 dengan sistem operasi Linux CentOS release 7-9, pada VPS telah terinstal SSH Server agar VPS dapat diakses melalui perangkat lain melalui jaringan internet seperti terlihat pada gambar 4.1 berikut: (Hanif 2018).

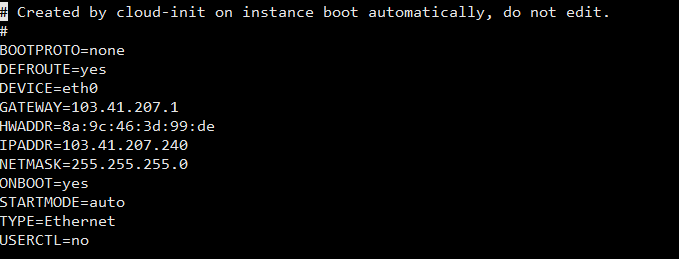
**Gambar 4.1 Linux CentOS release 7-9**

#### **Hasil Instalasi CentOS Web Panel**

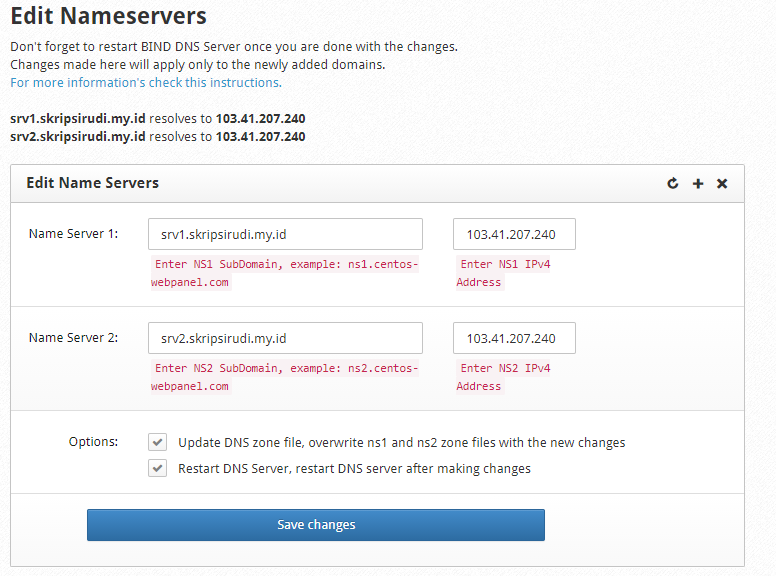
CentOS Web Panel digunakan untuk memudahkan dalam melakukan instalasi dan konfigurasi server karena proses instalasi server akan dilakukan secara otomatis dan proses konfigurasi server dapat dilakukan dengan mudah melalui halaman konfigurasi CentOS Web Panel yang berbasis web. Tahap instalasi CentOS Web Panel berisikan tiga perintah yaitu perintah untuk masuk pada direktori src yang bertujuan sebagai lokasi penyimpanan *file installer* *CWP* dengan perintah *#cd /usr/local/src*, perintah untuk men*download* *file installer* CWP versi terbaru dengan perintah *#wget* [*http://centos-webpanel.com/cwp-latest*](http://centos-webpanel.com/cwp-latest), perintah untuk menginstal *file installer* yang telah di *download* dengan perintah *#sh cwp-latest*, hasil instalasi CWP seperti terlihat pada gambar 4.2 berikut: (Hanif 2018).

**Gambar 4.2 Hasil Instalasi CWP**

#### **Hasil Konfigurasi DNS Server**

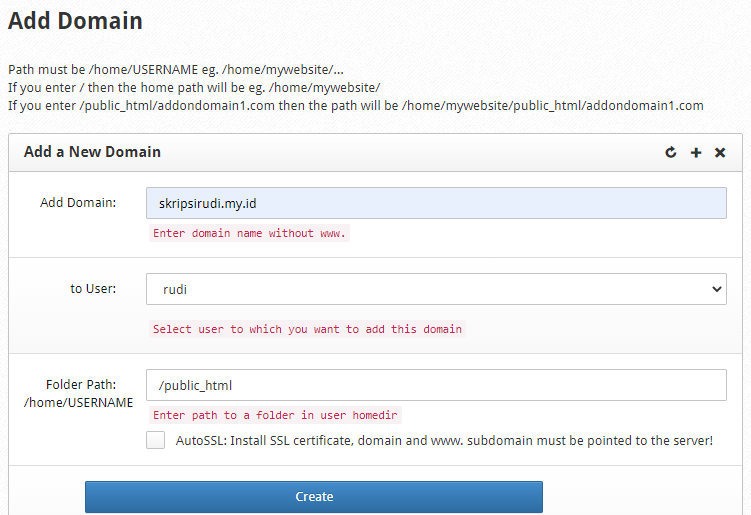
Tahap konfigurasi DNS server berisikan konfigurasi interface, konfigurasi name server dan konfigurasi file revers lookup zone. Konfigurasi *interface* sudah dilakukan oleh pihak penyedia jasa *VPS*, yang perlu dilakukan penyesuaian kebutuhan *mail server* yang di atur pada CWP yang telah di install (Hanif 2018).

Gambar 4.3 Konfigurasi Interface

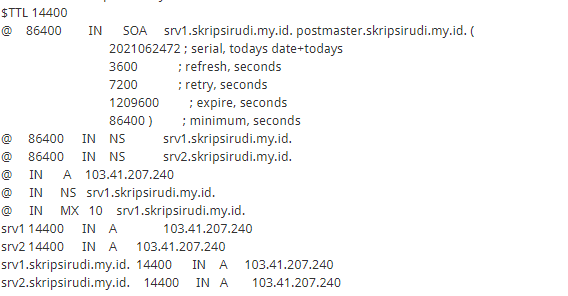
****Untuk melakukan konfigurasi *name server* dilakukan pada halaman konfigurasi *CWP* dengan memilih *menu DNS Functions* kemudian pilih *menu Edit Nameservers* IPs seperti terlihat pada gambar 4.4 berikut. (Hanif 2018)

**Gambar 4.4 Konfigurasi Name Server**

Untuk dapat memetakan nama *domain* ke alamat *IP* dan agar *domain* dapat diakses dengan nama alias maka perlu dibuat *file forward-lookup zone* dengan cara masuk pada menu *Domains* lalu masuk pada *sub menu* *Add Domain* seperti terlihat pada gambar 4.5 berikut. (Hanif 2018)

******Gambar 4.5 Konfigurasi *Domain***

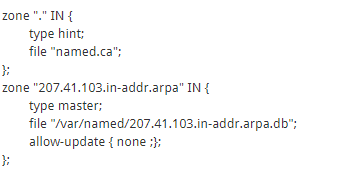
Jika konfigurasi *domain* berhasil maka secara otomatis akan terbuat *file forward-lookup zone* yang diberi nama skripsirudi.my.id.db, pada baris record @ IN A 103.41.207.240 yang berfungsi untuk memetekan nama *host* ke alamat *IP*, pada baris *record* @ IN NS srv1.skripsirudi.my.id. yang berfungsi untuk memetakan sebuah nama domain ke dalam satu daftar dari server DNS untuk domain skripsirudi.my.id, pada baris record @ IN MX 10 srv1.skripsirudi.my.id. yang berfungsi untuk memetakan sebuah nama domain ke dalam daftar mail exchange server untuk domain skripsirudi.my.id, pada 4 baris terakhir merupakan record CNAME atau Canonical Name yang berfungsi agar nama domain skripsirudi.my.id dapat diakses menggunakan nama alias www.skripsirudi.my.id, dan mail.skripsirudi.my.id seperti terlihat pada gambar 4.6 berikut. (Hanif 2018)

******Gambar 4.6 *File* skripsirudi.my.id.db**

Untuk dapat memetakan alamat *IP* ke nama *domain* maka perlu dibuat *file reverse-lookup zone* pada terminal dengan perintah *#nano /var/named/* *207.41.103.in-addr.arpa.db.* pada baris *record* @ IN NS srv1.skripsirudi.my.id. yang berfungsi untuk memetakan sebuah nama domain ke dalam satu daftar dari server DNS untuk domain skripsirudi.my.id, pada 2 baris setelahnya terdapat record pointer yang berfungsi untuk memetakan nama domain ke dalam alamat IP seperti terlihat pada gambar 4.7 berikut. (Hanif 2018)



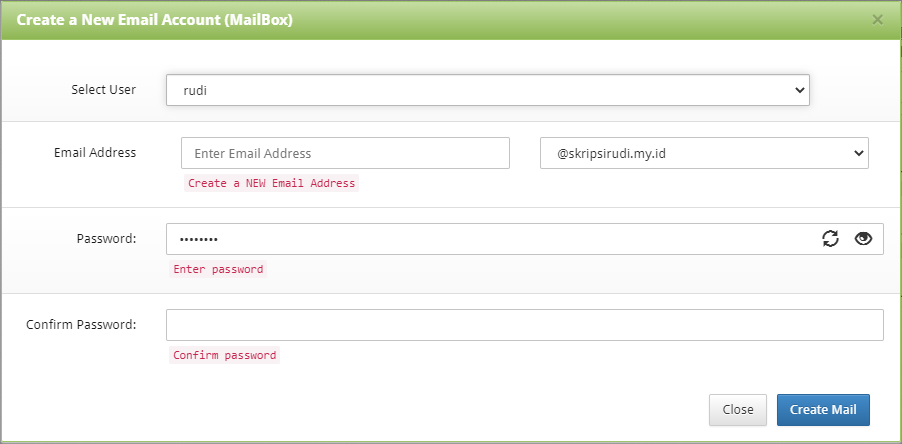
Gambar 4. 7 *File* *207.41.103.in-addr.arpa.db*

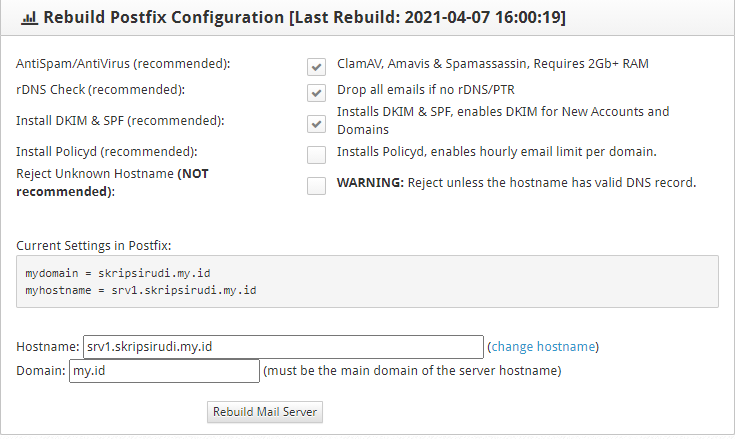
Pada *file* named.conf ditambahkan beberapa perintah yaitu zone "skripsirudi.my.id" adalah nama domain yang akan digunaka, selanjudnya yaitu type master adalah tipe DNS server yaitu primary DNS, pada baris lokasi file forward zone, kemudian pada baris zone "207.41.103.in-addr.arpa" IN adalah lingkup network dalam domain yang akan digunakan sebagai reverse, baris type master adalah tipe DNS server yaitu primary DNS, baris 8 adalah lokasi file reverse *zone*, setelah semua konfigurasi selesai disarankan untuk me*restart DNS server* yang terdapat pada dashboard CPW pada bagian server service. Seperti terlihat pada gambar 4.8 berikut. (Hanif 2018)

**Gambar 4.8 *File* named.conf**

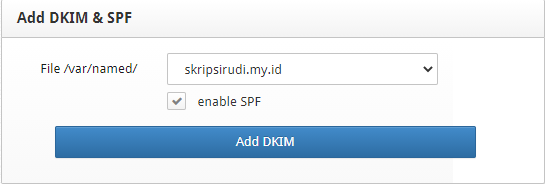
#### **Hasil Konfigurasi Mail Server**

Untuk dapat mengecek fungsi *mail server* maka perlu membuat akun *email* pada *mail server* dengan cara masuk pada menu *Email* kemudian pilih *sub menu Add Email Account* seperti terlihat pada gambar 4.9 berikut. (Hanif 2018)

******Gambar 4.9 Membuat Akun *Email***

Proses instalasi *DKIM*, *SPF*, *Anti Spam,* dan *Anti Virus* dilakukan pada *menu* *Email* kemudian masuk pada *sub menu* *MailServer Manager*, centang *check box* AntiSpam/AntiVirus, Install DKIM & SPF, dan rDNS Check untuk melakukan instalasi *Spam-Assassin, ClamAV, Amavis, DKIM,* dan *SPF* seperti terlihat pada gambar 4.10 berikut. (Hanif 2018)

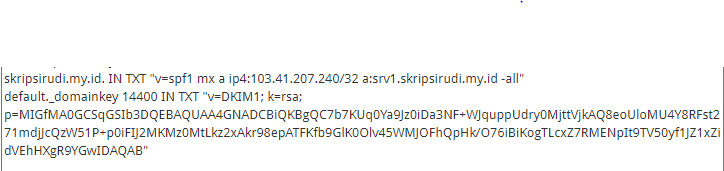
**Gambar 4.10 Instalasi *DKIM*, *SPF, Anti Spam,* dan *Anti Virus***

******Konfigurasi *DKIM* dilakukan pada *menu Email* kemudian masuk pada sub menu *DKIM Manager,* seperti terlihat pada gambar 4.11 berikut. (Hanif 2018)

Gambar 4.11 Menambah *DKIM Record* pada *File Zone*

Konfigurasi SPF dilakukan pada menu Email kemudian masuk pada sub menu SPF Manager, seperti terlihat pada gambar 4.12 berikut.(Hanif 2018)

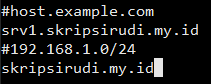
Gambar 4.12 Menambah *SPF Record* pada *File Zone*

Pada *file* skripsirudi.my.id.db akan terlihat tambahan dua baris dibagian paling bawah seperti terlihat pada gambar 4.13 berikut. (Hanif 2018)

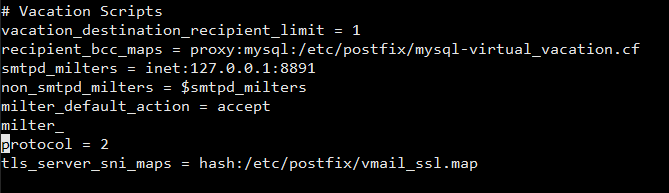
Gambar 4.13 *DKIM* dan *SPF Record*

Pada baris skripsirudi.my.id. IN TXT "v=spf1 mx a ip4:103.41.207.240/32 a:srv1.skripsirudi.my.id -all" merupakan *record SPF,* v=spf1 berarti versi *SPF* yang digunakan adalah *SPF* versi, a:srv1.skripsirudi.my.id berarti hanya mengizinkan pengiriman *email* dengan *hostname* srv1.skripsirudi.my.id, ip4: 103.41.207.240/32 yang berarti hanya mengizinkan pengiriman email dari *server* dengan alamat *IP* 103.41.207.240, -all berarti menolak semua *email* yang tidak sesuai dengan aturan tersebut, (Hanif 2018).

Pada baris *record* *DKIM,* dimana parameter v=DKIM1 berarti versi *DKIM* yang digunakan yaitu *DKIM* versi 1, parameter k=rsa berarti jenis kriptografi yang digunakan adalah rsa, dan parameter p yaitu *public key* yang digunakan (Hanif 2018).

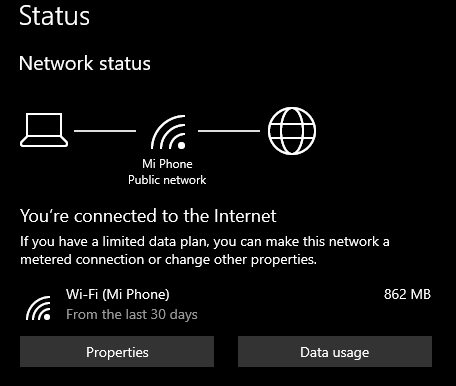
(Hanif 2018) Agar srv1.skripsirudi.my.id menjadi *host* yang dipercaya maka harus ditambahkan *hostname* pada baris 2 pada *file* TrustedHosts dibaris yang paling bawah dengan perintah *#nano /etc/opendkim/TrustedHosts* seperti pada gambar 4.14 berikut.

Gambar 4.14 Konfigurasi *File* TrustedHosts

(Hanif 2018) Pada *file* main.cf ditambahkan beberapa parameter seperti smtpd\_milters = inet:127.0.0.1:8891, non\_smtpd\_milters = $smtpd\_milters, milter\_default\_action = accept, dan milter\_protocol = 2 yang berfungsi untuk mem*filter email*, seperti terlihat pada gambar 4.15 berikut.

**Gambar 4.15 Konfigurasi File main.cf**

### **Hasil Konfigurasi *Client***

(Hanif 2018) Komputer *client* berfungsi sebagai *Mail User Agent (MUA)*, untuk dapat mengakses *mail server* maka komputer *client* harus terkoneksi dengan jaringan *internet* seperti terlihat pada gambar 4.16 berikut.

Gambar 4.16 Terhubung ke *Internet*

## **Hasil Uji Coba**

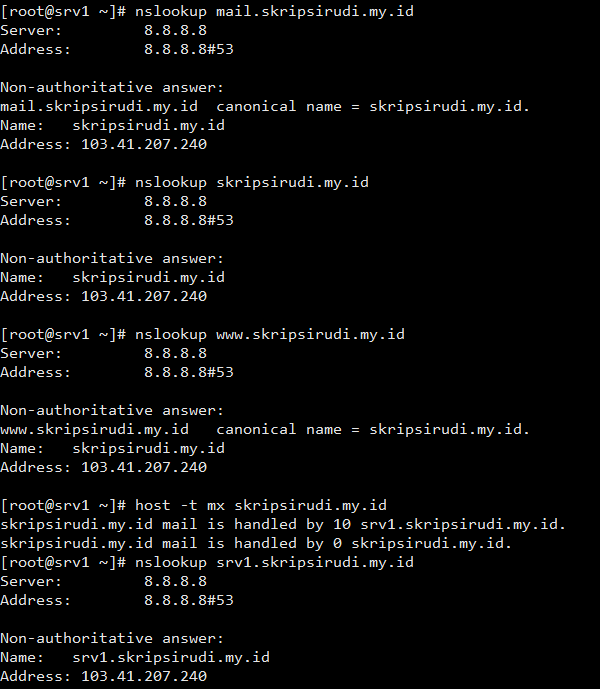
Tahap uji coba ini terdiri dari 2 bagian yaitu verifikasi konfigurasi dan uji coba menggunakan berbagai macam skenario (Hanif 2018).

### **Verifikasi Konfigurasi**

Pada tahap hasil verifikasi konfigurasi ini dilakukan untuk mengetahui apakah hasil konfigurasi yang dilakukan sebelumnya berhasil atau tidak (Hanif 2018).

#### **Verifikasi Konfigurasi DNS Server**

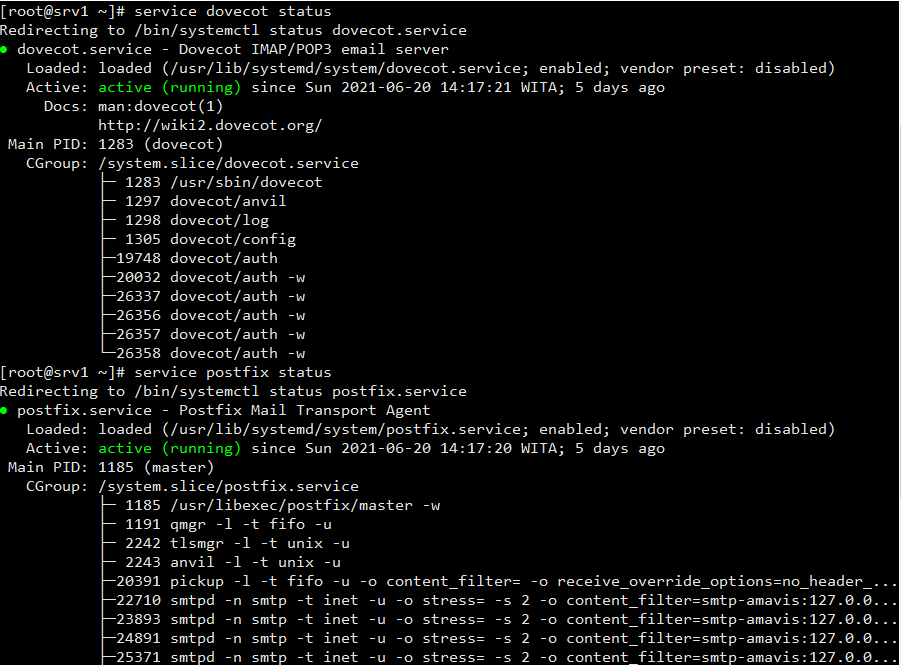
(Hanif 2018) Untuk mengecek fungsi forward-lookup, CNAME, reverse-lookup, dan fitur *mail exchanger* dapat digunakan perintah nslookup dan host –t mx pada terminal seperti terlihat pada gambar 4.17 berikut.

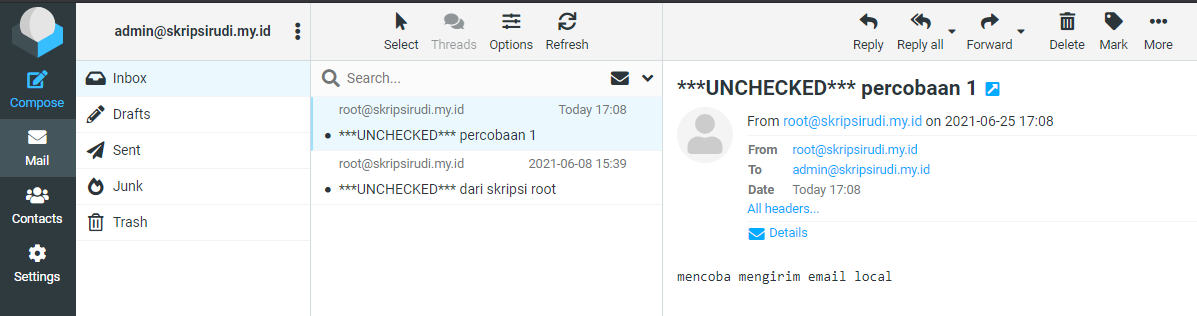
****

**Gambar 4.17 Verifikasi Konfigurasi *DNS Server***

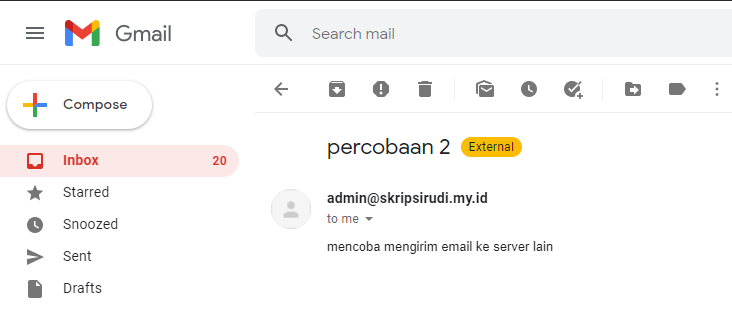
#### **Verifikasi Konfigurasi Mail Server**

(Hanif 2018) Verifikasi konfigurasi *mail server* dapat dilakukan dengan cara menulis perintah *#service dovecot status* dan *#service postfix status* pada terminal seperti terlihat pada gambar 4.18 berikut.

******Gambar 4.18 Verifikasi Konfigurasi *Mail Server***

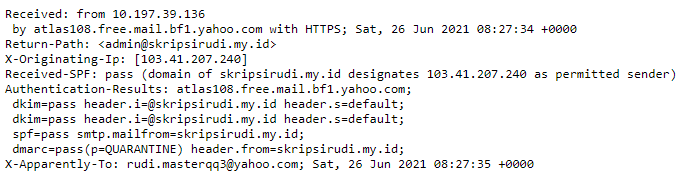
(Hanif 2018) Melakukan pengiriman *email* dengan cara mengirim *email* antar pengguna pada *mail server* yang sama dan mengirim *email* antar pengguna pada *mail server* yang berbeda seperti terlihat pada gambar 4.19 dan 4.20 berikut.

Gambar 4.19 Mengirim *Email* pada *User Email Local*

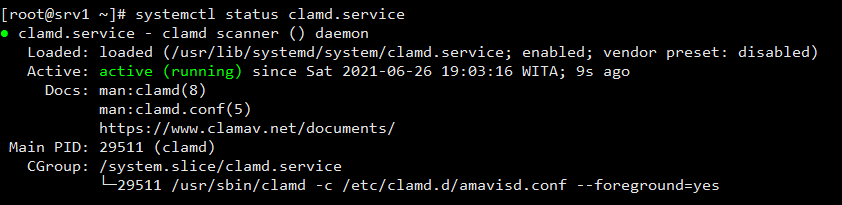


**Gambar 4.20 Mengirim *Email* Pada *Mail Server* Lain**

Verifikasi fungsi *DKIM*, *SPF,* dan *DMARC* dapat dilakukan dengan cara mengirim email ke alamat email [rudi.masterqq3@yahoo.com](mailto:rudi.masterqq3@yahoo.com) seperti pada gambar 4.21 berikut.

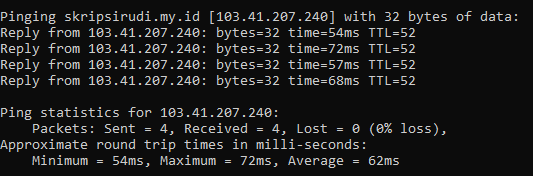


Gambar 4.21 Verifikasi Fungsi *DKIM*, *SPF,* dan *DMARC*

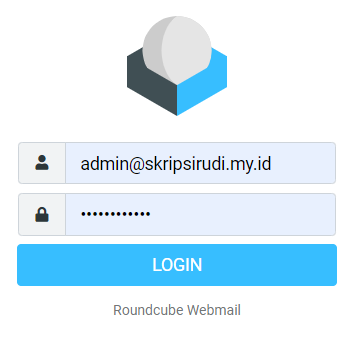
Verifikasi fungsi ClamAV dilakukan dengan menggunakan perintah *#systemctl status clamd.service* pada remote ssh sever, seperti terlihat pada gambar 4.22 berikut.

Gambar 4.22 Verifikasi Fungsi *ClamAV*

#### **Verifikasi Konfigurasi Client**

(Hanif 2018) Verifikasi konfigurasi *client* dilakukan agar memastikan domain yang di buat telah connect secara online dengan server dengan cara melakukan ping pada *mail server dengan perintah >ping skripsirudi.my.id* seperti pada gambar 4.23 berikut.

Gambar 4.23 Ping *Mail Server*

(Hanif 2018) Verifikasi konfigurasi pada *client* juga dapat dilakukan dengan cara mengakses *Mail User Agent* dengan menggunakan aplikasi *browser* kemudian mengakses alamat *URL* *http://skripsirudi.my.id/webmail/* seperti terlihat pada gambar 4.24 berikut.

Gambar 4.24 Akses *MUA roundcube*

### **Skenario Uji Coba**

Pada tahap skenario hasil uji coba ini berisikan tentang uji coba sebelum diterapkannya filtering, otentikasi, dan otorisasi email spam.

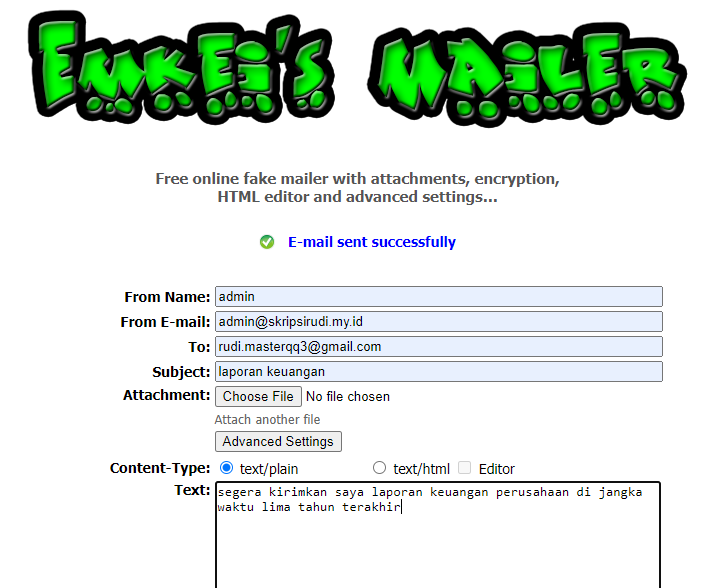
#### **Uji Coba Sebelum Diterapkan Filtering, Otentikasi, dan Otorisasi**

Adapun uji coba yang dilakukan sebelum diterapkan *filtering*, otentikasi, dan otorisasi *email* adalah uji coba mengirim *email spoofing*, uji coba mengirim *email spam*, uji coba mengirim *email* yang mengandung *virus*, dan uji coba pengecekan *header email*.

##### **Uji Coba mengirim *Email Spoofing***

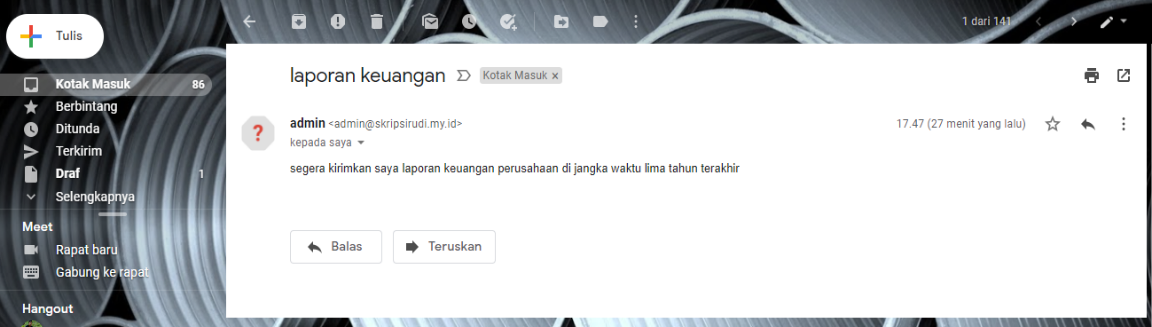
Uji coba mengirim *email spoofing* dilakukan dengan mengirim *email spoofing* menggunakan *Emkei’s Fake Mailer* ke *Gmail, Yahoo! Mail,* dan skripsirudi.my.id

###### **Uji Coba Mengirim *Email Spoofing* ke *Gmail***

Scenario uji coba untuk menguji protocol *DMARC, DKIM* dan *SPF* dilakukan dengan cara mengirim email *spoofing,* misalakan ada perusahaan bank yang bernama Bnkspoof yang bergerak di bidang perbankan untuk masyarakat. Bankspoof mempunyai pesaing dalam menjalankan bisnis perbankannya, dimna pesaing tersebut berusaha menjatuhkan Bankspoof dengan cara melakukan penipuan dengan mengirim email spoofing dengan *fake mailer,* sebelum melakukan penipuan terlebih dahulu mencari tahu email perusahaan Bankspoof, setelah mengetahui email dari perusahaan Bankspoof maka pesain teresebut memulai aksinya mengirim email spoofing yang mengatasnamakan direktur Bankspoof, pesaing tersebut menunjukan email ke staf keuagan Bankspoof, email spoofing tersebut berisikan perintah mengirim laporan keuangan Bank spoof dalam jangka waktu lima tahun terahir. Setelah semua informasi yang di perlukan telah di dapat, dimana nama direkturnya admin dan nama pegawainya root maka pesaing tersebut memulai email spoofing dengan cara membuka situs www.emkei.cz kepada pegawai staf keuangan root dengan alamat email rudi.masterqq3@gmail.com dengan mengatasnamakan direktur Bankspoof yang bernama admin dengan alamat email [admin@skripsirudi.my.id](mailto:admin@skripsirudi.my.id), isi email terbebut memerintahkan staf keuangan Bankspoof untuk mengirimkan laporan keuangan Bankspoof lima tahun terakhir, seperti pada gambar 4.25 berikut.

Gambar 4. 25 Emke’I Fake mailer

Pada gambar diatas terlihat tampilan dari *Emkei’s Fake Mailer*, pada *text box From Name* diisi dengan nama direktur Bankspoof, pada *text box From E-mail* diisi dengan alamat *email* direktur Bankspoof, pada *text box To* diisi dengan alamat *email* staf keungan Bankspoof, pada *text box Subject* diisi dengan subjek *email*, dan *text box Text* diisi dengan pesan dari *email spoofing*, jika pada *email* Bankspoof belum menerapkan protokol *DMARC,* *SPF* dan *DKIM* maka *email* tersebut berhasil terkirim dengan proses sebagai berikut:

* + - 1. Pesaing tersebut melakukan pengiriman *email spoofing* menggunakan *Emkei’s Fake Mailer* dengan cara memasukan *URL* www.emkei.cz pada *browser,* kemudian pada situs Emkei’s Fake Mailer pesaing tersebut menuliskan alamat pengirim *email* yaitu root@skripsirudi.my.id dan alamat penerima email adalah rudi.masterqq3@gmail.com.
      2. Email spoofing tersebut di akses melalui *mail server* gmail.com oleh alamat email rudi.masterqq3@gmail.com tanpa adanya proses otentikasi dan otorisasi oleh protokol *DMARC,* *DKIM* dan *SPF* sehingga *email spoofing* tersebut berhasil terkirim kealamat *email* rudi.masterqq3@gmail.com seperti terlihat pada gambar 4.26 berikut.

Gambar 4. 26 Email spoofing

Setelah *email* tersebut masuk ke *inbox* maka staf keuangan Bankspoof akan membaca *email spoofing* tersebut.

###### **Uji Coba Mengirim *Email Spoofing* ke *Yahoo! Mail***

Dengan menggunakan skenario yang sama seperti pada uji coba mengirim *email spoofing* ke *Gmail*, namum pada uji coba ini akan di uji pengiriman *email spoofing* pada layanan *email Yahoo! Mail* dengan mengatasnamakan salah satu *user* yang ada pada *mail server* skripsirudi.my.id, proses otentikasi dan otorisasi akan sama dengan proses otorisasi dan otentikasi pada uji coba pertama terlihat seperti gambar 4.27 berikut.

Gambar 4. 27 mengirim spoofing ke yahoo mail

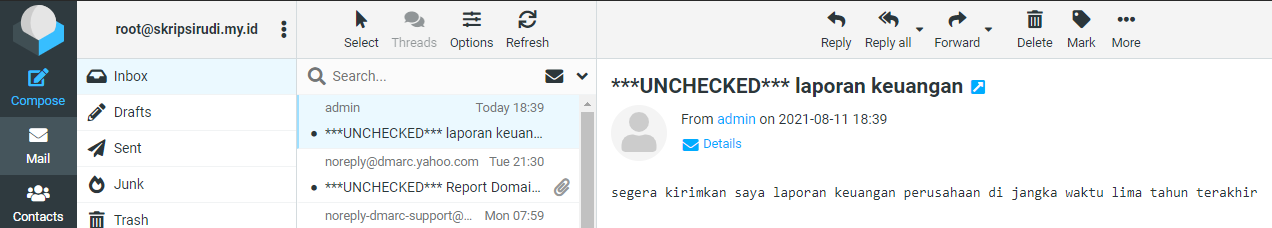
*Email spoofing* diatas berhasil terkirim ke alamat *email* rudi.masterqq3@yahoo.com terlihat seperti pada gambar 4.28 berikut.

Gambar 4. 28 *Email Spoofing* Terkirim ke *Yahoo! Mail*

###### **Uji Coba Mengirim *Email Spoofing* pada skripsirudi.my.id**

Dengan menggunakan skenario yang sama seperti pada uji coba mengirim *email spoofing* ke layanan *email* *Gmail,* namum pada uji coba ini akan di uji pengiriman *email spoofing* pada *mail server* skripsirudi.my.id dengan mengatasnamakan salah satu *user* yang ada pada *mail server* skripsirudi.my.id, proses otentikasi dan otorisasi akan sama dengan proses otorisasi dan otentikasi pada uji coba mengirim *email spoofing* ke *Gmail* terlihat seperti gambar 4.29 berikut.

Gambar 4. 29 mengirim spoofing ke skripsirudi.my.id

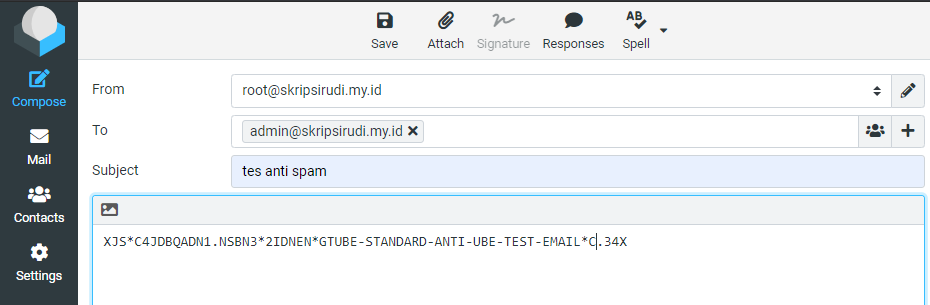
*Email spoofing* tersebut diatas berhasil terkirim ke alamat *email* [naufalhanif@skripsian.online](mailto:naufalhanif@skripsian.online) terlihat seperti pada gambar 4.30 berikut.

Gambar 4. 30 *Email Spoofing* Terkirim ke User skripsirudi.my.id

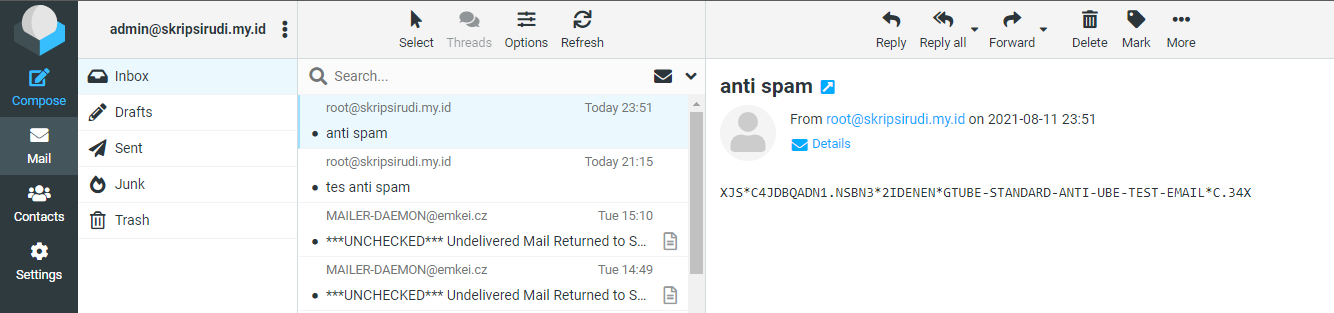
##### **Uji Coba Mengirim *Email* *Spam***

Uji coba mengirim *email spam* dilakukan dengan mengirim *email spam* menggunakan layanan *email* skripsirudi.my.id, *Yahoo! Mail*, dan *Gmail* ke layanan *email* skripsirudi.my.id.

###### **Mengirim *Email Spam* dari skripsirudi.my.id**

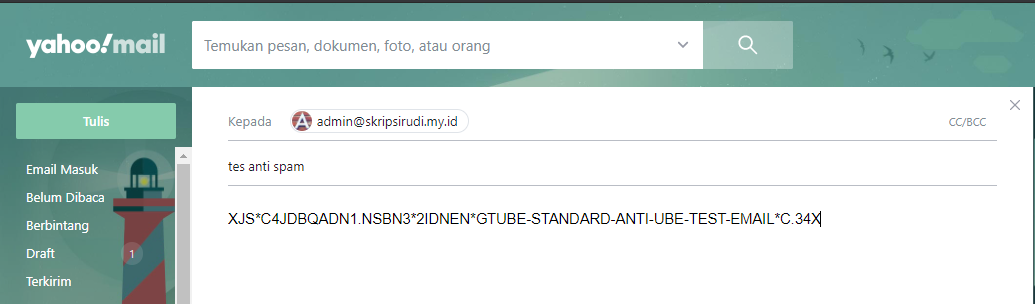
Uji coba kedua adalah dengan mengirim *email spam* menggunakan layanan *email* skripsian.online ke layanan e*mail* skripsian.online, isi pesan yang digunakan adalah XJS\*C4JDBQADN1.NSBN3\*2IDNEN\*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL\*C.34X yang merupakan standar GTUBE untuk menguji kinerja *anti spam* terlihat seperti gambar 4.31 berikut. (Klop and Csuka 2018)

Gambar 4. 31 Mengirim *Email Spam* dari skripsirudi.my.id

*Email spam* tersebut diatas berhasil terkirim ke alamat *email* admin@skripsirudi.my.id karena belum ada penerapan *anti spam* pada *mail server* skripsirudi.my.id terlihat seperti pada gambar 4.32 berikut.

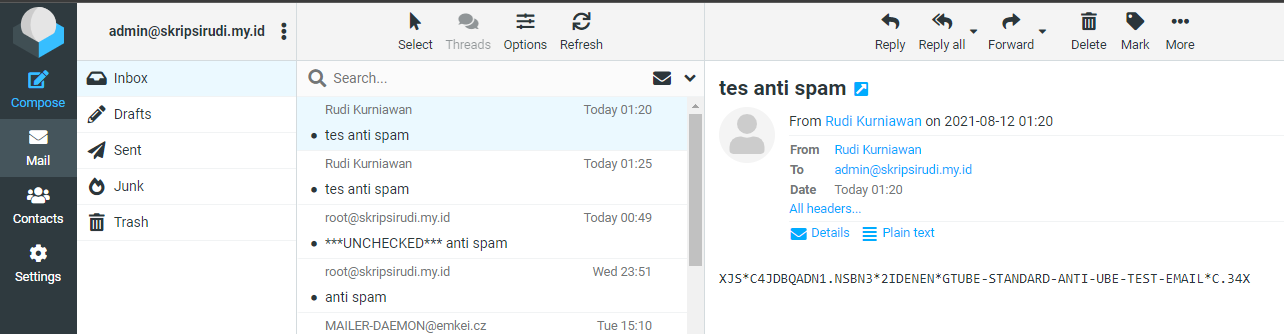
Gambar 4. 32 email spam dari skripsirudi.my.id terkirim

###### **Mengirim *Email Spam* dari *Yahoo! Mail***

Dengan menggunakan skenario yang sama seperti pada uji coba mengirim *email spam* dari layanan *email* skripsian.online ke layanan *email* skripsian.online, namum pada uji coba ini akan di uji pengiriman *email spam* ke layanan e*mail* skripsian.online dari layanan *email* *Yahoo! Mail* terlihat seperti gambar 4.33 berikut.

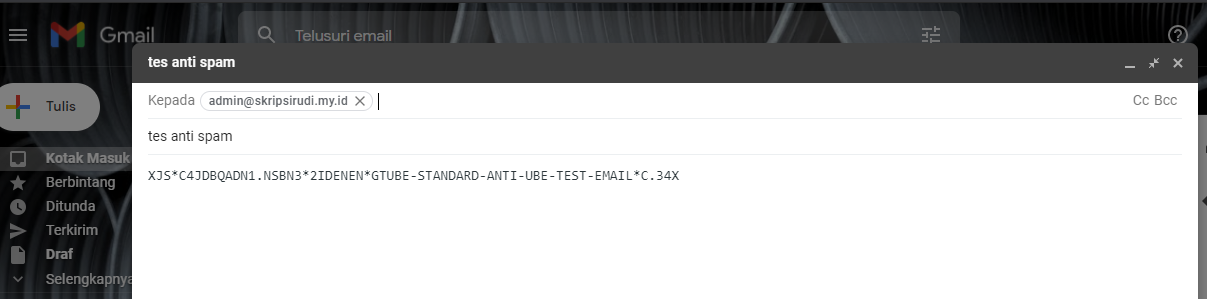
Gambar 4. 33 Mengirim *Email Spam* dari *Yahoo! Mail*

*Email spam* tersebut diatas berhasil terkirim ke alamat *email* admin@skripsirudi.my.id karena belum ada penerapan *anti spam* pada *mail server* skripsirudi.my.id terlihat seperti pada gambar 4.34 berikut.

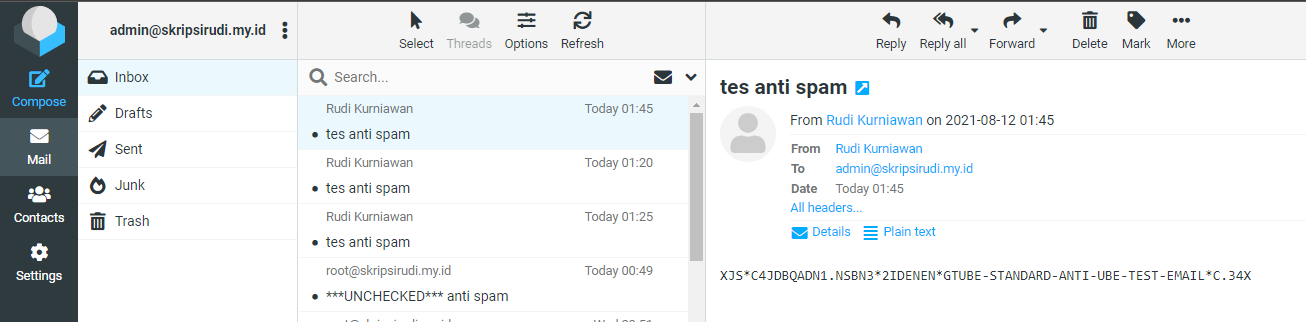


Gambar 4. 34 *Email Spam* dari *Yahoo! Mail* Terkirim

###### **Uji Coba Mengirim *Email Spam* dari *Gmail***

Dengan menggunakan skenario yang sama seperti pada uji coba mengirim *email spam* dari layanan *email* skripsirudi.my.id ke layanan *email* skripsirudi.my.id, namum pada uji coba ini akan di uji pengiriman *email* *spam* ke layanan e*mail* skripsirudi.my.id dari layanan *email Gmail* terlihat seperti gambar 4.35 berikut.

Gambar 4. 35 Mengirim *Email Spam* dari *Gmail*

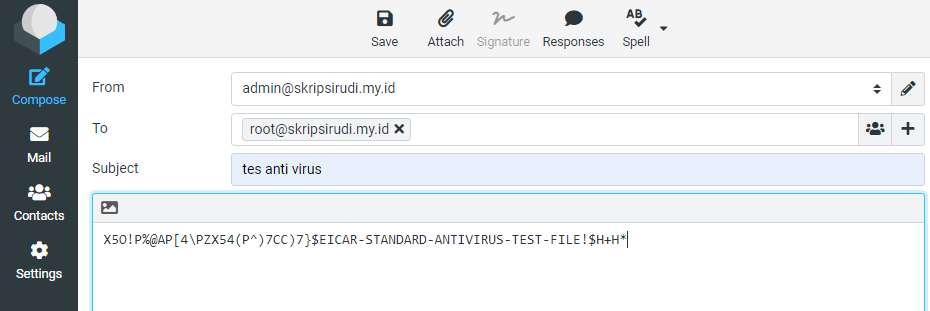
*Email spam* tersebut diatas berhasil terkirim ke alamat *email* admin@skripsirudi.my.id karena belum ada penerapan *anti spam* pada *mail server* skripsirudi.my.id terlihat seperti pada gambar 4.36 berikut.

Gambar 4. 36 *Email Spam* dari *Gmail* Terkirim

##### **Uji Coba Mengirim *Email* yang Mengandung *Virus***

Uji coba pengiriman *email* yang mengandung *virus* dilakukan dengan mengirim *email* yang mengandung *virus* dari layanan *email* skripsirudi.my.id, *Yahoo! Mail*, dan *Gmail* ke layanan *email* skripsirudi.my.id.

###### **Uji Coba Mengirim *Email* yang Mengandung *Virus* dari skripsirudi.my.id**

Uji coba pengiriman *email* yang mengandung *virus* dilakukan dengan mengirim *email* yang berisi X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H\* yang merupakan standar *EICAR* untuk melakukan tes *anti virus mail server*, *email* dikirim dari layanan *email* skripsirudi.my.id ke layanan *email* skripsirudi.my.id, seperti pada gambar 4.37 berikut. (Abrams 1999)

Gambar 4. 37 *EICAR Test* dari skripsirudi.my.id

Setelah *email* tersebut dikirim pada salah satu *user* *email* yang ada pada *mail server* skripsirudi.my.id maka *email* yang mengandung *virus* tersebut berhasil terkirim ke *user* yang berada pada *mail server* skripsirudi.my.id seperti terlihat pada gambar 4.38 berikut

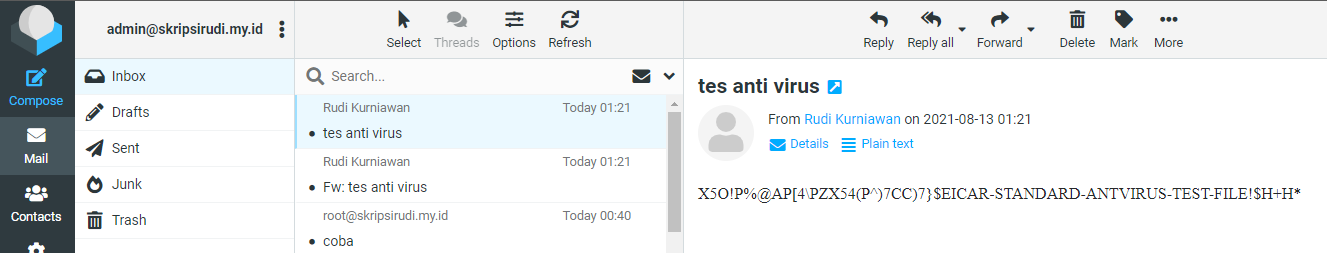
Gambar 4. 38 Email Mengandung Virus dari skripsirudi.my.id Terkirim

###### **Uji Coba Mengirim *Email* yang Mengandung *Virus* dari *Yahoo! Mail***

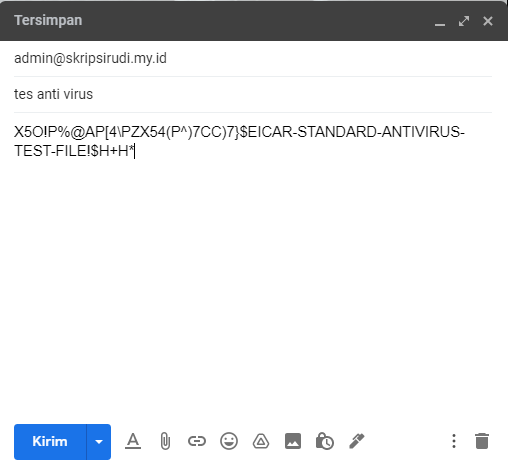
Uji coba pengiriman *email* yang mengandung *virus* dilakukan dengan mengirim *email* dengan isi X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H\* yang merupakan standar *EICAR* untuk melakukan tes *anti virus mail server*, *email* dikirim dari layanan *email* *Yahoo! Mail* ke layanan *email* skripsirudi.my.id, seperti pada gambar 4.39 berikut. (Abrams 1999)

Gambar 4. 39 *EICAR Test* dari *Yahoo! Mail*

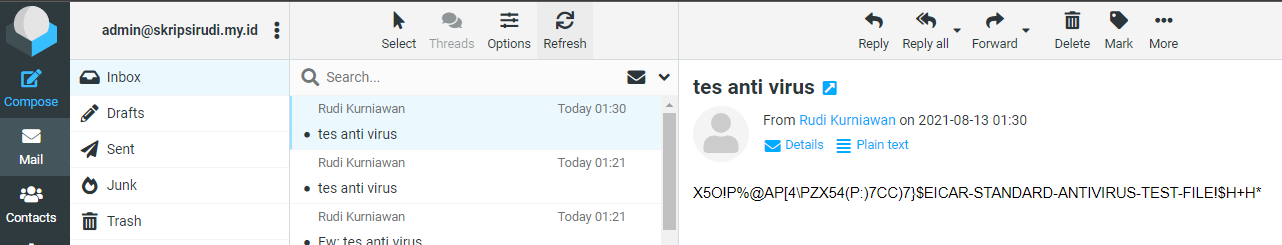
Setelah *email* tersebut dikirim pada salah satu *user* *email* yang ada pada *mail server* skripsian.online, maka *email* yang mengandung *virus* tersebut berhasil terkirim ke *user email* yang berada pada *mail server* skripsian.online seperti terlihat pada gambar 4.40 berikut.

Gambar 4. 40 *Email* Mengandung *Virus* dari *Yahoo! Mail* Terkirim

###### **Uji Coba Mengirim *Email* yang Mengandung *Virus* dari *Gmail***

Uji coba pengiriman *email* yang mengandung *virus* dilakukan dengan mengirim *email* dengan isi X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H\* yang merupakan standar *EICAR* untuk melakukan tes *anti virus mail server*, *email* dikirim dari layanan *email Gmail* ke layanan *email* skripsirudi.my.id, seperti pada gambar 4.41 berikut.(Abrams 1999)

Gambar 4. 41 *EICAR Test* dari *Gmail*

Setelah *email* tersebut dikirim pada salah satu pengguna *email* yang ada pada *mail server* skripsirudi.my.id maka *email* yang mengandung *virus* tersebut berhasil terkirim ke penerima yang berada pada *mail server* skripsirudi.my.id seperti terlihat pada gambar 4.42 berikut.

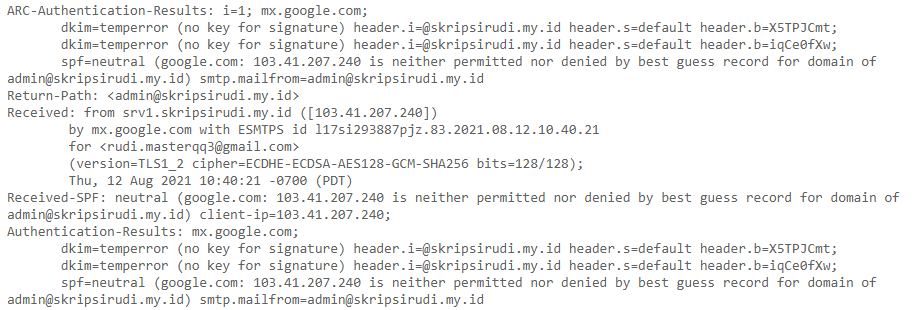
Gambar 4. 42 *Email* Mengandung *Virus* dari *Gmail* Terkirim

##### **Uji Coba Pengecekan *Header Email***

Uji coba pengecekan *header email* dilakukan dengan membandingkan *header email* yang dikirim dari layanan *email* skripsirudi.my.id ke layanan *email Gmail*, *Yahoo! Mail*, dan skripsirudi.my.id sebelum dan setelah penerapan *DMARC,* *DKIM*, *SPF*, *anti spam*, dan *anti virus*.

###### ***Header Email* pada *Gmail***

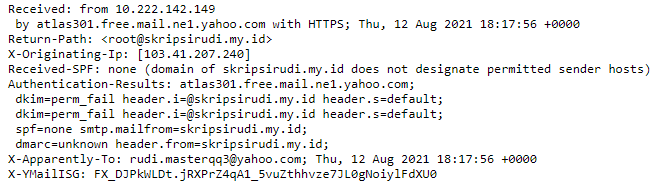
Uji coba ini dilakukan dengan mengirim *email* dari salah satu *user email* yang ada pada skripsirudi.my.id ke salah satu *user email* yang ada pada *Gmail* kemudian melakukan pengecekan *header email* tersebut dan melakukan perbandingan terhadap *header email* sebelum dan setelah penerapan *DMARC,* *DKIM*, *SPF, anti spam,* dan *anti virus*, *header email* sebelum diterapkannya *DMARC,* *DKIM*, *SPF, anti spam,* dan *anti virus* terlihat seperti gambar 4.43 berikut.



Gambar 4. 43 Cuplikan *Header Email* pada Gmail Sebelum Penerapan

Pada gambar 4.43 terlihat pada cuplikan *header email* hanya terdapat parameter *DKIM* *=temperror* dan Received-SPF: neutral belum terdapat parameter *DMARC* atau tanda tangan *digital* dan *X-Virus-Scanned* karena belum ada penerapan *DMARC,* *DKIM*, *ClamAV*, dan *Amavisd-New*.

###### ***Header Email* pada *Yahoo! Mail***

Uji coba ini dilakukan dengan mengirim *email* menggunakan salah satu *user email* yang ada pada skripsirudi.my.id ke salah satu *user* yang ada pada *Yahoo! Mail* kemudian melakukan pengecekan *header email* tersebut dan melakukan perbandingan terhadap *header email* sebelum dan setelah penerapan *DMAR,* *DKIM*, *SPF, anti spam,* dan *anti virus*, *header email* sebelum diterapkannya *DMAR, DKIM*, *SPF, anti spam,* dan *anti virus* terlihat seperti gambar 4.44 berikut.

Gambar 4. 44 Cuplikan *Header Email* pada *Yahoo! Mail* Sebelum Penerapan

Pada gambar 4.44 dapat dilihat cuplikan *haeder email* belum terdapat parameter *X-Virus-Scanned* karena belum ada penerapan *ClamAV* dan *Amavisd-New*, parameter *Received-SPF* bernilai *none* karena belum ada penerapan *SPF*, dan parameter dkim=perm\_fail dan dmarc=unknown yang berarti belum ada tanda tangan *digital* karena belum diterapkan *DMARC* dan *DKIM*.

###### **Header *Email* pada skripsirudi.my.id**

Uji coba ini dilakukan dengan mengirim *email* menggunakan salah satu *user email* yang ada pada skripsirudi.my.id ke salah satu *user email* yang ada pada skripsirudi.my.id kemudian melakukan pengecekan *header email* dan melakukan perbandingan terhadap *header email* sebelum dan setelah penerapan *DMARC,* *DKIM*, *SPF, anti spam,* dan *anti virus*, *header email* sebelum diterapkannya *DMARC,* *DKIM*, *SPF, anti spam,* dan *anti virus* terlihat seperti gambar 4.45 berikut.

Gambar 4. 45 Cuplikan *Header Email* pada skripsian Sebelum Penerapan

Pada gambar 4.45 terlihat *haeder email* belum terdapat parameter *X-Virus-Scanned* dan *DKIM* masih bernilai dkim=neutral karena belum diterapkan *Amavisd-New* dan protocol  *DMARC* dan *DKIM*..

#### **Setelah Diterapkan Filtering, Otentikasi dan Otorisasi**

Uji coba yang dilakukan setelah diterapkan *filtering*, otentikasi, dan otorisasi *email* adalah uji coba mengirim *email spoofing*, uji coba mengirim *email spam*, uji coba mengirim *email* yang mengandung *virus*, dan uji coba pengecekan *header email* (Hanif 2018).

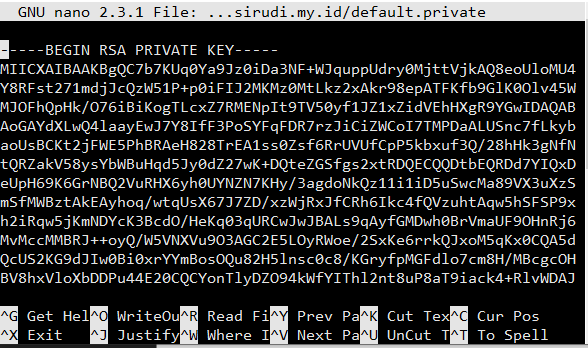
##### **Uji Coba Mengirim *Email Spoofing***

Uji coba mengirim *email spoofing* dilakukan dengan mengirim *email spoofing* dari *Emkei’s Fake Mailer* ke *Gmail*, *Yahoo! Mail*, dan skripsirudi.my.id dengan mengatasnamakan salah satu *user email* yang ada pada skripsirudi.my.id (Hanif 2018).

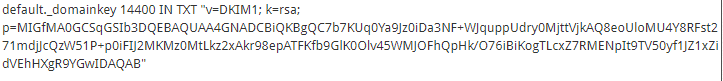
###### **Uji Coba Mengirim *Email Spoofing* ke *Gmail***

(Hanif 2018) Proses uji coba mengirim *email spoofing* pada *email server* akan berbeda setelah protocol *DMARC,* *SPF* dan *DKIM* diterapkan pada *mail server* karena protokol *DMARC,* *SPF* dan *DKIM* akan melakukan otentikasi dan otorisasi pada setiap *email* yang datang dari *mail server* skripsirudi.my.id. Proses yang terjadi setelah penerapan protokol *DMARC,* *SPF* dan *DKIM* adalah sebagai berikut:

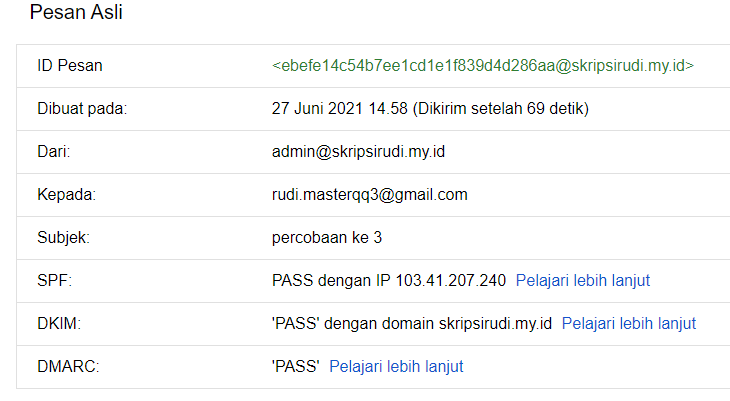
* + - 1. Pesaing tersebut melakukan pengiriman *email spoofing* menggunakan Emkei’s *Fake* *Mailer* dengan cara membuka situs www.emkei.cz menggunakan *browser* kemudian pada situs www.emkei.cz pesaing tersebut menuliskan alamat pengirim *email* yaitu [admin@skripsirudi.my.id](mailto:admin@skripsirudi.my.id) dan alamat penerima *email* yaitu [rudi.masterqq3@gmail.com](mailto:rudi.masterqq3@gmail.com).
      2. Ketika *email spoofing* tersebut melewati *mail server* *Emkei’s Fake Mailer* maka *email spoofing* tersebut tidak mendapatkan *private key* yang hanya terdapat pada *mail server* skripsirudi.my.id terlihat seperti gambar 4.56 berikut.

******Gambar 4. 46 *Private Key* pada skripsirudi.my.id**

* + - 1. Ketika *email spoofing* tersebut masuk ke *mail server* *Gmail* maka *email* tersebut akan dianggap sebagai *spam* karena *email* tersebut tidak mempunyai *private key* yang ada pada *mail server* skripsirudi.my.id yang cocok dengan *public key* yang telah diletakan pada *DNS server* skripsirudi.my.id sehingga pesan tersebut tidak memiliki tanda tangan *digital* pada *header email* (proses *DKIM*) terlihat seperti gambar 4.47 dan 4.48 berikut.



Gambar 4.47 *Public Key* pada *DNS Server* skripsirudi.my.id

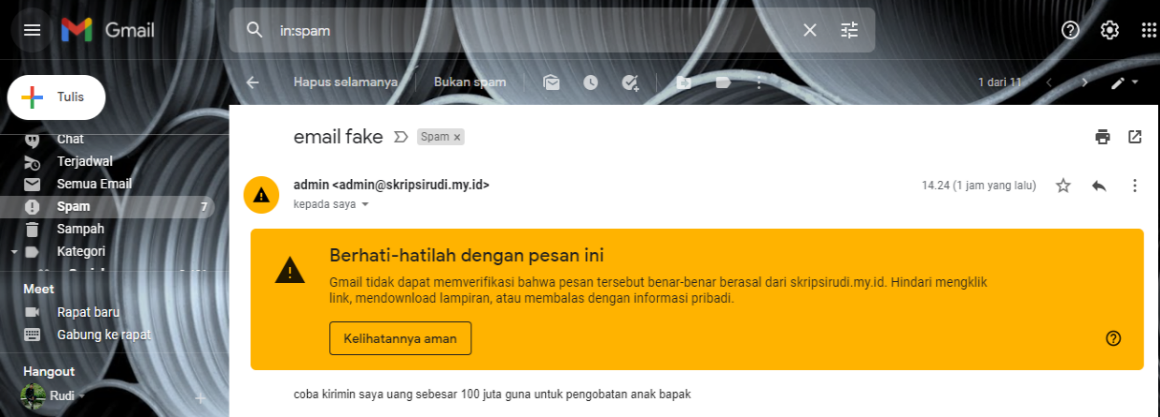
**Gambar 4.48 Cuplikan *Header Email***

* + - 1. Selanjutnya *mail server* *Gmail* akan melakukan pengecekan *SIDF* (*Sender ID Framework*) pada *record DNS server* skripsirudi.my.id, karena alamat *IP* *Emkei’s Fake Mailer* adalah 101.99.94.155 maka *email spoofing* tersebut dianggap sebagai *spam* dikarenakan *record SPF* dan *DMARC* yang ada pada *DNS server* skripsirudi.my.id hanya mengizinkan pengiriman *email* dari alamat yang telah diotorisasi yaitu alamat *IP* 103.41.207.240 yang merupakan alamat mail server skripsirudi.my.id dan nilai dari parameter *Received-SPF* dan *DMARC* pada *header email* adalah *fail* sehingga *email* tersebut akan ditandai sebagai *email spam* oleh *server Gmail* dan *email spoofing* tersebut tidak diblok oleh *Gmail*  di kerenakan record pada *DMARC* untuk mengkarantina email sehingga email terbebut di masukan ke folder spam (proses *SPF* dan *DMARC*) terlihat seperti gambar 4.49 dan 4.50 berikut.

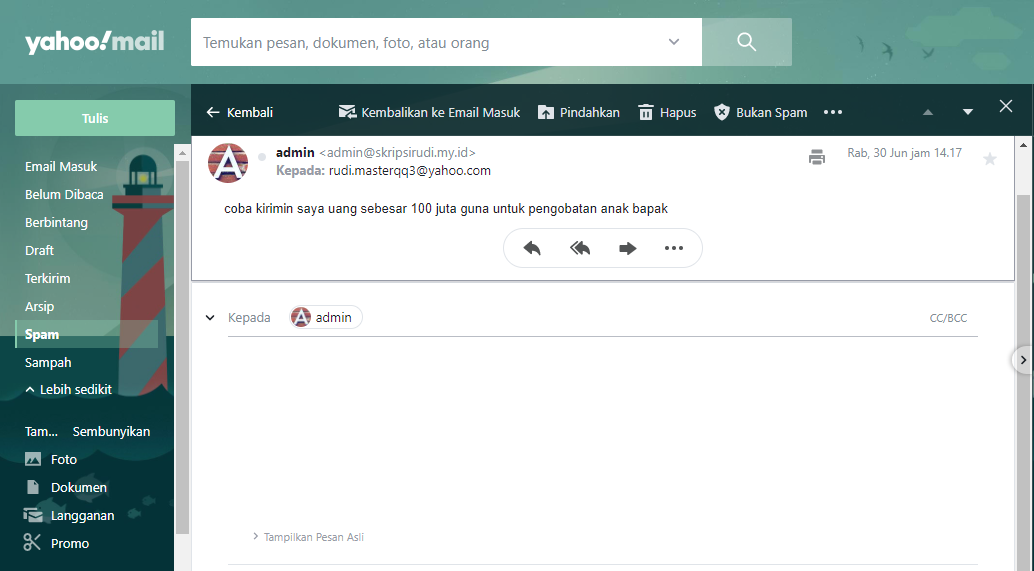
Gambar 4.49 *SPF Record* pada skripsirudi.my.id

Gambar 4. 50 *DMARC Record* pada skripsirudi.my.id

* + - 1. Hasil verifikasih pengiriman email fake dari emkei.cz ke mail dengan mengatas nama kan salah satu user email yaitu [admin@skripsirudi.my.id](mailto:admin@skripsirudi.my.id) yang kemudian terindikasi sebagai spam oleh gmail terlihat seperti gambar 4.51 berikut.

******Gambar 4. 51 terindikasi spam oleh gmail**

###### **Uji Coba Mengirim *Email Spoofing* ke *Yahoo! Mail***

Selain mengirim *email spoofing* pada *Gmail*, pengiriman *email spoofing* juga dilakukan pada *Yahoo! Mail* untuk membandingkan perlakuan yang diberikan pada *email spoofing* antara dua layanan *email* tersebut. Pada *Gmail*, *email spoofing* yang masuk langsung di karantina sehingga *email spoofing* masuk pada *folder spam* penerima *email* sedangkan pada *Yahoo! Mail,* *email spoofing* dimasukan kedalam *folder spam* penerima *email* seperti gambar 4.52 berikut. (Hanif 2018)

Gambar 4. 52 *Email Spoofing* Masuk ke *Folder Spam*

###### **Coba Mengirim *Email Spoofing* ke skripsirudi.my.id**

Selain mengirim *email spoofing* ke *Gmail* dan *Yahoo! Mail*, pengiriman *email spoofing* juga dilakukan pada skripsirudi.my.id untuk membandingkan perlakuan yang diberikan pada *email spoofing* antara dua layanan *email* tersebut. Pada *Gmail*, *email spoofing* yang masuk langsung langsung masuk pada folder spam, pada *Yahoo! Mail*, *email spoofing* dimasukan kedalam *folder spam* penerima *email*, dan pada skripsirudi.my.id *email spoofing* masuk pada *folder inbox*, seperti gambar 4.53 berikut. (Hanif 2018).

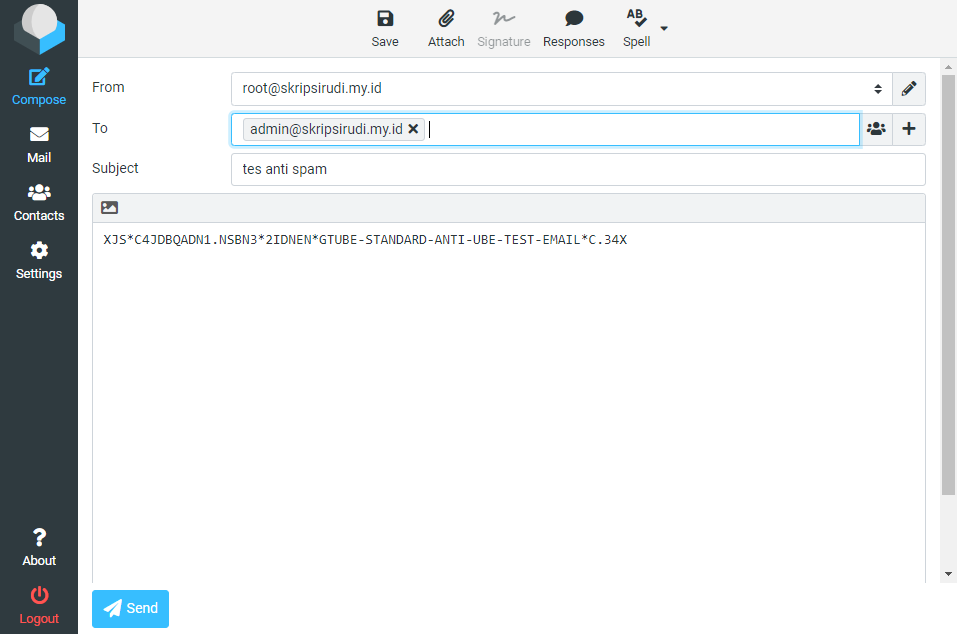
Gambar 4. 53 *Email Spoofing* Masuk pada *Folder Inbox*

###### **Uji Coba Mengirim *Email Spam***

Uji coba mengirim *email spam* dilakukan dengan mengirim *email spam* menggunakan layanan *email* skripsirudi.my.id, *Yahoo! Mail*, dan *Gmail* ke layanan *email* skripsirudi.my.id.

###### **Uji Coba Mengirim *Email Spam* dari skripsirudi.my.id**

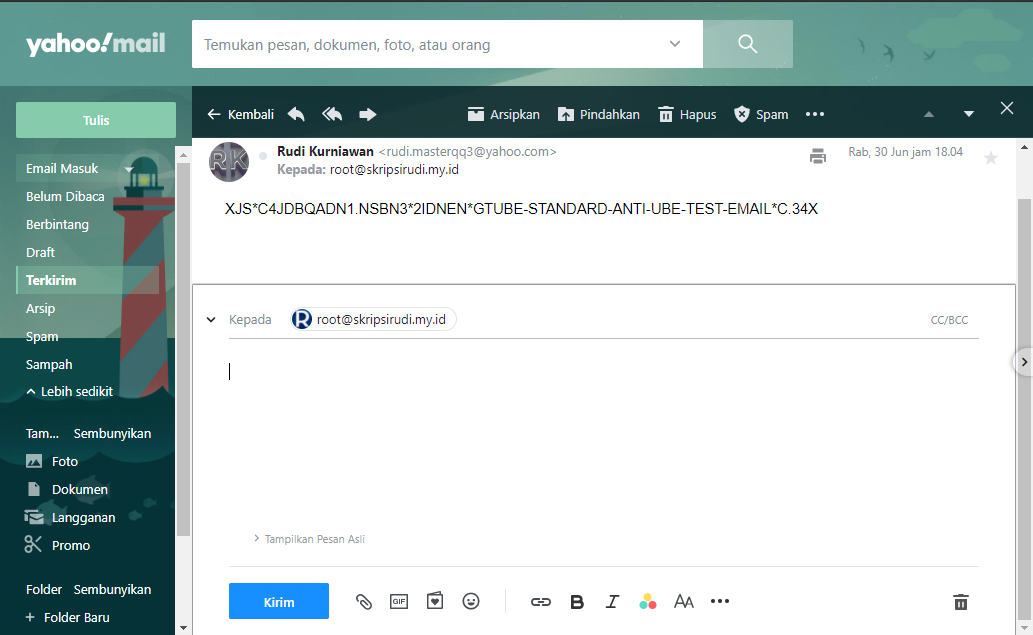
Uji coba mengirim *email spam* dari layanan *email* skripsirudi.my.id ke layanan *email* skripsirudi.my.id adalah dengan mengirim *email spam* menggunakan layanan *email* skripsirudi.my.id ke layanan *email* skripsirudi.my.id, isi pesan yang digunakan adalah XJS\*C4JDBQADN1.NSBN3\*2IDNEN\*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL\*C.34X yang merupakan standar GTUBE untuk menguji kinerja *anti spam* terlihat seperti gambar 4.54 berikut. (Hanif 2018). (Klop and Csuka 2018)

Gambar 4. 54 Mengirim *Email Spam* dari skripsirudi.my.id Setelah Penerapan

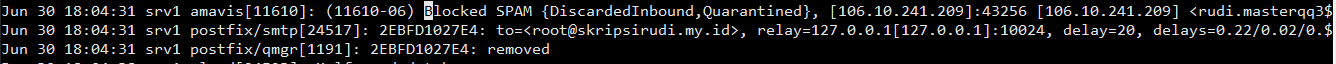
*Email spam* tersebut diatas diblokir oleh *Amavisd-New* karena terindikasi sebagai *email spam* oleh *SpamAssassin*, hasil pem*filter*an *email spam* dapat dilihat pada *mail log* dengan menggunakan perintah *#cat /var/log/maillog* seperti terlihat pada gambar 4.55 berikut. (Hanif 2018).

Gambar 4. 55 *Email* dari skripsirudi.my.id Terindikasi *Spam*

###### **Uji Coba Mengirim *Email Spam* dari *Yahoo mail***

Uji coba mengirim *email spam* dari layanan *email* *Yahoo! Mail* ke skripsirudi.my.id adalah dengan mengirim *email spam* menggunakan layanan *email Yahoo! Mail* ke layanan *email* skripsirudi.my.id, isi pesan yang digunakan adalah XJS\*C4JDBQADN1.NSBN3\*2IDNEN\*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL\*C.34X yang merupakan standar GTUBE untuk menguji kinerja *anti spam* terlihat seperti gambar 4.56 berikut. (Klop and Csuka 2018)

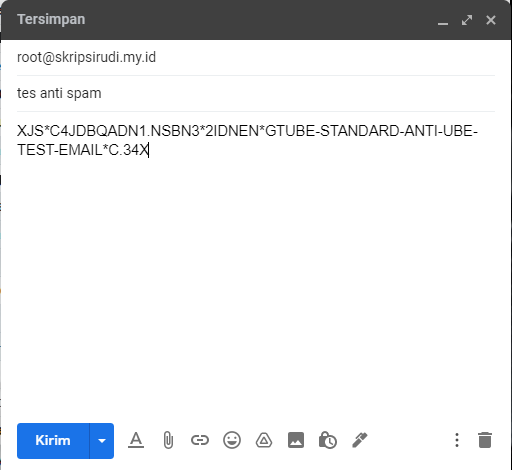
Gambar 4. 56 Mengirim *Email Spam* dari *Yahoo! Mail* Setelah Penerapan

*Email spam* tersebut diatas diblokir oleh *Amavisd-New* karena terindikasi sebagai *email spam* oleh *SpamAssassin*, hasil pem*filter*an *email spam* dapat dilihat pada *mail log* dengan menggunakan perintah *#cat /var/log/maillog* seperti terlihat pada gambar 4.57 berikut.

Gambar 4. 57 *Email* dari *Yahoo! Mail* Terindikasi *Spam*

###### **Uji Coba Mengirim *Email Spam* dari *Gmail***

Uji coba mengirim *email spam* dari layanan *email* *Gmail* ke layanan *email* skripsirudi.my.id adalah dengan mengirim *email spam* menggunakan layanan *email Gmail* ke layanan *email* skripsirudi.my.id, isi pesan yang digunakan adalah XJS\*C4JDBQADN1.NSBN3\*2IDNEN\*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL\*C.34X yang merupakan standar GTUBE untuk menguji kinerja *anti spam* terlihat seperti gambar 4.58 berikut. (Klop and Csuka 2018)

**Gambar 4. 58 Mengirim *Email Spam* dari *Gmail* Setalah Penerapan**

*Email spam* tersebut diatas diblokir oleh *Amavisd-New* karena terindikasi sebagai *email spam* oleh *SpamAssassin*, hasil pem*filter*an *email spam* dapat dilihat pada *mail log* dengan menggunakan perintah *#cat /var/log/maillog* seperti terlihat pada gambar 4.59 berikut.

Gambar 4. 59 *Email* dari *Gmail* Terindikasi *Spam*

###### **Uji Coba Mengirim *Email* *Spam* Tanpa *GTUBE Test***

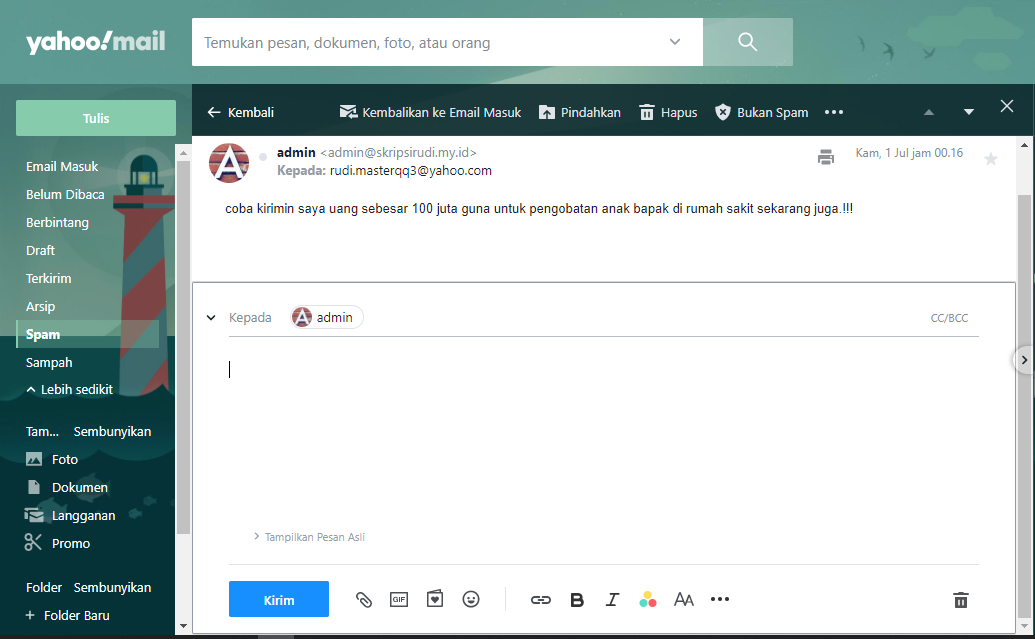
Uji coba mengirim *email* yang terindikasi *spam* oleh *Yahoo! Mail* adalah dengan mengirim *email* melalui *Emkei’s Fake Mailer* dengan *format*

*email* *spam* yang berisi penipuan atau promosi suatu produk seperti terlihat pada gambar 4.60 berikut.



Gambar 4. 60 *Email* Dengan Format *Spam*

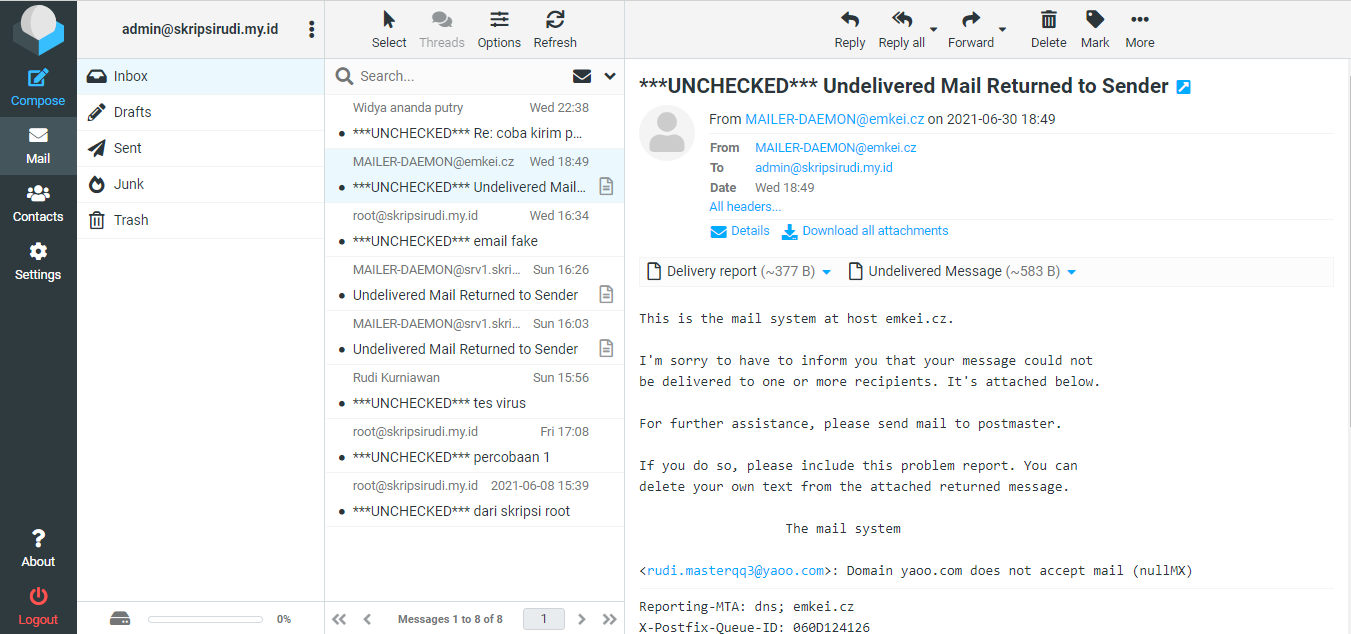
*Email* dengan *format spam* tersebut terkirim ke *Yahoo! Mail* dan masuk ke dalam *folder spam* seperti terlihat pada gambar 4.61 berikut.

******Gambar 4. 61 *Email* Terindikasi Sebagai *Spam* oleh *Yahoo! Mail***

*Yahoo! Mail* mengindikasi bahwa *email* diatas merupakan *spam* sehingga protocol *dmarc* mengkarantina email tersebut sehingga pesan terindikasi sebagai email spam terlihat pada header email bagian dmarc=fail(p=QUARANTINE) seperti pada gambar 4.62 berikut.



Gambar 4. 62 header *dmarc*

Pada email skripsirudi.my.id terlihat protocol *DMARC* yang melaporkan pesan email sebelumnya yang mengandung spoofing yang di kirim melalui emal emkei.cz telah di verifikasih bahwa pesan tersebut mengandung spoofing kemudian pesan tersebut di kirim kembali ke email skripsirudi.my.id, terlihat seperti gambar 4.63 berikut.

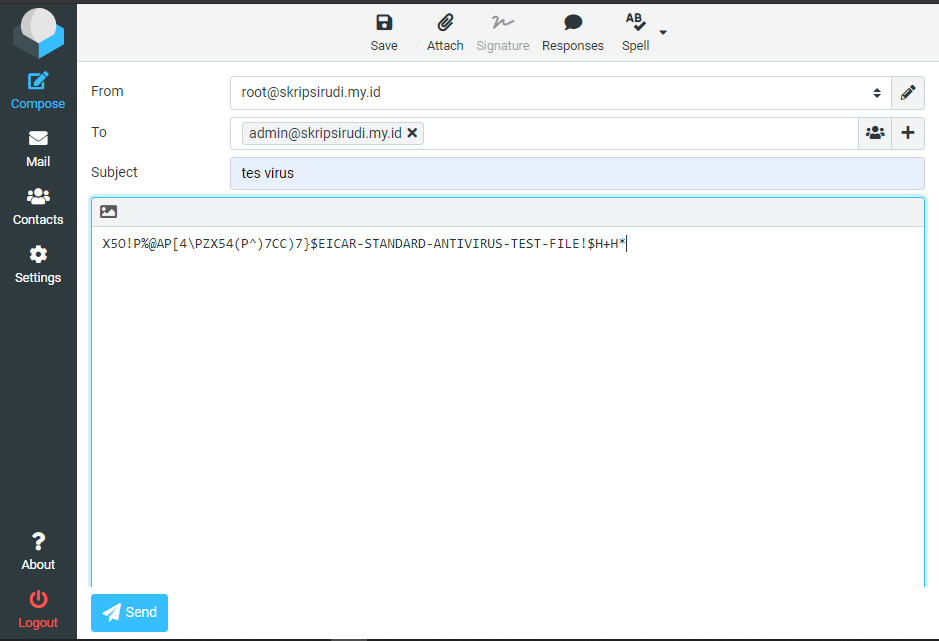
Gambar 4. 63 hasil report *DMARC* setelah protocol di terapkan

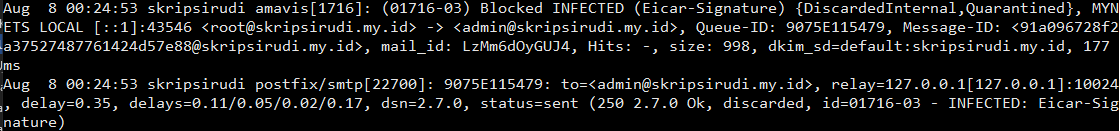
###### **Uji Coba Mengirim *Email* yang Mengandung *Virus***

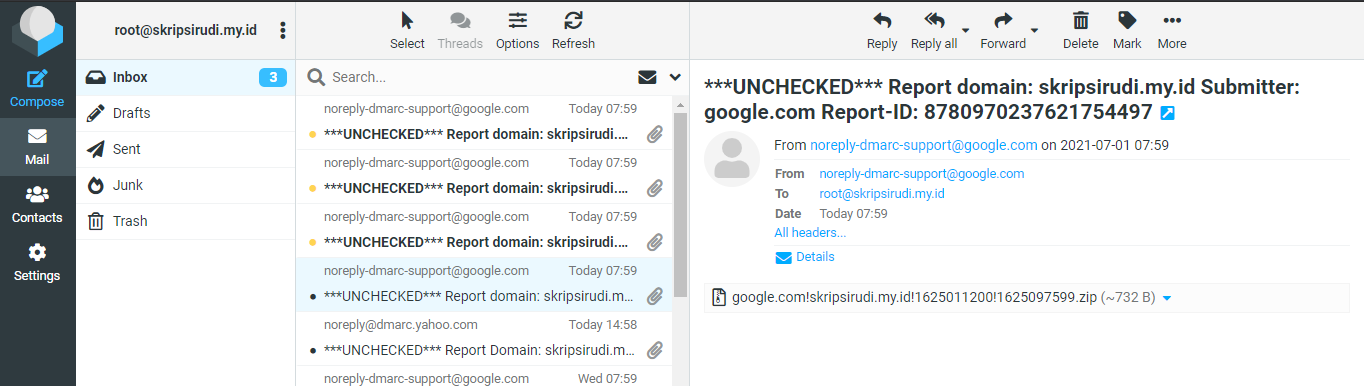
Uji coba mengirim *email* yang mengandung *virus* dilakukan dengan mengirim *email* yang mengandung *virus* dari layanan *email* skripsirudi.my.id, *Yahoo! Mail*, dan *Gmail* ke layanan *email* skripsirudi.my.id.

###### **Uji Coba Mengirim *Email* yang Mengandung *Virus* dari skripsirudi.my.id**

Uji coba pengiriman *email* yang mengandung *virus* dilakukan dengan mengirim *email* dengan isi X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H\* yang merupakan standar *EICAR* untuk melakukan tes *anti virus mail server*, *email* yang mengandung *virus* dikirim dari layanan *email* skripsirudi.my.id ke layanan *email* skripsirudi.my.id, seperti pada gambar 4.64 Berikut. (Abrams 1999)

******Gambar 4. 64 *EICAR Test* dari skripsirudi.my.id Setelah Penerapan**

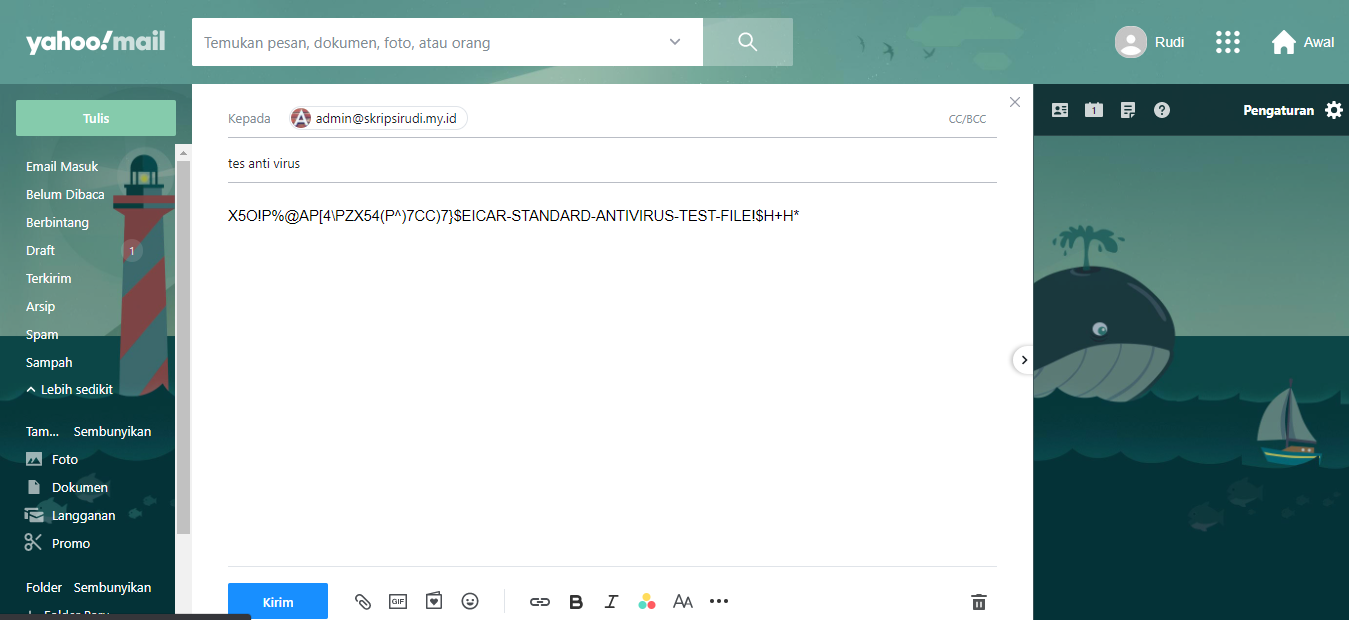
Setelah *email* yang mengandung *virus* tersebut dikirim ke salah satu *user email* yang ada pada *mail servrer* skripsirudi.my.id maka *email* tersebut akan di blok oleh *Amavis-New* dan di deteteksi sebagai virus oleh *ClamAV*, namun terdapat report *DMARC* yang memberitahukan bawah email tersebut mengandung virus sehingga pesan yang masuk tidak dapat di baca, hanya report pesan, seperti terlihat pada gambar 4.65 dan gambar 4.66 berikut.

Gambar 4. 65 email local dari skripsirudi.my.id terblok

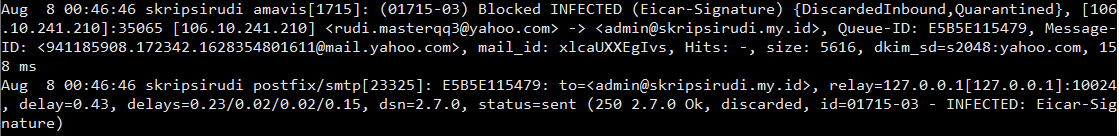
Gambar 4. 66 report email yang mengandung virus

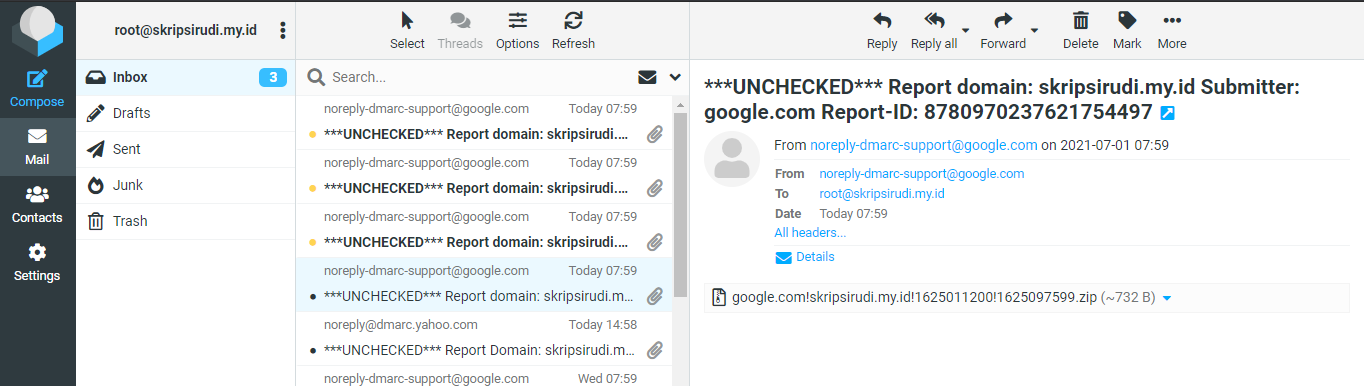
###### **Uji Coba Mengirim *Email* yang Mengandung *Virus* dari *Yahoo! Mail***

Uji coba mengirim *email* yang mengandung *virus* dilakukan dengan mengirim *email* dengan isi X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H\* yang merupakan standar *EICAR* untuk melakukan tes *anti virus mail server, email* yang mengandung *virus* dikirim dari layanan *email Yahoo! Mail* ke layanan *email* skripsirudi.my.id, seperti pada gambar 4.67 berikut.(Abrams 1999)

******Gambar 4. 67 *EICAR Test* dari *Yahoo! Mail* Setelah Penerapan**

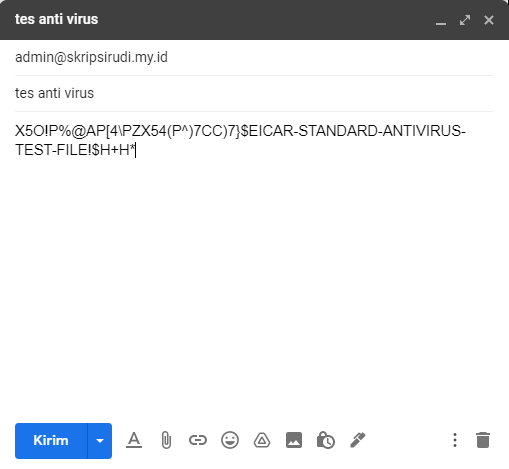
Setelah *email* yang mengandung *virus* tersebut dikirim ke salah satu *user email* yang ada pada *mail servrer* skripsirudi.my.id maka *email* tersebut akan di blok oleh *Amavis-New* dan di deteteksi sebagai virus oleh *ClamAV*, namun terdapat report *DMARC* yang memberitahukan bawah email tersebut mengandung virus sehingga pesan yang masuk tidak dapat di baca, hanya report pesan, seperti terlihat pada gambar 4.68 dan gambar 4.69 berikut

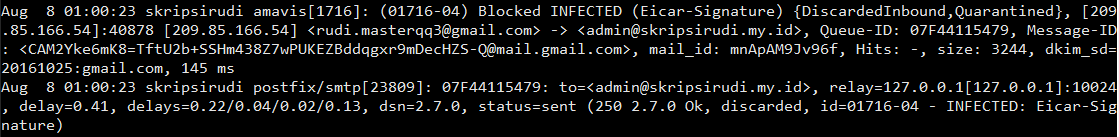
******Gambar 4. 68 email dari** [**rudi.masterqq3@yahoo.com**](mailto:rudi.masterqq3@yahoo.com) **ke skripsirudi.my.id terblok**

******Gambar 4. 69 report email yang mengandung virus**

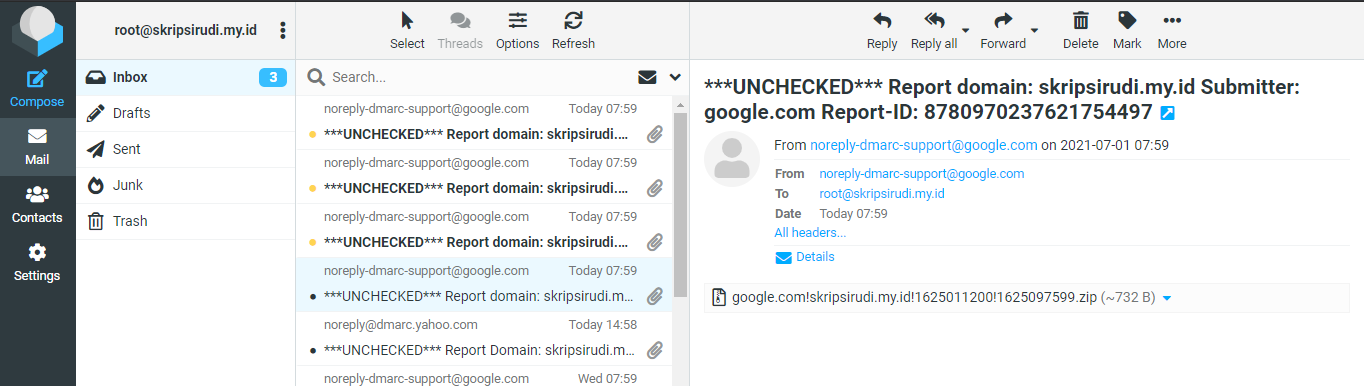
###### **Uji Coba Mengirim *Email* yang Mengandung *Virus* dari *Gmail***

Uji coba mengirim *email* yang mengandung *virus* dilakukan dengan mengirim *email* dengan isi X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H\* yang merupakan standar *EICAR* untuk melakukan tes *anti virus mail server, email* yang mengandung *virus* di kirim dari layanan *email Gmail Mail* ke layanan *email* skripsirudi.my.id, seperti pada gambar 4.70 berikut. (Abrams 1999)

******Gambar 4. 70 *EICAR Test* dari *Gmail* Setelah Penerapan**

Setelah *email* yang mengandung *virus* tersebut dikirim ke salah satu *user email* yang ada pada *mail servrer* skripsirudi.my.id maka *email* tersebut akan di blok oleh *Amavis-New* dan di deteteksi sebagai virus oleh *ClamAV*, namun terdapat report *DMARC* yang memberitahukan bawah email tersebut mengandung virus sehingga pesan yang masuk tidak dapat di baca, hanya report pesan, seperti terlihat pada gambar 4.71 dan gambar 72 berikut.

Gambar 4. 71 email di blok oleh antivirus client

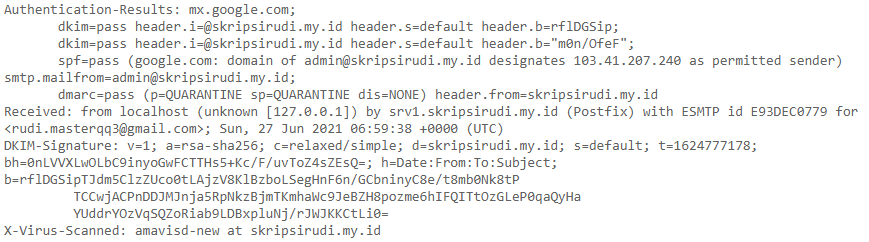
Gambar 4. 72 report email yang mengandung virus

##### **Uji coba pengecekan *header email***

Uji coba pengecekan *header email* dilakukan dengan membandingkan *header email* yang di kirim dari skripsirudi.my.id ke *Gmail, Yahoo! Mail*, dan skripsirudi.my.id sebelum dan setelah penerapan protocol *DMARC,* *DKIM, SPF, anti spam*, dan *anti virus*.

###### ***Header Email* pada *Gmail***

Uji coba ini dilakukan dengan mengirim *email* menggunakan salah satu *user email* yang ada pada layanan *email* skripsirudi.my.id ke salah satu *user email* yang ada pada layanan *email* *Gmail* kemudian melakukan pengecekan *header email* tersebut dan melakukan perbandingan terhadap *header email* setelah penerapan protocol *DMARC,* *DKIM*, *SPF, anti spam,* dan *anti virus*, *header email* terlihat seperti gambar 4.73 berikut.

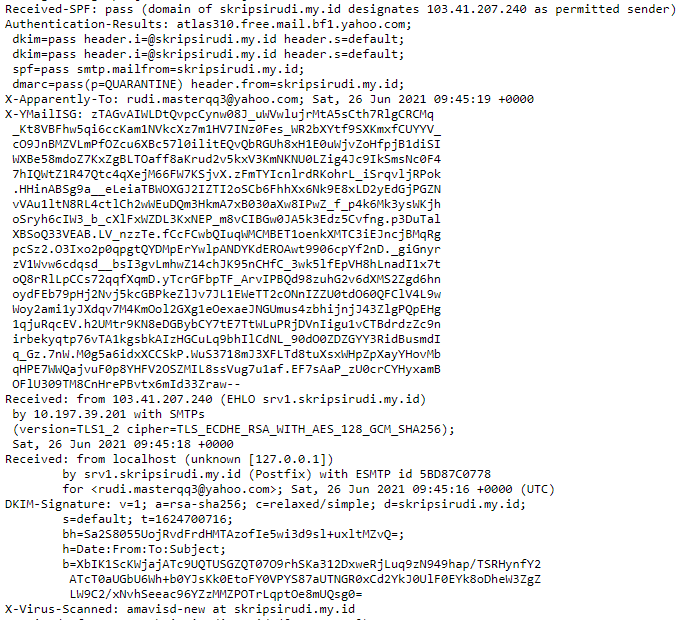


Gambar 4. 73 Cuplikan *Header Email* pada *Gmail* Setelah Penerapan

Pada gambar 4.73 terlihat perbedaan *header email* setelah penerapan protocol *DMARC, DKIM, SPF*, dan *anti virus* yaitu terdapat tambahan parameter *DMARC* yang bernilai dmarc*= pass, X-Virus-Scanned*, dan *DKIM-Signature* yang bernilai dkim=pass.

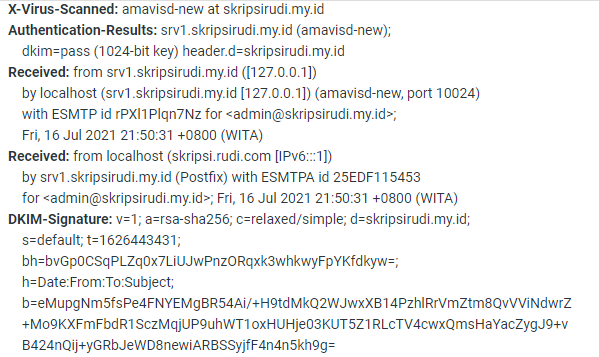
###### ***Header Email* pada *Yahoo! Mail***

Uji coba ini dilakukan dengan mengirim *email* menggunakan salah satu *user email* yang ada pada layanan *email* skripsirudi.my.id ke salah satu *user* yang ada pada layanan *email Yahoo! Mail* kemudian melakukan pengecekan *header email* tersebut setelah penerapan protocol *DMARC,*  *DKIM*, *SPF, anti spam,* dan *anti virus*, *header email* terlihat seperti gambar 4.74 berikut.

******Gambar 4. 74 Cuplikan *Header Email* pada *Yahoo! Mail* Setelah Penerapan**

Pada gambar 4.53 terlihat perbedaan *header email* setelah penerapan protocol *DMARC, DKIM*, *SPF*, *anti spam*, dan *anti virus* yaitu nilai dari parameter *Received-SPF* yang awalnya *none* menjadi *pass*, parameter *dkim* yang awalnya neutral menjadi *pass*, parameter *dmarc* yang menjadi pass dan terdapat tambahan parameter *DKIM-Signature* dan *X-Virus-Scanned,* (Hanif 2018).

###### ***Header Email* pada skripsirudi.my.id**

Uji coba ini dilakukan dengan mengirim *email* menggunakan salah satu *user email* yang ada pada layanan *email* skripsirudi.my.id ke salah satu *user* yang ada pada layanan *email skripsirudi.my.id* kemudian melakukan pengecekan *header email* tersebut setelah penerapan protocol *DMARC,*  *DKIM*, *SPF, anti spam,* dan *anti virus*, *header email* terlihat seperti gambar 4.75 berikut.

Gambar 4. 75 Cuplikan *Header Email* skripsirudi.my.idSetelah Penerapan

Pada gambar 4.76 terlihat perbedaan *header email* setelah penerapan protocol *DMARC,* *DKIM, SPF, anti spam*, dan *anti virus* yaitu terdapat tambahan parameter *DKIM-Signature* dan *X-Virus-Scanned*, serta terlihat *port* yang menghubungkan antara *MTA* dengan *Amavisd-New* yaitu *port* 10024.

## **Analisa Hasil Uji Coba**

Pada tahap ini akan dilakukan analisa hasil uji coba yang telah di lakukan sebelumnya. Pada analisa hasil uji coba akan di tampilkan analisa hasil uji coba pengiriman *email spoofing* sebelum dan setelah penerapan protocol *DMARC,* *DKIM* dan *SPF*, pengiriman *email spam* sebelum dan setelah penerapan *anti spam*, pengiriman *email* yang mengandung *virus* sebelum dan setelah penerapan *anti virus*, dan pengecekan *header email* sebelum dan setelah penerapan protocol *DMARC,* *DKIM*, *SPF*, *anti spam*, dan *anti virus* (Hanif 2018)*.*

### **Analisa Hasil Uji Coba Pengiriman *Email Spoofing***

Cara yang dapat digunakan untuk mengetahui apakah sudah dilakukan proses otorisasi dan otentikasi oleh protocol *DMARC,* *DKIM* dan *SPF* adalah dengan melakukan pengiriman *email spoofing* menggunakan *Emkei’s Fake Mailer* dengan mengatasnamakan salah satu *user email* pada *mail server* skripsirudi.my.id, kemudian *email* tersebut dikirim ke layanan *email Gmail*, *Yahoo! Mail*, dan skripsirudi.my.id. Berikut Analisa hasil ujicoba perbandingan sebelum diterapkan protocol *DMARC,* *DKIM* dan *SPF* dan setelah diterapakan protocol *DMARC,* *DKIM* dan *SPF* yang dilakukan pada uji coba sebelumnya, seperti terlihat pada tabel 4.1 berikut. (Hanif 2018).

Tabel 4. 1 Perbandingan Sebelum dan Setelah Penerapan protocol *DMARC,* *DKIM* dan *SPF*

| **NO** | ***Fake Mailer*** | **Layanan *Email* yang diatasnamakan** | **Layanan *Email* Penerima** | **Sebelum Penerapan** | **Setelah Penerapan** |
| --- | --- | --- | --- | --- | --- |
| 1 | *Emkei’s Fake Mailer* | Skripsirudi.my.id | *Gmail* | Masuk *Folder Inbox* | Diblokir  Dan di report oleh DMARC |
| 2 | *Emkei’s Fake Mailer* | Skripsirudi.my.id | *Yahoo! Mail* | Masuk *Folder Inbox* | Masuk *Folder Spam* |
| 3 | *Emkei’s Fake Mailer* | Skripsirudi.my.id | Skripsirudi.my.id | Masuk *Folder Inbox* | Masuk *Folder Inbox* |

Berdasarkan tabel 4.1 perbandingan sebelum dan setelah penerapan protocol *DMARC,* *DKIM* dan *SPF* dengan melakukan pengiriman *email spoofing* yang dikirim menggunakan *Emkei’s Fake Mailer* ke layanan *email* *Gmail*, *Yahoo! Mail*, dan skripsirudi.my.id sebelum penerapan protocol *DMARC,* *DKIM* dan *SPF* yaitu *email spoofing* berhasil masuk ke *folder inbox* penerima *email* yang berada pada *mail server* *Gmail*, *Yahoo! Mail*, dan skripsirudi.my.id sedangkan setelah penerapan protocol *DMARC,* *DKIM* dan *SPF*, *email spoofing* tersebut diblokir dan *dmarc*  mereport email, dimasukan ke *folder spam* oleh layanan *email Yahoo! Mail* dan dimasukan ke *folder inbox* oleh layanan *email* skripsirudi.my.id. (Hanif 2018).

### **Analisa Hasil Uji Coba Pengiriman *Email Spam***

Analisa penerapan *anti spam* dilakukan dengan mengirim *email spam* dengan menggunakan layanan *email* skripsirudi.my.id, *Yahoo! Mail*, dan *Gmail* ke layanan *email* skripsirudi.my.id untuk menguji kinerja *anti spam* sebelum dan setelah penerapan *anti spam* seperti terlihat pada tabel 4.2 berikut.(Hanif 2018).

Tabel 4.2 Perbandingan Sebelum dan Setelah Penerapan *Anti Spam*

| **NO** | **Layanan *Email* Pengirim** | **Layanan *Email* Penerima** | **Sebelum Penerapan** | **Setelah Penerapan** |
| --- | --- | --- | --- | --- |
| 1 | *Yahoo! Mail* | Skripsirudi.my.id | Masuk *Folder Inbox* | Diblokir |
| 2 | *Gmail* | Skripsirudi.my.id | Masuk *Folder Inbox* | Diblokir |
| 3 | Skipsirudi.my.id | Skripsirudi.my.id | Masuk *Folder Inbox* | Diblokir |

Berdasarkan tabel 4.2 dapat disimpulkan bahwa sebelum penerapan *anti spam*, tidak terjadi pemblokiran *email spam* oleh *Amavisd-New* sehingga *email spam* dapat masuk pada *folder inbox* pengguna yang berada pada *mail server* skripsirudi.my.id, sedangkan setelah penerapan *anti spam*, terjadi proses pemblokiran *email spam* oleh *Amavisd-New* sehingga *email* yang terindikasi sebagai *spam* langsung diblokir sebelum sampai pada *folder* penerima *email* (Hanif 2018).

### **Analisa Hasil Uji Coba Mengirim *Email* Mengandung *Virus***

Analisa penerapan *anti virus* dilakukan dengan mengirim *email spam* dengan menggunakan layanan *email* skripsirudi.my.id, *Yahoo! Mail*, dan *Gmail* ke layanan *email* skripsirudi.my.id untuk menguji kinerja *anti spam* sebelum dan setelah penerapan *anti spam* seperti terlihat pada tabel 4.3. (Hanif 2018).

Tabel 4.3 Perbandingan Sebelum Penerapan *Anti virus*

| **NO** | **Layanan *Email* Pengirim** | **Layanan *Email* Penerima** | **Sebelum Penerapan** | **Setelah Penerapan** |
| --- | --- | --- | --- | --- |
| 1 | *Yahoo! Mail* | Skripsirudi.my.id | Masuk *Folder Inbox* | Diblokirdan di report oleh dmarc |
| 2 | *Gmail* | Skripsirudi.my.id | Masuk *Folder Inbox* | Diblokirdan di report oleh dmarc |
| 3 | Skripsirudi.my.id | Skripsirudi.my.id | Masuk *Folder Inbox* | Diblokirdan di report oleh dmarc |

Berdasarkan tabel 4.3, dapat disimpulkan bahwa sebelum penerapan *anti virus*, tidak terjadi proses pemblokiran *email* yang mengandung *virus* oleh *Amavisd-New* sehingga *email* yang mengandung *virus* dapat masuk pada *folder inbox* pengguna *email* yang berada pada *mail server* skripsirudi.my.id, sedangkan setelah penerapan *anti virus*, tidak terjadi pemblokiran *email* namun ada report *DMARC* yang mereport email yang mengandung *virus* sehingga *email* yang terindikasi mengandung *virus* langsung di report (Hanif 2018).

### **Analisa Hasil Uji Coba Pengecekan *Header Email***

Analisa pengecekan *header email* dilakukan dengan melihat *header email* sebelum dan setelah penerapan protocol *DMARC,* *DKIM*, *SPF*, *anti spam*, dan *anti virus*. Perbedaan *header email* sebelum dan setelah diterapkan protocol *DMARC,* *DKIM*, *SPF, anti spam,* dan *anti virus* terlihat seperti pada tabel 4.4 berikut.

Tabel 4.4 Perbandingan Header Email Sebelum dan Setelah Penerapan

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **NO** | **Uji Coba** | **Layanan Email** | **DKIM-Signature** | **DMARC** | **X-Virus-Scanned** | **Nilai Received-SPF** |
| 1 | Sebelum Penerapan | Gmail | *DKIM* *=temperror* | - | - | neutral |
| Yahoo! Mail | dkim=perm\_fail | - | - | none |
| Skripsirudi.my.id | dkim=neutral | - | - | - |
| 2 | Setelah Penerapan | Gmail | Pass | Pass | Ada | Pass |
| Yahoo! Mail | Pass | Pass | Ada | Pass |
| Skripsirudi.my.id | Pass | - | Ada | - |

Catatan : keterangan “-“ bermakna tidak terdapat pengaturan paramenter tersebut.

Berdasarkan tabel 4.4, sebelum penerapan protocol *DMARC,* *DKIM*, *SPF*, *anti spam*, dan *anti virus* terdapat parameter *DKIM-Signature* yang bernilao *temperror* dan tidak terdapat parameter *X-Virus-Scanned*, namun *Received-SPF* bernilai *neutral* pada *header email* di *Gmail*, sedangkan setelah penerapan protocol *DMARC,* *DKIM*, *SPF*, *anti spam*, dan *anti virus* terdapat parameter dmarc=pass, *DKIM-Signature* dan *X-Virus-Scanned*, serta *Received-SPF* bernilai *Pass* pada *header email* di *Gmail*.

Sebelum penerapan protocol *DMARC*, *DKIM*, *SPF*, *anti spam*, dan *anti virus* tidak terdapat parameter *DKIM-Signature* yang bernilai *perm\_fail* dan tidak ada parameter *X-Virus-Scanned*, serta *Received-SPF* bernilai *none* pada *header email* di *Yahoo! Mail*, sedangkan setelah penerapan protocol *DMARC*, *DKIM*, *SPF*, *anti spam*, dan *anti virus* terdapat parameter dmarc=pass, *DKIM-Signature* bernilai Pass dan *X-Virus-Scanned*, serta *Received-SPF* bernilai *Pass* pada *header email* di *Yahoo! Mail*.

Sebelum penerapan protocol *DMARC*, *DKIM*, *SPF*, *anti spam*, dan *anti virus* terdapat parameter *DKIM-Signature* yang bernilai *neutral* dan tidak ada parameter *X-Virus-Scanned,* sedangkan parameter *SPF-Received* juga tidak ada pada *header email* di skripsirudi.my.id, sedangkan setelah penerapan protocol *DMARC*, *DKIM*, *SPF*, *anti spam*, dan *anti virus* terdapat parameter *DKIM-Signature* yang benilai Pass dan *X-Virus-Scanned*, namun tetap tidak terdapat parameter *Received-SPF* dan *DMARC* pada *header email* di skripsirudi.my.id. (Hanif 2018).