

## BAB IV

### HASIL DAN PEMBAHASAN

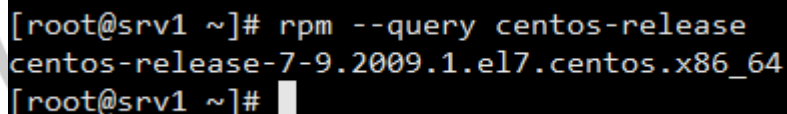
Bab ini memuat tentang pembahasan dan instalasi, konfigurasi mail server, serta Analisa dan hasil uji coba.

#### 4.1 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).

##### 4.1.1 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).



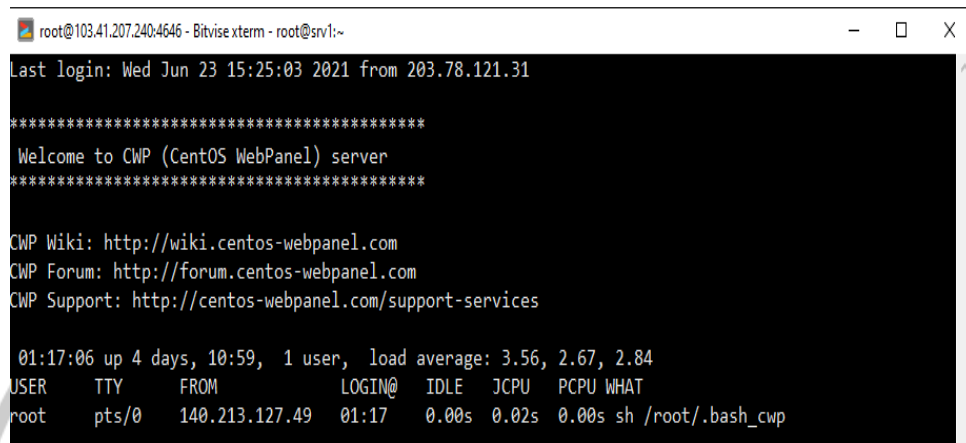
```
[root@srv1 ~]# rpm --query centos-release
centos-release-7-9.2009.1.el7.centos.x86_64
[root@srv1 ~]#
```

Gambar 4.1 Linux CentOS release 7-9

##### 4.1.2 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 mendownload *file installer CWP* versi terbaru

dengan perintah `#wget 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).



```

root@103.41.207.240:4646 - Bitvise xterm - root@srv1:~
Last login: Wed Jun 23 15:25:03 2021 from 203.78.121.31

*****
Welcome to CWP (CentOS WebPanel) server
*****

CWP Wiki: http://wiki.centos-webpanel.com
CWP Forum: http://forum.centos-webpanel.com
CWP Support: http://centos-webpanel.com/support-services

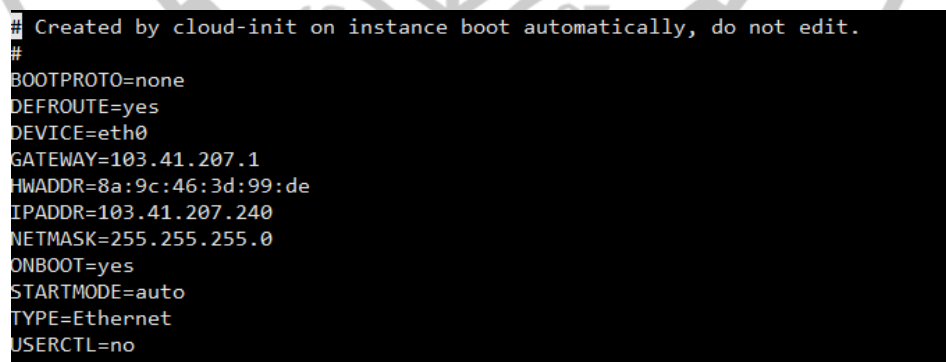
01:17:06 up 4 days, 10:59, 1 user, load average: 3.56, 2.67, 2.84
USER  TTY      FROM          LOGIN@  IDLE   JCPU   PCPU   WHAT
root  pts/0    140.213.127.49 01:17   0.00s  0.02s  0.00s  sh /root/.bash_cwp

```

Gambar 4.2 Hasil Instalasi CWP

#### 4.1.3 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).



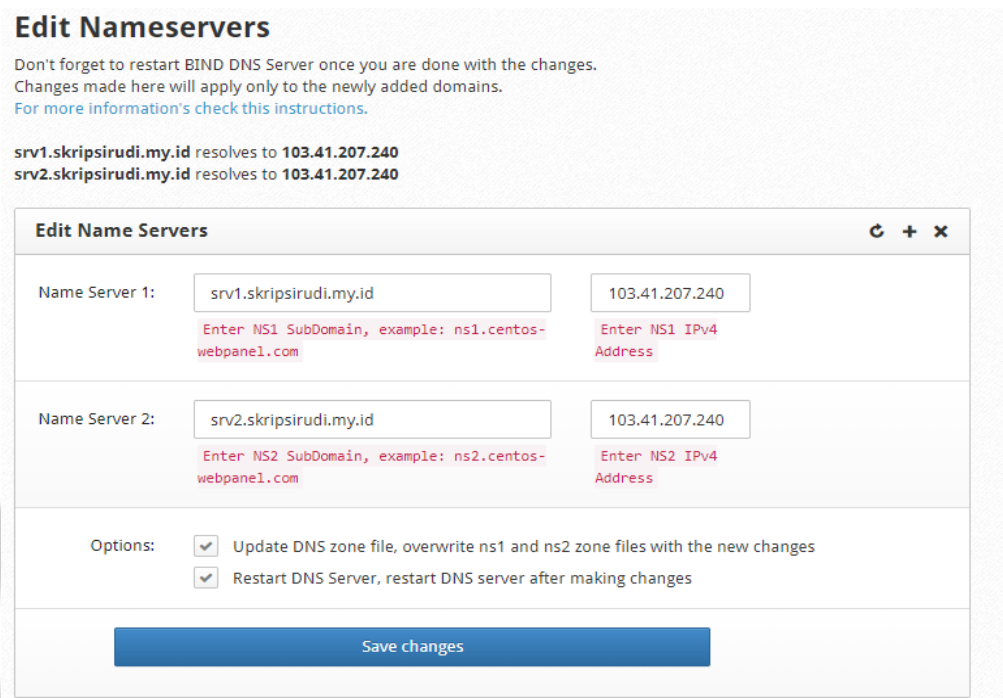
```

# Created by cloud-init on instance boot automatically, do not edit.
#
BOOTPROTO=none
DEFROUTE=yes
DEVICE=eth0
GATEWAY=103.41.207.1
HWADDR=8a:9c:46:3d:99:de
IPADDR=103.41.207.240
NETMASK=255.255.255.0
ONBOOT=yes
STARTMODE=auto
TYPE=Ethernet
USERCTL=no

```

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)



**Edit Nameservers**

Don't forget to restart BIND DNS Server once you are done with the changes.  
Changes made here will apply only to the newly added domains.  
[For more information's check this instructions.](#)

srv1.skripsirudi.my.id resolves to 103.41.207.240  
srv2.skripsirudi.my.id resolves to 103.41.207.240

Edit Name Servers	
Name Server 1:	<div> <div>srv1.skripsirudi.my.id</div> <div>103.41.207.240</div> </div> <div> <div>Enter NS1 SubDomain, example: ns1.centos-webpanel.com</div> <div>Enter NS1 IPv4 Address</div> </div>
Name Server 2:	<div> <div>srv2.skripsirudi.my.id</div> <div>103.41.207.240</div> </div> <div> <div>Enter NS2 SubDomain, example: ns2.centos-webpanel.com</div> <div>Enter NS2 IPv4 Address</div> </div>
Options:	<div> <input checked="" type="checkbox"/> Update DNS zone file, overwrite ns1 and ns2 zone files with the new changes           <input checked="" type="checkbox"/> Restart DNS Server, restart DNS server after making changes         </div>
<div>Save changes</div>	

**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)

## Add Domain

Path must be /home/USERNAME eg. /home/mywebsite/...

If you enter / then the home path will be eg. /home/mywebsite/

If you enter /public\_html/addondomain1.com then the path will be /home/mywebsite/public\_html/addondomain1.com

Add a New Domain

Add Domain:

skripsirudi.my.id

Enter domain name without www.

to User:

rudi

Select user to which you want to add this domain

Folder Path:

/public\_html

/home/USERNAME

Enter path to a folder in user homedir

☐ AutoSSL: Install SSL certificate, domain and www. subdomain must be pointed to the server!

Create

**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 memetakan 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)

```

$TTL 14400
@ 86400 IN SOA srv1.skripsirudi.my.id. postmaster.skripsirudi.my.id. (
    2021062472 ; serial, todays date+todays
    3600 ; refresh, seconds
    7200 ; retry, seconds
    1209600 ; expire, seconds
    86400 ) ; minimum, seconds
@ 86400 IN NS srv1.skripsirudi.my.id.
@ 86400 IN NS srv2.skripsirudi.my.id.
@ IN A 103.41.207.240
@ IN NS srv1.skripsirudi.my.id.
@ IN MX 10 srv1.skripsirudi.my.id.
srv1 14400 IN A 103.41.207.240
srv2 14400 IN A 103.41.207.240
srv1.skripsirudi.my.id. 14400 IN A 103.41.207.240
srv2.skripsirudi.my.id. 14400 IN A 103.41.207.240

```

**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)

```

$TTL 144000
@ IN SOA srv1.skripsirudi.my.id. root.skripsirudi.my.id. (
    2017082100 ;serial, todays date+todays
    86400 ;refresh, seconds
    7200 ;retry, seconds
    3600000 ;expire, seconds
    86400 ;minimum, seconds
)
@ IN NS srv1.skripsirudi.my.id.
240 IN PTR skripsirudi.my.id.
240 IN PTR srv1.skripsirudi.my.id.
240 IN PTR srv2.skripsirudi.my.id.

```

**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 digunakan, selanjutnya 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 merestart DNS server yang terdapat pada dashboard CPW pada bagian server service. Seperti terlihat pada gambar 4.8 berikut. (Hanif 2018)

```
zone "." IN {
    type hint;
    file "named.ca";
};

zone "207.41.103.in-addr.arpa" IN {
    type master;
    file "/var/named/207.41.103.in-addr.arpa.db";
    allow-update { none };
};
```

Gambar 4.8 File `named.conf`

#### 4.1.4 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)

**Create a New Email Account (MailBox)**

Select User: rudi

Email Address: Enter Email Address @skripsirudi.my.id

Password: \*\*\*\*\*

Confirm Password:

Buttons: Close, Create Mail

**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)

**Rebuild Postfix Configuration [Last Rebuild: 2021-04-07 16:00:19]**

AntiSpam/AntiVirus (recommended): ☒ ClamAV, Amavis & Spamassassin, Requires 2Gb+ RAM

rDNS Check (recommended): ☒ Drop all emails if no rDNS/PTR

Install DKIM & SPF (recommended): ☒ Installs DKIM & SPF, enables DKIM for New Accounts and Domains

Install Policyd (recommended): ☐ Installs Policyd, enables hourly email limit per domain.

Reject Unknown Hostname (**NOT recommended**): ☐ **WARNING:** Reject unless the hostname has valid DNS record.

Current Settings in Postfix:

```
mydomain = skripsirudi.my.id
myhostname = srv1.skripsirudi.my.id
```

Hostname: srv1.skripsirudi.my.id (change hostname)

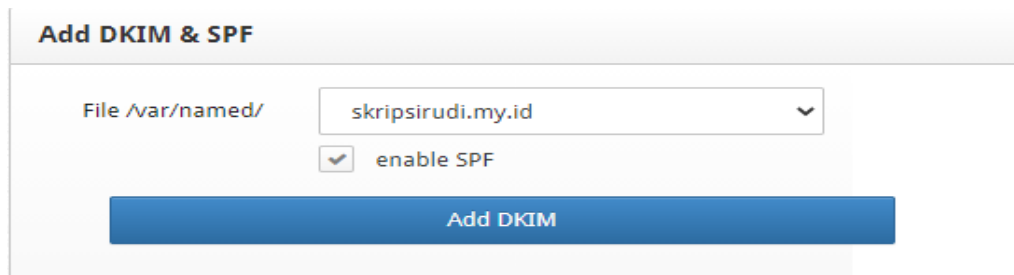
Domain: my.id (must be the main domain of the server hostname)

Rebuild Mail Server

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

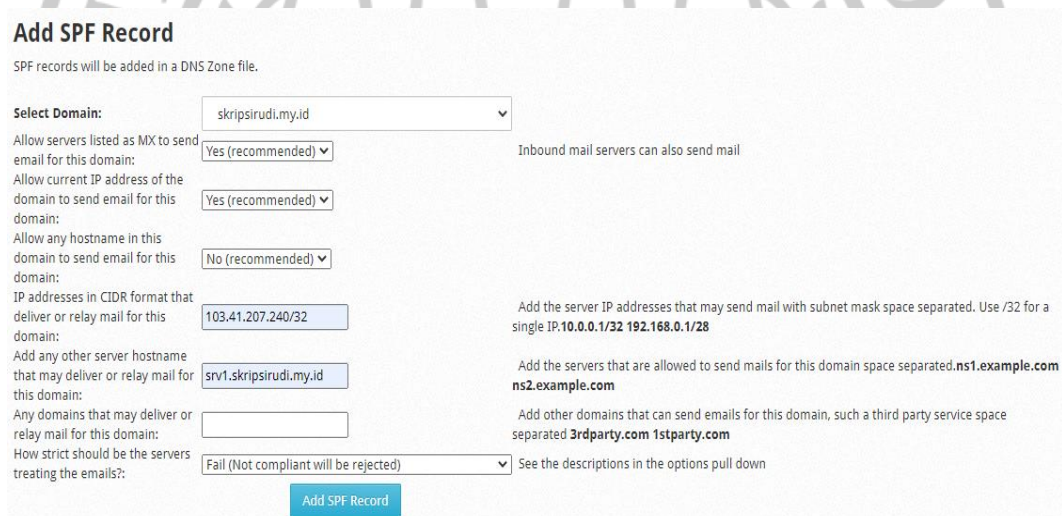


Konfigurasi *DKIM* dilakukan pada *menu Email* kemudian masuk pada sub menu *DKIM Manager*, seperti terlihat pada gambar 4.11 berikut. (Hanif 2018)



**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)

```
skripsirudi.my.id. IN TXT "v=spf1 mx a ip4:103.41.207.240/32 a:srv1.skripsirudi.my.id -all"
default._domainkey 14400 IN TXT "v=DKIM1; k=rsa;
p=MIGfMA0GC5qG5Ib3DQEBAQUAA4GNADCBiQKBgQC7b7KUq0Ya9Jz0iDa3NF+WJquppUdry0MjttVjkaQ8eoUloMU4Y8RFst2
71mdjjcQzW51P+p0iFJJ2MKMz0MtLkz2xAkr98epATFKfb9GIK0Olv45WMJOFhQpHk/O76iBiKogTLcxZ7RMENpIt9TV50yf1JZ1xZi
dVEhHXgR9YGwIDAQAB"
```

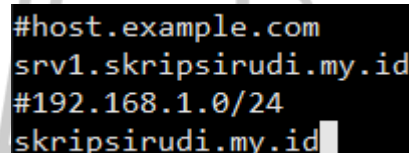
**Gambar 4.13 *DKIM dan SPF Record***



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).

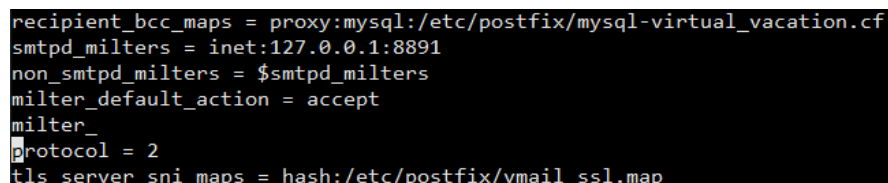
(Hanif 2018) Agar `srv1.skripsirudi.my.id` menjadi *host* yang dipercaya maka harus ditambahkan *hostname* pada baris 2 pada *file* `TrustedHosts` dibaris yang paling bawah dengan perintah `#nano /etc/opendkim/TrustedHosts` seperti pada gambar 4.14 berikut.



```
#host.example.com
srv1.skripsirudi.my.id
#192.168.1.0/24
skripsirudi.my.id
```

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 memfilter *email*, seperti terlihat pada gambar 4.15 berikut.

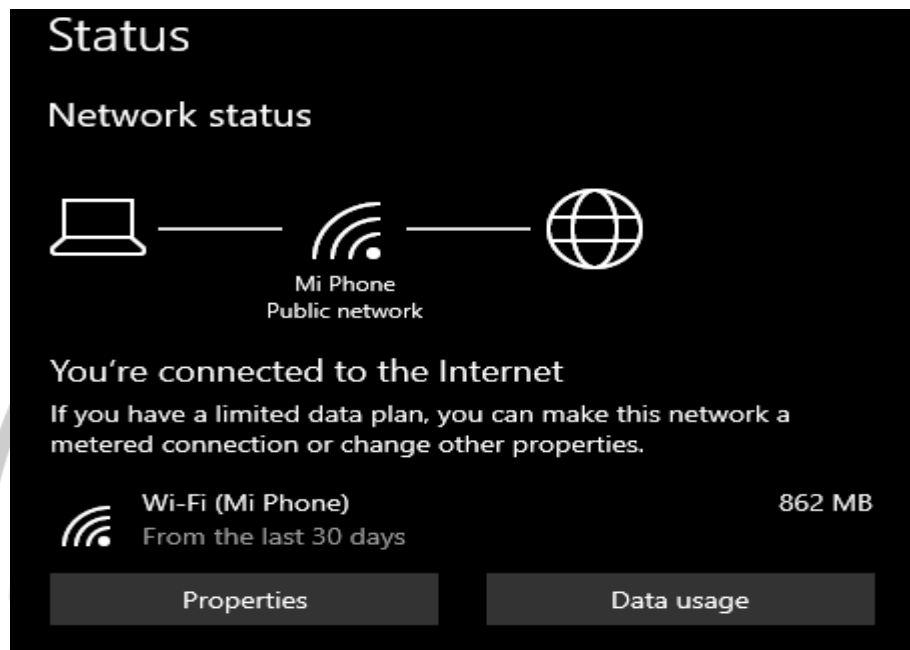


```
recipient_bcc_maps = proxy:mysql:/etc/postfix/mysql-virtual_vacation.cf
smtpd_milters = inet:127.0.0.1:8891
non_smtpd_milters = $smtpd_milters
milter_default_action = accept
milter_protocol = 2
tls_server_sni_maps = hash:/etc/postfix/vmail_ssl.map
```

Gambar 4.15 Konfigurasi File `main.cf`

#### 4.1.5 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*

#### 4.2 Hasil Uji Coba

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

##### 4.2.1 Verifikasi Konfigurasi

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

##### 4.2.2 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.

```

[root@srv1 ~]# nslookup mail.skripsirudi.my.id
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
mail.skripsirudi.my.id canonical name = skripsirudi.my.id.
Name:   skripsirudi.my.id
Address: 103.41.207.240

[root@srv1 ~]# nslookup skripsirudi.my.id
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
Name:   skripsirudi.my.id
Address: 103.41.207.240

[root@srv1 ~]# nslookup www.skripsirudi.my.id
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
www.skripsirudi.my.id canonical name = skripsirudi.my.id.
Name:   skripsirudi.my.id
Address: 103.41.207.240

[root@srv1 ~]# host -t mx skripsirudi.my.id
skripsirudi.my.id mail is handled by 10 srv1.skripsirudi.my.id.
skripsirudi.my.id mail is handled by 0 skripsirudi.my.id.
[root@srv1 ~]# nslookup srv1.skripsirudi.my.id
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
Name:   srv1.skripsirudi.my.id
Address: 103.41.207.240

```

Gambar 4.17 Verifikasi Konfigurasi *DNS Server*

#### 4.2.3 Verifikasi Konfigurasi *Mail Server*

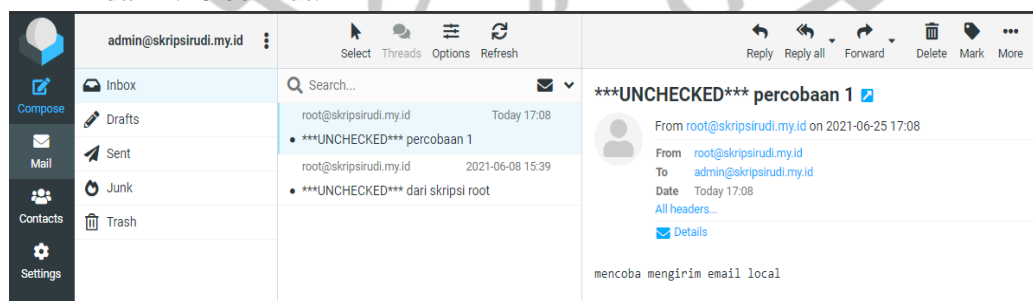
(Hanif 2018) Verifikasi konfigurasi *mail server* dapat dilakukan dengan cara menulis perintah *#service dovecot status* dan *#service postfix status* pada terminal seperti terlihat pada gambar 4.18 berikut.

```
[root@srv1 ~]# service dovecot status
Redirecting to /bin/systemctl status dovecot.service
• dovecot.service - Dovecot IMAP/POP3 email server
  Loaded: loaded (/usr/lib/systemd/system/dovecot.service; enabled; vendor preset: disabled)
  Active: active (running) since Sun 2021-06-20 14:17:21 WITA; 5 days ago
  Docs: man:dovecot(1)
        http://wiki2.dovecot.org/
  Main PID: 1283 (dovecot)
  CGroup: /system.slice/dovecot.service
          └─ 1283 /usr/sbin/dovecot
             └─ 1297 dovecot/anvil
                └─ 1298 dovecot/log
                   └─ 1305 dovecot/config
                      └─ 19748 dovecot/auth
                         └─ 20032 dovecot/auth -w
                            └─ 26337 dovecot/auth -w
                               └─ 26356 dovecot/auth -w
                                  └─ 26357 dovecot/auth -w
                                     └─ 26358 dovecot/auth -w

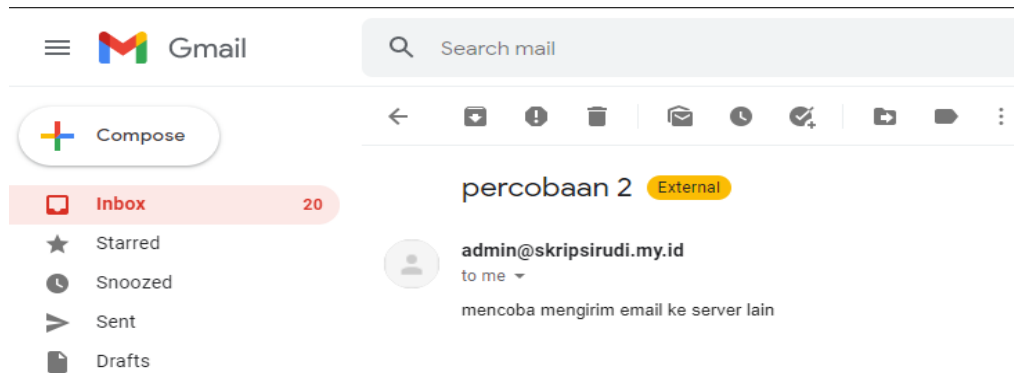
[root@srv1 ~]# service postfix status
Redirecting to /bin/systemctl status postfix.service
• postfix.service - Postfix Mail Transport Agent
  Loaded: loaded (/usr/lib/systemd/system/postfix.service; enabled; vendor preset: disabled)
  Active: active (running) since Sun 2021-06-20 14:17:20 WITA; 5 days ago
  Main PID: 1185 (master)
  CGroup: /system.slice/postfix.service
          └─ 1185 /usr/libexec/postfix/master -w
             └─ 1191 qmgr -l -t fifo -u
                └─ 2242 tlsmgr -l -t unix -u
                   └─ 2243 anvil -l -t unix -u
                      └─ 20391 pickup -l -t fifo -u -o content_filter= -o receive_override_options=no_header...
                         └─ 22710 smtpd -n smtp -t inet -u -o stress= -s 2 -o content_filter=smtp-amavis:127.0.0...
                            └─ 23893 smtpd -n smtp -t inet -u -o stress= -s 2 -o content_filter=smtp-amavis:127.0.0...
                               └─ 24891 smtpd -n smtp -t inet -u -o stress= -s 2 -o content_filter=smtp-amavis:127.0.0...
                                  └─ 25371 smtpd -n smtp -t inet -u -o stress= -s 2 -o content_filter=smtp-amavis:127.0.0...
```

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` seperti pada gambar 4.21 berikut.

```
Received: from 10.197.39.136
  by atlas108.free.mail.bf1.yahoo.com with HTTPS; Sat, 26 Jun 2021 08:27:34 +0000
Return-Path: <admin@skripsirudi.my.id>
X-Originating-Ip: [103.41.207.240]
Received-SPF: pass (domain of skripsirudi.my.id designates 103.41.207.240 as permitted sender)
Authentication-Results: atlas108.free.mail.bf1.yahoo.com;
  dkim=pass header.i=@skripsirudi.my.id header.s=default;
  dkim=pass header.i=@skripsirudi.my.id header.s=default;
  spf=pass smtp.mailfrom=skripsirudi.my.id;
  dmarc=pass (p=QUARANTINE) header.from=skripsirudi.my.id;
X-Apparently-To: rudi.masterqq3@yahoo.com; Sat, 26 Jun 2021 08:27:35 +0000
```

**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.

```
[root@srv1 ~]# systemctl status clamd.service
● clamd.service - clamd scanner () daemon
   Loaded: loaded (/usr/lib/systemd/system/clamd.service; enabled; vendor preset: disabled)
   Active: active (running) since Sat 2021-06-26 19:03:16 WITA; 9s ago
     Docs: man:clamd(8)
           man:clamd.conf(5)
           https://www.clamav.net/documents/
  Main PID: 29511 (clamd)
    CGroup: /system.slice/clamd.service
            └─29511 /usr/sbin/clamd -c /etc/clamd.d/amavisd.conf --foreground=yes
```

**Gambar 4.22 Verifikasi Fungsi *ClamAV***

#### 4.2.4 Verifikasi Konfigurasi *Client*

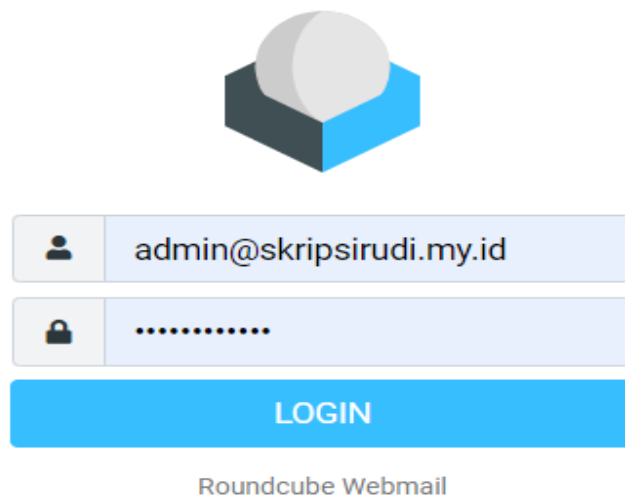
(Hanif 2018) Verifikasi konfigurasi *client* dilakukan agar memastikan domain yang di buat telah connect secara online dengan server dengan cara melakukan ping pada *mail server dengan perintah >ping skripsirudi.my.id* seperti pada gambar 4.23 berikut.

```
Pinging skripsirudi.my.id [103.41.207.240] with 32 bytes of data:
Reply from 103.41.207.240: bytes=32 time=54ms TTL=52
Reply from 103.41.207.240: bytes=32 time=72ms TTL=52
Reply from 103.41.207.240: bytes=32 time=57ms TTL=52
Reply from 103.41.207.240: bytes=32 time=68ms TTL=52

Ping statistics for 103.41.207.240:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 54ms, Maximum = 72ms, Average = 62ms
```

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*



### 4.3 Skenario Uji Coba

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

#### 4.3.1 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*.

#### 4.3.2 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*

#### 4.3.3 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 *Bankspooft* yang bergerak di bidang perbankan untuk masyarakat. *Bankspooft* mempunyai pesaing dalam menjalankan bisnis perbankannya, dimana pesaing tersebut berusaha menjatuhkan *Bankspooft* dengan cara melakukan penipuan dengan mengirim email *spoofing* dengan *fake mailer*, sebelum melakukan penipuan terlebih dahulu mencari tahu email perusahaan *Bankspooft*, setelah mengetahui email dari perusahaan *Bankspooft* maka pesaing tersebut memulai aksinya mengirim email *spoofing* yang mengatasnamakan direktur *Bankspooft*, pesaing tersebut menunjukan email ke staf keuangan *Bankspooft*, email *spoofing* tersebut berisikan perintah mengirim laporan keuangan *Bank spooft* dalam jangka waktu lima tahun terakhir. Setelah semua informasi yang di perlukan telah di dapat, dimana nama direktornya admin dan nama pegawainya root maka pesaing tersebut memulai email *spoofing* dengan cara membuka situs [www.emkei.cz](http://www.emkei.cz) kepada pegawai staf keuangan root dengan alamat email

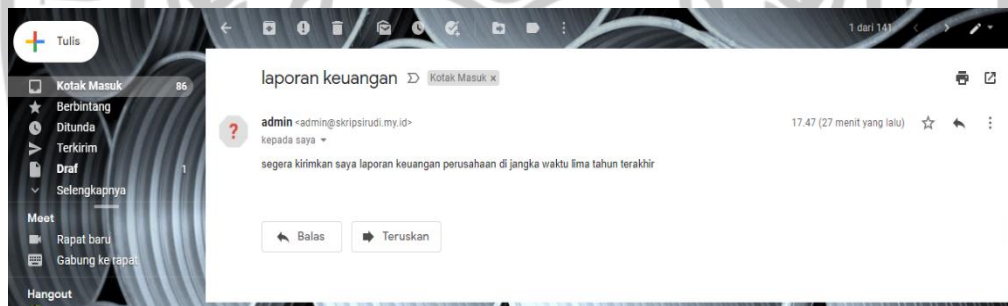
rudi.masterqq3@gmail.com dengan mengatasnamakan direktur Bankspooft yang bernama admin dengan alamat email admin@skripsirudi.my.id, isi email tersebut memerintahkan staf keuangan Bankspooft untuk mengirimkan laporan keuangan Bankspooft lima tahun terakhir, seperti pada gambar 4.25 berikut.



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 Bankspooft, pada *text box From E-mail* diisi dengan alamat *email* direktur Bankspooft, pada *text box To* diisi dengan alamat *email* staf keuangan Bankspooft, pada *text box Subject* diisi dengan subjek *email*, dan *text box Text* diisi dengan pesan dari *email spoofing*, jika pada *email* Bankspooft 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 Bankspooft akan membaca *email spoofing* tersebut.

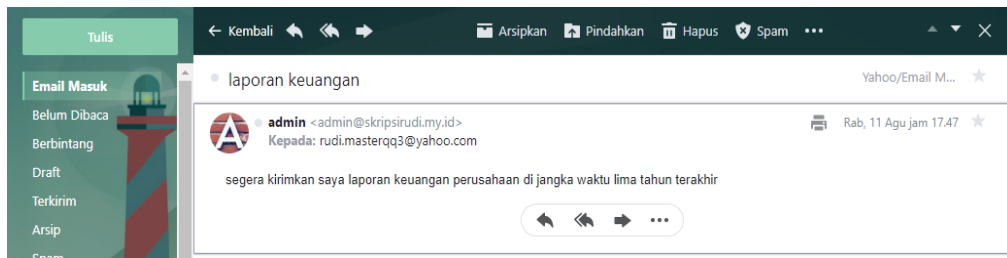
#### 4.3.4 Uji Coba Mengirim *Email Spoofing* ke *Yahoo! Mail*

Dengan menggunakan skenario yang sama seperti pada uji coba mengirim *email spoofing* ke *Gmail*, namun 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.

The screenshot displays the 'FakeMail's Mailer' web interface. At the top, it says 'Free online fake mailer with attachments, encryption, HTML editor and advanced settings...'. A green checkmark icon and the text 'E-mail sent successfully' are visible. Below this, the email details are shown in a form: 'From Name: admin', 'From E-mail: admin@skripsirudi.my.id', 'To: rudi.masterqq3@yahoo.com', and 'Subject: laporan keuangan'. The 'Attachment' section shows 'Choose File' and 'No file chosen'. There are links for 'Attach another file' and 'Advanced Settings'. The 'Content-Type' section has radio buttons for 'text/plain' (selected), 'text/html', and a checkbox for 'Editor'. The 'Text' field contains the message: 'segera kirimkan saya laporan keuangan perusahaan di jangka waktu lima tahun terakhir'.

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

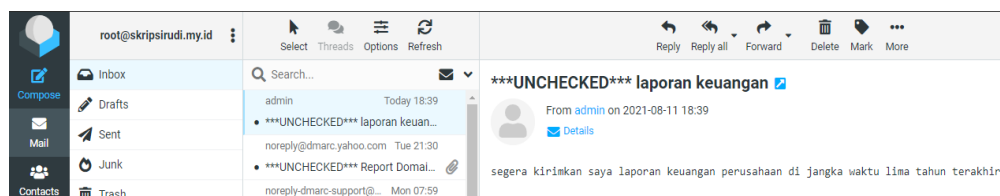
#### 4.3.5 Uji Coba Mengirim Email Spoofing pada skripsirudi.my.id

Dengan menggunakan skenario yang sama seperti pada uji coba mengirim *email spoofing* ke layanan *email Gmail*, namun pada uji coba ini akan di uji pengiriman *email spoofing* pada *mail server skripsirudi.my.id* dengan mengatasmakan 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 terlihat seperti pada gambar 4.30 berikut.



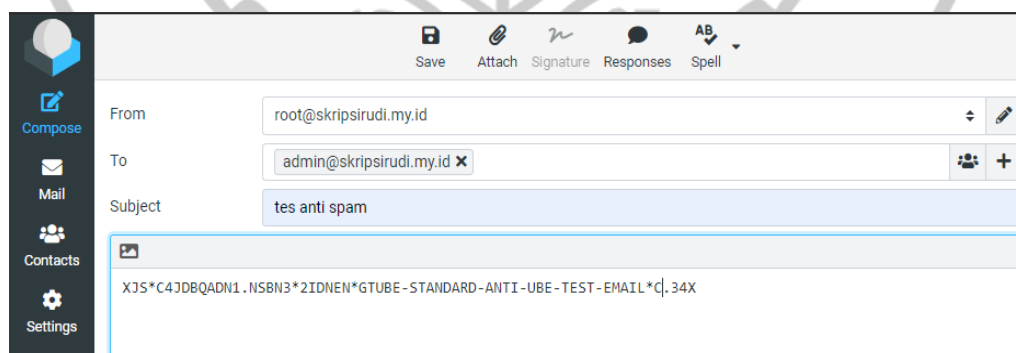
**Gambar 4. 30 Email Spoofing Terkirim ke User skripsirudi.my.id**

#### 4.3.6 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.

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

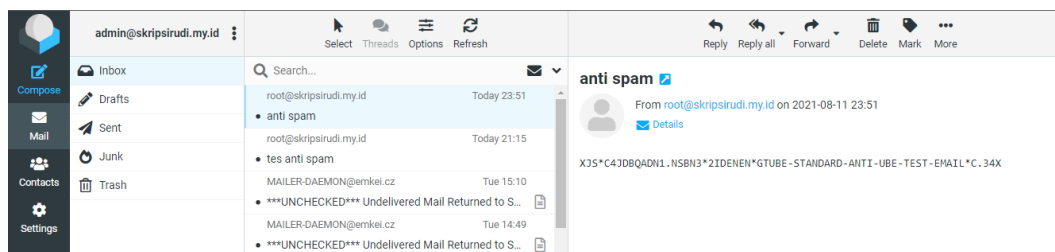
Uji coba kedua adalah dengan mengirim *email spam* menggunakan layanan *email* skripsian.online ke layanan *email* skripsian.online, isi pesan yang digunakan adalah XJS\*C4JDBQADN1.NSBN3\*2IDNEN\*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL\*C.34X yang merupakan standar GTUBE untuk menguji kinerja *anti spam*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



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



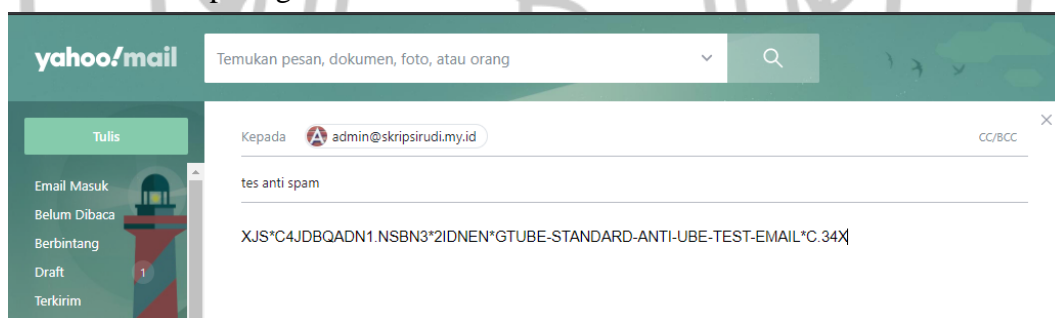
*Email spam* tersebut diatas berhasil terkirim ke alamat *email* admin@skripsirudi.my.id karena belum ada penerapan *anti spam* pada *mail server* skripsirudi.my.id terlihat seperti pada gambar 4.32 berikut.



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

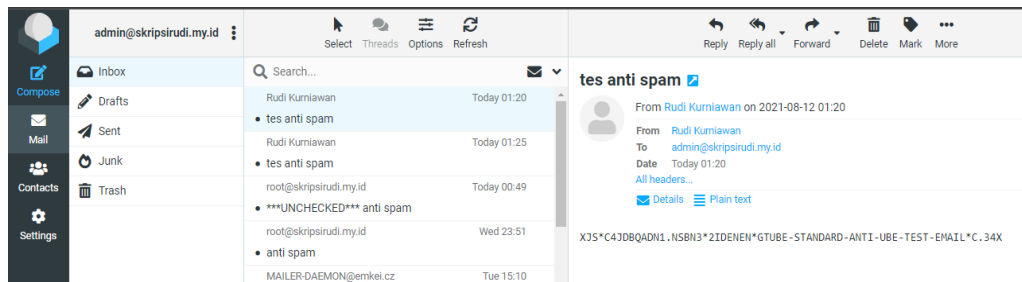
#### 4.3.8 Mengirim *Email Spam* dari *Yahoo! Mail*

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 *email* skripsian.online dari layanan *email* *Yahoo! Mail* terlihat seperti gambar 4.33 berikut.



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

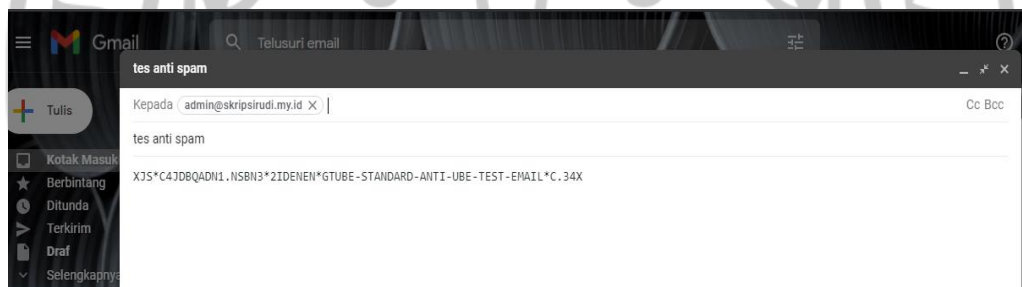
*Email spam* tersebut diatas berhasil terkirim ke alamat *email* admin@skripsirudi.my.id karena belum ada penerapan *anti spam* pada *mail server* skripsirudi.my.id terlihat seperti pada gambar 4.34 berikut.



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

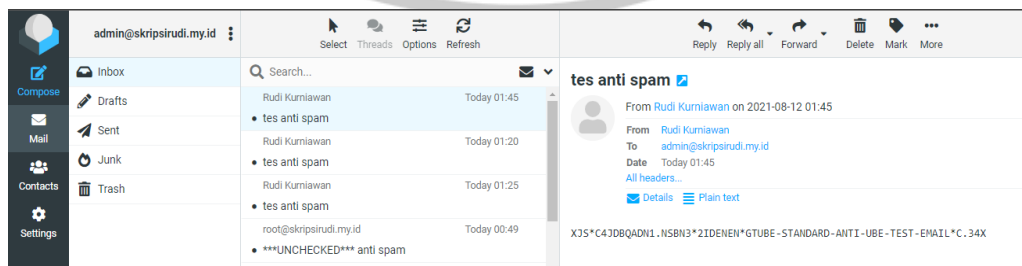
#### 4.3.9 Uji Coba Mengirim Email Spam dari Gmail

Dengan menggunakan skenario yang sama seperti pada uji coba mengirim *email spam* dari layanan *email* skripsirudi.my.id ke layanan *email* skripsirudi.my.id, namun pada uji coba ini akan di uji pengiriman *email spam* ke layanan *email* 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.



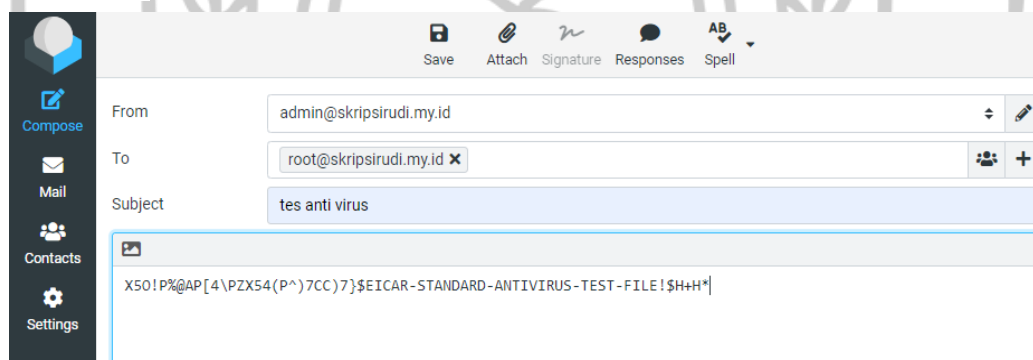
**Gambar 4. 36 Email Spam dari Gmail Terkirim**

#### 4.3.10 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.

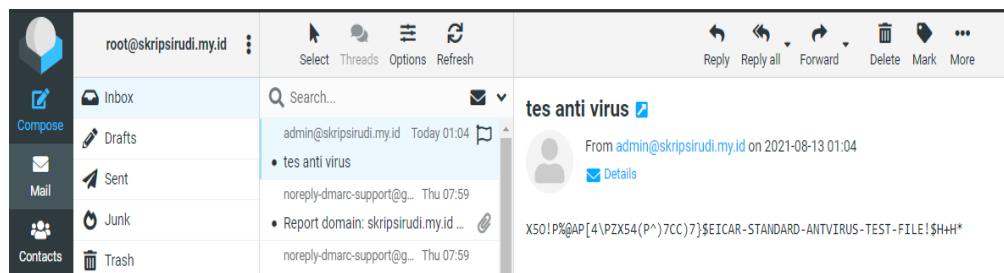
#### 4.3.11 Uji Coba Mengirim *Email* yang Mengandung *Virus* dari skripsirudi.my.id

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**

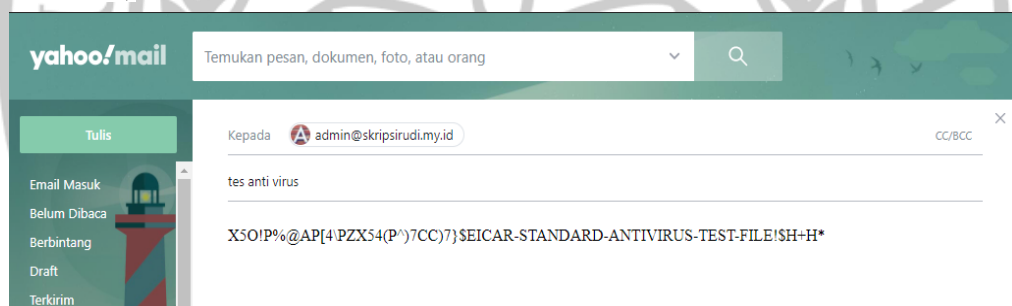
Setelah *email* tersebut dikirim pada salah satu *user email* yang ada pada *mail server* skripsirudi.my.id maka *email* yang mengandung *virus* tersebut berhasil terkirim ke *user* yang berada pada *mail server* skripsirudi.my.id seperti terlihat pada gambar 4.38 berikut



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

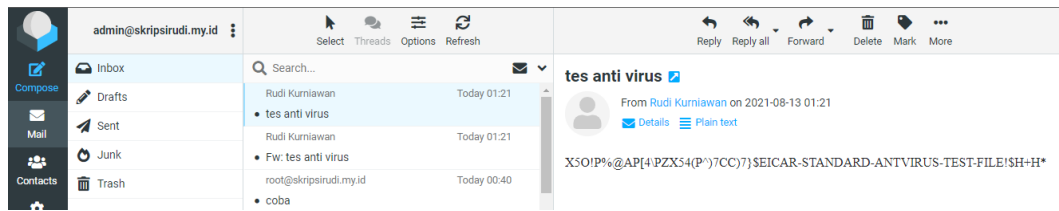
#### 4.3.12 Uji Coba Mengirim *Email* yang Mengandung *Virus* dari *Yahoo! Mail*

Uji coba pengiriman *email* yang mengandung *virus* dilakukan dengan mengirim *email* dengan isi X5O!P%@AP[4PZX54(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**

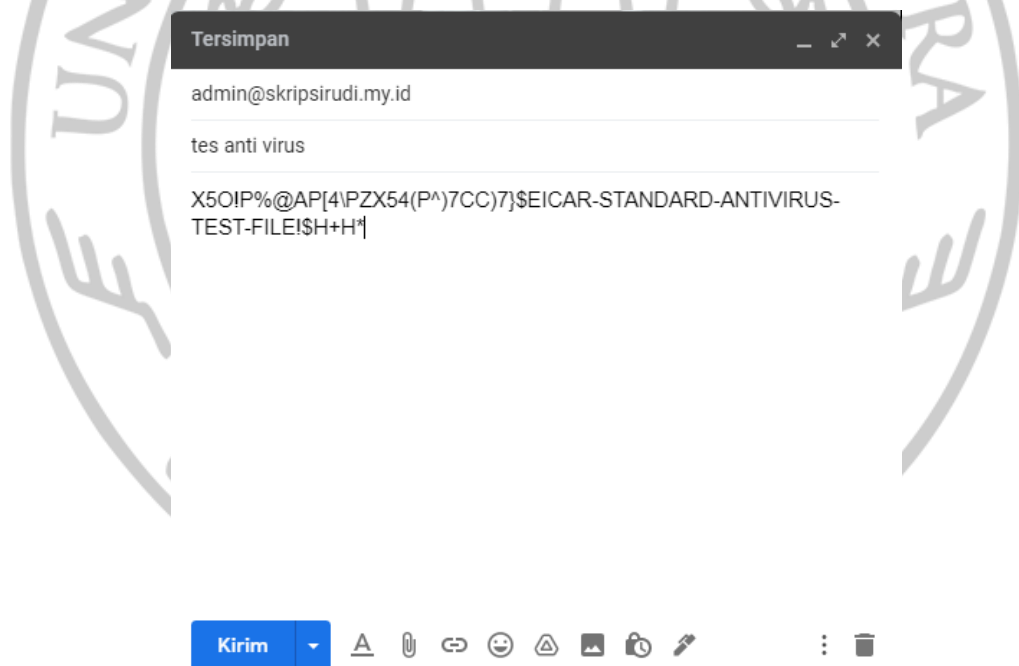
Setelah *email* tersebut dikirim pada salah satu *user email* yang ada pada *mail server skripsian.online*, maka *email* yang mengandung *virus* tersebut berhasil terkirim ke *user email* yang berada pada *mail server skripsian.online* seperti terlihat pada gambar 4.40 berikut.



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

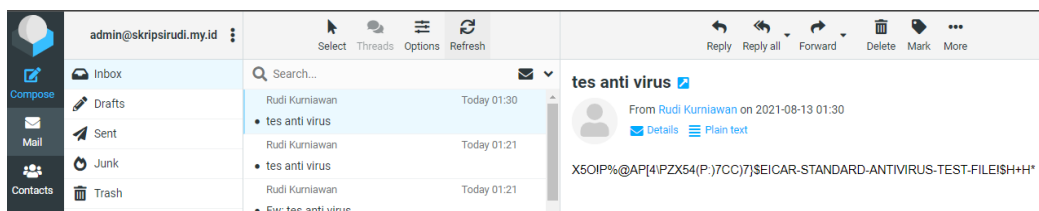
#### 4.3.13 Uji Coba Mengirim Email yang Mengandung Virus dari Gmail

Uji coba pengiriman *email* yang mengandung *virus* dilakukan dengan mengirim *email* dengan isi X5O!P% @AP[4PZX54(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**

#### 4.3.14 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*.

#### 4.3.15 *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.



```
ARC-Authentication-Results: i=1; mx.google.com;
dkim=tempererror (no key for signature) header.i=@skripsirudi.my.id header.s=default header.b=X5TPJCmt;
dkim=tempererror (no key for signature) header.i=@skripsirudi.my.id header.s=default header.b=iqCe0fXw;
spf=neutral (google.com: 103.41.207.240 is neither permitted nor denied by best guess record for domain of
admin@skripsirudi.my.id) smtp.mailfrom=admin@skripsirudi.my.id
Return-Path: <admin@skripsirudi.my.id>
Received: from srv1.skripsirudi.my.id ([103.41.207.240])
by mx.google.com with ESMTPS id l17si293887pjz.83.2021.08.12.10.40.21
for <rudi.masterqq3@gmail.com>
(version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128);
Thu, 12 Aug 2021 10:40:21 -0700 (PDT)
Received-SPF: neutral (google.com: 103.41.207.240 is neither permitted nor denied by best guess record for domain of
admin@skripsirudi.my.id) client-ip=103.41.207.240;
Authentication-Results: mx.google.com;
dkim=tempererror (no key for signature) header.i=@skripsirudi.my.id header.s=default header.b=X5TPJCmt;
dkim=tempererror (no key for signature) header.i=@skripsirudi.my.id header.s=default header.b=iqCe0fXw;
spf=neutral (google.com: 103.41.207.240 is neither permitted nor denied by best guess record for domain of
admin@skripsirudi.my.id) smtp.mailfrom=admin@skripsirudi.my.id
```

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

Pada gambar 4.43 terlihat pada cuplikan *header email* hanya terdapat parameter *DKIM =tempererror* 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*.

#### 4.3.16 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.

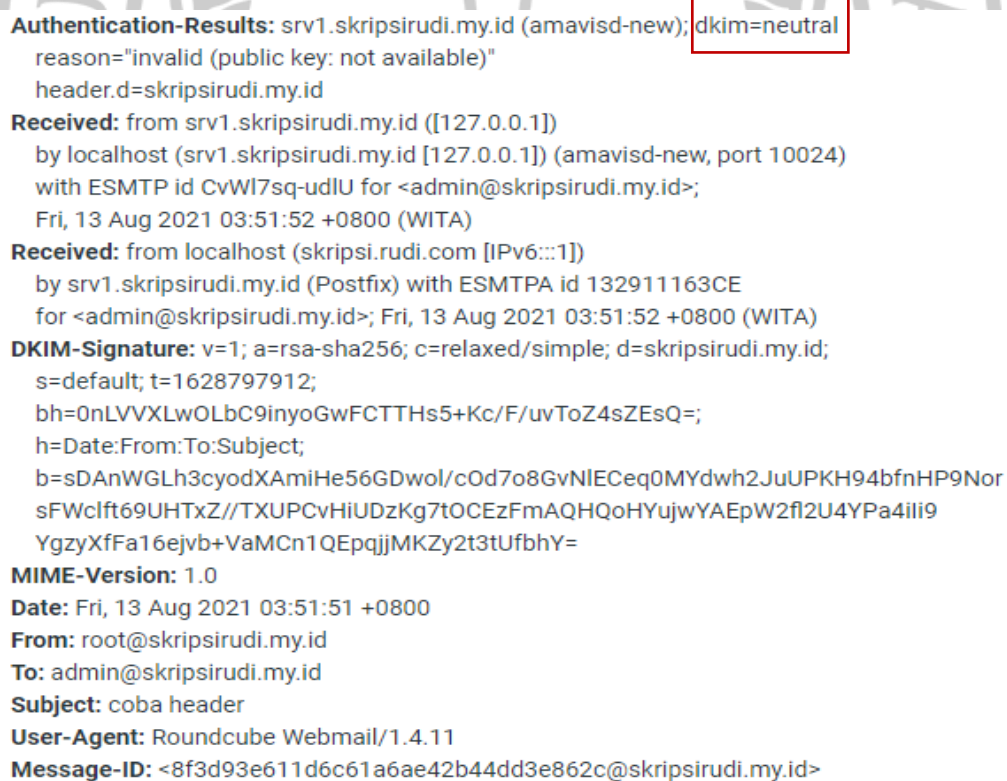
```
Received: from 10.222.142.149
by atlas301.free.mail.ne1.yahoo.com with HTTPS; Thu, 12 Aug 2021 18:17:56 +0000
Return-Path: <root@skripsirudi.my.id>
X-Originating-IP: [103.41.207.240]
Received-SPF: none (domain of skripsirudi.my.id does not designate permitted sender hosts)
Authentication-Results: atlas301.free.mail.ne1.yahoo.com;
dkim=perm_fail header.i=@skripsirudi.my.id header.s=default;
dkim=perm_fail header.i=@skripsirudi.my.id header.s=default;
spf=none smtp.mailfrom=skripsirudi.my.id;
dmarc=unknown header.from=skripsirudi.my.id;
X-Apparently-To: rudi.masterqq3@yahoo.com; Thu, 12 Aug 2021 18:17:56 +0000
X-YMailISG: FX_DJPKWLDt.jRXPrZ4qA1_5vuZthhvze7JL0gNoiylFdXU0
```

**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*.

#### 4.3.17 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.



**Authentication-Results:** srv1.skripsirudi.my.id (amavisd-new); dkim=neutral  
 reason="invalid (public key: not available)"  
 header.d=skripsirudi.my.id

**Received:** from srv1.skripsirudi.my.id ([127.0.0.1])  
 by localhost (srv1.skripsirudi.my.id [127.0.0.1]) (amavisd-new, port 10024)  
 with ESMTP id CvWI7sq-udIU for <admin@skripsirudi.my.id>;  
 Fri, 13 Aug 2021 03:51:52 +0800 (WITA)

**Received:** from localhost (skripsi.rudi.com [IPv6:::1])  
 by srv1.skripsirudi.my.id (Postfix) with ESMTPA id 132911163CE  
 for <admin@skripsirudi.my.id>; Fri, 13 Aug 2021 03:51:52 +0800 (WITA)

**DKIM-Signature:** v=1; a=rsa-sha256; c=relaxed/simple; d=skripsirudi.my.id;  
 s=default; t=1628797912;  
 bh=0nLVVXLwOLbC9inyoGwFCTTHs5+Kc/F/uvToZ4sZEsQ=;  
 h=Date:From:To:Subject;  
 b=sDAnWGLh3cyodXAmiHe56GDwol/cOd7o8GvNIECeq0MYdwh2JuUPKH94bfnHP9Nor  
 sFWclft69UHTxZ//TXUPCvHiUDzKg7tOCEzFmAQHqoHYujwYAEpW2fl2U4YPa4iii9  
 YgzyXfFa16ejvb+VaMCn1QEppjjMKZy2t3tUfbhY=

**MIME-Version:** 1.0  
**Date:** Fri, 13 Aug 2021 03:51:51 +0800  
**From:** root@skripsirudi.my.id  
**To:** admin@skripsirudi.my.id  
**Subject:** coba header  
**User-Agent:** Roundcube Webmail/1.4.11  
**Message-ID:** <8f3d93e611d6c61a6ae42b44dd3e862c@skripsirudi.my.id>

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*..

#### 4.3.18 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).

#### 4.3.19 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 mengatasmakan salah satu *user email* yang ada pada *skripsirudi.my.id* (Hanif 2018).

#### 4.3.20 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](http://www.emkei.cz) menggunakan *browser* kemudian pada situs [www.emkei.cz](http://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.

```
GNU nano 2.3.1 File: ...sirudi.my.id/default.private
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQC7b7KUq0Ya9Jz0iDa3NF+WJquppUdry0MjttVjkAQ8eoUloMU4
Y8RFst271mdjJcQzW51P+p0iFIJ2MKMz0MtLkz2xAkr98epATFKfb9G1K00lv45W
MJOHfQpHk/O76iBiKogTLcxZ7RMENpIt9TV50yf1JZ1xZidVEhHXgR9YGwIDAQAB
AoGAYdXLwQ4laayEwJ7Y8Iff3PoSYFqFDR7rzJiCiZWCoI7TMPDaALUSnc7fLkyb
aoUsBCKt2jFWE5PhBRAeH828TrEA1ss0Zsf6RrUVUfCpP5kxbxuf3Q/28hHk3gNfN
tQRZakV58ysYbWBUHqd5Jy0dZ27wK+DQteZGSfgs2xtRDQECQDtbEQRDd7YIQxD
eUpH69K6GrNBQ2VuRHX6yh0UYNZN7KH/3agdoNkQz11i1iD5uSwcMa89VX3uXzS
mSfMWBztAkEAyhoq/wtqUsX67J7ZD/xzWjRxJfCRh6Ik4fQVzuhtAqw5hSFSP9x
h2iRqw5jKmNDYcK3Bcd0/HeKq03qURCwJwJBALs9qAyfGMDwh0BrVmaUF90HnRj6
MvMccMMBRJ++oyQ/W5VNXVu903AGC2E5LOyRWoe/2SxKe6rrkQJxoM5qKx0CQA5d
QcUS2KG9dJIw0Bi0xrYYmBos0Qu82H5lNsc0c8/KGryfpMGFDlo7cm8H/MBcgcoH
BV8hxVloXbDDPu44E20CQCYonTlyDZ094kWfYITHl2nt8uP8aT9iack4+RlvWDAJ
^G Get Hel^O WriteOu^R Read Fi^Y Prev Pa^K Cut Tex^C Cur Pos
^X Exit ^J Justify^W Where I^V Next Pa^U UnCut T^T To Spell
```

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

3. 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.

```
default._domainkey 14400 IN TXT "v=DKIM1; k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC7b7KUq0Ya9Jz0iDa3NF+WJquppUdry0MjttVjkAQ8eoUloMU4Y8RFst2
71mdjJcQzW51P+p0iFIJ2MKMz0MtLkz2xAkr98epATFKfb9G1K00lv45WMJOHfQpHk/O76iBiKogTLcxZ7RMENpIt9TV50yf1JZ1xZi
dVEhHXgR9YGwIDAQAB"
```

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

## Pesan Asli

ID Pesan	<ebefe14c54b7ee1cd1e1f839d4d286aa@skripsirudi.my.id>
Dibuat pada:	27 Juni 2021 14.58 (Dikirim setelah 69 detik)
Dari:	admin@skripsirudi.my.id
Kepada:	rudi.masterqq3@gmail.com
Subjek:	percobaan ke 3
SPF:	PASS dengan IP 103.41.207.240 <a href="#">Pelajari lebih lanjut</a>
DKIM:	'PASS' dengan domain skripsirudi.my.id <a href="#">Pelajari lebih lanjut</a>
DMARC:	'PASS' <a href="#">Pelajari lebih lanjut</a>

Gambar 4.48 Cuplikan *Header Email*

4. 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* dikarenakan *record* pada *DMARC* untuk mengkarantina email sehingga email tersebut di masukan ke folder spam (proses *SPF* dan *DMARC*) terlihat seperti gambar 4.49 dan 4.50 berikut.

```
skripsirudi.my.id. IN TXT "v=spf1 mx a ip4:103.41.207.240/32 a:sv1.skripsirudi.my.id -all"
```

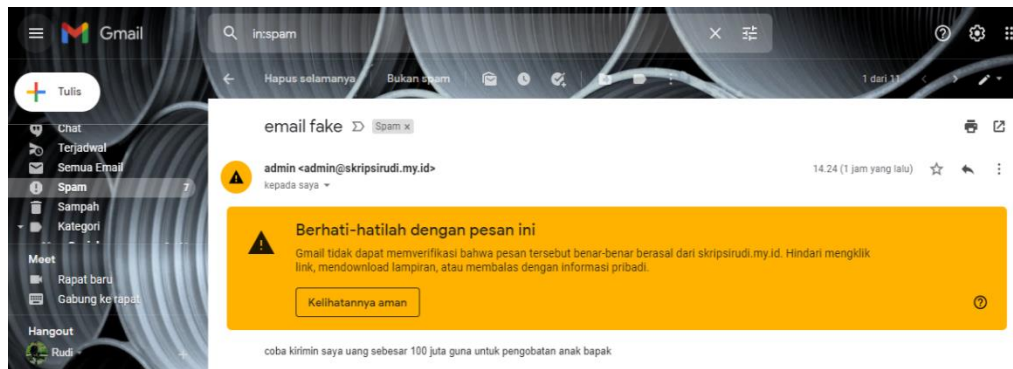
Gambar 4.49 *SPF Record* pada skripsirudi.my.id

```
_dmarc 14400 IN TXT "v=DMARC1; p=quarantine; pct=100; rua=mailto:root@skripsirudi.my.id"
```

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



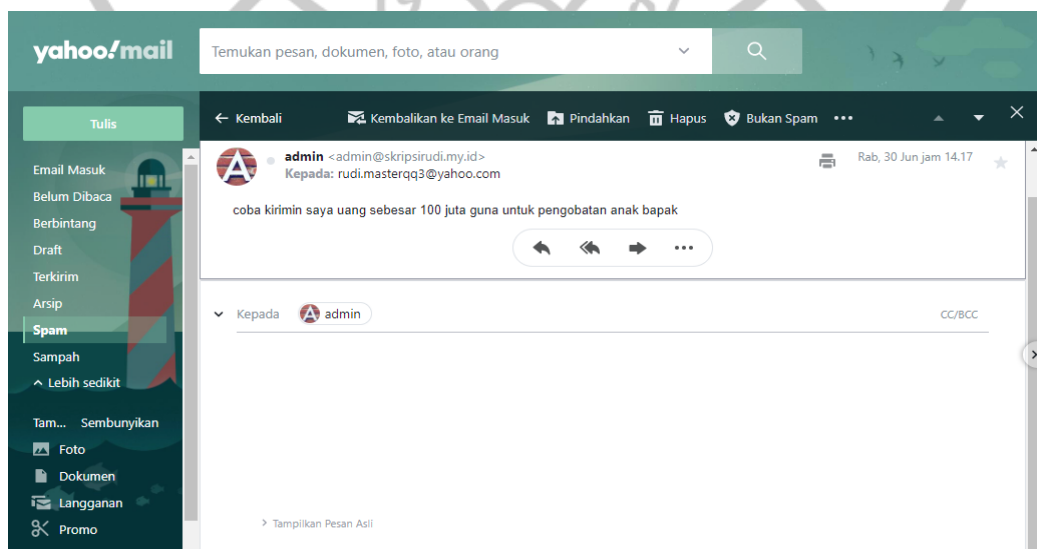
5. Hasil verifikasi pengiriman email fake dari emkei.cz ke mail dengan mengatas nama kan salah satu user email yaitu admin@skripsirudi.my.id yang kemudian terindikasi sebagai spam oleh gmail terlihat seperti gambar 4.51 berikut.



Gambar 4. 51 terindikasi spam oleh gmail

#### 4.3.21 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* dimasukkan kedalam *folder spam* penerima *email* seperti gambar 4.52 berikut. (Hanif 2018)

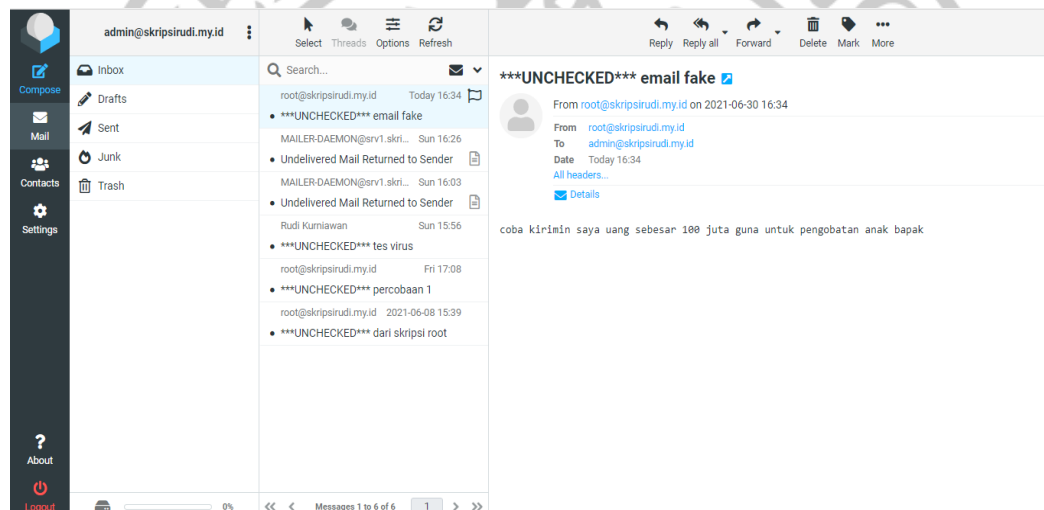


Gambar 4. 52 *Email Spoofing* Masuk ke *Folder Spam*



#### 4.3.22 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*

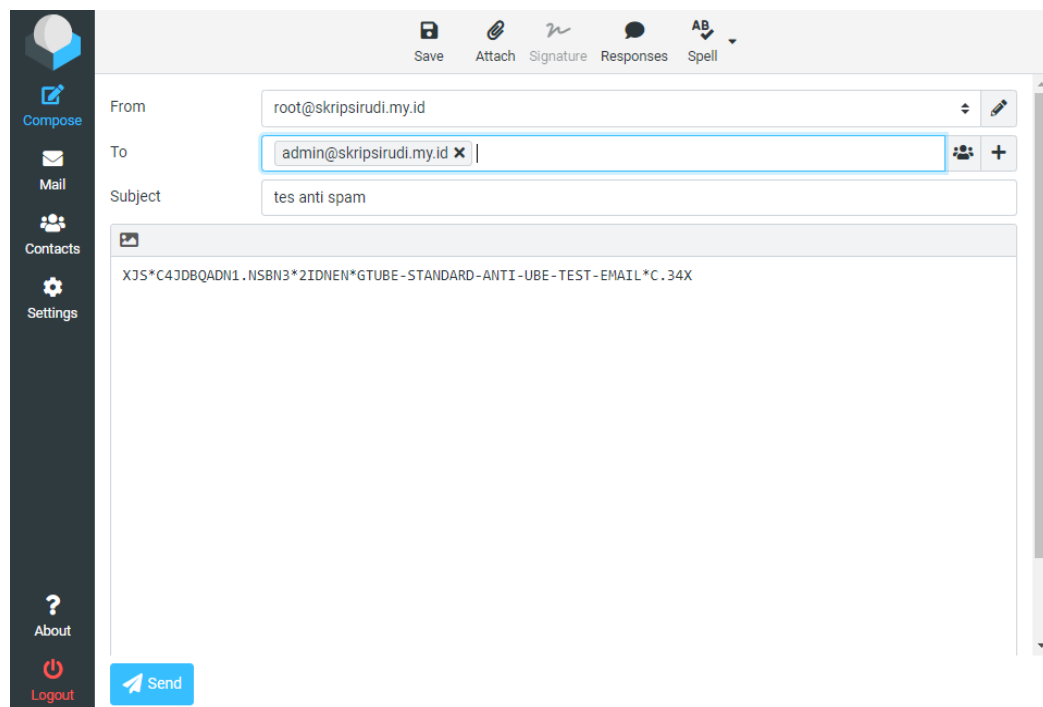
#### 4.3.23 Uji Coba Mengirim *Email Spam*

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.

#### 4.3.24 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 pemfilteran *email spam* dapat dilihat pada *mail log* dengan menggunakan perintah `#cat /var/log/maillog` seperti terlihat pada gambar 4.55 berikut. (Hanif 2018).

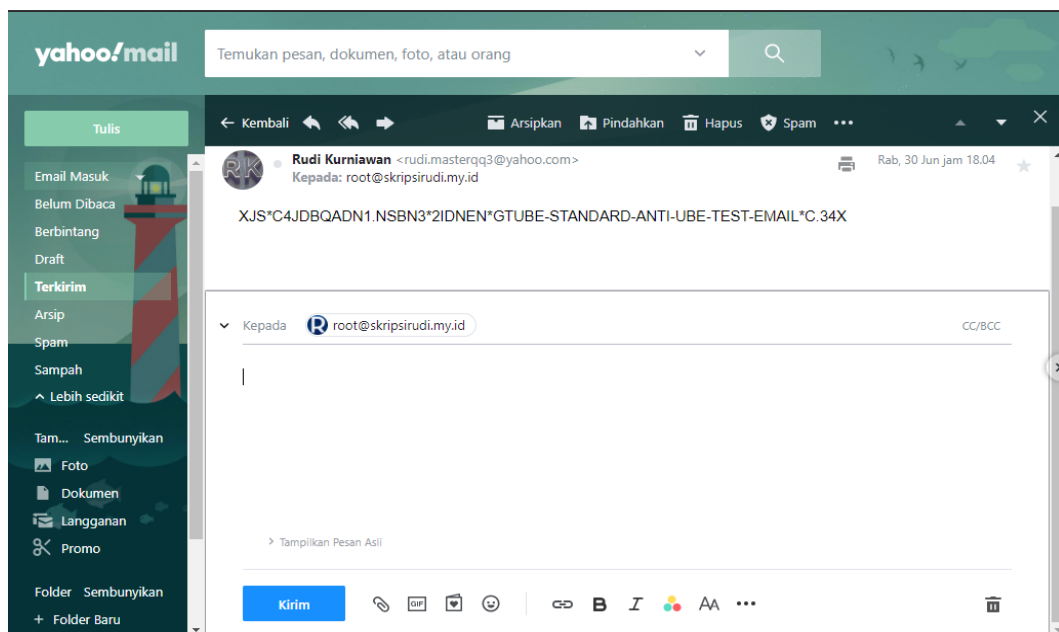
```
Jun 30 17:12:12 srv1 amavis[11541]: (11541-05) Blocked SPAM {DiscardedInternal,Quarantined}, MYNETS LOCAL [::1]:38244 <root@skripsirudi.my.id>
Jun 30 17:12:12 srv1 postfix/smtp[17750]: 2DA85C0779: to=<admin@skripsirudi.my.id>, relay=127.0.0.1[127.0.0.1]:10024, delay=10, delays=0.15, dsn=4.0.0, status=sent (250 OK)
Jun 30 17:12:12 srv1 postfix/qmgr[1191]: 2DA85C0779: removed
```

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

#### 4.3.25 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 pemfilteran email spam dapat dilihat pada mail log dengan menggunakan perintah `#cat /var/log/maillog` seperti terlihat pada gambar 4.57 berikut.

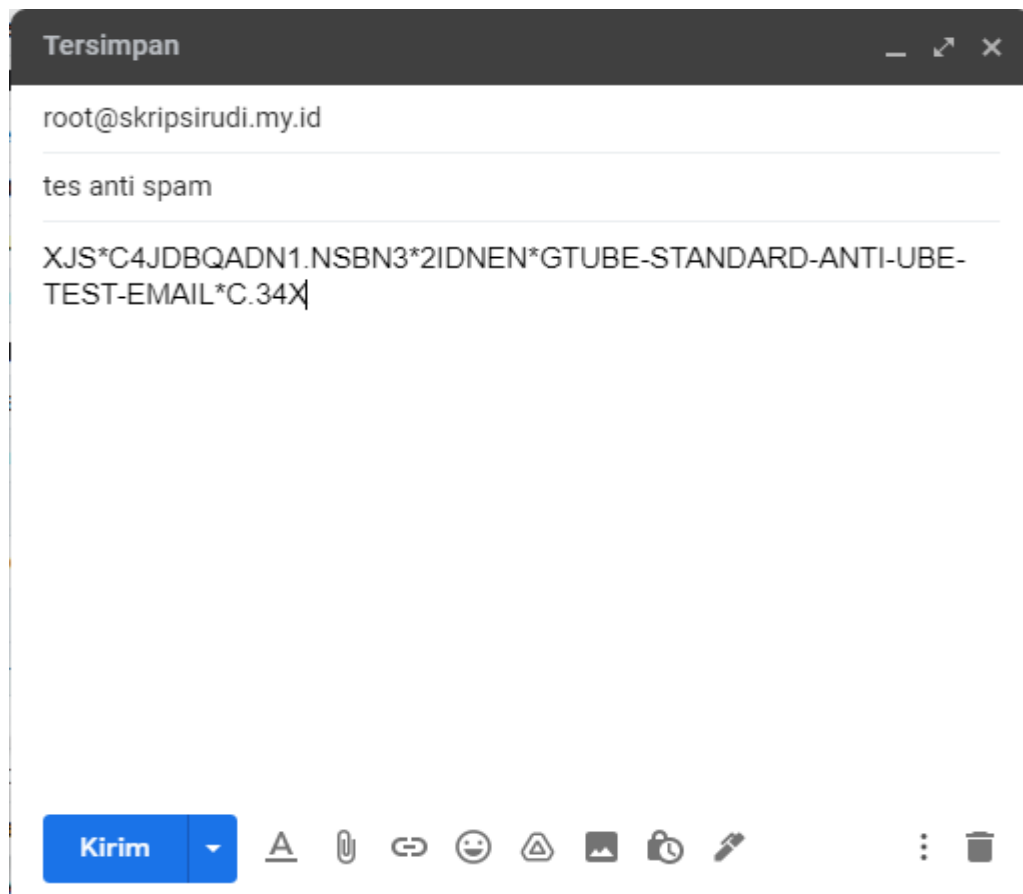
```
Jun 30 18:04:31 srv1 amavis[11610]: (11610-06) Blocked SPAM {DiscardedInbound,Quarantined}, [106.10.241.209]:43256 [106.10.241.209] <rudi.masterqq3$
Jun 30 18:04:31 srv1 postfix/smtp[24517]: 2EBFD1027E4: to=<root@skripsirudi.my.id>, relay=127.0.0.1[127.0.0.1]:10024, delay=20, delays=0.22/0.02/0.0$
Jun 30 18:04:31 srv1 postfix/qmgr[1191]: 2EBFD1027E4: removed
```

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

#### 4.3.26 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* Setelah Penerapan

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

```
Dun 30 18:29:39 srv1 amavis[11541]: (11541-07) Blocked SPAM (DiscardedInbound,Quarantined), [209.85.166.43]:38693 [209.85.166.43] <rudi.masterqq3@gmail.com>
Dun 30 18:29:39 srv1 postfix/smtp[24931]: A66E21027E4: to=<root@skripsirudi.my.id>, relay=127.0.0.1[127.0.0.1]:10024, delay=41, delays=5.2/0.02/0.02/0.02, dsn=2.0.0, status=sent (250 OK)
Dun 30 18:29:39 srv1 postfix/qmgr[1191]: A66E21027E4: removed
```

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

#### 4.3.27 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.



**Free online fake mailer with attachments, encryption, HTML editor and advanced settings...**

✔ E-mail sent successfully

**From Name:** admin

**From E-mail:** admin@skripsirudi.my.id

**To:** rudi.masterqq3@yahoo.com

**Subject:** email fake

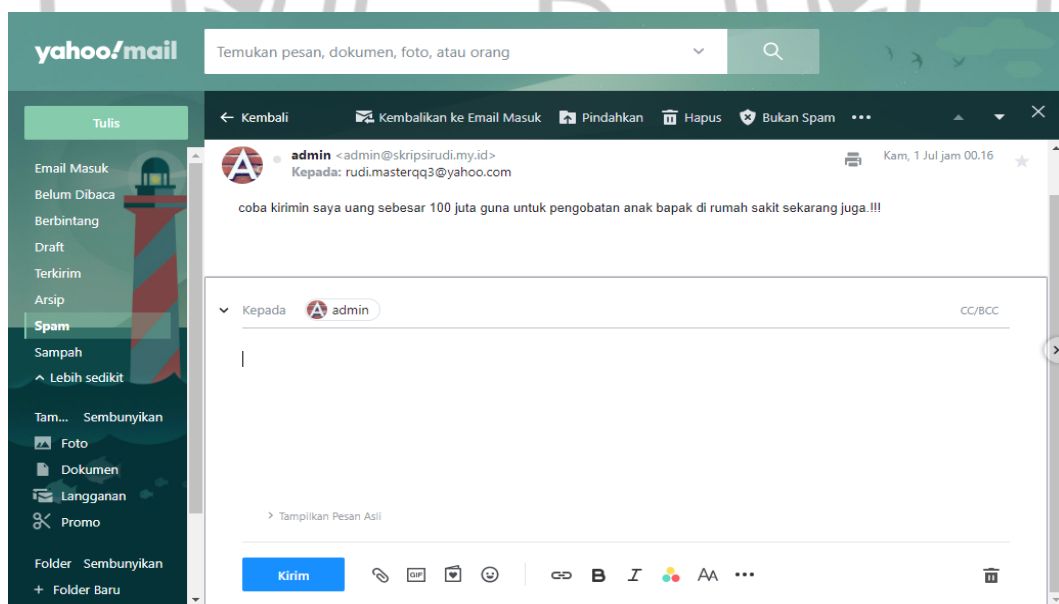
**Attachment:** Choose File No file chosen  
Attach another file  
Advanced Settings

**Content-Type:** ☒ text/plain ☐ text/html ☐ Editor

**Text:** coba kirimin saya uang sebesar 100 juta guna untuk pengobatan anak bapak di rumah sakit sekarang juga.!!!

**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.



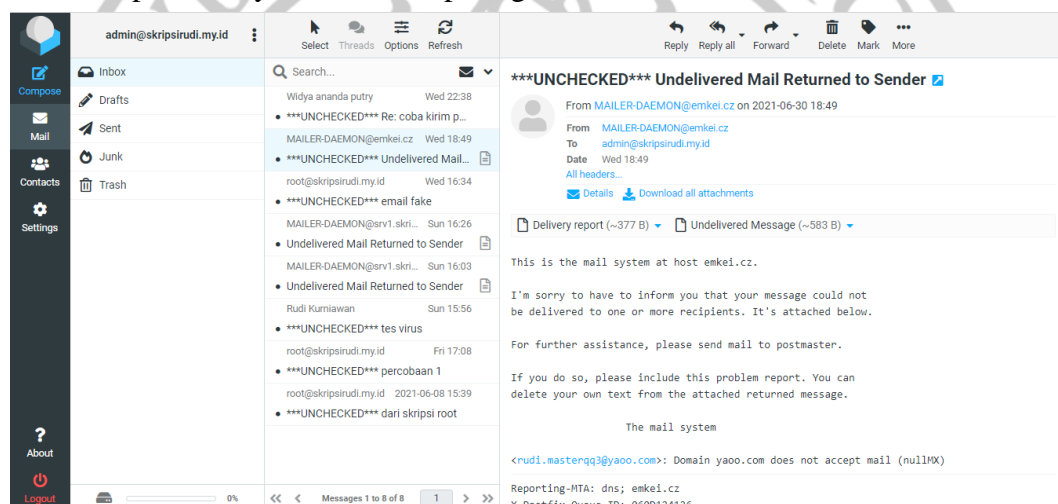
**Gambar 4. 61 Email Terindikasi Sebagai Spam oleh Yahoo! Mail**

*Yahoo! Mail* mengindikasikan 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.

```
Authentication-Results: atlas308.free.mail.gq1.yahoo.com;
dkim=unknown;
spf=fail smtp.mailfrom=skripsirudi.my.id;
dmarc=fail(p=QUARANTINE) header.from=skripsirudi.my.id;
```

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 email emkei.cz telah di verifikasi bahwa pesan tersebut mengandung spoofing kemudian pesan tersebut di kirim kembali ke email skripsirudi.my.id, terlihat seperti gambar 4.63 berikut.



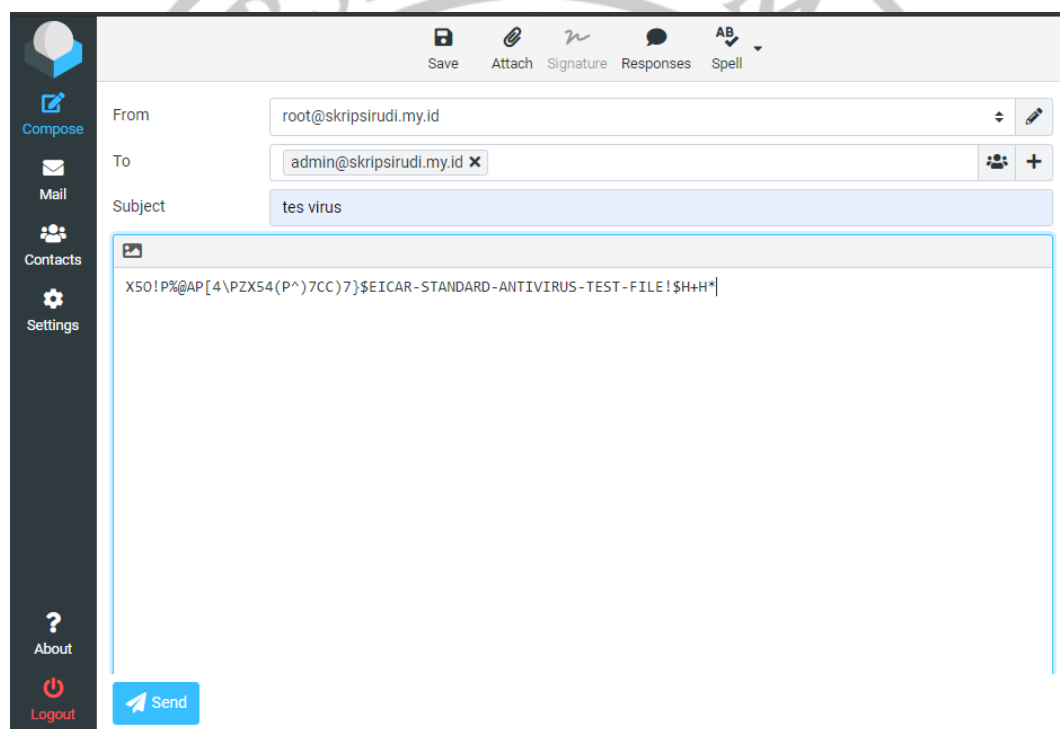
Gambar 4. 63 hasil report *DMARC* setelah protocol di terapkan

#### 4.3.28 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.

#### 4.3.29 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

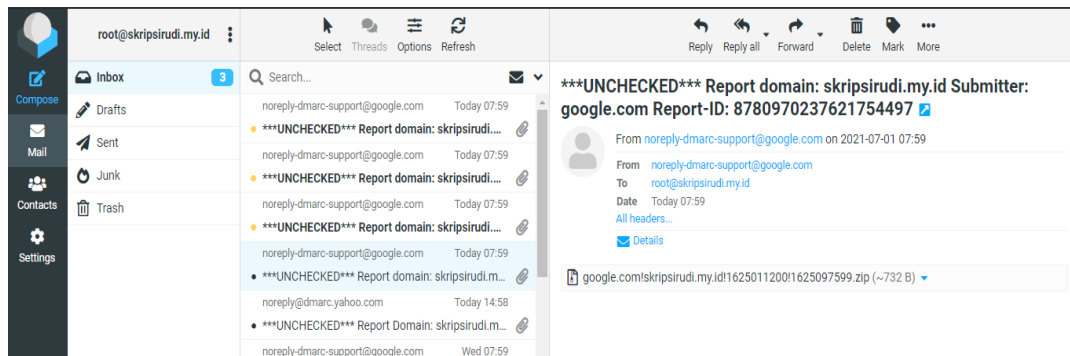
Setelah *email* yang mengandung *virus* tersebut dikirim ke salah satu *user email* yang ada pada *mail server* skripsirudi.my.id maka *email* tersebut akan di blok oleh *Amavis-New* dan di deteksi sebagai virus oleh *ClamAV*, namun terdapat report *DMARC* yang memberitahukan bawah email tersebut mengandung virus



sehingga pesan yang masuk tidak dapat di baca, hanya report pesan, seperti terlihat pada gambar 4.65 dan gambar 4.66 berikut.

```
Aug 8 00:24:53 skripsirudi amavis[1716]: (01716-03) Blocked INFECTED (Eicar-Signature) {DiscardedInternal,Quarantined}, MYN
ETS LOCAL [::1]:43546 <root@skripsirudi.my.id> -> <admin@skripsirudi.my.id>, Queue-ID: 9075E115479, Message-ID: <91a096728f2
a37527487761424d57e88@skripsirudi.my.id>, mail_id: LzMm6dOyGUJ4, Hits: -, size: 998, dkim_sd=default:skripsirudi.my.id, 177
ms
Aug 8 00:24:53 skripsirudi postfix/smtp[22700]: 9075E115479: to=<admin@skripsirudi.my.id>, relay=127.0.0.1[127.0.0.1]:10024
, delay=0.35, delays=0.11/0.05/0.02/0.17, dsn=2.7.0, status=sent (250 2.7.0 Ok, discarded, id=01716-03 - INFECTED: Eicar-Sig
nature)
```

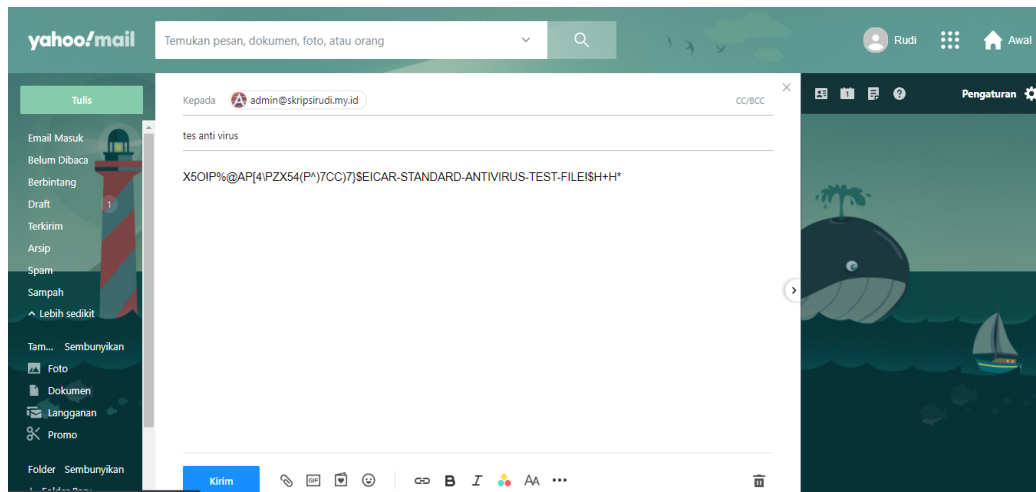
**Gambar 4. 65 email local dari skripsirudi.my.id terblok**



**Gambar 4. 66 report email yang mengandung virus**

#### 4.3.30 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[4PZX54(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)

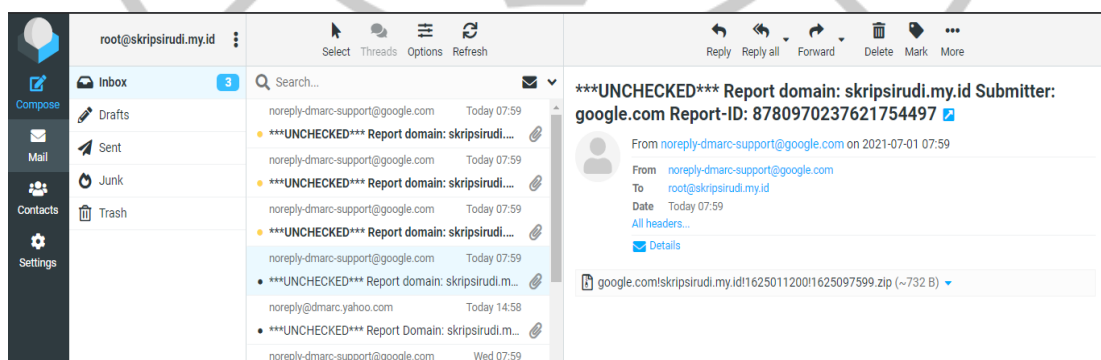


Gambar 4. 67 EICAR Test dari Yahoo! Mail Setelah Penerapan

Setelah *email* yang mengandung *virus* tersebut dikirim ke salah satu *user email* yang ada pada *mail server* skripsirudi.my.id maka *email* tersebut akan di blok oleh *Amavis-New* dan di deteksi 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

```
Aug 8 00:46:46 skripsirudi amavis[1715]: (01715-03) Blocked INFECTED (Eicar-Signature) (DiscardedInbound,Quarantined), [106.10.241.210]:35065 [106.10.241.210] <rudi.masterqq3@yahoo.com> -> <admin@skripsirudi.my.id>, Queue-ID: E5B5E115479, Message-ID: <941185908.172342.1628354801611@mail.yahoo.com>, mail_id: xlcaUXEglvs, Hits: -, size: 5616, dkim_sd=s2048:yahoo.com, 158 ms
Aug 8 00:46:46 skripsirudi postfix/smtp[23325]: E5B5E115479: to=<admin@skripsirudi.my.id>, relay=127.0.0.1[127.0.0.1]:10024, delay=0.43, delays=0.23/0.02/0.02/0.15, dsn=2.7.0, status=sent (250 2.7.0 Ok, discarded, id=01715-03 - INFECTED: Eicar-Signature)
```

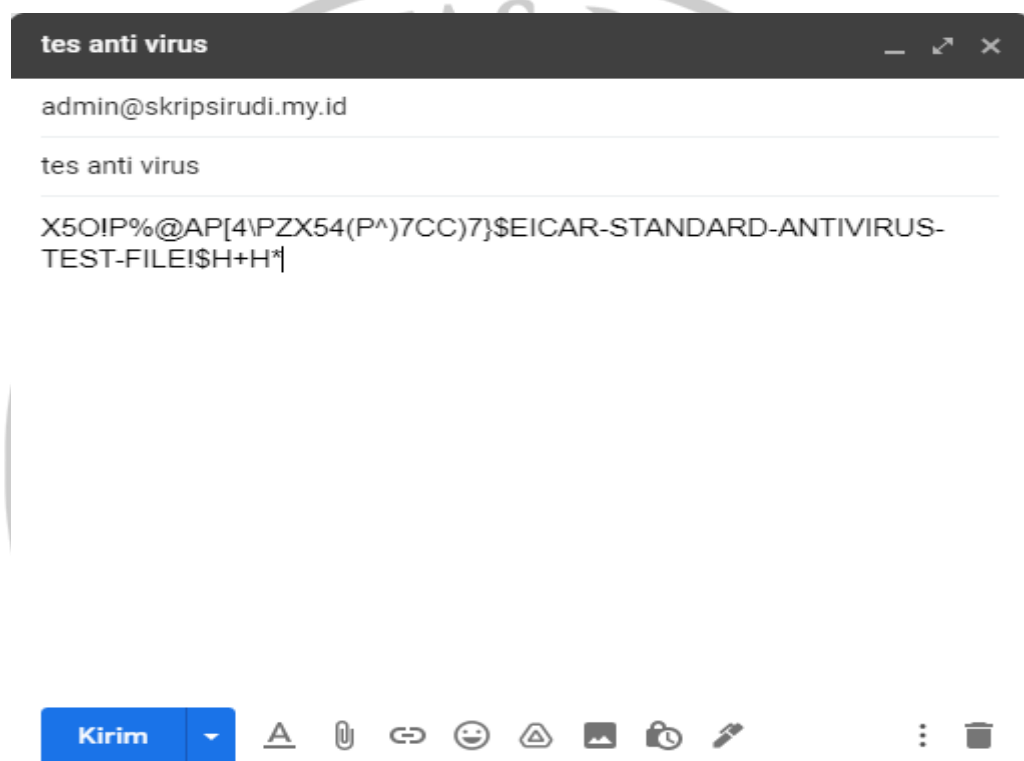
Gambar 4. 68 email dari rudi.masterqq3@yahoo.com ke skripsirudi.my.id terblok



Gambar 4. 69 report email yang mengandung virus

#### 4.3.31 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)



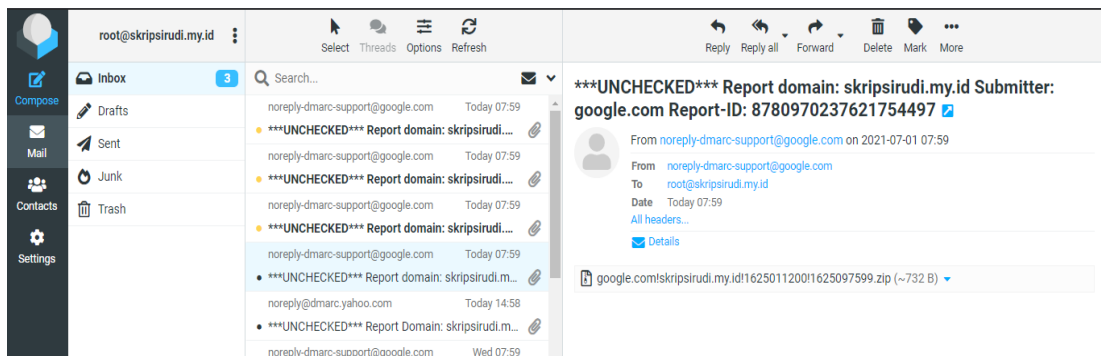
Gambar 4. 70 *EICAR Test* dari *Gmail* Setelah Penerapan

Setelah *email* yang mengandung *virus* tersebut dikirim ke salah satu *user email* yang ada pada *mail server* skripsirudi.my.id maka *email* tersebut akan di blok oleh *Amavis-New* dan di deteksi 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.

```
Aug 8 01:00:23 skripsirudi amavis[1716]: (01716-04) Blocked INFECTED (Eicar-Signature) {DiscardedInbound,Quarantined}, [209.85.166.54]:40878 [209.85.166.54] <rudi.masterqq3@gmail.com> -> <admin@skripsirudi.my.id>, Queue-ID: 07F44115479, Message-ID: <CAM2Yke6mK8=TftU2b+SSHm438Z7wPUKEZBddqgr9mDechZS-Q@mail.gmail.com>, mail_id: mnApAM9Jv96f, Hits: -, size: 3244, dkim_sd=20161025:gmail.com, 145 ms
Aug 8 01:00:23 skripsirudi postfix/smtp[23809]: 07F44115479: to=<admin@skripsirudi.my.id>, relay=127.0.0.1[127.0.0.1]:10024, delay=0.41, delays=0.22/0.04/0.02/0.13, dsn=2.7.0, status=sent (250 2.7.0 Ok, discarded, id=01716-04 - INFECTED: Eicar-Signature)
```

Gambar 4. 71 email di blok oleh antivirus client



Gambar 4. 72 report email yang mengandung virus

#### 4.3.32 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*.

#### 4.3.33 *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.

```

Authentication-Results: mx.google.com;
  dkim=pass header.i=@skripsirudi.my.id header.s=default header.b=rflDGSip;
  dkim=pass header.i=@skripsirudi.my.id header.s=default header.b="m0n/Ofef";
  spf=pass (google.com: domain of admin@skripsirudi.my.id designates 103.41.207.240 as permitted sender)
  smtp.mailfrom=admin@skripsirudi.my.id;
  dmarc=pass (p=QUARANTINE sp=QUARANTINE dis=NONE) header.from=skripsirudi.my.id
Received: from localhost (unknown [127.0.0.1]) by srv1.skripsirudi.my.id (Postfix) with ESMTP id E93DEC0779 for
<rudi.masterqq3@gmail.com>; Sun, 27 Jun 2021 06:59:38 +0000 (UTC)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=skripsirudi.my.id; s=default; t=1624777178;
bh=0nLVVXLwOLbc9inyoGwFCTTHs5+Kc/F/uvToZ4sZEsQ=; h=Date:From:To:Subject;
b=rflDGSipTJdm5ClzZUco0tLAjzV8K1BzboLSegHnF6n/GCbninyC8e/t8mb0Nk8tP
  TCCwJACpDDJMjnjja5RpNkzBjmTKmhawC9JeBZH8pozme6hIFQITtOzGLEP0qaQyHa
  YUddrYOzVqSQZoRiab9LDBxpluNj/rJWJKKCtLi0=
X-Virus-Scanned: amavisd-new at skripsirudi.my.id

```

**Gambar 4.73 Cuplikan Header Email pada Gmail Setelah Penerapan**

Pada gambar 4.73 terlihat perbedaan *header email* setelah penerapan protokol *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*.

#### **4.3.34 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 protokol *DMARC*, *DKIM*, *SPF*, *anti spam*, dan *anti virus*, *header email* terlihat seperti gambar 4.74 berikut.

```

Received-SPF: pass (domain of skripsirudi.my.id designates 103.41.207.240 as permitted sender)
Authentication-Results: atlas310.free.mail.bf1.yahoo.com;
dkim=pass header.i=@skripsirudi.my.id header.s=default;
dkim=pass header.i=@skripsirudi.my.id header.s=default;
spf=pass smtp.mailfrom=skripsirudi.my.id;
dmarc=pass(p=QUARANTINE) header.from=skripsirudi.my.id;
X-Apparently-To: rudi.masterqq3@yahoo.com; Sat, 26 Jun 2021 09:45:19 +0000
X-YMailISG: zTAGvAIWLDtQvpcCynw08J_uWVwlujrMtA5sCth7RlgCRCMq
_Kt8VBfhw5q16ccKam1NVkcXz7m1HV7INz0Fes_WR2bXYtf9SXXmxfCUYYV_
_c09JnBMZVLmPfoZcu6XBC5710ilitEQvQbRGU8xH1E0uWjvZoHfPjB1diSI
WXB58mdoZ7KxZgBLTOaff8aKrud2v5kxV3KmNKNu0LZig4Jc9IkSmsNc0F4
7hIQWtZ1R47QtC4qXeJm66FW7KSjvX.zFmTYIcnlrdRKohrL_iSrqljRPok
.HhinABSg9a_eLeiaTBW0XGJ2IZTI2oScb6FhhXx6Nk9E8xLD2yEdGjPGZN
vVAu1ltN8RL4ct1Ch2wWEuDQm3Hkma7xBO30aXw8IPwZ_f_p4k6Mk3ysWKjh
oSryh6cIW3_b_cXlFwZDL3KxNEP_m8vCIBGw0JA5k3Edz5Cvfnng.p3DuTa1
XBSoQ33VEAB.LV_nzzTe.fCcFCwbQIuqWMCBET1oenkXMTc3iEJncjBMqRg
pcSz2.O3Ixo2p0qpgtQYDMpErYwlpANDYKdEROAwT9906cpYf2nD._giGnyr
zVlWwv6cdqsd_bsI3gvLmhwZ14chJK95nCHfC_3wk51fEpVH8hLnadI1x7t
oQ8rRLpCCs72qqfXqmD.yTcrGFbPTF_ArvIPBQd98zuhG2v6dXMS2Zgd6hn
oydFEb79pHj2Nvj5kcGBPkeZ1Jv7JL1EWeTT2cONnIZZU0td060QFC1V4L9w
Woy2ami1yJXdqV7M4KmOo12GXg1eOexaeJNGUmus4zbhijnjJ43Z1gPQpEHg
1qjuRqcEV.h2UMtr9KN8eDGBYbCY7tE7TtWLuPRjDVnIigu1vCTBdrdzZc9n
irbekyqtp76vTA1kgsbkAiZHGCUlq9bhlCdNL_90d00ZDZGY3RidBusmdI
q_Gz.7nW.M0g5a6idxxCCSkP.WuS3718mJ3XFLTd8tuXsxWHPzXayYHovMb
qHPE7WwQajvuF0p8YHFV20SZMIL8ssVug7u1af.EF7sAaP_zU0crCYHyxamB
OFLU309TM8CnHrePBvtX6mId33Zraw--
Received: from 103.41.207.240 (EHLO srv1.skripsirudi.my.id)
by 10.197.39.201 with SMTPs
(version=TLS1_2 cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256);
Sat, 26 Jun 2021 09:45:18 +0000
Received: from localhost (unknown [127.0.0.1])
by srv1.skripsirudi.my.id (Postfix) with ESMTP id 5BD87C0778
for <rudi.masterqq3@yahoo.com>; Sat, 26 Jun 2021 09:45:16 +0000 (UTC)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=skripsirudi.my.id;
s=default; t=1624700716;
bh=Sa2S8055UojRvdFrdHMTAzoFie5wi3d9sl+uxltMZvQ=;
h=Date:From:To:Subject;
b=XbIK1ScKWjajATc9UQTUSGZQT0709rhSKa312DxweRjLuq9zN949hap/TSRHynfY2
ATc0aUGbU6Wh+b0YJ3Kk0EtoFY0VPYS87aUTNGR0xCd2YkJOULF0EYk8oDheW3ZgZ
LW9C2/xNvhSeaac96YzZmMZPOTrLqpt0e8mUQsg0=
X-Virus-Scanned: amavisd-new at skripsirudi.my.id

```

**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).

#### 4.3.35 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.

```

X-Virus-Scanned: amavisd-new at skripsirudi.my.id
Authentication-Results: srv1.skripsirudi.my.id (amavisd-new);
dkim=pass (1024-bit key) header.d=skripsirudi.my.id
Received: from srv1.skripsirudi.my.id ([127.0.0.1])
by localhost (srv1.skripsirudi.my.id [127.0.0.1]) (amavisd-new, port 10024)
with ESMTP id rPXl1Plqn7Nz for <admin@skripsirudi.my.id>;
Fri, 16 Jul 2021 21:50:31 +0800 (WITA)
Received: from localhost (skripsi.rudi.com [IPv6:::1])
by srv1.skripsirudi.my.id (Postfix) with ESMTPA id 25EDF115453
for <admin@skripsirudi.my.id>; Fri, 16 Jul 2021 21:50:31 +0800 (WITA)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=skripsirudi.my.id;
s=default; t=1626443431;
bh=bvGp0CSqPLZq0x7LiUJwPnzORqkx3whkwyFpYKfdkyw=;
h=Date:From:To:Subject;
b=eMupgNm5fsPe4FNYEMgBR54Ai/+H9tdMkQ2WJwxXB14PzhlRrVmZtm8QvVVINdwrZ
+Mo9KXFmFbdR1SczMqjUP9uhWT1oxHUHje03KUT5Z1RLcTV4cwXQmsHaYacZygJ9+v
B424nQij+yGRbJeWD8newiARBSSyjfF4n4n5kh9g=

```

**Gambar 4. 75 Cuplikan Header Email skripsirudi.my.id Setelah Penerapan**

Pada gambar 4.76 terlihat perbedaan *header email* setelah penerapan protokol *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.

#### 4.4 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 protokol *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 protokol *DMARC, DKIM, SPF, anti spam, dan anti virus* (Hanif 2018).



#### 4.4.1 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 diterapkan 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***

N O	<i>Fake Mailer</i>	Layanan <i>Email</i> yang di atasnamakan	Layanan <i>Email</i> Penerima	Sebelum Penerapan	Setelah Penerapan
1	<i>Emkei's Fake Mailer</i>	Skripsirudi.my.id	<i>Gmail</i>	Masuk <i>Folder Inbox</i>	Diblokir Dan di report oleh <i>DMARC</i>
2	<i>Emkei's Fake Mailer</i>	Skripsirudi.my.id	<i>Yahoo! Mail</i>	Masuk <i>Folder Inbox</i>	Masuk <i>Folder Spam</i>
3	<i>Emkei's Fake Mailer</i>	Skripsirudi.my.id	Skripsirudi.my.id	Masuk <i>Folder Inbox</i>	Masuk <i>Folder Inbox</i>

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 protokol *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).

#### 4.4.2 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	<i>Yahoo! Mail</i>	<i>Skripsirudi.my.id</i>	Masuk Folder Inbox	Diblokir
2	<i>Gmail</i>	<i>Skripsirudi.my.id</i>	Masuk Folder Inbox	Diblokir
3	<i>Skripsirudi.my.id</i>	<i>Skripsirudi.my.id</i>	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).

#### 4.4.3 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***

N O	Layanan <i>Email</i> Pengirim	Layanan <i>Email</i> Penerima	Sebelum Penerapan	Setelah Penerapan
1	<i>Yahoo! Mail</i>	Skripsirudi.my.id	Masuk <i>Folder Inbox</i>	Diblokir dan di report oleh dmarc
2	<i>Gmail</i>	Skripsirudi.my.id	Masuk <i>Folder Inbox</i>	Diblokir dan di report oleh dmarc
3	Skripsirudi.my.id	Skripsirudi.my.id	Masuk <i>Folder Inbox</i>	Diblokir dan 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).

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

Analisa pengecekan *header email* dilakukan dengan melihat *header email* sebelum dan setelah penerapan protokol *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	<i>DKIM =temperror</i>	-	-	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 parameter tersebut.

Berdasarkan tabel 4.4, sebelum penerapan protocol *DMARC*, *DKIM*, *SPF*, *anti spam*, dan *anti virus* terdapat parameter *DKIM-Signature* yang bernilai *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](mailto:skripsirudi.my.id). (Hanif 2018).

