

**ANALISA PENERAPAN DOMAINKEYS IDENTIFIED MAIL
(DKIM), SENDER POLICY FRAMEWORK (SPF), ANTI SPAM,
DAN ANTI VIRUS PADA MAIL SERVER**

SKRIPSI



Oleh :

**NAUFAL HANIF
1410530129**

**PROGRAM STUDI TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) BUMIGORA
MATARAM
2018**

**ANALISA PENERAPAN DOMAINKEYS IDENTIFIED MAIL
(DKIM), SENDER POLICY FRAMEWORK (SPF), ANTI SPAM,
DAN ANTI VIRUS PADA MAIL SERVER**

SKRIPSI



Diajukan Sebagai Salah Satu Syarat untuk Memenuhi Kebulatan Studi
Jenjang Strata Satu (S1) Program Studi Teknik Informatika
Pada Sekolah Tinggi Manajemen Informatika dan Komputer
(STMIK) Bumigora Mataram

Oleh :

**NAUFAL HANIF
1410530129**

**PROGRAM STUDI TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) BUMIGORA
MATARAM
2018**

**ANALISA PENERAPAN DOMAINKEYS IDENTIFIED MAIL
(DKIM), SENDER POLICY FRAMEWORK (SPF), ANTI SPAM,
DAN ANTI VIRUS PADA MAIL SERVER**

SKRIPSI

Diajukan Sebagai Salah Satu Syarat untuk Memenuhi Kebulatan Studi
Jenjang Strata Satu (S1) Program Studi Teknik Informatika
Pada Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK)
Bumigora Mataram

Oleh :

**NAUFAL HANIF
1410530129**



SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) BUMIGORA MATARAM
PROGRAM STUDI TEKNIK INFORMATIKA

SKRIPSI

JUDUL : Analisa Penerapan *Domainkeys Identified Mail (DKIM)*, *Sender Policy Framework (SPF)*, *Anti Spam*, dan *Anti Virus* Pada *Mail Server*
NAMA : Naufal Hanif
NIM : 1410530129
NPM/NIRM : 14.8.349.74.75.0.5.0129
PROGRAM STUDI : Teknik Informatika
JENJANG : Strata Satu (S1)
DIUJIKAN : Jum'at, 27 Juli 2018

Menyetujui,

I Putu Hariyadi, M.Kom
Pembimbing I

Tanggal Menyetujui : 28/8 - 2018

Akbar Juliansyah, ST., M.MT
Pembimbing II

Tanggal Menyetujui : 26/8 2018

Telah diterima dan disetujui sebagai salah satu syarat untuk memperoleh
Gelar Akademik Sarjana Komputer (S.Kom)

Mengetahui,
Ni Gusti Ayu Dasriani, M.Kom
Ketua Program Studi S1 Teknik Informatika

Tanggal Mengetahui : 28 Agustus 2018

**ANALISA PENERAPAN DOMAINKEYS IDENTIFIED MAIL
(DKIM), SENDER POLICY FRAMEWORK (SPF), ANTI SPAM,
DAN ANTI VIRUS PADA MAIL SERVER**

LEMBAR PENGESAHAN PENGUJI

Diajukan Sebagai Salah Satu Syarat untuk Memenuhi Kebulatan Studi
Jenjang Strata Satu (S1) Program Studi Teknik Informatika
Pada sekolah Tinggi Manajemen Informatika dan Komputer
(STMIK) Bumigora Mataram

Oleh :

**NAUFAL HANIF
1410530129**

Disetujui oleh Penguji:

1. Raisul Azhar, M.T
NIK. 98.6.87

2. Lalu Zazuli Azhar, M.Kom
NIK. 16.6.255


18/2018


B.M.J.

KATA PENGANTAR

Puji syukur penulis panjatkan kepada Allah SWT yang telah memberikan rahmat-Nya sehingga penulis dapat menyelesaikan Skripsi yang berjudul “Analisa Penerapan *DomainKeys Identified Mail (DKIM)*, *Sender Policy Framework (SPF)*, *Anti Spam*, dan *Anti Virus* pada *Mail Server*”.

Terselesaikannya skripsi ini tidak terlepas dari bantuan berbagai pihak, dan dengan segala kerendahan hati penulis ingin menyampaikan ucapan terima kasih serta penghargaan setinggi-tingginya kepada:

1. Bapak Heroe Santoso, M.Kom, selaku ketua Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Bumigora Mataram.
2. Ibu Ni Gusti Ayu Dasriani, M.Kom, selaku ketua Program Studi S1 Teknik Informatika.
3. Bapak I Putu Hariyadi, M.Kom, selaku Pembimbing Utama dalam mengerjakan skripsi ini.
4. Bapak Akbar Juliansyah, ST., M.MT, selaku Pembimbing Kedua dalam mengerjakan skripsi ini.
5. Bapak/Ibu dosen yang telah memberikan ilmu selama dalam perkuliahan.
6. Tidak terlupakan Ibu dan Bapak tercinta serta Saudara dan Keluarga yang telah memberikan dukungan moril dan materi serta mendo'akan, memberikan semangat dan dorongan dalam penyelesaian skripsi ini.
7. Semua teman-teman dan sahabat yang selalu setia memberikan motivasi dan setia membantu selama penyusunan skripsi ini.

8. Serta semua pihak yang tidak dapat penulis sebutkan satu persatu yang turut membantu dan mendukung kelancaran penyusunan skripsi ini.

Semoga skripsi ini dapat memberikan manfaat yang sebesar-besarnya pada kita semua. Sebagai manusia biasa yang mempunyai keterbatasan dan kekurangan, maka penulis menyadari bahwa skripsi ini masih banyak kekurangan, baik dalam teknik penulisan, pembahasan, dan penyajian, untuk itu penulisa terbuka untuk menerima kritik dan saran yang membangun dari pembaca untuk kesempurnaan dari skripsi ini.

Mataram, Agustus 2018

Penulis,



SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) BUMIGORA MATARAM

LEMBAR PERNYATAAN KEASLIAN

Saya yang bertandatangan di bawah ini:

Nama : Naufal Hanif
NIM : 1410530129
Program studi : S1 Teknik Informatika
Kompetensi : Jaringan Komputer

Menyatakan bahwa skripsi yang berjudul:

**ANALISA PENERAPAN DOMAINKEYS IDENTIFIED MAIL (DKIM),
SENDER POLICY FRAMEWORK (SPF), ANTI SPAM, DAN ANTI VIRUS
PADA MAIL SERVER**

Benar-benar merupakan hasil karya pribadi dan seluruh sumber yang dikutip maupun dirujuk telah saya nyatakan dengan benar dan apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka saya bersedia menerima sanksi akademik sesuai dengan aturan yang berlaku.

Mataram, 14 Agustus 2018

Naufal Hanif
NIM. 1410530129

IZIN PENGGUNAAN

Skripsi ini merupakan syarat kelulusan pada Program Studi S1 Teknik Informatika STMIK Bumigora Mataram, dengan ini penulis setuju jika skripsi ini digandakan (diduplikasi) baik sebagian maupun seluruhnya, ataupun dikembangkan untuk kepentingan akademis yang disetujui oleh pembimbing penulis, Pembantu Ketua I atau Ketua STMIK Bumigora.

Untuk dimaklumi, bahwa menduplikasi, mempublikasikan atau menggunakan skripsi ini, maupun bagian-bagiannya dengan tujuan komersial / keuntungan finansial, tidak diizinkan tanpa adanya izin tertulis dari STMIK Bumigora. Jika hal ini dilanggar maka STMIK Bumigora akan memberikan sanksi sesuai dengan hukum yang berlaku.

Penghargaan akademis terkait isi dari skripsi ini adalah pada penulis dan STMIK Bumigora.

Permintaan izin untuk menduplikasi atau menggunakan materi dari skripsi ini baik sebagian maupun seluruhnya harus ditujukan pada:

Pembantu Ketua I

Ketua Program Studi S1 Teknik Informatika

STMIK Bumigora Mataram

ABSTRAK

Email spam, email spoofing, dan virus yang didistribusikan melalui *email* merupakan hal yang tidak diinginkan oleh pengguna *email*. *Email spam* akan sangat mengganggu pengguna *email* dan akan menghabiskan banyak sumber daya *mail server*. *Email spoofing* merupakan tindakan kejahatan yang memanfaatkan *email* sebagai sarana untuk melakukan penipuan. Sedangkan virus yang didistribusikan melalui *email* biasanya dikirimkan oleh pihak yang tidak bertanggung jawab yang bertujuan untuk menginfeksi *mail server* ataupun komputer pengguna *email*. *Email spam, email spoofing, dan email* yang mengandung *virus* dapat menimbulkan kerugian yang sangat besar baik bagi penyedia layanan *email* maupun bagi pengguna *email*. Berdasarkan latar belakang tersebut maka mendorong penulis untuk menganalisa penerapan *DKIM, SPF, Anti Spam, dan Anti Virus* sehingga *mail server* dapat terhindar dari *email spam, virus* dan pengguna *email* dapat terhindar dari aktifitas *spoofing*.

Perancangan dan analisa penerapan *DKIM, SPF, anti spam, dan anti virus* ini menggunakan metodologi *NDLC*, yaitu metode pengembangan jaringan komputer yang diawali dengan menganalisa artikel ilmiah, buku, dan jurnal untuk mendapatkan informasi mengenai *DKIM, SPF, anti spam, dan anti virus*. Merancang sistem *filtering email spam, spoofing, dan virus*, melakukan simulasi instalasi dan konfigurasi. Tahap berikutnya adalah implementasi dimana pada tahap ini dilakukan penerapan sistem yang telah dirancang sebelumnya dan melakukan uji coba pada sistem *filtering email spam, spoofing, dan virus*. Tahapan yang terakhir adalah tahap *monitoring* dimana akan dilakukan pengawasan terhadap sistem yang telah dibuat untuk mengetahui tingkat keberhasilan sistem yang telah dibuat.

Hasil atau keluaran yang akan dicapai yaitu *mail server* dapat terhindar dari *email spam, email spoofing, dan virus* untuk memastikan keamanan dan kenyamanan pengguna *email* serta menghindari dampak kerugian yang dapat ditimbulkan oleh *email spam, email spoofing, dan virus*.

Kesimpulan dari penelitian ini adalah penerapan protokol *DomainKeys Identified Mail* dapat mencegah *email spoofing* dengan cara melakukan otentifikasi menggunakan metode pencocokan *private key* dan *public key* (*Asymmetric keys*). Sedangkan penerapan protokol *Sender Policy Framework* dapat mencegah *email spoofing* dengan cara melakukan otorisasi menggunakan metode pencocokan alamat *IP* server pengirim. Sebaliknya penerapan *SpamAssassin, ClamAV, dan Amavisd-New* dapat mencegah masuknya *email spam* dan *virus* dengan cara melakukan pengecekan *header, body, and attachment email*.

Kata Kunci: *DomainKeys Identified Mail (DKIM), Sender Policy Framework (SPF), SpamAssassin, ClamAV, Amavisd-New, Mail Server*

DAFTAR ISI

Halaman

HALAMAN SAMPUL	
HALAMAN JUDUL	
HALAMAN PENGESAHAN	
KATA PENGANTAR	i
LEMBAR PERNYATAAN KEASLIAN.....	ii
IZIN PENGGUNAAN	iv
ABSTRAK.....	v
DAFTAR ISI	vi
DAFTAR GAMBAR.....	ix
DAFTAR TABEL.....	xii
DAFTAR LAMPIRAN	xiii

BAB I PENDAHULUAN

1.1. Latar Belakang	1
1.2. Perumusan Masalah.....	3
1.3. Batasan Masalah.....	3
1.4. Tujuan dan Manfaat Penulisan	5
1.4.1. Tujuan	5
1.4.2. Manfaat	5
1.5. Metodologi penelitian.....	6
1.6. Sistematika Penulisan	8

BAB II LANDASAN TEORI

2.1. Jaringan Komputer	10
2.2. Model Lapisan OSI/.....	11
2.3. <i>Transmission Control Protocol / Internet Protocol (TCP/IP)</i>	16
2.4. Keamanan Jaringan Komputer	17
2.5. Jenis-jenis Layanan Keamanan Jaringan	18
2.6. <i>Email Spoofing</i> dan <i>Phising</i>	19
2.7. Server.....	20
2.8. Linux.....	20

Halaman

2.9.	<i>Linux CentOS</i>	21
2.10.	<i>Centos Web Panel</i>	22
2.11.	<i>Surat Elektronik</i>	22
2.12.	<i>Mail Server</i>	23
2.13.	<i>Mail Protocol</i>	25
2.14.	<i>Postfix</i>	26
2.15.	<i>Dovecot</i>	26
2.16.	<i>Roundcube</i>	27
2.17.	<i>Domain Name System (DNS)</i>	27
2.18.	<i>DNS Server</i>	27
2.19.	<i>Bind9</i>	28
2.20.	<i>HTTP</i>	28
2.21.	<i>HTTP Server</i>	29
2.22.	<i>Apache HTTP Server</i>	29
2.23.	<i>Email Spam</i>	29
2.24.	<i>Spam Filter</i>	30
2.27.	<i>SpamAssassin, ClamAV, dan Amavisd-New</i>	30
2.28.	<i>DomainKeys Identified Mail (DKIM) dan OpenDKIM</i>	32
2.29.	<i>Sender Policy Framework (SPF)</i>	33
2.30.	<i>Gmail</i>	35
2.31.	<i>Emkei's Mailer</i>	35
2.32.	<i>Yahoo! Mail</i>	35

BAB III METODOLOGI DAN PERANCANGAN

3.1.	Tahap Analisa (<i>Analysis</i>)	36
3.1.1.	Pengumpulan Data	36
3.1.2.	Analisa Data.....	37
3.2.	Tahap Desain (<i>Design</i>).....	39
3.2.1	Rancangan Sistem <i>Filtering Email Spam, Virus dan Spoofing</i>	39
3.2.2	Rancangan Jaringan Uji Coba	41
3.2.3	Rancangan Pengalamatan <i>IP</i>	42
3.2.4	Rancangan Akun <i>Email</i>	42

Halaman

3.2.5	Kebutuhan Perangkat Keras dan Perangkat Lunak	43
3.3.	Tahap Simulasi (<i>Prototyping</i>).....	44
3.3.1.	Instalasi Dan Konfigurasi	45
3.3.2.	Ujicoba	45
3.4.	Tahap Implementasi	46
3.5.	Tahap <i>Monitoring</i>	46

BAB IV HASIL DAN PEMBAHASAN

4.1.	Hasil Instalasi Dan Konfigurasi	48
4.1.1.	Hasil Instalasi Dan Konfigurasi <i>Server</i>	48
4.1.2.	Hasil Konfigurasi <i>Client</i>	58
4.2.	Hasil Uji Coba.....	58
4.2.1.	Verifikasi Konfigurasi	58
4.2.2.	Skenario Uji Coba	62
4.3.	Analisa Hasil Uji Coba	105
4.3.1.	Analisa Hasil Uji Coba Pengiriman <i>Email Spoofing</i>	105
4.3.2	Analisa Hasil Uji Coba Pengiriman <i>Email Spam</i>	106
4.3.3	Analisa Hasil Uji Coba Mengirim <i>Email</i> Mengandung <i>Virus</i>	107
4.3.4	Analisa Hasil Uji Coba Pengecekan <i>Header Email</i>	108

BAB V PENUTUP

5.1.	Kesimpulan.....	110
5.2.	Saran.....	110

DAFTAR REFERENSI

LAMPIRAN

DAFTAR GAMBAR

	Halaman
Gambar 1.1 Fase <i>NDLC</i>	6
Gambar 2.1 <i>Layer OSI</i>	11
Gambar 2.2 Perbandingan <i>Layer TCP/IP</i> dan <i>Layer OSI</i>	16
Gambar 2.3 Proses pengiriman <i>email</i>	24
Gambar 2.4 Cara Kerja <i>SpamAssassin</i> , <i>ClamAV</i> , dan <i>Amavisd-New</i>	32
Gambar 2.5 Cara Kerja <i>DKIM</i>	33
Gambar 2.6 Cara Kerja <i>SPF</i>	34
Gambar 3.1 Rancangan Sistem <i>Filtering Email Spam, Spoofing</i> , dan <i>Virus</i>	39
Gambar 3.2 Rancangan Topologi Uji Coba	41
Gambar 4.1 Linux CentOS release 7.3.1611.....	48
Gambar 4.2 Hasil Instalasi CWP	49
Gambar 4.3 Konfigurasi Interface.....	50
Gambar 4.4 Konfigurasi Name Server.....	51
Gambar 4.5 Konfigurasi <i>Domain</i>	51
Gambar 4.6 <i>File</i> skripsi.online.db.....	52
Gambar 4. 7 <i>File</i> named.ip4.skripsi.online.db	53
Gambar 4.8 <i>File</i> named.conf	53
Gambar 4.9 Membuat Akun <i>Email</i>	54
Gambar 4.10 Instalasi <i>DKIM, SPF, Anti Spam, dan Anti Virus</i>	55
Gambar 4.11 Menambah <i>DKIM Record</i> pada <i>File Zone</i>	55
Gambar 4.12 Menambah <i>SPF Record</i> pada <i>File Zone</i>	56
Gambar 4.13 <i>DKIM</i> dan <i>SPF Record</i>	56
Gambar 4.14 Konfigurasi <i>File TrustedHosts</i>	57
Gambar 4.15 Konfigurasi <i>File main.cf</i>	57
Gambar 4.16 Terhubung ke <i>Internet</i>	58
Gambar 4.17 Verifikasi Konfigurasi <i>DNS Server</i>	59
Gambar 4.18 Verifikasi Konfigurasi <i>Mail Server</i>	60
Gambar 4.19 Mengirim <i>Email</i> pada <i>User Email Local</i>	60
Gambar 4.20 Mengirim <i>Email</i> Pada <i>Mail Server Lain</i>	60
Gambar 4.21 Verifikasi Fungsi <i>DKIM, SPF, dan SpamAssassin</i>	61
Gambar 4.22 Verifikasi Fungsi <i>ClamAV</i>	61
Gambar 4.23 Ping <i>Mail Server</i>	62
Gambar 4.24 Akses <i>MUA</i>	62
Gambar 4.25 <i>Emkei's Fake Mailer</i>	65
Gambar 4.26 <i>Email Spoofing</i>	66
Gambar 4.27 Balasan <i>Email Spoofing</i>	67
Gambar 4. 28 Mengirim <i>Email Spoofing</i> ke <i>Yahoo! Mail</i>	68
Gambar 4.29 <i>Email Spoofing</i> Terkirim ke <i>Yahoo! Mail</i>	68
Gambar 4. 30 Mengirim <i>Email Spoofing</i> ke skripsi.online.....	69

Halaman

Gambar 4. 31 <i>Email Spoofing</i> Terkirim ke <i>User skripsi.online</i>	70
Gambar 4.32 Mengirim <i>Email Spam</i> dari <i>skripsi.online</i>	71
Gambar 4.33 <i>Email Spam</i> dari <i>skripsi.online</i> Terkirim.....	71
Gambar 4.34 Mengirim <i>Email Spam</i> dari <i>Yahoo! Mail</i>	72
Gambar 4.35 <i>Email Spam</i> dari <i>Yahoo! Mail</i> Terkirim	72
Gambar 4.36 Mengirim <i>Email Spam</i> dari <i>Gmail</i>	73
Gambar 4.37 <i>Email Spam</i> dari <i>Gmail</i> Terkirim.....	73
Gambar 4.38 Mengirim <i>Email Spam</i> Tanpa <i>GTUBE TEST</i>	74
Gambar 4.39 <i>Email</i> Terindikasi Sebagai <i>Spam</i> oleh <i>Yahoo! Mail</i>	75
Gambar 4.40 Mengirim <i>Email Spam</i> Tanpa <i>Format GTUBE Test</i>	76
Gambar 4. 41 <i>Email Spam</i> Tanpa <i>GTUBE Test</i> Terkirim	76
Gambar 4. 42 <i>EICAR Test</i> dari <i>skripsi.online</i>	77
Gambar 4.43 Email Mengandung Virus dari <i>skripsi.online</i> Terkirim.....	78
Gambar 4.44 <i>EICAR Test</i> dari <i>Yahoo! Mail</i>	78
Gambar 4. 45 <i>Email</i> Mengandung <i>Virus</i> dari <i>Yahoo! Mail</i> Terkirim	79
Gambar 4.46 <i>EICAR Test</i> dari <i>Gmail</i>	80
Gambar 4.47 <i>Email</i> Mengandung <i>Virus</i> dari <i>Gmail</i> Terkirim.....	80
Gambar 4.48 Lampiran Terdeteksi Sebagai <i>Virus</i>	81
Gambar 4.49 Mengirim <i>Virus</i> Sebelum Penerapan <i>Anti Virus</i>	82
Gambar 4.50 <i>Virus</i> Berhasil Terkirim ke Kotak Masuk Pengguna <i>Email</i>	82
Gambar 4.51 <i>Header Email</i> Tanpa Parameter <i>X-Virus-Scanned</i>	82
Gambar 4.52 Cuplikan <i>Header Email</i> pada <i>Gmail</i> Sebelum Penerapan	83
Gambar 4.53 Cuplikan <i>Header Email</i> pada <i>Yahoo! Mail</i> Sebelum Penerapan....	84
Gambar 4.54 Cuplikan <i>Header Email</i> pada <i>skripsi.online</i> Sebelum Penerapan	85
Gambar 4.55 <i>Private Key</i> pada <i>skripsi.online</i>	86
Gambar 4.56 <i>Public Key</i> pada <i>DNS Server</i> <i>skripsi.online</i>	87
Gambar 4.57 Cuplikan <i>Header Email</i>	87
Gambar 4.58 <i>SPF Record</i> pada <i>skripsi.online</i>	88
Gambar 4.59 Parameter <i>Received-SPF</i> pada <i>Header Email</i>	88
Gambar 4.60 Pemberitahuan dari <i>Mail System Emkei's Fake Mailer</i>	88
Gambar 4.61 <i>Email Spoofing</i> Masuk ke <i>Folder Spam</i>	89
Gambar 4.62 <i>Email Spoofing</i> Masuk pada <i>Folder Inbox</i>	90
Gambar 4.63 Mengirim <i>Email Spam</i> dari <i>skripsi.online</i> Setelah Penerapan ...	91
Gambar 4.64 <i>Email</i> dari <i>skripsi.online</i> Terindikasi <i>Spam</i>	91
Gambar 4.65 Mengirim <i>Email Spam</i> dari <i>Yahoo! Mail</i> Setelah Penerapan	92
Gambar 4.66 <i>Email</i> dari <i>Yahoo! Mail</i> Terindikasi <i>Spam</i>	92
Gambar 4.67 Mengirim <i>Email Spam</i> dari <i>Gmail</i> Setalah Penerapan.....	93
Gambar 4.68 <i>Email</i> dari <i>Gmail</i> Terindikasi <i>Spam</i>	93
Gambar 4.69 <i>Email</i> Dengan <i>Format Spam</i>	94
Gambar 4.70 <i>Email</i> Terindikasi Sebagai <i>Spam</i> oleh <i>Yahoo! Mail</i>	95
Gambar 4.71 Mengirim <i>Email Spam</i> Tanpa <i>Format GTUBE Test</i>	96
Gambar 4. 72 <i>Default Score SpamAssassin</i>	96

Halaman

Gambar 4.73 Skor <i>Email</i> yang Terindikasi Sebagai <i>Spam</i>	97
Gambar 4.74 <i>EICAR Test</i> dari skripsi.ononline Setelah Penerapan	97
Gambar 4.75 <i>Email</i> dari skripsi.ononline Terblok	98
Gambar 4.76 <i>EICAR Test</i> dari <i>Yahoo! Mail</i> Setelah Penerapan.....	99
Gambar 4.77 <i>Email</i> dari <i>Yahoo! Mail</i> Terblok.....	99
Gambar 4.78 <i>EICAR Test</i> dari <i>Gmail</i> Setelah Penerapan.....	100
Gambar 4.79 <i>Email</i> dari <i>Gmail</i> Terblok	101
Gambar 4.80 Lampiran Terdeteksi Sebagai <i>Virus</i>	101
Gambar 4.81 Mengirim <i>Virus</i> Setelah Penerapan <i>Anti Virus</i>	102
Gambar 4.82 <i>Email</i> Terdeteksi Mengandung <i>Virus</i>	102
Gambar 4.83 Cuplikan <i>Header Email</i> pada <i>Gmail</i> Setelah Penerapan.....	103
Gambar 4. 84 Cuplikan <i>Header Email</i> pada <i>Yahoo! Mail</i> Setelah Penerapan... 104	
Gambar 4.85 Cuplikan <i>Header Email</i> pada skripsi.ononline Setelah Penerapan	105

DAFTAR TABEL

	Halaman
Tabel 3.1 Jurnal Ilmiah Tentang <i>Email Spam, Spoofing, dan Virus</i>	36
Tabel 3.2 Pengalamatan <i>IP</i>	42
Tabel 3.3 Kebutuhan Akun <i>Email</i>	42
Tabel 3.4 Spesifikasi <i>VPS</i>	43
Tabel 3.5 Spesifikasi <i>Client</i>	43
Tabel 4.1 Perbandingan Sebelum dan Setelah Penerapan <i>DKIM</i> dan <i>SPF</i>	106
Tabel 4.2 Perbandingan Sebelum dan Setelah Penerapan <i>Anti Spam</i>	107
Tabel 4.3 Perbandingan Sebelum Penerapan <i>Anti virus</i>	107
Tabel 4.4 Perbandingan Header Email Sebelum dan Setelah Penerapan.....	108

DAFTAR LAMPIRAN

Halaman

LAMPIRAN A: *HEADER EMAIL* A.1

BAB I

PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi saat ini sudah begitu pesat sehingga teknologi dapat memudahkan pekerjaan manusia hampir di segala bidang, surat elektronik adalah salah satu dari kemajuan teknologi dalam bidang komunikasi sehingga fungsi dari surat dapat digantikan dengan adanya surat elektronik, efisiensi biaya dan waktu menjadi alasan yang membuat banyak orang beralih dari surat menuju surat elektronik.

Hoiriyah, Sugiantoro, dan Prayudi (2016) menyebutkan bahwa salah satu layanan internet yang banyak digunakan adalah *email*. *email* merupakan surat elektronik yang berbasis *file* teks, namun dengan perkembangan teknologi, email lebih atraktif terhadap penggunanya, tidak hanya dapat mengirim *file* teks, tetapi juga dapat mengirim *file* audio, video, foto dan *file* ekstensi lainnya. Terdapat ancaman serius mengiringi kemudahan yang diberikan oleh *email* dengan memanfaatkan *email* sebagai media untuk melakukan tindak kejahatan di dunia siber, karena *email* merupakan alat transportasi utama bagi *spam*, *virus* dan *malware* dalam jaringan. *Spam* adalah *email* yang tidak diinginkan, *email spam* dikirim kepada seseorang penerima dan pesan tersebut tidak ada gunanya untuk penerima. *Spam* dikirim pada jaringan untuk meningkatkan konsumsi sumber daya, dengan kata lain untuk meningkatkan lalu lintas jaringan (*Suryana, Akbar, Widiyasono, 2016*). Nurlina & Irmayana (2014)

menyebutkan bahwa tidak semua *email spam* masuk pada *folder spam* yang telah disediakan dan *email* yang bukan *spam* terkadang masuk pada *folder spam* sehingga *email* penting terkadang tidak dibaca oleh penerima *email*. *Email* juga merupakan sumber utama dari kebanyakan aktivitas kriminal pada *internet*, salah satu ancaman dari tindak kejahatan yang menggunakan *email* adalah *email spoofing*. *Email spoofing* dianggap sebagai tindakan berbahaya karena melakukan manipulasi data pada *header email* untuk menyamar sebagai orang atau organisasi yang sah, contohnya seperti melakukan pengiriman *email* dengan nama pengirim seolah dari administrator suatu organisasi. Pengirim *email spoofing* menyerang dengan berbagai macam isi pesan untuk membuat korbannya percaya.

Email spam, spoofing, dan virus sangat tidak diinginkan oleh pengguna maupun penyedia layanan *email* sehingga perlu diterapkan suatu sistem yang dapat mencegah *email spam, spoofing, dan virus*. Sistem pencegahan *email spam, spoofing, dan virus* diharapkan dapat mengurangi dampak kerugian yang diakibatkan oleh *email spam, spoofing, dan virus*.

DKIM dan *SPF* dapat digunakan untuk melakukan otentikasi dan otorisasi *email* sehingga akun *email client* akan terbebas dari tindakan *spoofing*. Penerapan *Anti Spam* dan *Anti Virus* juga diperlukan agar *email server* terhindar dari *email spam* dan *virus*, metode yang diterapkan oleh *Anti Spam* dan *Anti Virus* yaitu dengan melakukan pengecekan *header, body, dan attachment email*.

Manfaat dari penerapan *DKIM*, *SPF*, *Anti Spam* dan *Anti Virus* adalah untuk menghemat sumber daya *mail server* dengan cara memblokir surat elektronik yang dianggap sebagai *spam*, meningkatkan kualitas keamanan surat elektronik sehingga pengguna dapat terhindar dari aktifitas *spoofing* serta *virus* dan *malware* yang disisipkan melalui surat elektronik.

1.2. Perumusan Masalah

Adapun rumusan masalah pada skripsi ini adalah bagaimana menganalisa penerapan *DKIM*, *SPF*, *Anti Spam*, dan *Anti Virus* pada *mail server* agar *mail server* dapat terhindar dari *email spam*, *virus* dan pengguna *email* dapat terhindar dari aktifitas *spoofing*.

1.3. Batasan Masalah

Batasan masalah yang digunakan dalam penyusunan skripsi ini untuk menjadikan pembahasan menjadi lebih terarah dan fokus adalah sebagai berikut:

1. Rancangan uji coba diimplementasikan menggunakan *VPS* yang disewa pada penyedia layanan *VPS*. Pada *VPS* akan dilakukan instalasi *CentOS Web Panel*, konfigurasi *DNS server*, konfigurasi *Mail server*, dan komputer *client* digunakan untuk mengakses *Mail User Agent* berbasis web (*Roundcube*).
2. Sistem operasi *VPS* yang digunakan adalah *CentOS 7.3.1611*.
3. Aplikasi yang digunakan untuk memudahkan instalasi dan konfigurasi server adalah *CentOS Web Panel*.
4. Aplikasi *MTA* yang digunakan adalah *Postfix* untuk mengirim *email*.

5. Aplikasi *MDA* yang digunakan adalah Dovecot untuk menerima *email*.
6. Aplikasi *MUA* yang digunakan adalah *Roundcube* sebagai aplikasi *email* di sisi pengguna.
7. Aplikasi *DNS server* yang digunakan adalah *bind9* agar *email server* dapat diakses menggunakan nama *domain* skripsiian.online.
8. Aplikasi *HTTP server* yang digunakan adalah Apache agar *Mail Transfer Agent* berbasis web dapat diakses melalui *browser*.
9. Aplikasi yang digunakan untuk membuat *DKIM record key* adalah *OpenDKIM*.
10. Validasi surat elektronik menggunakan *SpamAssassin*, *ClamAV*, dan *Amavisd-New* sebagai *anti spam* dan *anti virus*.
11. *Email* yang digunakan untuk uji coba adalah *email server* skripsiian.online, *Emkei's Fake Mailer*, *Yahoo! Mail* *Gmail*, dan *ridho.org*.
12. Pengujian yang dilakukan dengan mengirim surat elektronik yang terindikasi sebagai *spam* dan *ham*, kemudian melakukan pengiriman *email spoofing*, dan email yang mengandung virus, serta mengecek header email sebelum dan setelah penerapan *DKIM*, *SPF*, *anti spam*, dan *anti virus*.
13. Pengujian *DKIM* dan *SPF* dilakukan dengan cara mengirim *email spoofing* menggunakan *Emkei's Fake Mailer* kemudian *email spoofing* tersebut dikirim ke *Gmail* dan *Yahoo! Mail*.

14. Pengujian *Anti Spam* dan *Anti Virus* dilakukan dengan cara mengirim *email spam* dan *email* yang mengandung *virus* ke *mail server* skripsiian.online.

1.4. Tujuan dan Manfaat Penulisan

1.4.1. Tujuan

Adapun tujuan dari penulisan skripsi ini adalah untuk menganalisa penerapan *DKIM*, *SPF*, *Anti Spam* dan *Anti Virus* pada *mail server* agar *mail server* terhindar dari *email spam*, *virus* dan aktifitas *spoofing* yang dilakukan oleh pihak yang tidak bertanggung jawab.

1.4.2. Manfaat

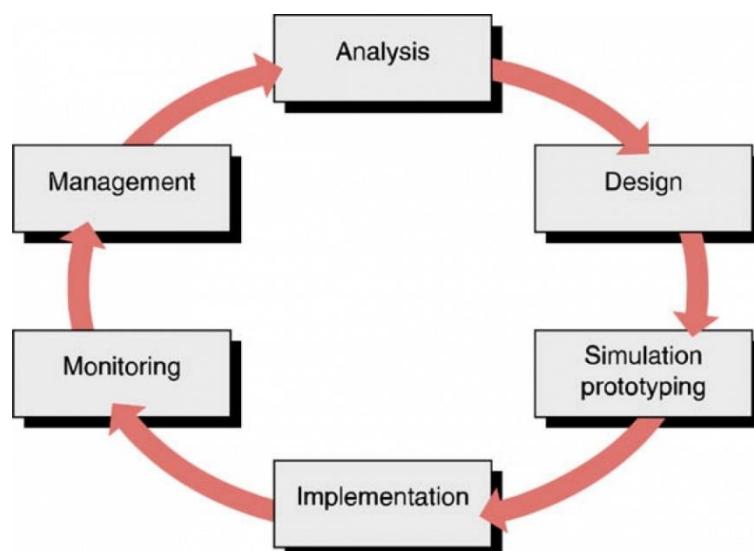
Adapun manfaat dari penelitian ini adalah sebagai berikut:

1. Bagi Diri Sendiri
 - a. Dapat menambah ilmu pengetahuan penulis sehingga dapat diterapkan pada dunia kerja.
 - b. Dapat menjadi tempat untuk mengimplementasikan ilmu pengetahuan yang telah didapat selama berada dibangku perkuliahan.
 - c. Sebagai syarat untuk menyelesaikan jenjang pendidikan Strata 1 (S1) pada program studi Teknik Informatika di STMIK Bumigora.
2. Bagi Keilmuan
 - a. Dapat menjadi bahan rujukan untuk pengembangan penelitian berikutnya terutama dalam bidang yang sama.

- b. Dapat menjadi sarana untuk melatih kemampuan dalam menulis karya ilmiah.
3. Bagi Masyarakat
 - a. Dapat memberikan pengetahuan terkait dengan analisa penanganan *email spam*, *virus* dan aktifitas *spoofing* menggunakan *DKIM*, *SPF*, *Anti Spam*, dan *Anti Virus*.
 - b. Dapat memberikan solusi cara penerapan *DKIM*, *SPF*, *Anti Spam*, dan *Anti Virus* pada *mail server*.

1.5. Metodologi penelitian

Nurfajar, Kurniawan, dan Yunan (2015) menyebutkan bahwa *Network Development Life Cycle* adalah suatu metode yang digunakan dalam mengembangkan atau merancang jaringan infrastruktur yang memungkinkan terjadinya pemantauan jaringan untuk mengetahui statistik dan kinerja jaringan. *NDLC* mempunya enam fase, keenam fase tersebut dapat dilihat seperti pada gambar 1.1 berikut.



Gambar 1.1 Fase NDLC

Sumber: Nurfajar, Kurniawan, dan Yunan, 2015

Dari keenam fase yang terdapat pada *NDLC*, penulis hanya menggunakan lima fase antara lain sebagai berikut:

1. *Analysis*

Pada fase ini penulis melakukan pengumpulan data dengan cara studi literatur, yaitu penulis membaca artikel ilmiah, buku, dan jurnal untuk mendapatkan informasi mengenai *DKIM*, *SPF*, *Anti Spam*, dan *Anti Virus*. Data-data yang telah terkumpul kemudian dianalisa.

2. *Design*

Pada fase ini penulis membuat rancangan yang meliputi rancangan jaringan uji coba, rancangan pengalamatan *IP*, rancangan sistem *filtering*, otentikasi, dan otorisasi *email* menggunakan *DKIM*, *SPF*, *Anti Spam*, dan *Anti Virus*, serta kebutuhan perangkat keras dan perangkat lunak.

3. *Simulation Prototyping*

Setelah melakukan analisa dan desain, tahap berikutnya adalah melakukan simulasi dan membuat *prototype* berdasarkan pada desain yang telah dirancang sebelumnya (Nurfajar, Kurniawan, dan Yunan, 2015). Pada fase ini dilakukan instalasi dan konfigurasi serta uji coba *DKIM*, *SPF*, *Anti Spam*, dan *Anti Virus* menggunakan berbagai macam skenario.

4. *Implementation*

Pada fase ini penulis akan menerapkan semua yang telah direncanakan dan di desain pada tahapan sebelumnya.

Pada fase ini penulis akan membangun sebuah *mail server* kemudian pada *mail server* tersebut akan diterapkan *DKIM*, *SPF*, *Anti Spam*, dan *Anti Virus* untuk mengotentikasi, mengotorisasi dan memvalidasi *email* dan penulis akan melakukan analisa pada *mail server* sebelum dan sesudah penerapan *DKIM*, *SPF*, *Anti Spam*, dan *Anti Virus*.

5. *Monitoring*

Setelah melakukan implementasi, tahapan *monitoring* adalah tahapan penting dalam merancang desain jaringan, tujuan dari tahapan *monitoring* adalah untuk memastikan jaringan komputer berjalan sesuai dengan tujuan pada tahap analisis (Nurfajar, Kurniawan, dan Yunan, 2015). Pada fase ini penulis akan melakukan *monitoring* terhadap aktifitas *spam*, dan *virus* pada *mail server* skripsi.ononline dengan menggunakan *maillog* server skripsi.ononline serta melakukan *monitoring* terhadap aktifitas *spoofing* pada penyedia layanan *email* yaitu *Yahoo! Mail* dan *Gmail*.

1.6. Sistematika Penulisan

Adapun sistematika penulisan yang digunakan pada skripsi ini adalah sebagai berikut:

BAB I Pendahuluan

Bab ini berisi latar belakang, perumusan masalah, batasan masalah, tujuan dan manfaat penulisan, metodologi penelitian, dan sistematika penulisan.

BAB II Landasan Teori

Bab ini berisi tentang teori-teori yang melandasi penelitian ini, antara lain jaringan komputer, *OSI*, *TCP/IP*, keamanan jaringan komputer, tujuan keamanan jaringan komputer, *Spoofing*, *Phising*, *Server*, *Linux*, *Linux CentOS*, *CentOS Web Panel*, *Email*, *Mail Server*, *POP3*, *IMAP*, *SMTP*, *Postfix*, *Dovecot*, *Roundcube*, *DNS*, *DNS Server*, *BIND9*, *HTTP* dan *HTTPS*, *HTTP Server*, *Apache HTTP Server*, *Email Spam*, *Anti Spam*, *SpamAssassin*, *ClamAV*, *Amavisd-New*, *DKIM*, *OpenDKIM*, *SPF*, *Gmail*, *Emkei's Mailer*, *Yahoo! Mail*.

BAB III Metodologi Penelitian

Bab ini berisi tentang metodologi penelitian yang digunakan dan fase-fase dari metodologi penelitian yang digunakan pada penelitian ini.

BAB IV Hasil dan Pembahasan

Bab ini berisi tentang pembahasan hasil konfigurasi, uji coba, dan analisa terhadap uji coba yang telah dilakukan.

BAB V Penutup

Bab ini berisi tentang kesimpulan dan saran untuk pengembangan skripsi ini selanjutnya.

BAB II

LANDASAN TEORI

2.1. Jaringan Komputer

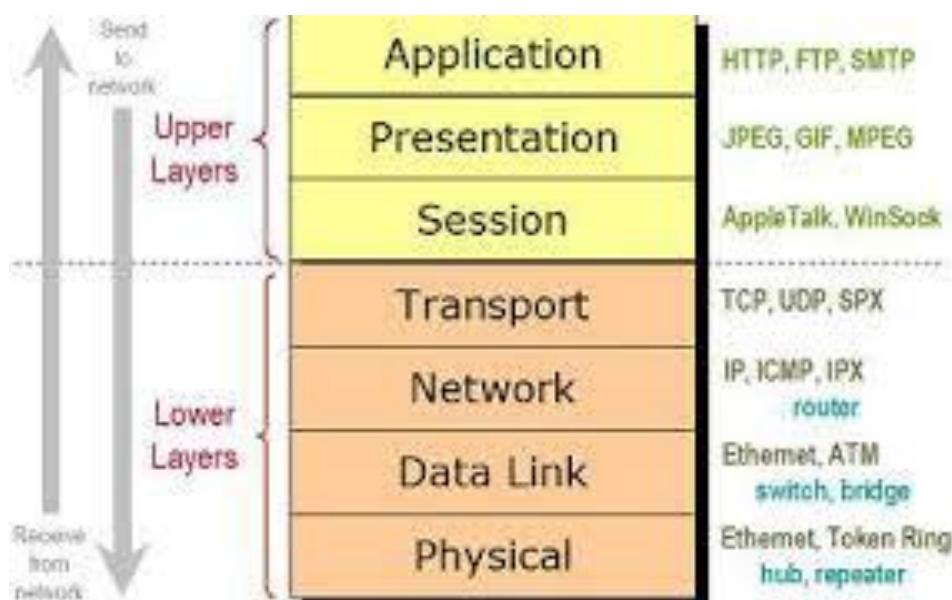
Menurut Haryanto & Riadi (2014) sebuah jaringan komputer biasanya terdiri dari dua atau lebih komputer yang saling terhubung satu sama lain serta dapat saling berbagi sumber daya seperti *CDROM*, *printer*, pertukaran *file*, atau memungkinkan untuk saling berkomunikasi secara elektronik, komputer dapat terhubung melalui media transmisi seperti kabel, saluran telepon, gelombang radio, satelit atau infrared. Sedangkan menurut Masero, Triyono, dan Andayati (2013) jaringan komputer merupakan sekumpulan perangkat yang dapat digunakan untuk menyimpan dan memanipulasi data elektronis serta pesan-pesan, saling terkait sehingga dapat berbagi pakai berupa data, perangkat keras, dan perangkat lunak. Jaringan komputer adalah sekelompok komputer otonom yang saling berhubungan satu sama lain menggunakan protokol komunikasi sehingga dapat saling berbagi informasi, aplikasi, dan perangkat keras secara bersama-sama, tujuan membangun jaringan komputer adalah untuk membawa secara tepat tanpa adanya kesalahan dari sisi pengirim menuju ke sisi penerima melalui media komunikasi (Ardiantoro, Triyono, Fatkhiyah, 2016).

Berdasarkan dari ketiga pengertian tersebut dapat disimpulkan bahwa jaringan komputer adalah sebuah sistem yang menghubungkan *node-node* yang terdapat pada jaringan komputer dengan menggunakan media komunikasi tertentu sehingga *node-node* pada jaringan komputer

dapat saling berbagi sumber daya, berkomunikasi, dan saling bertukar informasi untuk mencapai suatu tujuan yang sama.

2.2. Model Lapisan OSI

Model *Open System Interconnection* (OSI) diciptakan oleh *International Organization for Standardization* (ISO) yang menyediakan kerangka logika terstruktur bagaimana proses komunikasi data berinteraksi melalui jaringan, standar ini dikembangkan untuk industri komputer agar komputer dapat berkomunikasi pada jaringan yang berbeda secara efisien (Kader, Najoan, dan Sinsuw, 2014).



Gambar 2.1 Layer OSI
Sumber: Sujana, 2014

Menurut Sujana (2014) terdapat tujuh *layer* pada model OSI dan setiap *layer* memiliki tanggung jawab khusus pada proses komunikasi data:

1. *Physical*

Pada *physical layer* tidak memiliki protokol yang spesifik, karena pada *physical layer* hanya mengirimkan *bit* data.

2. *Data Link*

Terdapat dua protokol pada *data link layer* yaitu:

- *PPP (Point to Point Protocol)*

Protokol yang digunakan untuk komunikasi *point to point* pada suatu jaringan.

- *SLIP (Serial Line Internet Protocol)*

Protokol yang digunakan untuk menghubungkan *serial*.

3. *Network*

Terdapat tiga protokol pada *network layer* yaitu:

- *IP (Internetworking Protocol)*

Mekanisme transmisi yang digunakan untuk mentransportasikan data dalam paket yang disebut *datagram*.

- *ARP (Address Resolution Protocol)*

Protokol yang digunakan untuk mengetahui alamat IP berdasarkan alamat fisik dari sebuah komputer.

- *RARP (Reverse Address Resolution Protocol)*

Protokol yang digunakan untuk mengetahui alamat fisik melalui alamat IP komputer.

- *ICMP (Internet Control Message Protocol)*

Mekanisme yang digunakan oleh sejumlah *host* untuk mengirim notifikasi datagram yang mengalami masalah pada *hostnya*.

- *IGMP (Internet Group Message Protocol)*

Protokol yang digunakan untuk memberi fasilitas pesan yang simultan kepada grup penerima.

4. *Transport*

Terdapat dua protokol pada *transport layer* yaitu:

- *TCP (Transmission Control Protocol)*

Protokol yang menyediakan layanan penuh pada lapisan *transport* untuk aplikasi.

- *UDP (User Datagram Protocol)*

Protokol *connectionless* dan *procces-to-procces* yang hanya menambahkan alamat *port*, *checksum error control* dan panjang informasi data pada *layer* diatasnya.

5. *Session*

Terdapat empat protokol pada *session layer* yaitu:

- *NETBIOS*

Berfungsi sebagai penyiaran pesan, maksudnya adalah memungkinkan *user* mengirim pesan tunggal secara serempak ke komputer lain yang terkoneksi. *NETBEUI* (*NETBIOS Extended User Interface*) berfungsi sama dengan *NETBIOS* hanya sedikit dikembangkan lagi dengan menambah fungsi yang memungkinkan bekerja dengan perangkat keras dan perangkat lunak.

- *ADSP (AppleTalk Data Stream Protocol)*

Fungsi dari protokol ini adalah untuk memantau aliran data dianatara dua komputer dan untuk memeriksa aliran data tersebut tidak terputus.

- *PAP (Printer Access Protocol)*

Berfungsi sebagai *printer postscript* untuk melakukan akses pada jaringan *Apple Talk* dan untuk mengendalikan bagaimana pola komunikasi antar *node*.

- *SPDU (Session Protocol Data Unit)*

Berfungsi sebagai penghubung antara dua *session service user*.

6. *Presentation*

Terdapat tiga protokol pada *layer presentation* yaitu:

- *TELNET*

Protokol yang digunakan untuk melakukan *remote access* ke suatu *host*.

- *SMTP (Simple Mail Transfer Protocol)*

Salah satu protokol yang digunakan dalam pengiriman *email* di internet atau untuk mengirim data dari komputer pengirim *email* ke server *email* penerima.

- *SNMP (Simple Network Management Protocol)*

Protokol yang digunakan dalam suatu manajemen jaringan.

7. *Application*

Terdapat sembilan protokol pada *layer application* yaitu:

- *HTTP (Hyper Text Transfer Protocol)*

Protokol yang digunakan untuk mentransfer dokumen dan web dalam sebuah *web browser* melalui *www*.

- *FTP (File Transfer Protocol)*

Protokol *internet* yang berjalan dalam lapisan aplikasi yang merupakan standar untuk mentransfer *file* komputer dalam sebuah jaringan *internet*.

- *NFS (Network File System)*

Jaringan komputer yang memungkinkan pengguna di klien komputer untuk mengakses *file* melalui jaringan dengan cara yang sama saat mengakses *file* pada sumber penyimpanan lokal.

- *DNS (Domain Name System)*

Protokol yang digunakan untuk memberikan suatu nama *domain* pada sebuah alamat *IP* agar lebih mudah diingat.

- *POP3 (Post Office Protocol)*

Protokol yang digunakan untuk mengambil *mail* dari suatu *mail transfer agent* yang akhirnya *mail* tersebut akan didownload kedalam jaringan lokal.

- *MIME (Multipurpose Internet Mail Extension)*

Protokol yang digunakan untuk mengirim *file binary* dalam bentuk teks.

- *SMB (Server Message Block)*

Protokol yang digunakan untuk mentransfer server-server *file* ke DOS dan Windows.

- *NNTP (Network News Transfer Protocol)*

Protokol yang digunakan untuk menerima dan mengirim *newsgroup*.

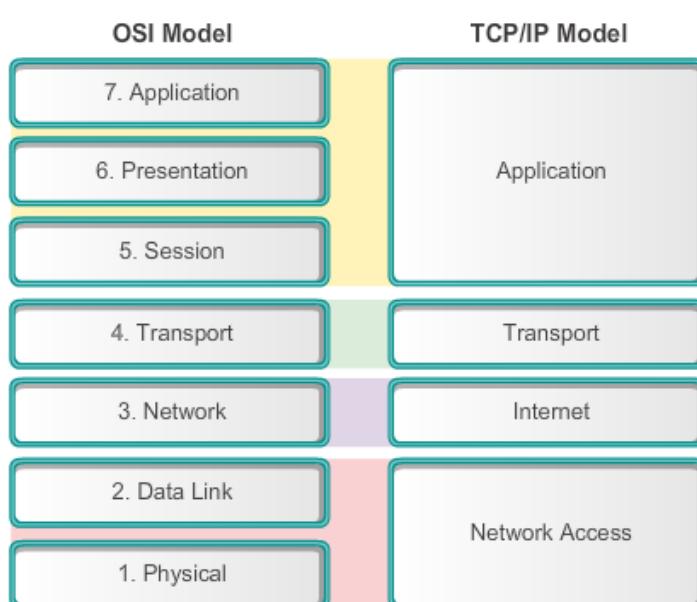
- *DHCP (Dynamic Host Configuration Protocol)*

Layanan yang memberikan alamat *IP* kepada komputer yang memintanya secara otomatis.

2.3. *Transmission Control Protocol / Internet Protocol (TCP/IP)*

TCP/IP didefinisikan sebagai protokol jaringan yang berperan dalam membangun *environment* jaringan global seperti *internet*. Protokol direferensikan pula sebagai suit *protocol DoD* ("deehohdee") karena mereka pada dasarnya dikembangkan oleh komunitas riset *Advanced Research Projects Agency* (ARPA) dari *US Department of Defense (DoD)*.

Nama *TCP/IP* diambil dari dua 'Keluarga' protokol fundamental, yaitu *TCP* dan *IP*. Meskipun demikian, suit masih memiliki protokol utama lainnya seperti *UDP* dan *ICMP*. Protokol bekerja sama dalam memberikan *framework networking* yang digunakan oleh banyak protokol aplikasi berbeda, di mana masing-masing digunakan untuk tujuan berbeda (Kader, Najoan, dan Sinsuw, 2014).



Gambar 2.2 Perbandingan Layer TCP/IP dan Layer OSI

Sumber: Wardoyo, Ryadi, dan Fahrizal, 2014

Berikut fungsi dari masing-masing *layer* pada protokol *TCP/IP* (Riadi, 2011):

1. *Network Access Layer*

Layer network access merupakan gabungan antara dua *layer* yaitu *network interface layer* dan *physical layer*, *network interface layer* berfungsi untuk mengirim data ke *layer physical* melalui device jaringan kemudian dilanjutkan oleh *layer physical* yang merupakan sistem kabel yang digunakan untuk proses mengirim dan menerima data.

2. *Internet Layer*

Pada lapisan *internet* terjadi proses pengambilan paket dari lapisan *transport* dan menambahkan informasi alamat sebelum mengirimkannya ke lapisan *network interface*.

3. *Transport Layer*

Pada lapisan *transport* terdapat protokol seperti *TCP* dan *UDP* yang berfungsi menambahkan data *transport* ke paket dan melewatkannya ke lapisan *Internet*.

4. *Application Layer*

Pada lapisan *application* terdapat protokol seperti *FTP*, *Telnet*, *SMTP*, dan *NFS* dilaksanakan.

2.4. Keamanan Jaringan Komputer

Menurut Fitriani (2014) Keamanan jaringan komputer merupakan suatu proses untuk mencegah dan mengidentifikasi penggunaan yang tidak sah dari jaringan komputer. Langkah-langkah pencegahan membantu menghentikan pengguna yang tidak sah yang disebut “penyusup” untuk

mengakses setiap bagian dari sistem jaringan komputer. Tujuan keamanan jaringan komputer adalah untuk mengantisipasi resiko jaringan komputer berupa bentuk ancaman fisik maupun logik baik langsung ataupun tidak langsung mengganggu aktivitas yang sedang berlangsung dalam jaringan komputer.

2.5. Jenis-jenis Layanan Keamanan Jaringan

Menurut Fitriani (2014) terdapat beberapa jenis layanan keamanan jaringan, diantaranya:

1. Otentikasi (*Authentication*)

Layanan Otentikasi ada 2 macam. Pertama disebut dengan Otentikasi Entitas (*Entity Authentication*) yaitu layanan kemanan jaringan yang memberikan kepastian terhadap identitas sebuah entitas yang terlibat dalam komunikasi data. Kedua adalah Otentikasi Keaslian Data (*Data Origin Authentication*) yaitu layanan yang memberikan kepastian terhadap sumber sebuah data.

2. Kendali Akses (*Access Control*)

Kendali Akses adalah layanan keamanan jaringan yang menghalangi penggunaan tidak terotorisasi terhadap sumber daya. Pada aplikasi jaringan umunya kebijakan kemampuan (baca, modifikasi, tulis dan eksekusi sebuah data/layanan sistem) ditentukan oleh jenis pengguna.

3. Kerahasiaan Data (*Data Confidentiality*)

Kerahasiaan data adalah layanan keamanan jaringan yang memproteksi data tertransmisi terhadap pengungkapan oleh pihak yang tidak berwenang / berhak.

4. Keutuhan Data (*Data Integrity*)

Keutuhan data adalah layanan keamanan jaringan yang memastikan bahwa data yang diterima oleh penerima adalah benar-benar sama dengan data yang dikirim oleh pengirim.

5. *Non-Repudiation*

Layanan *non-repudiation* adalah layanan keamanan jaringan yang menghindari penolakan atas penerima atau pengirim data yang telah dikirim.

6. Ketersediaan (*Availability*)

Layanan *Availability* adalah layanan sistem yang membuat sumber daya sistem tetap dapat diakses dan digunakan ketika ada permintaan dari pihak yang berwenang. Serangan seperti *Denial of Service* membuat sistem tidak dapat diakses oleh pihak yang berwenang.

2.6. *Email Spoofing* dan *Phising*

Menurut Suryana, Akbar, dan Widiyasono (2016) *Email Spoofing* adalah kegiatan melakukan manipulasi data pada *header email*. Serangan yang paling populer dari *email spoofing* adalah serangan *phising*. *Email spoofing* dianggap sebagai tindakan yang berbahaya, karena melakukan manipulasi data pada *header email* untuk menyamar sebagai orang atau

organisasi yang berwenang, contohnya seperti melakukan pengiriman *email* dengan nama pengirim seolah-olah *email* tersebut dikirim oleh administrator suatu organisasi. Pengirim *email spoofing* menyerang dengan berbagai macam isi pesan untuk meyakinkan korbannya.

Menurut Suryana, Akbar, dan Widiyasono (2016) *Phising* adalah bentuk pencurian identitas secara *online* yang bertujuan untuk mencuri informasi sensitif seperti sandi dan informasi kartu kredit. Serangan *phising* menggunakan kombinasi teknik *social engineering* dan teknik *spoofing* untuk membujuk pengguna agar memberikan informasi sensitif yang dapat digunakan untuk memperoleh keuntungan pribadi, salah satu contohnya adalah keuntungan finansial. *Phiser* biasanya membajak sebuah halaman web dari bank, kemudian mengirim *email* kepada korbannya supaya korbannya mengunjungi situs berbahaya dengan tujuan untuk mengumpulkan informasi rekening bank dan nomor kartu milik korbannya.

2.7. Server

Server adalah sebuah sistem komputer yang menyediakan jenis layanan tertentu dalam sebuah jaringan komputer. Beberapa contoh layanan *server* adalah *DHCP Server*, *DNS Server*, *FTP Server*, *Web Server*, *Mail server*, *Database Server* dan lain-lain (Saputra & Syafrizal, 2012).

2.8. Linux

Menurut Harjono (2016) Linux adalah sebuah aplikasi atau program yang menggunakan kernel sebagai sistem operasi. *Script* pertama Linux dirancang dan ditulis oleh seorang mahasiswa dari Finlandia bernama

"Linus Torvalds" untuk arsitektur Intel 80386. Banyak orang memiliki peran penting dalam mengembangkan dan memperluas Linux di berbagai belahan dunia. Peralatan sistem dan pustakanya umumnya berasal dari sistem operasi GNU yang diumumkan tahun 1983 oleh Richard Stallman. Kontribusi GNU merupakan dasar dari munculnya nama alternatif GNU/LINUX. Dia menggunakan alat proyek GNU dan dengan demikian sistem operasi dikembangkan melalui proyek GNU/LINUX.

2.9. Linux *CentOS*

CentOS merupakan singkatan dari *Community ENTerprise Operating System* yang merupakan sebuah distribusi Linux sebagai bentuk dari usaha untuk menyediakan *platform* komputasi berkelas *enterprise* yang memiliki kompatibilitas kode biner sepenuhnya dengan kode sumber yang menjadi induknya, *Red Hat Enterprise Linux (RHEL)*. *RHEL* merupakan distribusi Linux berbayar yang menyediakan akses update atas perangkat lunak dan beragam jenis dukungan teknis. Distribusi Linux ini sebenarnya merupakan gabungan dari sejumlah perangkat lunak yang didistribusikan di bawah lisensi perangkat lunak yang bebas dan kode sumber atas paket perangkat lunak ini dirilis ke publik oleh *Red Hat*. *CentOS* tersedia secara gratis, dukungan teknis utamanya disediakan terhadap para pengguna melalui *mailing list*, forum berbasis web, ataupun *chat*. Proyek *CentOS* tidak berafiliasi dengan *Red Hat*, sehingga proyek *CentOS* berjalan tanpa mendapatkan bantuan apapun dari *Red Hat*. Untuk penggalangan dana, *CentOS* berbasis donasi dari para pengguna serta sponsor dari perusahaan-perusahaan yang menggunakannya (Wicitra, Utomo, dan Wardana, 2014).

2.10. *Centos Web Panel*

CentOS Web Panel adalah panel kontrol untuk *web hosting* yang dapat digunakan secara gratis dan dirancang untuk memanajemen *VPS* maupun *Dedicated Server* dengan cepat dan mudah tanpa harus menggunakan aplikasi *SSH Client*, menawarkan sejumlah besar opsi dan fitur untuk manajemen *server* dalam paket panel kontrolnya (Control Web Panel, n.d.).

2.11. **Surat Elektronik**

Surat elektronik adalah layanan yang diberikan oleh *internet* yang berkembang sejak tahun 1960, pada saat itu *internet* belum terbentuk, yang ada hanyalah kumpulan *mainframe* yang terbentuk sebagai jaringan. Mulai tahun 1980-an, surat elektronik sudah bisa dinikmati oleh khalayak umum. Surat elektronik adalah salah satu proses pengiriman surat melalui *internet* dengan menggunakan waktu yang sangat singkat. Surat elektronik merupakan salah satu dari sekian banyak layanan *internet* yang ada saat ini selain *Netnews*, *Telnet*, *File Transfer Protokol (FTP)* dan *World Wide Web (www)* dan masih banyak layanan yang lainnya. Layanan *internet* adalah berbagai program atau fasilitas yang disediakan oleh *internet*, dari layanan *internet* tersebut yang paling banyak digunakan adalah layanan surat elektronik. Penggunaan *electronic mail* (surat elektronik) sebagai media komunikasi yang ditunjang oleh banyaknya penyedia layanan di*internet* seperti Yahoo, Google, MSN, Wordpress, dan yang lainnya menunjukkan bahwa banyak orang melakukan komunikasi karena dengan komunikasi orang dapat beraktivitas dan meningkatkan kariernya (Mawarsih, 2014).

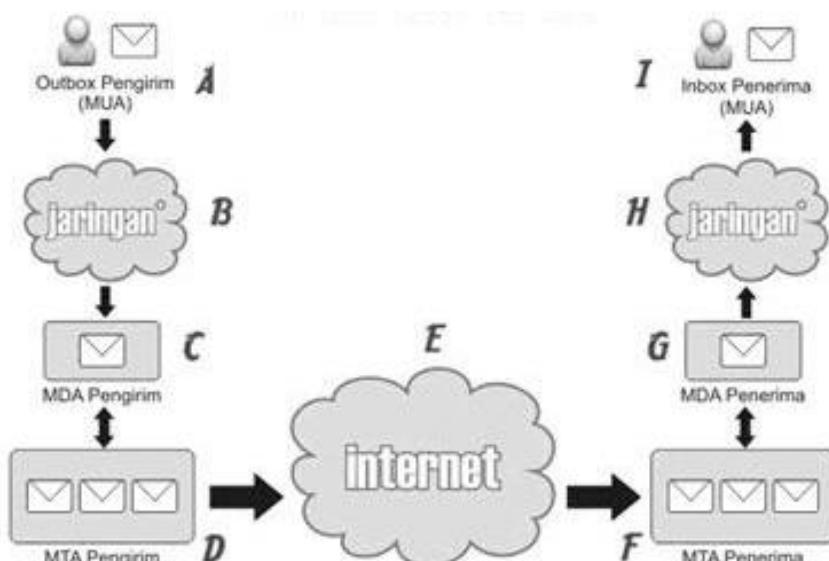
2.12. *Mail Server*

Menurut Desmira, Sumarto, dan Yuliani (2017) *Mail server dikenal sebagai sebuah mail transfer agent atau MTA, mail router atau mailer Internet adalah sebuah aplikasi yang akan menerima email masuk dari pengguna lokal (orang-orang dalam satu domain) dan jarak jauh pengirim dan meneruskan email keluar untuk pengiriman. Sebuah komputer yang didedikasikan untuk menjalankan aplikasi tersebut juga disebut sebagai mail server. Mail Server bisa diartikan sebagai induk atau rumah dari email, Setiap email yang dikirimkan dibuat untuk melewati sejumlah server mail sepanjang perjalanan ke penerima. Untuk user biasa, surat tersebut dikirim langsung tetapi proses adalah sesuatu yang dimengerti. Tanpa rangkaian Server Mail, pengguna hanya akan dapat mengirim email ke orang-orang yang memiliki alamat email dengan domain yang sama.*

Menurut Muarif & Irwan (2017) *Mail Server memiliki tiga komponen utama yang membentuknya, yakni Mail Transfer Agent (MTA), Mail Delivery Agent (MDA), dan Mail User Agent (MUA):*

1. Menurut Sadikin (2014) *Mail User Agent (MUA)* merupakan program yang digunakan oleh pemakai untuk membaca dan mengirim *email* pada komputer pribadinya. Contoh program atau perangkat lunak *Mail User Agent (MUA)* ini misalnya Microsoft Outlook, Microsoft Outlook Express, Lotus Notes, Pegasus Mail dan Thunderbird. *Mail User Agent (MUA)* mengambil *email* dari *email* server menggunakan protokol *Post Office Protocol (POP)* dan *Internet Message Access Protocol (IMAP)*.

2. *Mail Transfer Agent (MTA)* Mail Transfer Agent merupakan salah satu komponen penting pada server internet. Mail Transfer Agent bertanggung jawab untuk mentransfer email dari mail server mengirimkan sampai ke server penerima email. Kebutuhan pengguna atas jenis MTA yang digunakan juga beragam. Berbagai kriteria biasa digunakan untuk pertimbangan. Tiap-tiap program mail server memiliki kelebihan dan kekurangan tersendiri. Beberapa MTA memiliki fasilitas yang sangat hebat sehingga mampu digunakan untuk menangani email dalam jumlah ratusan bahkan sampai ribuan perhari (Desmira, Sumarto, Yuliani, 2017).
3. Menurut Crocker (2009) *Mail delivery agent* atau *message delivery agent* (MDA) adalah komponen perangkat lunak komputer yang bertanggung jawab atas pengiriman pesan email ke kotak pesan penerima lokal.



Gambar 2.3 Proses pengiriman email

Sumber: Pratama, 2008

Pada gambar 2.3 dapat dijelaskan proses pengiriman *email* dimulai dari proses A yaitu pengirim *email* mengirim *email* menggunakan *MUA*, kemudian *email* diteruskan pada *MDA* yang berfungsi untuk mengatur pengiriman *email* pada *mail server* lokal (proses C), jika *email* tersebut dikirim kepada penerima yang berada pada *mail server* yang berbeda maka *email* akan dikirim melalui *MTA* untuk diteruskan ke *mail server* penerima melalui jaringan *internet* (proses E) kemudian *email* tersebut diterima oleh *MTA* pada *mail server* penerima (proses F) dan dilanjutkan ke *MDA mail server* penerima (proses G) agar *email* dapat di unduh oleh penerima *email* melalui jaringan lokal (proses H dan I).

2.13. *Mail Protocol*

Menurut Desmira, Sumarto, dan Yuliani (2017) terdapat tiga *Mail Protocol*, yaitu:

1. *POP3 (Post Office Protocol version 3)*

POP3 merupakan protokol yang digunakan untuk pengelolaan *email*. *POP3* memudahkan seseorang dalam mendapatkan *email* mereka dari sebuah *mail server* tanpa perlu koneksi yang lama dengan *internet* yang tentu saja memakan biaya.

2. *IMAP (Internet Message Access Protocol)*

IMAP (Internet Message Access Protocol) sama halnya dengan *POP3*, maka pesan *email* akan sepenuhnya disimpan dalam *server email* dan menggunakan komputer lokal untuk mengirim dan mengambilnya kapanpun di inginkan. Tergantung dari

keinginan user. IMAP adalah protocol standar untuk mengakses atau mengambil email dari server.

3. SMTP (*Simple Mail Transfer Protocol*)

SMTP merupakan salah satu jenis protocol yang bekerja dalam hal pengiriman pesan-pesan berupa surat elektronik atau email pada sebuah jaringan internet.

2.14. Postfix

Menurut Hidayat (2010) “Postfix adalah *Mail Tranfer Agent* yang dapat diperoleh dengan gratis dan bersifat *open source*. *Postfix* merupakan *mail transfer agent default* untuk sejumlah sistem operasi yang bertipe unix. *Postfix* didistribusikan menggunakan lisensi umum *IBM 1.0* yang merupakan lisensi perangkat lunak bebas tetapi tidak kompatibel dengan *GPL*”.

Menurut Kusmaya (2016) Postfix ditulis oleh Wietse Venema dan termasuk salah satu proyek *freeware*. Mulai digarap Wietse saat berkunjung ke *IBMT. J. Watson Research*. Wietse diberi kesempatan oleh IBM untuk menulis *software* ini. *Original software* tersebut diberi nama Vmailer, namun diganti menjadi *Postfix* atas saran *IBM*.

2.15. Dovecot

Menurut Kusmaya (2016) “Dovecot adalah *open source* server *POP3* dan *IMAP* untuk Linux atau Unix. Program ini melengkapi *Postfix* dengan kinerja yang tinggi, kemudahan administrasi, dan keamanan yang solid. Dovecot merupakan sebuah aplikasi yang dijalankan untuk mengikuti protokol *IMAP* dan *POP3*.

2.16. *Roundcube*

Roundcube adalah solusi *webmail* gratis dan *open source* dengan antarmuka pengguna mirip *desktop* yang mudah dipasang atau dikonfigurasi dan berjalan pada server *LAMPP* standar. Tampilan menggunakan standar web terbaru untuk merender antar muka yang fungsional dan dapat disesuaikan. *Roundcube* menyertakan *library open-source* canggih lainnya seperti *PEAR*, *IMAP* yang berasal dari IlohaMail, pustaka Googiespell untuk pemeriksaan ejaan atau pembersih WasHTML oleh Frederic Motte (*Roundcube Open Source Webmail Software*, n.d.).

2.17. *Domain Name System (DNS)*

Menurut Saputra & Syafrizal (2012) *Domain Name System* adalah sebuah sistem yang menyimpan dan mengatur suatu informasi tentang penamaan *host* dari sebuah alamat *IP* menjadi sebuah karakter atau angka dalam sebuah jaringan internet yang di distribusikan pada *database*. *Domain name system* memiliki pengelolaan komponen inti yang terdiri dari *DNS resolver*, *Recursive DNS server* dan *Authoritative DNS server*. pada awal penggunaan *DNS* didalam jaringan komputer menggunakan *HOSTS.TXT* dari *SRI* (sekarang *SIR International*) yang berisi informasi dari nama komputer dan *IP address*.

2.18. *DNS Server*

Menurut Kusmaya (2016) *DNS server* adalah *distribute database system* yang digunakan untuk pencarian nama komputer di jaringan yang menggunakan *TCP/IP* (*Transmission Control Protocol/Internet Protocol*). *DNS server* biasa digunakan pada aplikasi yang terhubung ke *internet*

seperti *web browser* atau *email*, dimana *DNS server* dapat membantu memetakan *hostname* sebuah komputer ke *IP Address*.

2.19. *Bind9*

BIND9 adalah aplikasi *DNS server* yang paling umum digunakan di *internet*, khususnya di sistem unix, *bind9* merupakan standar *DNS server*. *BIND9* awalnya dibuat oleh empat orang mahasiswa dengan menggunakan CSRG di Universitas California, Berkeley dan pertama kali dirilis di dalam 4.3 BSD. Paul Vixie kemudian meneruskan pemrogramannya pada tahun 1988 saat bekerja di *DEC*. Saat ini, *Bind9* dikelola oleh Konsorsium sistem *internet*. *BIND9* awalnya ditulis pada awal 1980 dan didanai oleh *DARPA* (*Defense Advanced Research Projects Agency*). Pada pertengahan 1980-an, *DEC* (*Digital Equipment Corporation*) mengambil alih pengembangan *BIND9*. Satu dari pekerja itu adalah Paul Vixie, yang terus mengerjakan *BIND9* sesudah meninggalkan *DEC* (Hidayat, 2010).

2.20. *HTTP*

Menurut Zabar dan Novianto (2015) *HTTP* adalah sebuah protokol yang bekerja dengan cara meminta atau menjawab antara *client* dan *server*. Sebuah *client* *HTTP* seperti *web browser*, biasanya memulai permintaan dengan membuat hubungan *TCP/IP* ke *port* tertentu di tuan rumah yang jauh (biasanya *port* 80). Sebuah *server* *HTTP* yang mendengarkan di *port* tersebut menunggu *client* mengirim kode permintaan (*request*), seperti "GET / HTTP/1.1" (yang akan meminta halaman yang sudah ditentukan), diikuti dengan pesan *MIME* yang memiliki beberapa informasi kode kepala yang menjelaskan aspek dari permintaan tersebut

dan diikuti dengan badan dari data tertentu. Beberapa kepala (*header*) juga dapat ditulis atau tidak, sementara yang lainnya (seperti tuan rumah) diperlukan oleh protokol HTTP/1.1. Begitu menerima kode permintaan (dan pesan bila ada), *server* mengirim kembali kode jawaban, seperti "200 OK", dan sebuah pesan yang diminta, atau sebuah pesan *error* atau pesan lainnya. Pengembangan *HTTP* dikoordinasi oleh Konsorsium *World Wide Web* (*W3C*) dan grup kerja *Internet Engineering Task Force* (*IETF*), bekerja dalam publikasi satu seri *RFC*, yang paling terkenal *RFC 2616*, yang menjelaskan *HTTP/1.1*, versi *HTTP* yang umum digunakan sekarang.

2.21. *HTTP Server*

Menurut Syafrizal & Saputra (2012) *HTTP Server* adalah sebuah *software* yang melayani permintaan berupa *Hypertext Transfer Protocol* (*HTTP*) atau *Hypertext Transfer Protocol Secure* (*HTTPS*) dari komputer atau *client* yang terhubung dalam jaringan *internet* atau *intranet*.

2.22. *Apache HTTP Server*

Menurut Syafrizal dan Saputra (2012) *Apache HTTP Server* adalah *web server* yang dapat dijalankan di banyak sistem operasi, seperti *Unix*, *BSD*, *Linux*, *Microsoft Windows* dan *Novell Netware* serta *platform* lainnya yang berguna untuk melayani dan memfungsikan situs web.

2.23. *Email Spam*

Menurut Chandra, Indrawan, dan Sukajaya (2016) *Spam email* dapat didefinisikan sebagai "*unsolicited bulk email*" yaitu *email* yang dikirimkan kepada ribuan penerima. *Spam email* biasanya dikirimkan oleh suatu perusahaan untuk mengiklankan produknya. Hal ini menyebabkan

semakin padatnya antrian dari *mail server*. Banyak waktu yang terbuang untuk menghapus *email spam* dari kotak masuk, *spam* juga menyebabkan pemborosan biaya bagi pengguna yang menggunakan koneksi *dial-up*. Selain itu *spam* juga dapat membuang *bandwidth* dan dapat menyebabkan penerima di bawah umur mengakses situs-situs yang memiliki konten negatif. Banyaknya *spam* menyebabkan kerugian dalam hal sumber daya dan memerlukan banyak waktu untuk menghapusnya.

2.24. *Spam Filter*

Spam filter merupakan *software anti spam*, *Software anti spam* bekerja dengan cara menganalisa *email* yang datang dan menggunakan sejumlah metode untuk menentukan apakah *email* yang diterima adalah *email spam* atau bukan. Keberhasilan *spam filter* dalam mencegah masuknya *email spam* tergantung dari *software anti spam* yang digunakan serta metode-metode yang diterapkan oleh *software anti spam* untuk mendeteksi dan mencegah *email spam* (Fachrurrazi, 2014).

2.27. *SpamAssassin, ClamAV, dan Amavisd-New*

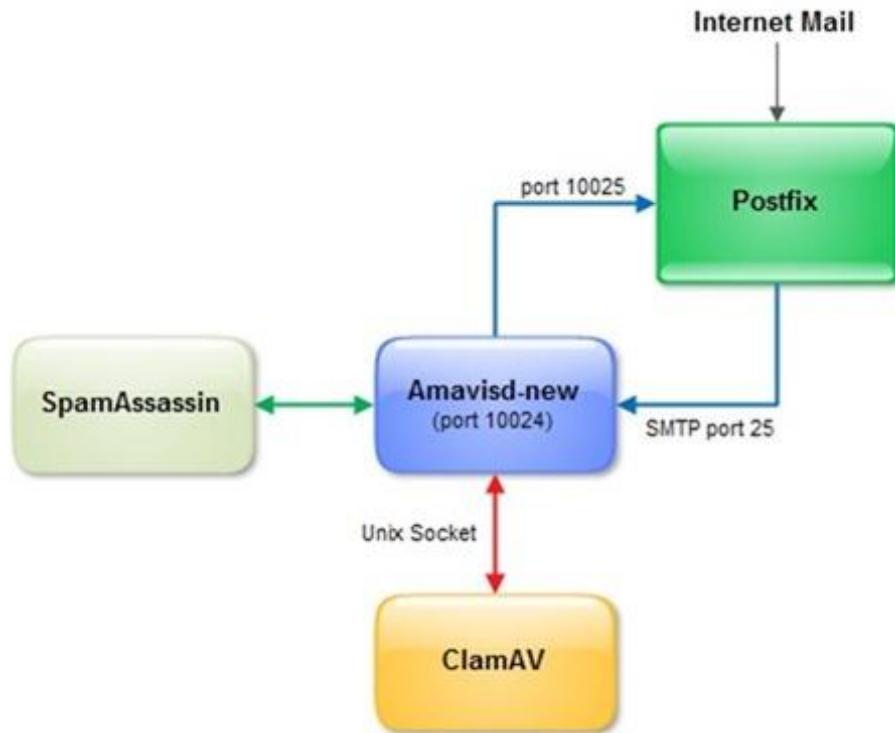
Menurut Irmayana & Nurlina (2014) *SpamAssassin* adalah aplikasi yang sudah teruji secara luas menggunakan proyek *open source* yang berfungsi sebagai *mail filter* untuk mendeteksi *spam*. *SpamAssassin* berjalan pada server dan sebagai *filter spam* sebelum sampai pada kotak masuk pengguna. *SpamAssassin* diintegrasikan dengan *mail server* agar secara otomatis menyaring semua *email spam* dan aturan penggunaan atau tes untuk menentukan *email spam* atau *ham*. *SpamAssassin* dapat memberikan tanda dengan mengubah *subject email* atau langsung menghapus *email spam* yang masuk.

SpamAssassin menggunakan berbagai mekanisme untuk menangani *email spam*, berikut mekanisme yang diterapkan *SpamAssassin*:

1. Pengecekan *header email*.
2. Pengecekan isi *email*.
3. Pengelompokan *email address* secara manual kedalam *whitelist* atau *blacklist*.
4. *Bayesian filtering*.
5. Penyaringan *database spam* kolaboratif (*DCC*, *Pyzor*, dan *Razor2*).
6. Berbasis jaringan seperti *blacklist URL*, *blacklist DNS*, *checksum* berbasis *filter*, dan algoritma *Hash*.

Menurut Kusmaya (2016) *ClamAV* adalah *anti virus open source* (*GPL*) yang dirancang untuk mendeteksi *trojan*, *virus*, *malware*, dan ancaman berbahaya lainnya. Secara *de facto* *ClamAV* adalah standar untuk pemindaian *mail gateway*.

Amavisd-new adalah antarmuka yang memiliki kinerja yang tinggi dan dapat diandalkan. *Amavisd-new* memiliki beberapa fitur seperti pemindai *virus* dan modul *SpamAssassin*. *Amavisd-new* berkomunikasi ke *MTA* melalui protokol *SMTP* atau *LMTP*, atau dengan menggunakan program pembantu (Martinec, 2016).



Gambar 2.4 Cara Kerja *SpamAssassin*, *ClamAV*, dan *Amavisd-New*

Sumber: Valsecchi, 2013

Cara kerja *SpamAssassin*, *ClamAV*, dan *Amavisd-New* dapat dilihat seperti gambar 2.4 yaitu *Amavisd-New* menerima *email* dari *Postfix* (*MTA*), kemudian menyebarkannya ke *ClamAV* dan *SpamAssassin* untuk memeriksa *spam* dan *virus* lalu mengembalikan *email* ke *Postfix* (*MTA*) untuk diteruskan ke penerima *email*.

2.28. *DomainKeys Identified Mail (DKIM)* dan *OpenDKIM*

Domain Keys Identified Mail (DKIM) adalah metode otentikasi *email* yang dirancang untuk mendeteksi *spoofing email*. Ini memungkinkan penerima untuk memeriksa bahwa *email* yang diklaim berasal dari *domain* tertentu memang diotorisasi oleh pemilik domain tersebut. Hal ini dimaksudkan untuk mencegah alamat pengirim palsu dalam *email* yang sering digunakan untuk melakukan *phishing* dan *spam email*. (Hansen, Crocker, Baker, 2009).

Menurut Barovih (2011) *OpenDKIM* adalah pengiriman *email* yang menggunakan mekanisme otentikasi *framework* menggunakan kunci publik yang dimasukan ke dalam *DNS* maupun *email*.



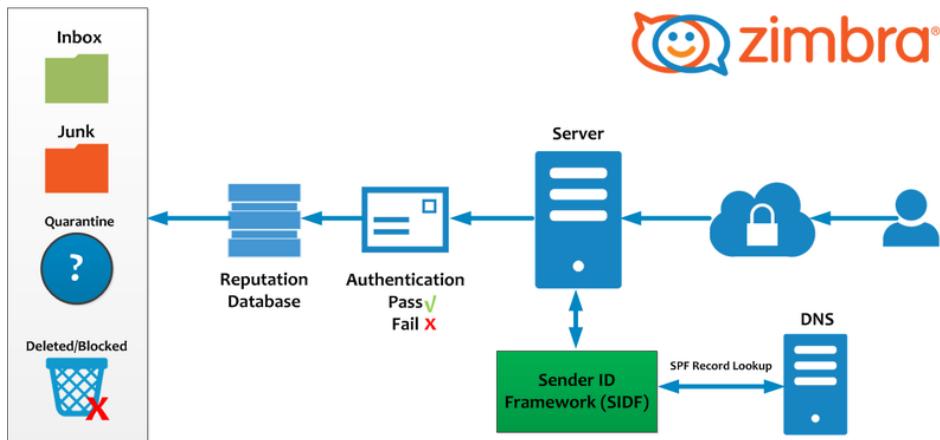
Gambar 2.5 Cara Kerja DKIM
Sumber: Zimbra Incorporation, 2005

Cara kerja *DKIM* dapat dilihat seperti pada gambar 2.5 yaitu *mail* server pengirim mempublish *public key* pada pada *DNS* server pengirim, setiap *email* yang dikirim melalui *mail* server pengirim akan diberikan *private key*, setelah *email* sampai pada *mail* server penerima maka *mail* server penerima akan mencocokan *private key* yang terdapat pada *email* dengan *public key* yang terdapat pada *DNS* server penerima, jika *public* dan *private key* cocok maka *email* tersebut dapat dipastikan berasal dari pengirim yang asli, namun jika *public* dan *private key* tidak cocok maka *email* tersebut dapat dipastikan sebagai *email spoofing*.

2.29. Sender Policy Framework (SPF)

Sender Policy Framework (SPF) adalah sistem validasi *email*, yang dirancang untuk mencegah *email* yang tidak diinginkan menggunakan sistem *spoofing*. Untuk memeriksa masalah keamanan umum ini, *SPF* akan memverifikasi *IP* sumber *email* dan membandingkannya dengan data

TXT DNS dengan konten SPF (*Zimbra Incorporation, Best Practices on Email Protection: SPF, DKIM and DMARC, 2005*).



Gambar 2.6 Cara Kerja SPF
Sumber: *Zimbra Incorporation, 2005*

Cara kerja *SPF* dapat dilihat seperti pada gambar 2.6 yaitu *email* yang dikirim oleh pengirim akan diteruskan pada *mail server* penerima, selanjutnya *mail server* penerima akan mengecek *Sender ID Framework* yang berada pada *DNS* server pengirim, jika alamat *IP* server pengirim *email* sesuai dengan alamat *IP* yang telah diotorisasi oleh *SPF record* pada *DNS* server pengirim *email* maka *email* tersebut akan diberi nilai *PASS*, namun jika alamat *IP* server pengirim *email* tidak sesuai dengan alamat *IP* yang telah diotorisasi oleh *SPF record* pada *DNS* server pengirim *email* maka *email* tersebut akan diberi nilai *FAIL* atau *SOFTFAIL* dan selanjutnya *database reputasi* akan memberi nilai pada *email* tersebut berdasarkan pada laporan *SPF* masing-masing *email* untuk dijadikan pertimbangan tindakan apa yang akan dilakukan pada *email* tersebut.

2.30. *Gmail*

Gmail adalah layanan *email* yang intuitif dan efisien. *Gmail* menyediakan penyimpanan sebesar 15 GB, dengan lebih sedikit *spam*, dan dapat diakses melalui perangkat seluler (*Gmail* .n.d).

2.31. *Emkei's Mailer*

Emkei's Mailer adalah *Mailer* palsu *online* gratis dengan berbagai fitur seperti lampiran, enkripsi, *Editor HTML*, dan pengaturan lanjutan. (*Emkei's Mailer*, 2009).

Emkei's Mailer dapat digunakan untuk mengirim *email spoofing* dengan memalsukan alamat *email* pengirim pesan. *Emkei's Mailer* dapat diakses menggunakan *browser* dengan alamat *domain* www.emkei.cz. *Emkei's Mailer* dapat diakses secara gratis sehingga memberikan kemudahan dalam mengirim *email spoofing*.

2.32. *Yahoo! Mail*

Yahoo! Mail merupakan sebuah penyedia surat elektronik (*webmail*) dari Yahoo!. *Yahoo! Mail* merupakan penyedia surat elektronik terbesar di *internet* dengan jutaan pengguna. Saingan utama *Yahoo! Mail* ialah *Windows Live Hotmail*, *Gmail* dan *AOL Mail* (Arrington, 2006).

BAB III

METODOLOGI DAN PERANCANGAN

Metode penelitian yang digunakan adalah *Network Development Life Cycle* (*NDLC*). Dari enam tahapan yang ada pada *NDLC*, penulis hanya menggunakan 5 tahapan yaitu *Analysis*, *Design*, *Simulation Prototyping*, *Implementation*, dan *Monitoring*.

3.1. Tahap Analisa (*Analysis*)

Pada fase ini penulis melakukan pengumpulan data dengan cara studi literatur, yaitu penulis membaca artikel ilmiah, buku, dan jurnal untuk mendapatkan informasi mengenai *email spam*, *email spoofing*, dan *virus*. Data-data yang telah terkumpul kemudian dianalisa. Tahap ini terdiri dari dua bagian yaitu pengumpulan data dan analisa data.

3.1.1. Pengumpulan Data

Pada tahap pengumpulan data, penulis menggunakan metode studi literatur yaitu dengan mempelajari beberapa jurnal ilmiah yang membahas tentang *email spam*, *email spoofing*, dan *virus*, selain itu penulis juga menggunakan e-book yang membahas tentang *email spam*, *virus*, dan *email spoofing*. Setelah membaca beberapa jurnal ilmiah diperoleh informasi tentang beberapa jurnal ilmiah yang berkaitan dengan *email spam*, *virus*, dan *email spoofing* seperti terlihat pada tabel 3.1 berikut.

Tabel 3.1 Jurnal Ilmiah Tentang *Email Spam*, *Spoofing*, dan *Virus*

No	Penulis	Tahun	Judul	Pembahasan
1	Andri Lesmana Suryana, R. Reza El Akbar, dan Nur Widiyasono	2016	Investigasi <i>Email Spoofing</i> dengan Metode <i>Digital Forensics</i>	Mengidentifikasi <i>email spoofing</i> menggunakan

			<i>Research Workshop (DFRWS)</i>	metode <i>DFRWS</i>
2	Hoiriyah, Bambang Sugiantoro, dan Yudi Prayudi	2016	Investigasi Forensik pada <i>E-mail Spoofing</i> menggunakan Metode <i>Header Analysis</i>	Membuat algoritma untuk membandingkan <i>header email spoofing</i> dan <i>email legitimate</i>
3	Nurlina dan Irmayana	2014	Studi Banding <i>Spam-Assassin Mail Server</i> Dengan dan Tanpa <i>Filter</i> di Sisi <i>Mail Client</i>	Membandingkan metode pengklasifikasi <i>email spam</i> dengan dan tanpa <i>filter</i> di sisi <i>client</i> menggunakan metode <i>naive bayes</i> dan <i>spamassassin</i>
4	Wirawan Nathaniel Chandra, Gede Indrawan, dan I Nyoman Sukajaya	2016	<i>Spam Filtering</i> Dengan Metode <i>Pos Tagger</i> dan Klasifikasi <i>Naive Bayes</i>	Memfilter kata penting pada email menggunakan metode <i>Pos Tagger</i> untuk dijadikan pembelajaran pada klasifikasi <i>Naive Bayes</i>
5	Ratih Yulia Hayuningtyas	2017	Aplikasi <i>Filtering of Spam Email</i> Menggunakan <i>Naive Bayes</i>	Membuat aplikasi <i>Mail User Agent</i> yang dapat memfilter <i>spam</i> dengan metode <i>Naive Bayes</i>

3.1.2. Analisa Data

Berdasarkan hasil dari pengumpulan data maka dapat diperoleh hasil analisa sebagai berikut:

1. Jurnal ilmiah pertama membahas tentang investigasi *email spoofing* menggunakan metode *DFRWS* yaitu dengan melakukan pengecekan *header email* secara manual.
2. Jurnal ilmiah kedua membahas tentang investigasi *email spoofing* menggunakan metode *header analysis* untuk menemukan pola *header email spoofing* kemudian membuat algoritma untuk mengklasifikasikan *email spoofing* dan *email legitimate*.
3. Jurnal ilmiah ketiga membahas tentang penerapan algoritma *naive bayes* disisi *client* yang akan meningkatkan akurasi pendekripsi *email spam* sebesar 99,98%.
4. Jurnal ilmiah keempat membahas tentang pemfilteran kata penting pada email menggunakan metode Pos Tagger untuk dijadikan pembelajaran pada klasifikasi Naive Bayes.
5. Jurnal ilmiah kelima membahas tentang pembuatan aplikasi *Mail User Agent* yang dapat memfilter *spam* dengan metode *Naive Bayes*.
6. Penanganan *email spoofing* belum menerapkan metode otentikasi dan otorisasi untuk menambah informasi pada *email header*.
7. Belum terdapat uji coba *ClamAV* sebagai *anti virus* pada *mail server*.

Dari hasil analisa tersebut maka mendorong penulis untuk melakukan penelitian tentang Analisa penerapan *Domainkeys Identified*

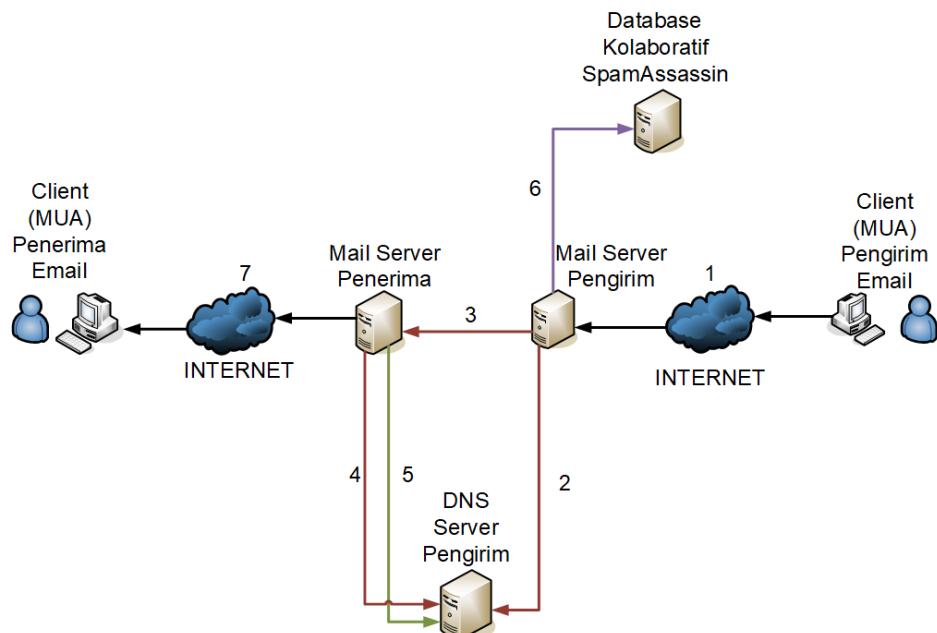
mail (DKIM), sender policy framework (SPF) Anti Spam, dan Anti Virus pada Mail Server.

3.2. Tahap Desain (*Design*)

Tahap ini terdiri dari 4 (empat) bagian yaitu rancangan sistem *filtering email spam, virus, dan spoofing*, rancangan jaringan ujicoba, rancangan pengalamanan *IP*, rancangan akun *email*, serta kebutuhan perangkat keras dan perangkat lunak.

3.2.1 Rancangan Sistem *Filtering Email Spam, Virus dan Spoofing*

Rancangan sistem *filtering email spam, virus dan spoofing* yang digunakan seperti terlihat pada gambar 3.1 berikut.



Gambar 3.1 Rancangan Sistem *Filtering Email Spam, Spoofing, dan Virus*

Berdasarkan gambar 3.1 tersebut maka rancangan sistem *filtering email spam, virus dan email spoofing* dapat dijelaskan sebagai berikut.

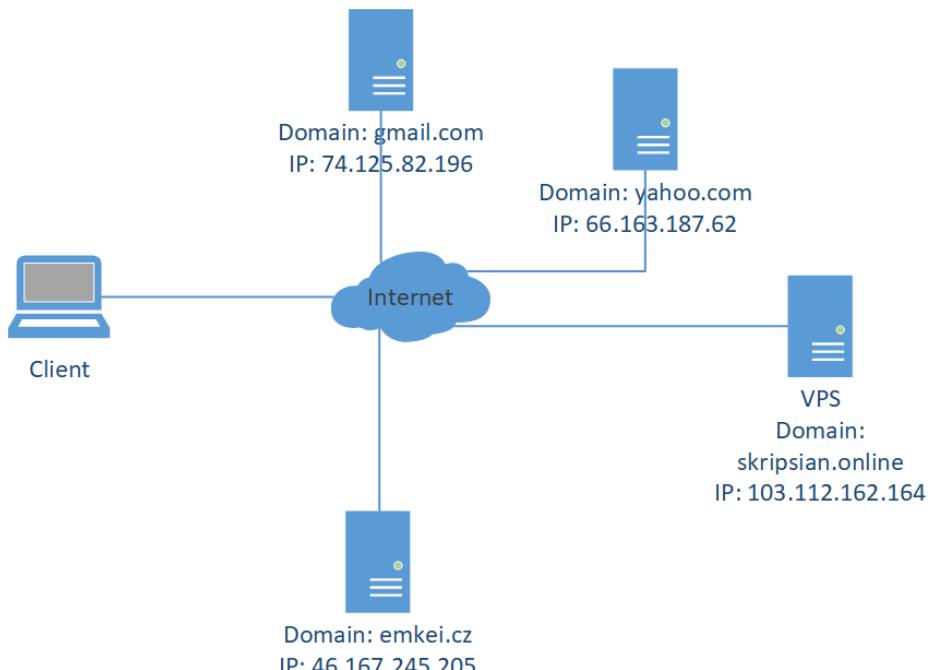
- a. Langkah 1 *user* mengirim *email* dengan menggunakan *Mail User Agent* berbasis web (*Roundcube*), *user* mengakses *Roundcube* menggunakan *browser*.
- b. Langkah 2 *Mail server* pengirim meneruskan *email* ke *mail server* penerima dengan menambahkan *private key* pada *header email*.
- c. Langkah 3 *Mail server* pengirim mempublish *public key* pada *DNS servemya*.
- b. Langkah 4 *Mail server* penerima mengambil *public key* yang ada pada *DNS server* pengirim *email* untuk dicocokan dengan *private key* yang ada pada *header email*, jika *private key* tidak cocok dengan *public key* maka *email* akan dianggap sebagai *email spam*, jika *private key* cocok dengan *public key* maka proses akan berlanjut pada langkah ke 5.
- c. Langkah 5 *Mail server* penerima mencocokan alamat *IP mail server* pengirim dengan *sender ID framework* pada *SPF record* yang berada pada *DNS server* pengirim, jika pada *SPF record* yang berada pada *DNS server* pengirim tidak mengotorisasi alamat *IP email server* pengirim *email* tersebut maka *email* tersebut akan diblok atau ditandai sebagai *spam*, jika alamat *email* pengirim telah diotorisasi oleh *administrator email server* maka proses akan berlanjut pada proses ke 6.
- d. Langkah 6 *Mail server* penerima melakukan pengecekan pada *database kolaboratif SpamAssassin*.
- e. Proses pemfilteran *email spam* selanjutnya adalah menggunakan *SpamAssassin* dan *ClamAV* sebagai *anti spam*

dan *anti virus email* dengan *Amavisd-New* sebagai penghubung antara *SMTP server* dengan *SpamAssassin* dan *ClamAV*.

Keterangan: garis merah mewakili proses *DKIM* (nomor 2, 3, dan 4), garis hijau mewakili proses *SPF* (nomor 5), dan garis ungu mewakili proses *SpamAssassin* (nomor 6).

3.2.2 Rancangan Jaringan Uji Coba

Rancangan jaringan uji coba yang digunakan seperti terlihat pada gambar 3.2 berikut.



Gambar 3.2 Rancangan Topologi Uji Coba

Rancangan ini diimplementasikan menggunakan *VPS* yang disewa pada penyedia layanan *VPS* dan pada *VPS* telah terinstal sistem operasi *CentOS Linux release 7.3.1611*, *VPS* yang telah disewa diberikan satu alamat *IP public* oleh penyedia layanan *VPS* yaitu 103.112.162.164. Pada *VPS* akan dilakukan instalasi *CentOS Web Panel*, konfigurasi *DNS server*, konfigurasi *Mail server*, dan pada komputer *client* telah terinstal sistem

operasi windows 10 dan aplikasi browser Google Chrome untuk mengakses *Mail User Agent* berbasis web (Roundcube).

3.2.3 Rancangan Pengalamatan IP

Pengalamatan IP merupakan salah satu bagian yang penting karena merupakan suatu identitas pengalamatan suatu *interface*. Berikut adalah pengalamatan IP pada masing-masing *interface* agar dapat saling berkomunikasi antar perangkat yang terhubung. Pengalamatan IP dapat dilihat seperti pada tabel 3.2 berikut.

Tabel 3.2 Pengalamatan IP

No	Perangkat	IP Address	Network	Interface
1	DNS Server, HTTP Server, SMTP Server, POP3/IMAP Server (VPS)	103.112.162.228/25	103.112.162.128	eth0
2	Client	DHCP	DHCP	-

3.2.4 Rancangan Akun Email

Berikut adalah kebutuhan akun *email* untuk mendukung apa yang akan dilakukan dalam membangun atau mempersiapkan implementasi seperti terlihat pada tabel 3.3 berikut.

Tabel 3.3 Kebutuhan Akun Email

No	Alamat Email	Domain
1	naufalhanif1477.nh@gmail.com	gmail.com
2	naufalhanif74@yahoo.com	yahoo.com
3	hendarto@skripsi.ononline	skripsi.ononline
4	hendarto@ridho.org	ridho.org
5	yunita@skripsi.ononline	skripsi.ononline
6	naufalhanif@skripsi.ononline	skripsi.ononline

3.2.5 Kebutuhan Perangkat Keras dan Perangkat Lunak

Berikut adalah kebutuhan perangkat keras dan perangkat lunak untuk mendukung apa yang akan dilakukan dalam membangun atau mempersiapkan implementasi yaitu:

1. Kebutuhan Perangkat Keras

Satu unit VPS dengan spesifikasi seperti terlihat pada tabel 3.4 berikut.

Tabel 3.4 Spesifikasi VPS

Komponen	Spesifikasi
CPU	Virtual CPU a7769a6388d5 1 Core (2400 MHz)
RAM	1 GB
Hard Drive	25 GB

Satu unit laptop dengan spesifikasi seperti terlihat pada tabel 3.5 berikut.

Tabel 3.5 Spesifikasi Client

Komponen	Spesifikasi
CPU	Intel Core i3-7100U, 2.4GHz
RAM	4 GB
Hard Drive	1 TB

2. Kebutuhan Perangkat Lunak

Adapun perangkat lunak yang dibutuhkan adalah sebagai berikut:

- a. *Linux CentOS release 7.3.1611* sebagai sistem operasi VPS.

- b. *CentOS Web Panel* sebagai *tool* untuk memudahkan dalam melakukan konfigurasi server.
- c. Dovecot sebagai *Mail Delivery Agent*.
- d. Postfix sebagai *Mail Transfer Agent*.
- e. Roundcube sebagai *Mail User Agent*.
- f. Apache sebagai web server.
- g. Bind9 sebagai *DNS server*.
- h. Microsoft Windows 10 sebagai sistem operasi *client*.
- i. Google Chrome sebagai *browser client* untuk mengakses *Roundcube*.

3.3. Tahap Simulasi (*Prototyping*)

Tahap ini terdiri dari 2 bagian yaitu instalasi dan konfigurasi pada VPS dan *client* serta melakukan uji coba menggunakan berbagai skenario dan memverifikasi hasil uji coba tersebut.

Uji coba pertama dilakukan dengan mengirim *email spoofing* melalui *Emkei's Mailer* dengan mengatasnamakan salah satu *user* yang berada pada *domain* skripsi.ononline kemudian mengirim *email spoofing* tersebut ke *mail server Gmail*, *Yahoo! Mail*, dan skripsi.ononline sebelum dan setelah penerapan *DKIM* dan *SPF* pada *mail server* skripsi.ononline.

Uji coba kedua dilakukan untuk menguji kinerja *Anti Spam* pada *mail server* skripsi.ononline dengan mengirim *email spam* melalui *Emkei's Fake Mailer*, *Gmail*, dan *Yahoo! Mail* kemudian mengirim *email spam* tersebut ke salah satu *user* yang berada pada *mail server* skripsi.ononline sebelum dan setelah penerapan *SpamAssassin*.

Uji coba ketiga dilakukan untuk menguji kinerja *anti virus* pada *mail server* skripsiian.online dengan cara mengirim *email* yang mengandung *virus* melalui *Emkei's Fake Mailer*, *Gmail*, dan *Yahoo! Mail* ke salah satu *user* yang ada pada *mail server* skripsiian.online sebelum dan setelah penerapan *ClamAV*.

Uji coba ketiga dilakukan dengan cara membandingkan *header email* yang dikirim oleh salah satu *user* yang berada pada *mail server* skripsiian.online ke *Gmail*, *Yahoo! Mail*, dan skripsiian.online sebelum dan setelah penerapan *DKIM*, *SPF*, *Anti Spam*, dan *Anti Virus*.

3.3.1. Instalasi Dan Konfigurasi

Instalasi dan konfigurasi *DKIM*, *SPF*, *Anti Spam*, dan *Anti Virus* dilakukan pada *VPS* yang berfungsi untuk memfilter *email spam* dan *virus* yang masuk serta untuk mencegah adanya *email spoofing* yang mengatasnamakan skripsiian.online, sedangkan pada komputer *client* sudah terinstal sistem operasi Windows 10 dan browser Google Chrome untuk mengakses *Mail User Agent* berbasis web (Roundcube), *client* harus terkoneksi dengan jaringan *internet* agar dapat mengakses *Mail User Agent* yang telah disediakan oleh *mail server* skripsiian.online.

3.3.2. Uji Coba

Pada tahap ujicoba ini tediri dari 2 bagian yaitu verifikasi konfigurasi dan ujicoba menggunakan berbagai skenario. Verifikasi konfigurasi dilakukan untuk memverifikasi fungsi *DNS server* dan *Mail server* dengan melakukan *nslookup* untuk memverifikasi fungsi *DNS server* dan melakukan pengiriman *email* antar pengguna yang berada pada *mail server* yang telah dibangun serta melakukan pengiriman *email* dari server

yang telah dibangun ke *email server* yang lainnya untuk memverifikasi fungsi *Mail server*. Sedangkan skenario ujicoba yang dilakukan meliputi pembuatan skenario yang terdiri dari beberapa skenario seperti uji coba sebelum diterapkannya *filtering email spam*, *virus*, dan *spoofing*, serta ujicoba sesudah diterapkannya *filtering email spam*, *virus* dan *spoofing*.

3.4. Tahap Implementasi

Tahap implementasi merupakan tahap penerapan sistem yang sudah dirancang, agar sistem yang telah dirancang dapat dioperasikan dan digunakan secara optimal sesuai dengan kebutuhan. Selain tahap implementasi akan dilakukan pengujian terhadap sistem yang baru dan akan dilihat kekurangan-kekurangan pada sistem yang baru untuk pengembangan sistem selanjutnya. Pada fase ini penulis akan membangun sebuah *mail server* kemudian pada *mail server* tersebut akan diterapkan *DKIM*, *SPF*, *Anti Spam* dan *Anti Virus* untuk memfilter, mengotorisasi, dan mengotentikasi *email*, kemudian penulis akan melakukan analisa pada *mail server* sebelum dan sesudah penerapan *DKIM*, *SPF*, *Anti Spam*, dan *Anti Virus*.

3.5. Tahap *Monitoring*

Setelah melakukan implementasi, tahapan *monitoring* adalah tahapan penting dalam merancang desain jaringan, tujuan dari tahapan *monitoring* adalah untuk memastikan jaringan komputer berjalan sesuai dengan tujuan pada tahap analisis. Pada fase ini penulis akan melakukan *monitoring* terhadap aktifitas *spam* pada *mail server* skripsi.ononline dengan menggunakan *maillog server* skripsi.ononline serta melakukan

monitoring terhadap aktifitas *spoofing* pada layanan *email* *Yahoo! Mail*, *Gmail*, dan skripsi. online.

BAB IV

HASIL DAN PEMBAHASAN

Bab ini memuat tentang pembahasan dari hasil instalasi dan konfigurasi, uji coba dan analisa 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*.

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 103.112.162.228 dengan sistem operasi Linux *CentOS release 7.3.1611*, pada *VPS* telah terinstal *SSH Server* agar *VPS* dapat diakses melalui perangkat lain melalui jaringan *internet* seperti terlihat pada gambar 4.1 berikut.

```
[root@nsl ~]# rpm --query centos-release  
centos-release-7-3.1611.el7.centos.x86_64
```

Gambar 4.1 Linux CentOS release 7.3.1611

4.1.1.1. 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.

```

root@ns1:/usr/local/src
#####
#      CWP Installed      #
#####

go to CentOS WebPanel Admin GUI at http://SERVER_IP:2030/
http:// 103.112.162.228 :2030
SSL: https:// 103.112.162.228 :2031
-----
Username: root
Password: ssh server root password
MySQL root Password: tIn8FxrjbQ71

#####
#      CentOS Web Panel MailServer Installer      #
#####
SSL Cert name (hostname): ns1.skripsiian.online
SSL Cert file location /etc/pki/tls/ private/certs
#####

visit for help: www.centos-webpanel.com
Write down login details and press ENTER for server reboot!
Press ENTER for server reboot!

```

Gambar 4.2 Hasil Instalasi CWP

4.1.1.2. 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 hanya menambahkan parameter `DNS1="103.112.162.228"` yang berada pada baris 17 yang berfungsi agar VPS menjadi *DNS server*, parameter lain yang perlu ditambahkan adalah `DOMAIN="skripsiian.online"` yang berada pada baris 18 yang bertujuan agar skripsiian.online menjadi domain VPS seperti te dilakukan pada *file ifcfg-eth0* dengan perintah `#nano`

/etc/sysconfig/network-scripts/ifcfg-eth0 seperti terlihat pada gambar 4.3 berikut.

```
1  TYPE="Ethernet"
2  BOOTPROTO="none"
3  DEFROUTE="yes"
4  IPV4_FAILURE_FATAL="no"
5  IPV6INIT="yes"
6  IPV6_AUTOCONF="yes"
7  IPV6_DEFROUTE="yes"
8  IPV6_FAILURE_FATAL="no"
9  IPV6_ADDR_GEN_MODE="stable-privacy"
10 NAME="eth0"
11 UUID="14360a85-09f4-45ef-824c-a0c8b5cb0b1f"
12 DEVICE="eth0"
13 ONBOOT="yes"
14 IPADDR="103.112.162.228"
15 PREFIX="25"
16 GATEWAY="103.112.162.129"
17 DNS1="103.112.162.228"
18 DOMAIN="skripsiian.online"
19 IPV6_PEERDNS="yes"
```

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.

Edit Name Servers

Name Server 1:	ns1.skripsi.online	103.112.162.228
	Enter NS1 SubDomain, example: ns1.centos-webpanel.com	
Name Server 2:	Enter NS2 SubDomain	Enter NS2 IP Adc
	Enter NS2 SubDomain, example: ns2.centos-webpanel.com	
Options:	<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	
Save changes		

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.

CWP6.admin

Load: 0.00 0.00 0.00

add_domain

Add Domain

Path must be /home/USERNAME eg. /home/mywebsite/...
If you enter / than 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 Domain:	skripsi.online
Enter domain name without www.	
to User:	naufal
Select user to which you want to add this domain	
Folder Path:	/public_html
Enter path to a folder in user homedir	
<input type="checkbox"/> 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 skripsi.online.db, pada baris 8 terdapat record @ IN A 103.112.162.228 yang berfungsi untuk memetakan nama *host* ke alamat *IP*, pada baris 9 terdapat record @ IN NS ns1.skripsi.online. yang berfungsi untuk memetakan sebuah nama *domain* ke dalam satu daftar dari *server DNS* untuk *domain* skripsi.online, pada baris 10 terdapat record @ IN MX 10 ns1.skripsi.online. yang berfungsi untuk memetakan sebuah nama *domain* ke dalam daftar *mail exchange server* untuk *domain* skripsi.online, pada baris 12 sampai 14 merupakan record CNAME atau *Canonical Name* yang berfungsi agar nama *domain* skripsi.online dapat diakses menggunakan nama alias www.skripsi.online, ftp.skripsi.online, dan mail.skripsi.online seperti terlihat pada gambar 4.6 berikut.

```

1 $TTL 86400
2 @ IN SOA ns1.skripsi.online. root.ns1.skripsi.online. (
3 | | | | | 2009052100 ; serial (d. adams)
4 | | | | | 3H ; refresh
5 | | | | | 15M ; retry
6 | | | | | 1W ; expiry
7 | | | | | 1D ) ; minimum
8 @ IN A 103.112.162.228
9 @ IN NS ns1.skripsi.online.
10 @ IN MX 10 ns1.skripsi.online.
11
12 www IN CNAME skripsi.online.
13 mail IN CNAME skripsi.online.
14 ftp IN CNAME skripsi.online.

```

Gambar 4.6 File skripsi.online.db

Untuk dapat memetakan alamat *IP* ke nama *domain* maka perlu dibuat *file reverse-lookup zone* pada terminal dengan perintah #nano /var/named/named.ip4.skripsi.online.db. pada baris 8 terdapat record @ IN NS ns1.skripsi.online. yang berfungsi untuk memetakan sebuah nama

domain ke dalam satu daftar dari server *DNS* untuk *domain* skripsi.ononline, pada baris 9 dan 10 terdapat *record pointer* yang berfungsi untuk memetakan nama *domain* ke dalam alamat *IP* seperti terlihat pada gambar 4.7 berikut.

```

1  $TTL 86400
2  @ IN SOA ns1.skripsi.ononline. root.ns1.skripsi.ononline. (
3      . . . . . 2009052100 ; Serial
4      . . . . . 28800 ; Refresh
5      . . . . . 14400 ; Retry
6      . . . . . 3600000 ; Expire
7      . . . . . 86400 ) ; Minimum
8  @ IN NS ns1.skripsi.ononline.
9  228 IN PTR skripsi.ononline.
10 228 IN PTR ns1.skripsi.ononline.|
```

Gambar 4.7 File named.ip4.skripsi.ononline.db

Pada file named.conf ditambahkan perintah pada baris 2 yaitu zone "skripsi.ononline" adalah nama *domain* yang akan digunakan, baris 3 yaitu type master adalah tipe *DNS server* yaitu *primary DNS*, baris 4 adalah lokasi *file forward zone*, kemudian pada baris 6 yaitu zone "162.112.103.in-addr.arpa" IN adalah lingkup *network* dalam *domain* yang akan digunakan sebagai *reverse*, baris 7 yaitu type master adalah tipe *DNS server* yaitu primary DNS, baris 8 adalah lokasi *file reverse zone*, setelah semua konfigurasi selesai ketikan perintah #service named restart untuk merestart *DNS server*. Seperti terlihat pada gambar 4.8 berikut.

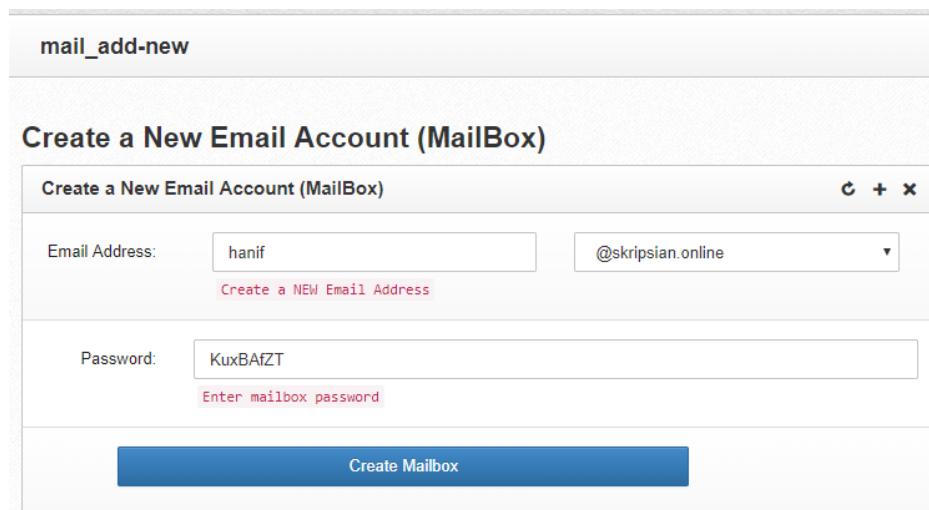
```

1 // zone skripsi.ononline
2 zone "skripsi.ononline" {
3     type master;
4     file "/var/named/skripsi.ononline.db"; };
5 // zone_end skripsi.ononline
6 zone "162.112.103.in-addr.arpa" IN {
7     type master;
8     file "named.ip4.skripsi.ononline.db"; };|
```

Gambar 4.8 File named.conf

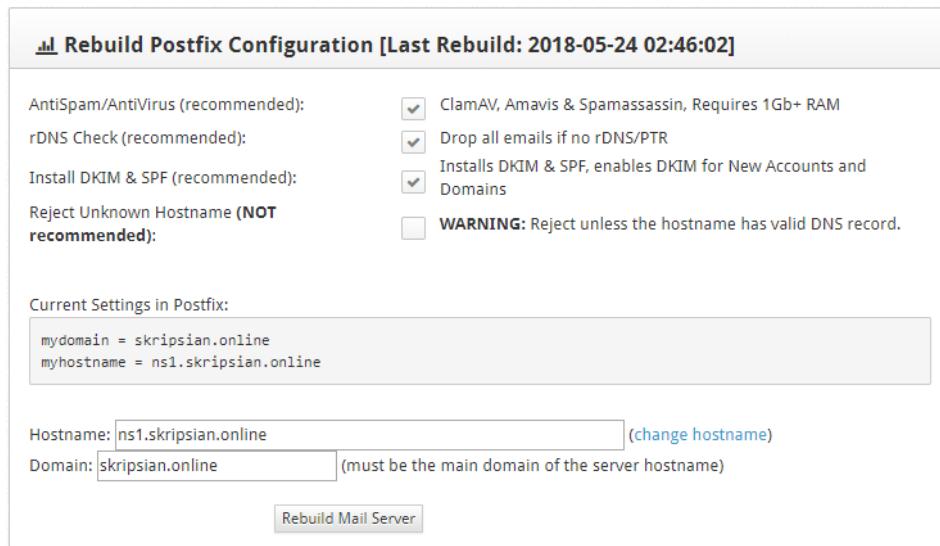
4.1.1.3. Hasil Konfigurasi *Mail Server*

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.



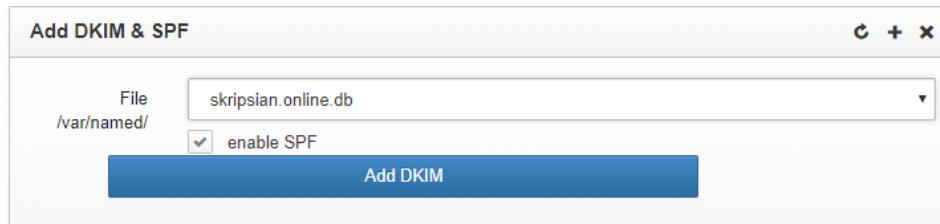
Gambar 4.9 Membuat Akun *Email*

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.



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.



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.

Add SPF Record

SPF records will be added in a DNS Zone file.

Select Domain:	skripsi.online
Allow servers listed as MX to send email for this domain:	Yes (recommended) ▾
Allow current IP address of the domain to send email for this domain:	Yes (recommended) ▾
Allow any hostname in this domain to send email for this domain:	No (recommended) ▾
IP addresses in CIDR format that deliver or relay mail for this domain:	<input type="text" value="103.112.162.228/32"/>
Add any other server hostname that may deliver or relay mail for this domain:	<input type="text" value="ns1.skripsi.online"/>
Any domains that may deliver or relay mail for this domain:	<input type="text"/>
How strict should be the servers treating the emails?:	Fail (Not compliant will be rejected) ▾
<input type="button" value="Add SPF Record"/>	

Gambar 4.12 Menambah SPF Record pada File Zone

Pada file skripsi.online.db akan terlihat tambahan dua baris dibagian paling bawah seperti terlihat pada gambar 4.13 berikut.

```

1 default._domainkey 14400 IN TXT "v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBg
2 QD0ukw3mQfcJGNKt/pkg3Buc+1/N5QsM9A/K4I7iw2JHQ2mIyaiCxkc5zvQLzO2P5Rz7nrGDIzrwHj7efonwU4en
3 VMMwdPlJppVS+TZXc+yP4H4ykq2a5tWefvk9oVluyje6+CLDziIMBhk6IgUOHuinXtoIB1NHaTwinem9eHwIDAQAB"
4
5 skripsi.online. IN TXT "v=spf1 mx a ip4:103.112.162.228/32 a:ns1.skripsi.online -all"
```

Gambar 4.13 DKIM dan SPF Record

Pada baris 1 skripsi.online.IN TXT "v=spf1 mx a ip4:103.112.162.228/32 a:ns1.skripsi.online -all" merupakan record SPF, v=spf1 berarti versi SPF yang digunakan adalah SPF versi, a:ns1.skripsi.online berarti hanya mengizinkan pengiriman *email* dengan *hostname* ns1.skripsi.online, ip4:103.112.162.228/32 yang berarti hanya mengizinkan pengiriman email dari server dengan alamat IP

103.112.162.228, -all berarti menolak semua *email* yang tidak sesuai dengan aturan tersebut.

Pada baris 2 adalah *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.

Agar ns1.skripsiian.online menjadi *host* yang dipercaya maka harus ditambahkan *hostname* pada baris 2 pada *file TrustedHosts* diberi yang paling bawah dengan perintah #nano /etc/opendkim/TrustedHosts seperti pada gambar 4.14 berikut.

```
1 #host.example.com
2 ns1.skripsiian.online
```

Gambar 4.14 Konfigurasi *File TrustedHosts*

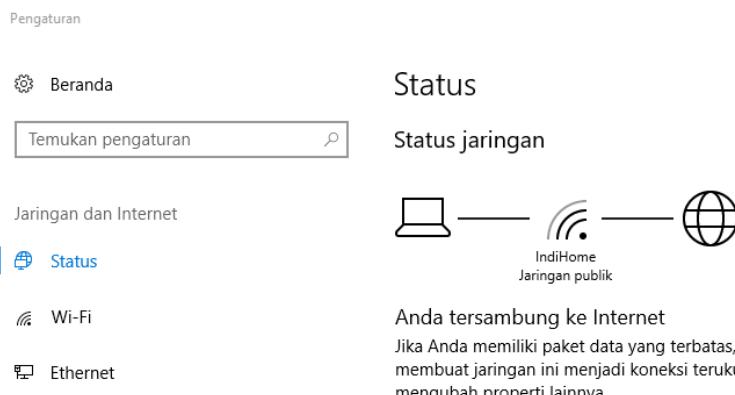
Pada *file main.cf* ditambahkan beberapa parameter seperti smtpd_milters = inet:127.0.0.1:8891, non_smtpd_milters = \$smtpd_milters, milter_default_action = accept, dan milter_protocol = 2 yang terdapat pada baris 1 sampai 4 yang berfungsi untuk memfilter *email*, seperti terlihat pada gambar 4.15 berikut.

```
1 smtpd_milters = inet:127.0.0.1:8891
2 non_smtpd_milters = $smtpd_milters
3 milter_default_action = accept
4 milter_protocol = 2
```

Gambar 4.15 Konfigurasi *File main.cf*

4.1.2. Hasil Konfigurasi Client

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

Pada tahap uji coba ini terdiri dari 2 bagian yaitu verifikasi konfigurasi dan uji coba menggunakan berbagai macam skenario.

4.2.1. Verifikasi Konfigurasi

Berikut ini adalah hasil verifikasi konfigurasi yang telah dilakukan sebelumnya untuk mengetahui apakah hasil konfigurasi yang dilakukan sebelumnya berhasil atau tidak.

4.2.1.1. Verifikasi Konfigurasi *DNS Server*

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@nsl ~]# nslookup skripsi.online
Server:      103.112.162.228
Address:     103.112.162.228#53

Name:   skripsi.online
Address: 103.112.162.228

[root@nsl ~]# nslookup ns1.skripsi.online
Server:      103.112.162.228
Address:     103.112.162.228#53

Name:   ns1.skripsi.online
Address: 103.112.162.228

[root@nsl ~]# nslookup www.skripsi.online
Server:      103.112.162.228
Address:     103.112.162.228#53

www.skripsi.online    canonical name = skripsi.online.
Name:   skripsi.online
Address: 103.112.162.228

[root@nsl ~]# nslookup mail.skripsi.online
Server:      103.112.162.228
Address:     103.112.162.228#53

mail.skripsi.online  canonical name = skripsi.online.
Name:   skripsi.online
Address: 103.112.162.228

[root@nsl ~]# nslookup 103.112.162.228
Server:      103.112.162.228
Address:     103.112.162.228#53

228.112.103.in-addr.arpa    name = skripsi.online.
228.112.103.in-addr.arpa    name = ns1.skripsi.online.

[root@nsl ~]# host -t mx skripsi.online
skripsi.online mail is handled by 0 skripsi.online.
```

Gambar 4.17 Verifikasi Konfigurasi *DNS Server*

4.2.1.2. Verifikasi Konfigurasi *Mail Server*

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.

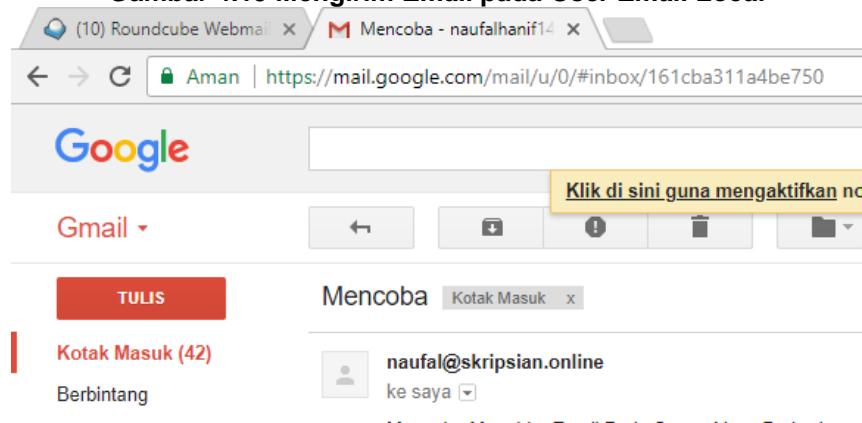
```
[root@nsl ~]# service dovecot status
dovecot (pid  4169) is running...
[root@nsl ~]# service postfix status
master (pid  7064) is running...
[root@nsl ~]#
```

Gambar 4.18 Verifikasi Konfigurasi Mail Server

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.

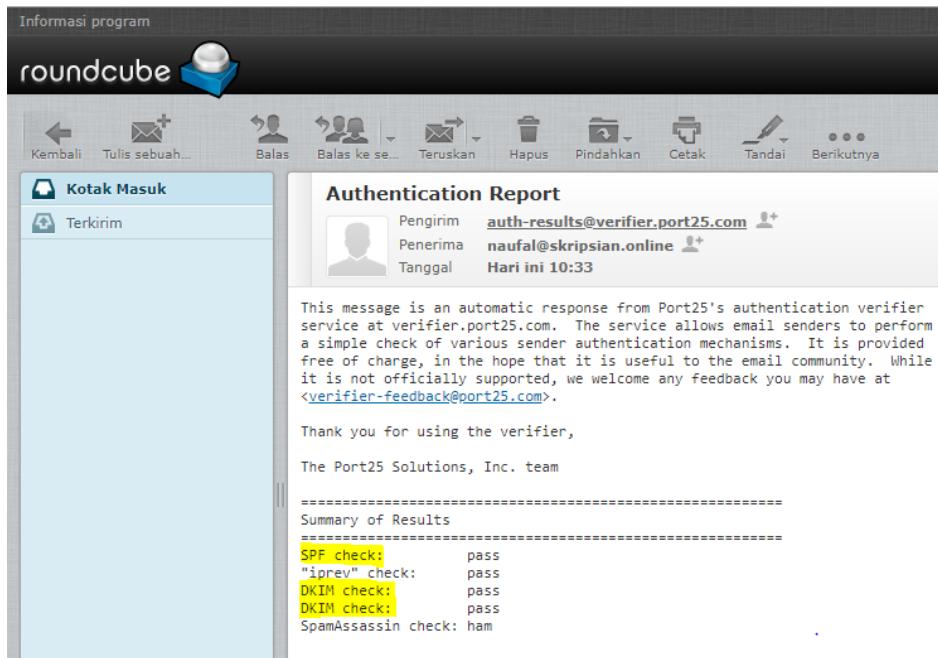


Gambar 4.19 Mengirim Email pada User Email Local



Gambar 4.20 Mengirim Email Pada Mail Server Lain

Verifikasi fungsi *DKIM*, *SPF* dan *SpamAssassin* dapat dilakukan dengan cara mengirim email ke alamat check-auth@verifier.port25.com seperti pada gambar 4.21 berikut.



Gambar 4.21 Verifikasi Fungsi DKIM, SPF, dan SpamAssassin

Verifikasi fungsi ClamAV dilakukan dengan cara masuk pada menu Dashboard di CentOS Web Panel, seperti terlihat pada gambar 4.22 berikut.



Gambar 4.22 Verifikasi Fungsi ClamAV

4.2.1.3. Verifikasi Konfigurasi Client

Verifikasi konfigurasi *client* dilakukan dengan cara melakukan ping pada *mail server* dengan perintah `>ping skripsi.ononline` seperti pada gambar 4.23 berikut.

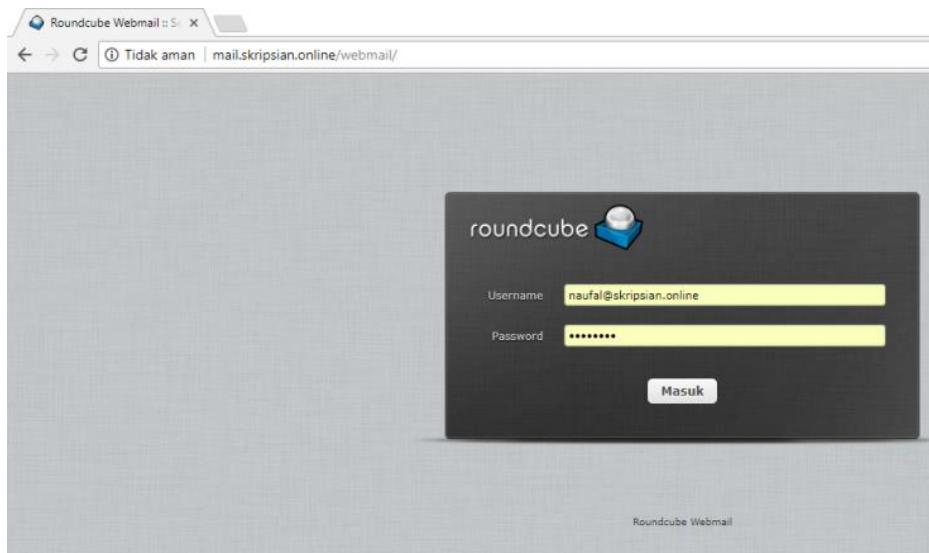
```
C:\Users\user>ping skripsi.online

Pinging skripsi.online [103.112.162.228] with 32 bytes of data:
Reply from 103.112.162.228: bytes=32 time=47ms TTL=57
Reply from 103.112.162.228: bytes=32 time=45ms TTL=57
Reply from 103.112.162.228: bytes=32 time=48ms TTL=57
Reply from 103.112.162.228: bytes=32 time=46ms TTL=57

Ping statistics for 103.112.162.228:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 45ms, Maximum = 48ms, Average = 46ms
```

Gambar 4.23 Ping Mail Server

Verifikasi konfigurasi pada *client* juga dapat dilakukan dengan cara mengakses *Mail User Agent* dengan menggunakan aplikasi *browser* kemudian mengakses alamat *URL* `skripsi.online/webmail/` seperti terlihat pada gambar 4.24 berikut.



Gambar 4.24 Akses MUA

4.2.2. Skenario Uji Coba

Adapun pada tahap skenario hasil uji coba ini berisikan tentang uji coba sebelum diterapkannya *filtering*, otentikasi, dan otorisasi *email spam* dan uji coba setelah diterapkannya *filtering*, otentikasi, dan otorisasi *email spam*.

4.2.2.1. 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*.

4.2.2.1.1. 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 *skripsi.ononline*.

4.2.2.1.1.1. Uji Coba Mengirim *Email Spoofing* ke *Gmail*

Skenario uji coba untuk menguji kinerja protokol *DKIM* dan *SPF* dilakukan dengan cara melakukan pengiriman *email spoofing*, misalkan skripsi *education center* adalah perusahaan yang bergerak dibidang pendidikan yaitu membuka kursus untuk para mahasiswa semester akhir yang sedang mengerjakan skripsi. Skripsi *education center* mempunyai pesaing didalam menjalankan bisnisnya sehingga pesaing tersebut berusaha untuk menjatuhkan skripsi *education center* dengan cara melakukan penipuan dengan mengirim *email spoofing* menggunakan *Fake Mailer*, sebelum melakukan *email spoofing*, pesaing tersebut terlebih dahulu mencari tahu alamat *email* bagian keuangan dan direktur skripsi *education center*, setelah pesaing tersebut mengetahui alamat *email* bagian keuangan dan direktur skripsi *education center* maka pesaing tersebut mulai mengirim *email spoofing* yang mengatasnamakan direktur

skripsi *education center*, pesaing tersebut menujukan *email spoofing* tersebut ke staf keuangan skripsi *education center*, *email spoofing* tersebut berisi perintah untuk mengirim laporan keuangan skripsi *education center* dalam jangka waktu lima tahun terakhir. Misalkan setelah pesaing tersebut mengumpulkan informasi yang diperlukan untuk melakukan *email spoofing* dan mengetahui bahwa nama pegawai dibagian keuangan tersebut adalah Naufal Hanif dengan alamat naufalhanif1477.nh@gmail.com kemudian telah diketahui bahwa nama direktur skripsi *education center* adalah Hendarto dengan alamat email hendarto@skripsi.online maka pesaing tersebut mulai melakukan *email spoofing* dengan cara membuka situs www.emkei.cz yang digunakan untuk mengirim *email spoofing*, pesaing tersebut mengirim *email spoofing* melalui www.emkei.cz kepada pegawai staf keuangan yaitu Naufal Hanif dengan alamat *email* naufalhanif1477.nh@gmail.com dengan mengatasnamakan direktur skripsi *education center* yang bernama Hendarto dengan alamat *email* hendarto@skripsi.online, isi *email* tersebut memerintahkan Naufal Hanif sebagai staf keuangan skripsi *education center* untuk mengirimkannya laporan keuangan skripsi *education center* dalam jangka waktu lima tahun terakhir, balasan *email spoofing* tersebut di arahkan ke *email server* yang dibuat sementara dengan domain ridho.org untuk menampung *email* balasan yang berisi laporan keuangan seperti pada gambar 4.25 berikut.

From Name: Hendarto

From E-mail: hendarto@skripsi.online

To: naufalhanif1477.nh@gmail.com

Subject: Laporan Keuangan

Attachment: No file selected.

Reply-To: hendarto@ridho.org

Errors-To:

Cc:

Bcc:

Priority: Low Normal High

X-Mailer: - none -

Confirm delivery:

Confirm reading:

Add Header:

SMTP Server: **Port:**

Date: Mon, 14 May 2018 01:14:50 +0000 (UTC) Current
 Delay sending to the specified time (future only)

Charset: utf-8

PGP/GPG Encrypt: No Yes Do not encrypt attachments

Receiver's Public Key:

Content-Type: text/plain text/html Editor

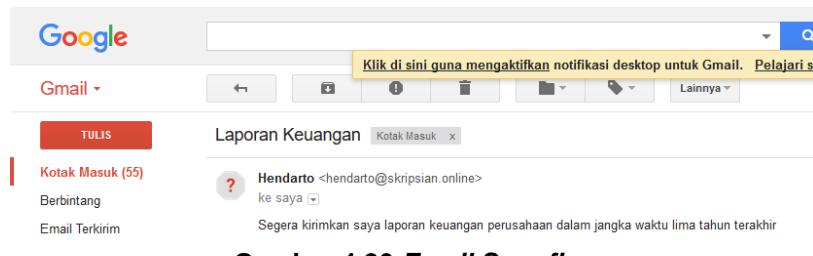
Text: Segera kirimkan saya laporan keuangan perusahaan dalam jangka waktu lima tahun terakhir

Gambar 4.25 Emkei's Fake Mailer

Pada gambar diatas terlihat tampilan dari *Emkei's Fake Mailer*, pada *text box From Name* diisi dengan nama direktur skripsi *education center*, pada *text box From E-mail* diisi dengan alamat *email* direktur skripsi *education center*, pada *text box To* diisi dengan alamat *email* staf keuangan skripsi *education center*, pada *text box Subject* diisi dengan subjek *email*, pada *text box Reply-To* diisi dengan alamat *email* yang digunakan untuk menerima *email* balasan dari *email spoofing* tersebut, dan

text box *Text* diisi dengan pesan dari *email spoofing*, jika pada *email server* skripsi *education center* belum menerapkan protokol *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 hendarto@skripsi.online dan alamat penerima *email* adalah naufalhanif1477.nh@gmail.com.
2. Email spoofing tersebut di akses melalui *mail server gmail.com* oleh alamat email naufalhanif1477.nh@gmail.com tanpa adanya proses otentikasi dan otorisasi oleh protokol *DKIM* dan *SPF* sehingga *email spoofing* tersebut berhasil terkirim kealamat *email* naufalhanif1477.nh@gmail.com seperti terlihat pada gambar 4.26 berikut.



Gambar 4.26 *Email Spoofing*

3. Setelah *email* tersebut masuk ke *inbox* Naufal Hanif maka Naufal Hanif akan membaca *email spoofing* tersebut kemudian *email spoofing* tersebut akan dibalas oleh Naufal Hanif dengan melampirkan laporan keungan yang akan terkirim kealamat

email hendarto@ridho.org sebagai alamat *email* untuk menerima balasan *email spoofing* seperti gambar 4.27 berikut.



Gambar 4.27 Balasan *Email Spoofing*

4.2.2.1.1.2. 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* *skripsi.onl...*, proses otentikasi dan otorisasi akan sama dengan proses otorisasi dan otentikasi pada uji coba pertama terlihat seperti gambar 4.28 berikut.

From Name: Hendarto
From E-mail: hendarto@skripsi.online
To: naufalhanif74@yahoo.com
Subject: Laporan Keuangan
Attachment: Pilih File Tidak ada file yang dipilih
 Attach another file

Content-Type: text/plain text/html Editor
Text: Kirimkan saya laporan keuangan dalam jangka waktu lima tahun terakhir

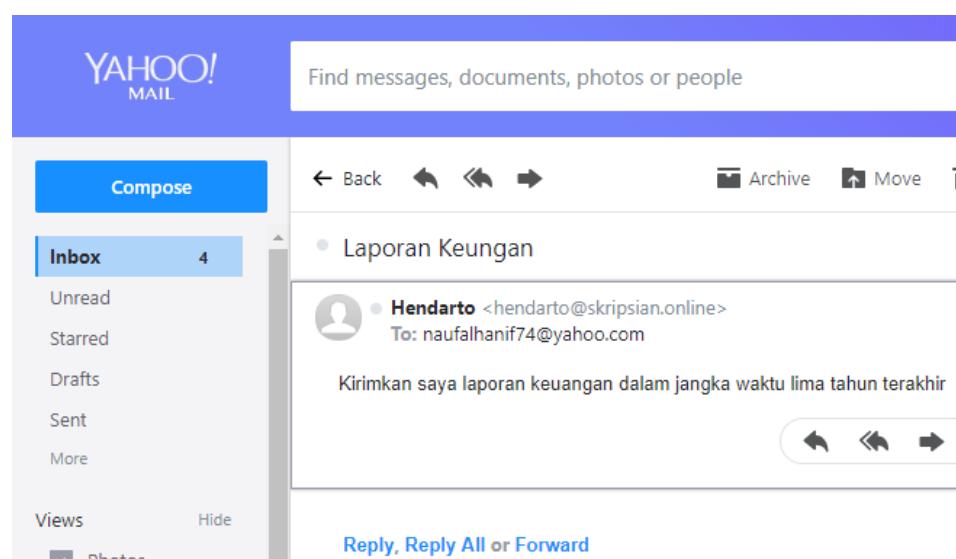
Captcha:

Saya bukan robot

 reCAPTCHA
Privasi · Persyaratan

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

Email spoofing tersebut diatas berhasil terkirim ke alamat *email* naufalhanif74@yahoo.com terlihat seperti pada gambar 4.29 berikut.



Gambar 4.29 Email Spoofing Terkirim ke *Yahoo! Mail*

4.2.2.1.1.3. Uji Coba Mengirim *Email Spoofing* pada skripsi.ononline

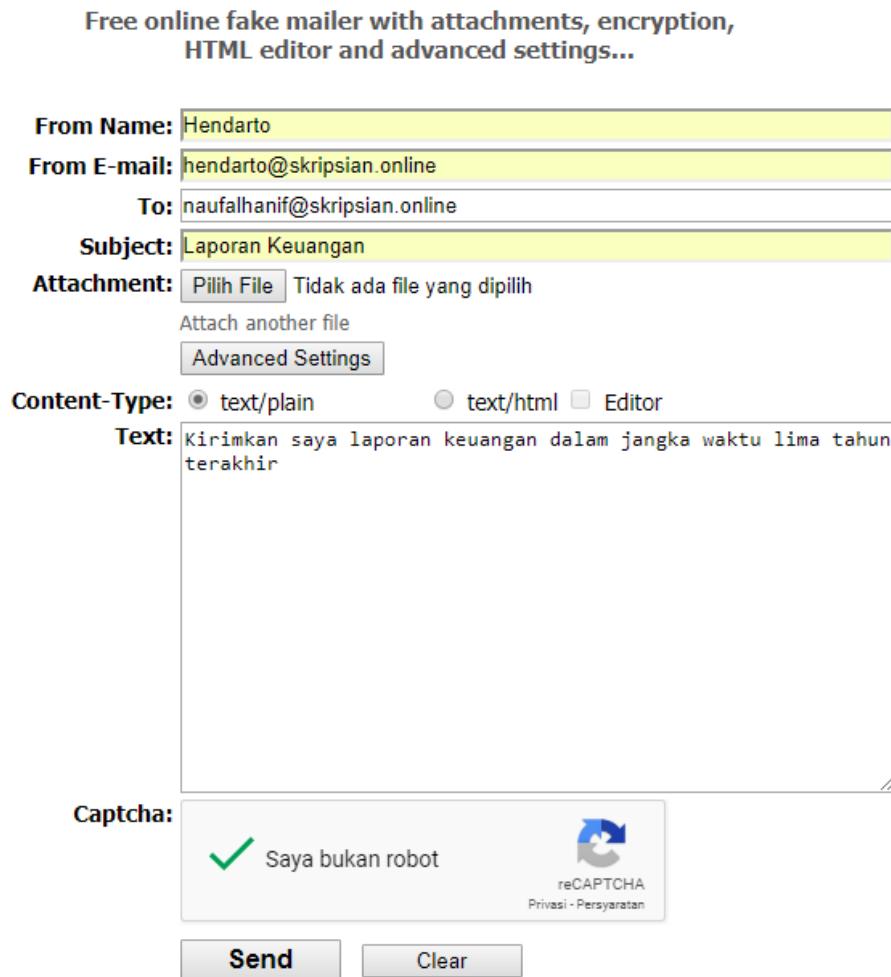
Dengan menggunakan skenario yang sama seperti pada uji coba mengirim *email spoofing* ke layanan *email Gmail*, namun pada uji coba ini akan di uji pengiriman *email spoofing* pada *mail server* skripsi.ononline dengan mengatasnamakan salah satu *user* yang ada pada *mail server* skripsi.ononline, proses otentikasi dan otorisasi akan sama dengan proses otorisasi dan otentikasi pada uji coba mengirim *email spoofing* ke *Gmail* terlihat seperti gambar 4.30 berikut.

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

From Name: Hendarto
From E-mail: hendarto@skripsi.ononline
To: naufalhanif@skripsi.ononline
Subject: Laporan Keuangan
Attachment: Pilih File Tidak ada file yang dipilih
Attach another file
Advanced Settings
Content-Type: text/plain text/html Editor
Text: Kirimkan saya laporan keuangan dalam jangka waktu lima tahun terakhir

Captcha: Saya bukan robot 
reCAPTCHA
Privasi - Persyaratan

Send **Clear**



Gambar 4. 30 Mengirim *Email Spoofing* ke skripsi.ononline

Email spoofing tersebut diatas berhasil terkirim ke alamat *email* naufalhanif@skripsi.ononline terlihat seperti pada gambar 4.31 berikut.



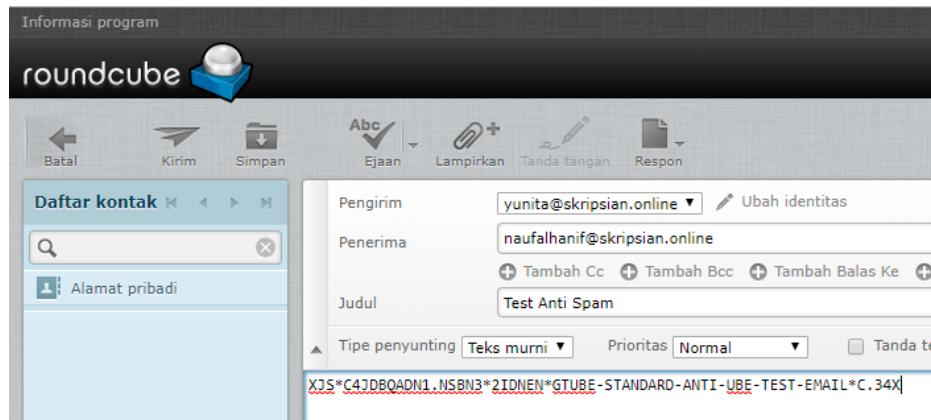
Gambar 4. 31 *Email Spoofing* Terkirim ke User skripsi.ononline

4.2.2.1.2. Uji Coba Mengirim *Email Spam*

Uji coba mengirim *email spam* dilakukan dengan mengirim *email spam* menggunakan layanan *email* skripsi.ononline, *Yahoo! Mail*, dan *Gmail* ke layanan *email* skripsi.ononline.

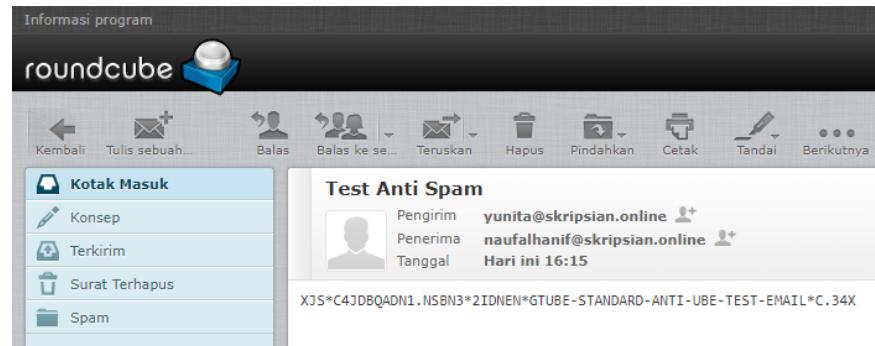
4.2.2.1.2.1. Uji Coba Mengirim *Email Spam* dari skripsi.ononline

Uji coba kedua adalah dengan mengirim *email spam* menggunakan layanan *email* skripsi.ononline ke layanan *email* skripsi.ononline, 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 4.32 berikut.



Gambar 4.32 Mengirim *Email Spam* dari skripsi.onl...

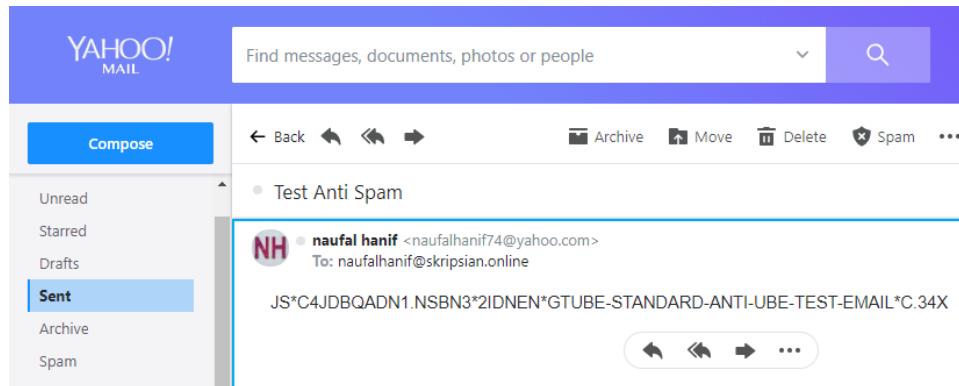
Email spam tersebut diatas berhasil terkirim ke alamat *email* naufalhanif@skripsi.onl... karena belum ada penerapan *anti spam* pada *mail server* skripsi.onl... terlihat seperti pada gambar 4.33 berikut.



Gambar 4.33 *Email Spam* dari skripsi.onl... Terkirim

4.2.2.1.2.2. Uji Coba Mengirim *Email Spam* dari *Yahoo! Mail*

Dengan menggunakan skenario yang sama seperti pada uji coba mengirim *email spam* dari layanan *email* skripsi.onl... ke layanan *email* skripsi.onl..., namun pada uji coba ini akan di uji pengiriman *email spam* ke layanan *email* skripsi.onl... dari layanan *email* *Yahoo! Mail* terlihat seperti gambar 4.34 berikut.



Gambar 4.34 Mengirim Email Spam dari Yahoo! Mail

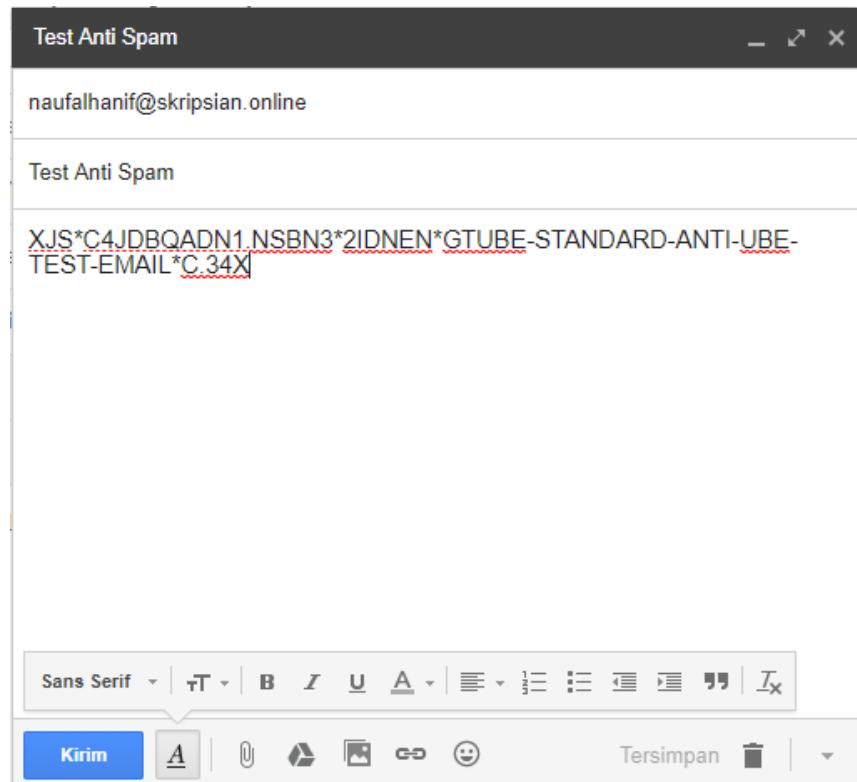
Email spam tersebut diatas berhasil terkirim ke alamat email naufalhanif@skripsi.onlne karena belum ada penerapan *anti spam* pada mail server skripsi.onlne terlihat seperti pada gambar 4.35 berikut.



Gambar 4.35 Email Spam dari Yahoo! Mail Terkirim

4.2.2.1.2.3. Uji Coba Mengirim Email Spam dari Gmail

Dengan menggunakan skenario yang sama seperti pada uji coba mengirim email spam dari layanan email skripsi.onlne ke layanan email skripsi.onlne, namun pada uji coba ini akan di uji pengiriman email spam ke layanan email skripsi.onlne dari layanan email Gmail terlihat seperti gambar 4.36 berikut.



Gambar 4.36 Mengirim *Email Spam* dari *Gmail*

Email spam tersebut diatas berhasil terkirim ke alamat *email* naufalhanif@skripsian.online karena belum ada penerapan *anti spam* pada *mail server* skripsian.online terlihat seperti pada gambar 4.37 berikut.



Gambar 4.37 *Email Spam* dari *Gmail* Terkirim

4.2.2.1.2.4. 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

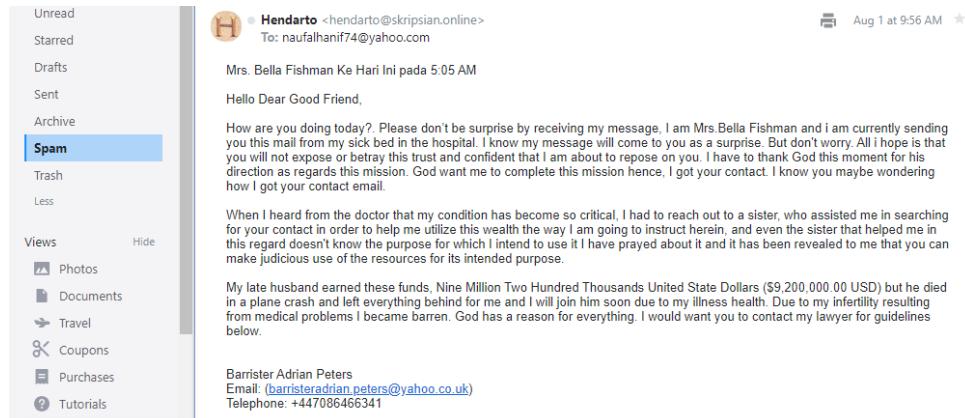
email spam yang berisi penipuan atau promosi suatu produk seperti terlihat pada gambar 4.38 berikut.

The screenshot shows an email client interface with the following fields filled:

- From Name:** Hendarto
- From E-mail:** hendarto@skripsi.ononline
- To:** naufalhanif74@yahoo.com
- Subject:** Coba
- Attachment:** Pilih File Tidak ada file yang dipilih
Attach another file
Advanced Settings
- Content-Type:** text/plain text/html Editor
- Text:** Mrs. Bella Fishman Ke Hari Ini pada 5:05 AM
Hello Dear Good Friend,
How are you doing today?. Please don't be surprise by receiving my message, I am Mrs.Bella Fishman and i am currently sending you this mail from my sick bed in the hospital. I know my message will come to you as a surprise. But don't worry. All i hope is that you will not expose or betray this trust and confident that I am about to repose on you. I have to thank God this moment for his direction as regards this mission. God want me to complete this mission hence, I got your contact. I know you maybe wondering how I got your contact email.
- Captcha:** Saya bukan robot 
reCAPTCHA
Privasi - Persyaratan
- Buttons:** Send, Clear

Gambar 4.38 Mengirim *Email Spam* Tanpa GTUBE TEST

Email dengan *format spam* tersebut terkirim ke *Yahoo! Mail* dan masuk ke dalam *folder spam* seperti terlihat pada gambar 4.39 berikut.



Gambar 4.39 Email Terindikasi Sebagai Spam oleh Yahoo! Mail

Yahoo! Mail mengindikasi bahwa *email* tersebut diatas merupakan *spam* sehingga *format email* tersebut diatas dapat dijadikan acuan untuk melakukan uji coba mengirim *email spam* tanpa *GTUBE test* dengan cara mengirim *email* seperti *format email* tersebut diatas dari *Emkei's Fake Mailer* ke salah satu *user* yang ada pada layanan *email* skripsi.ononline seperti terlihat pada gambar 4.40 berikut.

From Name: Hendarto

From E-mail: hendarto@skripsi.online

To: yunita@skripsi.online

Subject: Coba

Attachment: Pilih File Tidak ada file yang dipilih
Attach another file
Advanced Settings

Content-Type: text/plain text/html Editor

Text:

```
Mrs. Bella Fishman Ke Hari Ini pada 5:05 AM

Hello Dear Good Friend,

How are you doing today?. Please don't be surprise by receiving my message, I am Mrs.Bella Fishman and i am currently sending you this mail from my sick bed in the hospital. I know my message will come to you as a surprise. But don't worry. All i hope is that you will not expose or betray this trust and confident that I am about to repose on you. I have to thank God this moment for his direction as regards this mission. God want me to complete this mission hence, I got your contact. I know you maybe wondering how I got your contact email.
```

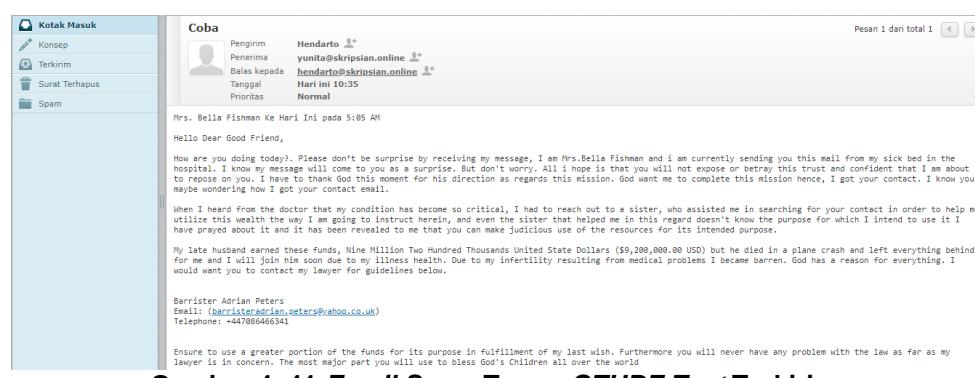
Captcha:


 Saya bukan robot
recaptcha.net
Privasi - Persyaratan

Send **Clear**

Gambar 4.40 Mengirim Email Spam Tanpa Format GTUBE Test

Email spam tanpa format GTUBE Test tersebut terindikasi sebagai email ham dan masuk pada kotak masuk pengguna layanan email skripsi.online karena belum ada penerapan SpamAssassin dan Amavisd-New seperti terlihat pada gambar 4.41 berikut.



Gambar 4.41 Email Spam Tanpa GTUBE Test Terkirim

4.2.2.1.3. Uji Coba Mengirim *Email* yang Mengandung *Virus*

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

4.2.2.1.3.1. Uji Coba Mengirim *Email* yang Mengandung *Virus* dari skripsi.ononline

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* skripsi.ononline ke layanan *email* skripsi.ononline, seperti pada gambar 4.42 berikut.



Gambar 4. 42 *EICAR Test* dari skripsi.ononline

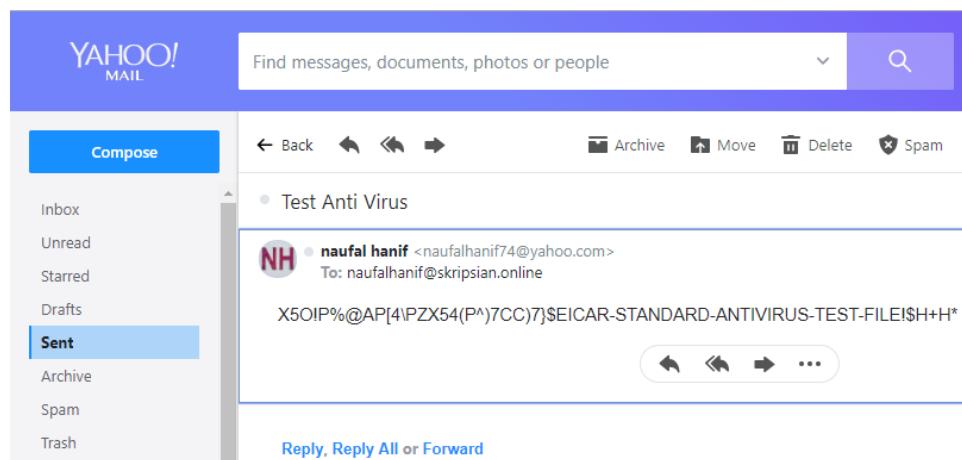
Setelah *email* tersebut dikirim pada salah satu *user email* yang ada pada *mail server* skripsi.ononline maka *email* yang mengandung *virus* tersebut berhasil terkirim ke *user* yang berada pada *mail server* skripsi.ononline seperti terlihat pada gambar 4.43 berikut.



Gambar 4.43 Email Mengandung Virus dari skripsian.online Terkirim

4.2.2.1.3.2. 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\ZX54(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* skripsian.online, seperti pada gambar 4.44 berikut.



Gambar 4.44 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*

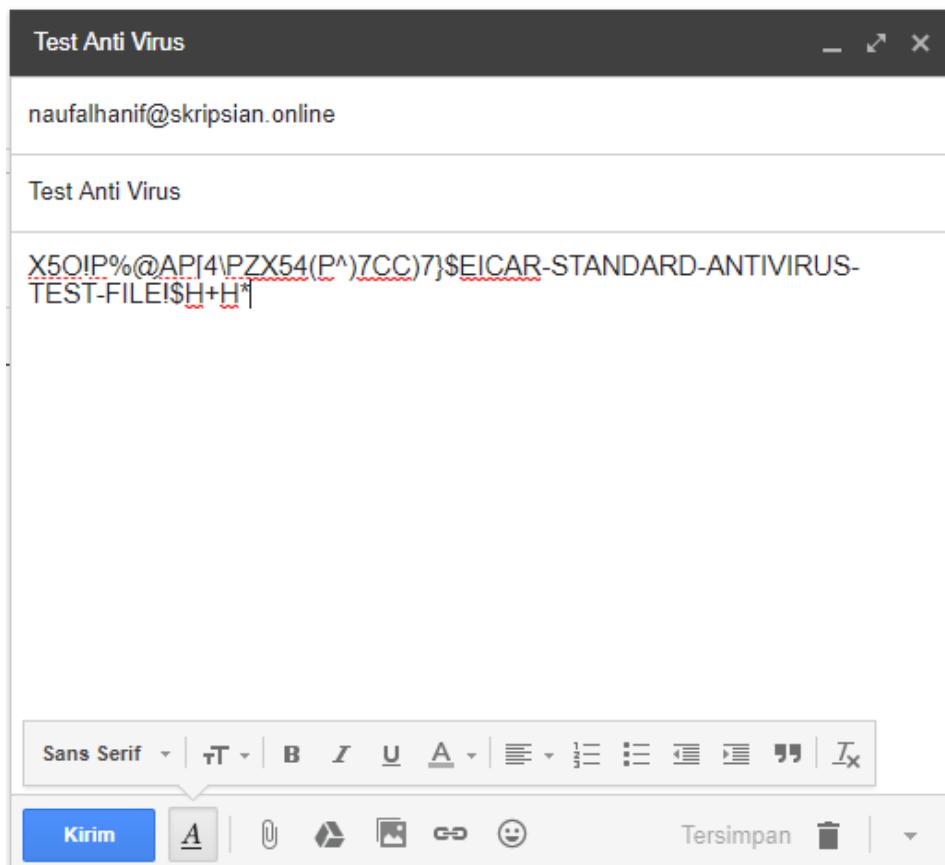
tersebut berhasil terkirim ke *user email* yang berada pada *mail server* skripsi.ononline seperti terlihat pada gambar 4.45 berikut.



Gambar 4.45 Email Mengandung Virus dari Yahoo! Mail Terkirim

4.2.2.1.3.3. 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* skripsi.ononline, seperti pada gambar 4.46 berikut.



Gambar 4.46 EICAR Test dari Gmail

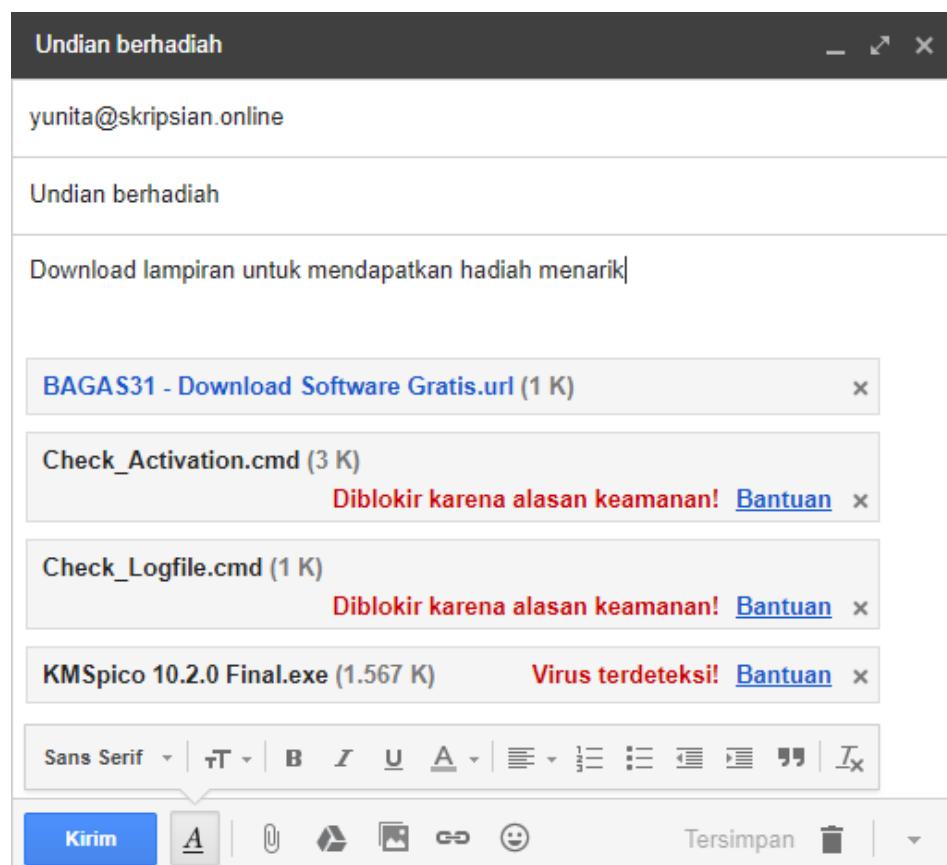
Setelah *email* tersebut dikirim pada salah satu pengguna *email* yang ada pada *mail server* skripsiian.online maka *email* yang mengandung *virus* tersebut berhasil terkirim ke penerima yang berada pada *mail server* skripsiian.online seperti terlihat pada gambar 4.47 berikut.



Gambar 4.47 Email Mengandung Virus dari Gmail Terkirim

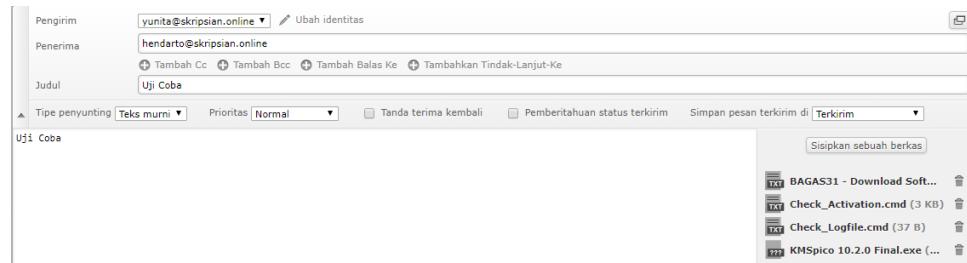
4.2.2.1.3.4. Uji Coba Mengirim *Email Virus* Tanpa EICAR Test

Uji coba mengirim *email* yang mengandung *virus* dilakukan dengan mengirim *email* dari layanan *email gmail*, *email* yang dikirim diberi lampiran berupa program *crack* dengan ekstensi .exe yang akan terdeteksi sebagai *virus* oleh *gmail* seperti terlihat pada gambar 4.48 berikut.



Gambar 4.48 Lampiran Terdeteksi Sebagai Virus

Lampiran yang telah terdeteksi sebagai *virus* oleh layanan *email gmail* akan dikirim ke layanan *email skripsi.ononline* untuk menguji layanan *email* skripsi.ononline sebelum penerapan *anti virus* seperti terlihat pada gambar 4.49 berikut.



Gambar 4.49 Mengirim Virus Sebelum Penerapan Anti Virus

Email yang mengandung *virus* tersebut berhasil terkirim dan masuk pada kotak masuk pengguna karena tidak ada proses pendekripsi *virus* yang dilakukan oleh *Amavisd-New*, proses pendekripsi *virus* juga dapat dilihat pada *header email* dengan mengecek parameter *X-Virus-Scanned*, apabila tidak terdapat parameter *X-Virus-Scanned* pada *header email*, maka belum terjadi proses pendekripsi *virus* pada *email* seperti terlihat pada gambar 4.50 dan 4.51 berikut.



Gambar 4.50 Virus Berhasil Terkirim ke Kotak Masuk Pengguna Email

```

Return-Path: <yunita@skripsiian.online>
Delivered-To: hendarto@skripsiian.online
Received: from localhost (localhost [IPV6:::1])
    by ns1.skripsiian.online (Postfix) with ESMTPA id C34823036881
    for <hendarto@skripsiian.online>; Thu,  2 Aug 2018 15:04:38 +0700 (WIB)
MIME-Version: 1.0
Content-Type: multipart/mixed;
    boundary="=_a842988ef9a52c888e4d9d947d1c96ce"
Date: Thu, 02 Aug 2018 15:04:38 +0700
From: yunita@skripsiian.online
To: hendarto@skripsiian.online
Subject: Uji Coba
Message-ID: <567b79c04caed0624f581f5b072046bd@skripsiian.online>
X-Sender: yunita@skripsiian.online
User-Agent: Roundcube Webmail/1.2.3

```

Gambar 4.51 Header Email Tanpa Parameter X-Virus-Scanned

4.2.2.1.4. Uji Coba Pengecekan *Header Email*

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

4.2.2.1.4.1. *Header Email* pada *Gmail*

Uji coba ini dilakukan dengan mengirim *email* dari salah satu *user email* yang ada pada skripsi.ononline 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 *DKIM*, *SPF*, *anti spam*, dan *anti virus*, *header email* sebelum diterapkannya *DKIM*, *SPF*, *anti spam*, dan *anti virus* terlihat seperti gambar 4.52 berikut.

```
Received-SPF: pass (google.com: best guess record for domain of naufalhanif@skripsi.ononline designates 103.112.162.228 as permitted sender) client-ip=103.112.162.228;
Authentication-Results: mx.google.com;
spf=pass (google.com: best guess record for domain of naufalhanif@skripsi.ononline designates 103.112.162.228 as permitted
sender) smtp.mailfrom=naufalhanif@skripsi.ononline
Received: from localhost (localhost [IPv6::1]) by ns1.skripsi.ononline (Postfix) with ESMTPA id 370623069661; Wed, 27 Jun 2018
12:06:51 +0700 (WIB)
MIME-Version: 1.0
```

Gambar 4.52 Cuplikan *Header Email* pada *Gmail* Sebelum Penerapan

Pada gambar 4.52 terlihat pada cuplikan *header email* hanya terdapat parameter Received-SPF dan belum terdapat parameter *DKIM-Signature* atau tanda tangan *digital* dan *X-Virus-Scanned* karena belum ada penerapan *DKIM*, *ClamAV*, dan *Amavisd-New*.

4.2.2.1.4.2. Header Email pada Yahoo! Mail

Uji coba ini dilakukan dengan mengirim *email* menggunakan salah satu *user email* yang ada pada skripsi.ononline 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 *DKIM*, *SPF*, *anti spam*, dan *anti virus*, *header email* sebelum diterapkannya *DKIM*, *SPF*, *anti spam*, dan *anti virus* terlihat seperti gambar 4.53 berikut.

```
Received-SPF: none (domain of skripsi.ononline does not designate permitted sender hosts)
X-Mailer: wd_by_YmDtGh6UaoekbpHdud9y6gul1V2y4qcVzHn1hdw
QKd9Y4J701B1S06tph0T6cosy0Umz2_jogIaxOg0nFTpaLXFozIZrgk1q5
zBQmIYTRGXG9D402N4c038v25ZKLmlyKhxc0R5z79memgqtRRRLU_kkT
K65Pt1yjEnfFI0HYYiklwlwDxD18K1775mWAc34_PtUVcw86cg1yo81YHPw
91tc6279w4fdRNQ05eSqvtX6_DwphbK2zE134aTtTROsdnfPLGw300sx
FQ1E8ewC_7N65Lyg3goUr88531LN_sdVNiij24FRdTVEYfaJ30dkTl0IxwY_Q
ABXhmFn4/Qle0xmkk1t73l96GH1HKerylRqlPLIOFpgatbsImMwFc18
Z3MzonRvHQAKV7q19Pp1UD06khkkLlbuuVMU5pVnQ01fAbhzrasQuRFd
kxDetH08gdUPDj30mEkpuvcTEOSXQLAQHTJzC7SBocF1PhEegusL1ng.w
o_pluA2LPRx42Zel0RTTymlW5p0p1wEM81kcnzPuzBvVnpwgFy6.Jsy4gkNt
m2lHVL81dezsYu4kTwiybh8nCxv3dLblihHSVe0QZjy7U2Uan0T.yqBp
DRsh01F9bDRfU02g1_MSuFDuAoJfalgugeYrnzE9H8etyeEA2LjQCnSmqc
ISPH83_8Mwzcf2818Funn7bLRGtn16Dwir1VfzhOvq111KAKK3J_vAn1zplk
CeoGY_95j1Lx7VsmgVU1ziuE13P7QKPrvYn_X_U9U8BpnC3Y1azCTJCG
claxhVvYCC0f7NaePDLewAf9tBnloI5jz1AHC1L9XuThB21HGsatCe3Jn
_XQg9uqhPSL3QvhzHANLW8lpKcRNWijg--
X-Originating-IP: [103.112.162.228]
Authentication-Result: mta4243.mail.ne1.yahoo.com from=skripsi.ononline; domainkeys=neutral (no sig); from=skripsi.ononline; dkim=neutral (no sig)
Received: from 127.0.0.1 (EHLO ns1.skripsi.ononline) (103.112.162.228)
```

Gambar 4.53 Cuplikan Header Email pada Yahoo! Mail Sebelum Penerapan

Pada gambar 4.53 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=neutral (no sig)* yang berarti belum ada tanda tangan *digital* karena belum diterapkan *DKIM*.

4.2.2.1.4.3. Header Email pada skripsi.ononline

Uji coba ini dilakukan dengan mengirim *email* menggunakan salah satu *user email* yang ada pada skripsi.ononline ke salah satu *user email* yang ada pada skripsi.ononline kemudian melakukan pengecekan *header email* dan melakukan perbandingan terhadap *header email* sebelum dan

setelah penerapan *DKIM*, *SPF*, *anti spam*, dan *anti virus*, *header email* sebelum diterapkannya *DKIM*, *SPF*, *anti spam*, dan *anti virus* terlihat seperti gambar 4.54 berikut.

```

Return-Path: <yunita@skripsi.onlne>
Delivered-To: naufalhanif@skripsi.onlne
Received: from localhost (localhost [IPv6:::1])
    by ns1.skripsi.onlne (Postfix) with ESMTPA id 18948306969F
        for <naufalhanif@skripsi.onlne>; Tue, 26 Jun 2018 16:15:08 +0700 (WIB)
MIME-Version: 1.0
Content-Type: text/plain; charset=US-ASCII;
    format=flowed
Content-Transfer-Encoding: 7bit
Date: Tue, 26 Jun 2018 16:15:07 +0700
From: yunita@skripsi.onlne
To: naufalhanif@skripsi.onlne
Subject: Test Anti Spam
Message-ID: <b935648c3ce1e2a691fdd459d3454b58@skripsi.onlne>
X-Sender: yunita@skripsi.onlne
User-Agent: Roundcube Webmail/1.2.3

```

Gambar 4.54 Cuplikan *Header Email* pada skripsi.onlne Sebelum Penerapan

Pada gambar 4.54 terlihat *header email* belum terdapat parameter *X-Virus-Scanned* dan *DKIM-Signature* karena belum diterapkan *Amavisd-New* dan *DKIM*.

4.2.2.2. Uji Coba Setelah Diterapkan Filtering, Otentikasi dan Otorisasi

Adapun 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*.

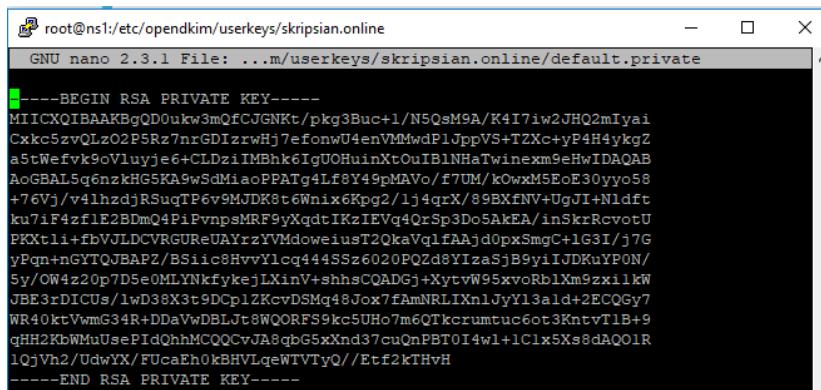
4.2.2.2.1. Uji Coba Mengirim *Email Spoofing*

Uji coba mengirim *email spoofing* dilakukan dengan mengirim *email spoofing* dari *Emkei's Fake Mailer* ke *Gmail*, *Yahoo! Mail*, dan *skripsi.onlne* dengan mengatasnamakan salah satu *user email* yang ada pada *skripsi.onlne*.

4.2.2.2.1.1. Uji Coba Mengirim *Email Spoofing* ke Gmail

Proses uji coba mengirim *email spoofing* pada *email server* akan berbeda setelah protokol *SPF* dan *DKIM* diterapkan pada *mail server* karena protokol *SPF* dan *DKIM* akan melakukan otentikasi dan otorisasi pada setiap *email* yang datang dari *mail server* skripsi.ononline. Proses yang terjadi setelah penerapan protokol *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 `hendarto@skripsi.ononline` dan alamat penerima *email* yaitu `naufalhanif1477.nh@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* skripsi.ononline terlihat seperti gambar 4.55 berikut.



```
root@ns1:/etc/opendkim/userkeys/skripsi.ononline
GNU nano 2.3.1 File: ...m/userkeys/skripsi.ononline/default.private

-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgDQ0ukw3mQfCUGNktpkg3Buc+1/N5QsM9A/K4I7iw2JHQ2mIyai
Cxck5zwQLz02PSRz7nrGDIzrWj7efonwU4enVMMwdplJpvVs+TZXc+yP4H4ykgZ
a5tWefvk9oVluyje6+CLDziIMBhk6IgOHuinXtOuIB1NhTwinxm9eHwIDAQAB
AoGBAL5q6nzkH65KA9wSdMiacoPATg4lf8Y49pMAVo/f7UM/k0wxM5EoE3Oyyo58
+76Vj/v4lhzdrJSuqTP6v9MJDk8t6Wnix6Kpg2/lj4qrX/89BXfNV+UgJI+Nldft
ku7iF4zf1B2BmQ4PiPvnpsMRF9yXqdtIKzIEVq4QzSp3Do5AkEA/in5krRcvotUP
PKXtli+fbVULDCVRGRReUAYrzYVmoweiusT2QkaVqlfAAjd0pxSmgC+lG3I/j7G
yPqn+nGYTQBAPZ/BSi1c8HvvYlcq44SSz6020PQ2d8Ylza5jB9yiIUDKuYPON/
5y/OW4zz0p7D5e0MLYNkfkykejLXinV+shhsCQADGj+XytvW95xvoRblXm9zxilkw
JBE3rDICUs/1wD38X3t9DCp1ZKcvDSMq48Jox7fAmNRILIXn1JyY13ald+2ECQGy7
WR40ktVwmG34R+DDaVwDBLJt8WQORFS9kc5UHo7m6QTkcrumtuc6ot3Kntv1LB+9
qHH2KbWMuUsePIdQhnMCQQCvJA8qbG5xXnd37cuQnPBT0I4wl+1Clx5Xs8dAQ01R
1QjVh2/UdwYX/FUcaEh0kBHVlqeWTVTyQ//Etf2kTHvH
-----END RSA PRIVATE KEY-----
```

Gambar 4.55 *Private Key* pada skripsi.ononline

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 skripsi.onlin*e yang cocok dengan *public key* yang telah diletakan pada *DNS server* skripsi.onlin sehingga pesan tersebut tidak memiliki tanda tangan *digital* pada *header email* (proses *DKIM*) terlihat seperti gambar 4.56 dan 4.57 berikut.

```
default._domainkey 14400 IN TXT "v=DKIM1; k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQAA4GNADCBiQKBgQD0ukw3mQfCJGNKt/pkg3Buc+1/N5QsM9A
/K4I7iw2jHQ2mIyaICxkc5zvQLzO2P5Rz7nrGDizrwHj7efonwU4enVMMwdP1JppVS+TZXc+yP4H4ykgZa5tWefvk9oVluyje6+C
LDziIMBhk6IgUOHuinXtoIBINHaTwinexm9eHwIDAQAB"
```

Gambar 4.56 Public Key pada DNS Server skripsi.onlin

```
Received: from emkei.cz (emkei.cz. [46.167.245.206])
by mx.google.com with ESMTPS id f5-v6si5000eda.356.2018.07.26.23.41.51
for <naufalhanif1477.n@gmail.com>
(version=TLS1_2 cipher=ECDSA-AES128-GCM-SHA256 bits=128/128);
Thu, 26 Jul 2018 23:41:51 -0700 (PDT)
Received-SPF: fail (google.com: domain of hendarto@skripsi.onlin does not designate 46.167.245.206 as permitted sender) client-ip=46.167.245.206;
Authentication-Results: mx.google.com;
spf=fail (google.com: domain of hendarto@skripsi.onlin does not designate 46.167.245.206 as permitted sender)
smtp.mailfrom=hendarto@skripsi.onlin
Received: by emkei.cz (Postfix, from userid 33) id CCA69D061A3; Fri, 27 Jul 2018 08:41:50 +0200 (CEST)
To: naufalhanif1477.n@gmail.com
Subject: Pemindahan Isi Saldo ke Rekening Baru
From: Hendarto <hendarto@skripsi.onlin>
X-Priority: 3 (Normal)
Importance: Normal
Errors-To: hendarto@skripsi.onlin
Reply-To: hendarto@skripsi.onlin
Content-Type: text/plain; charset=utf-8
```

Gambar 4.57 Cuplikan Header Email

4. Selanjutnya *mail server Gmail* akan melakukan pengecekan *SIDF* (*Sender ID Framework*) pada *record DNS server* skripsi.onlin, karena alamat *IP Emkei's Fake Mailer* adalah 46.167.245.205 maka *email spoofing* tersebut dianggap sebagai *spam* dikarenakan *record SPF* yang ada pada *DNS server* skripsi.onlin hanya mengizinkan pengiriman *email* dari alamat yang telah diotorisasi yaitu alamat *IP* 103.112.162.228 yang merupakan alamat mail server skripsi.onlin dan nilai dari parameter *Received-SPF* pada *header email* adalah *fail* sehingga *email* tersebut akan ditandai sebagai *email spam* oleh

server *Gmail* dan *email spoofing* tersebut diblok oleh *Gmail* (proses *SPF*) terlihat seperti gambar 4.58 dan 4.59 berikut.

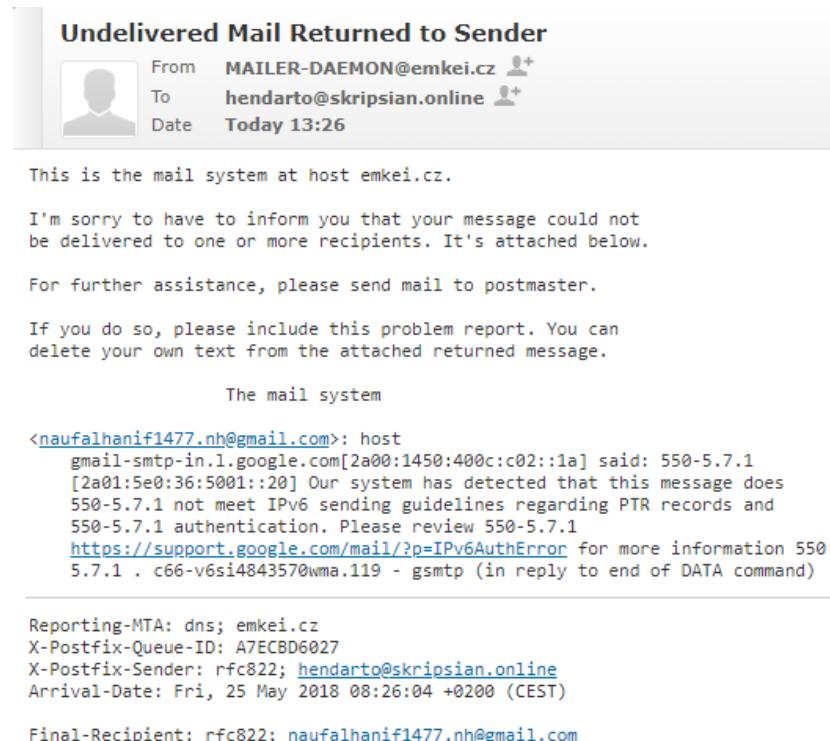
| skripsi.online. IN TXT "v=spf1 mx a ip4:103.112.162.228/32 a:ns1.skripsi.online a:ns2.skripsi.online -all"

Gambar 4.58 SPF Record pada skripsi.online

```
Received-SPF: fail (google.com: domain of hendarto@skripsi.online does not designate 46.167.245.206 as permitted sender) client-ip=46.167.245.206;
Authentication-Results: mx.google.com;
    spf=fail (google.com: domain of hendarto@skripsi.online does not designate 46.167.245.206 as permitted sender)
    smtp.mailfrom=hendarto@skripsi.online
Received: by emkei.cz (Postfix, from userid 33) id CCA69D61A3; Fri, 27 Jul 2018 08:41:50 +0200 (CEST)
```

Gambar 4.59 Parameter Received-SPF pada Header Email

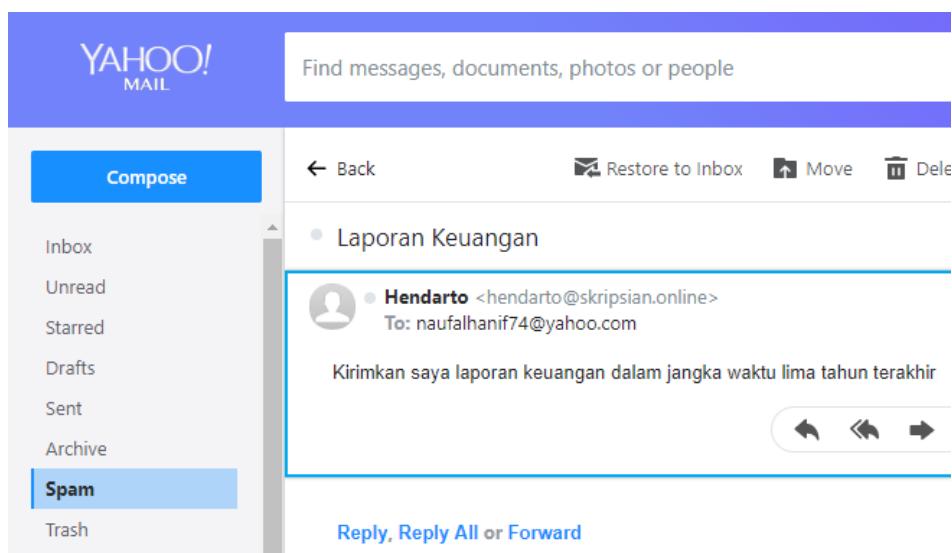
5. *Mail system Emkei's Fake Mailer* menerima kode error 550-5.7.1 dari server *Gmail* kemudian *mail system Emkei's Fake Mailer* mengirimkan pemberitahuan *error* tersebut ke alamat *email user* yang asli sehingga *user email* yang asli dapat mengetahui bahwa *emailnya* telah dimanfaatkan oleh orang yang tidak bertanggung jawab seperti terlihat pada gambar 4.60 berikut.



Gambar 4.60 Pemberitahuan Mail System Emkei's Fake Mailer

4.2.2.2.1.2. 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 diblokir sehingga *email spoofing* tidak masuk pada *folder inbox* ataupun *folder spam* penerima *email* sedangkan pada *Yahoo! Mail*, *email spoofing* tidak diblokir tetapi dimasukan kedalam *folder spam* penerima *email* seperti gambar 4.61 berikut.



Gambar 4.61 *Email Spoofing* Masuk ke *Folder Spam*

4.2.2.2.1.3. Uji Coba Mengirim *Email Spoofing* ke *skripsi.ononline*

Selain mengirim *email spoofing* ke *Gmail* dan *Yahoo! Mail*, pengiriman *email spoofing* juga dilakukan pada *skripsi.ononline* untuk membandingkan perlakuan yang diberikan pada *email spoofing* antara dua layanan *email* tersebut. Pada *Gmail*, *email spoofing* yang masuk langsung diblokir sehingga *email spoofing* tidak masuk pada *folder inbox* ataupun

folder spam penerima *email*, pada *Yahoo! Mail*, *email spoofing* tidak diblokir tetapi dimasukan kedalam *folder spam* penerima *email*, dan pada skripsi.ononline *email spoofing* masuk pada *folder inbox*, seperti gambar 4.62 berikut.



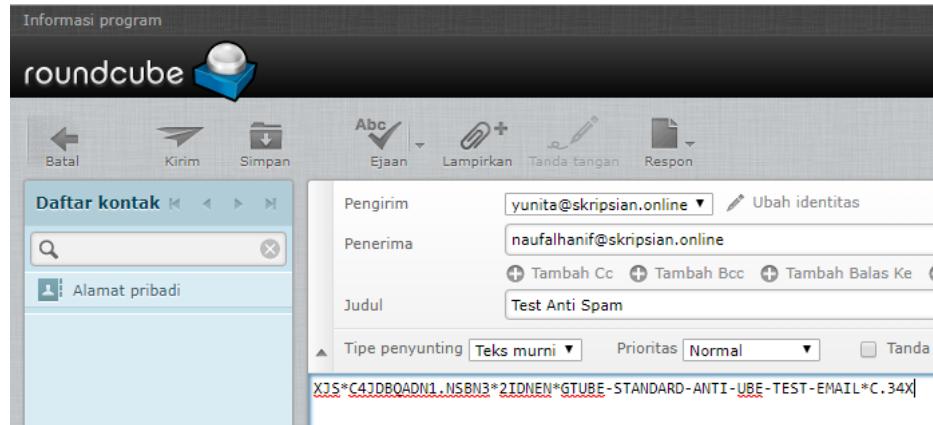
Gambar 4.62 *Email Spoofing* Masuk pada *Folder Inbox*

4.2.2.2.2. Uji Coba Mengirim *Email Spam*

Uji coba mengirim *email spam* dilakukan dengan mengirim *email spam* menggunakan layanan *email* skripsi.ononline, *Yahoo! Mail*, dan *Gmail* ke layanan *email* skripsi.ononline.

4.2.2.2.2.1. Uji Coba Mengirim *Email Spam* dari skripsi.ononline

Uji coba mengirim *email spam* dari layanan *email* skripsi.ononline ke layanan *email* skripsi.ononline adalah dengan mengirim *email spam* menggunakan layanan *email* skripsi.ononline ke layanan *email* skripsi.ononline, 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 4.63 berikut.



Gambar 4.63 Mengirim *Email Spam* dari skripsi.ononline Setelah Penerapan

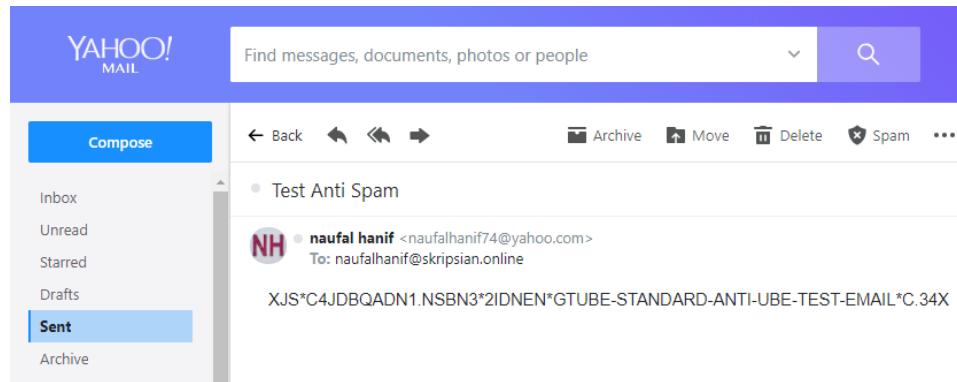
Email spam tersebut diatas diblokir oleh *Amavisd-New* karena terindikasi sebagai *email spam* oleh *SpamAssassin*, hasil pemfilteran *email spam* dapat dilihat pada *mail log* dengan menggunakan perintah `#cat /var/log/maillog` seperti terlihat pada gambar 4.64 berikut.

```
Jul  8 15:38:02 ns1 amavis[19909]: (19909-05) Blocked SPAM {DiscardedInternal,Quarantined}, MYNETS LOCAL [::1]:56012 <yunita@skripsi.ononline> -> <naufalhanif@skripsi.ononline>, Queue-ID: C401B303682F, Message-ID: <18e523e17d74006574b6f272f0210143@skripsi.ononline>, mail_id: fVHwfMK8L-po, Hits: 998.9, size: 1003, dkim_sd=default:skripsi.ononline, 2940 ms
Jul  8 15:38:02 ns1 postfix/smtp[23871]: C401B303682F: to=<naufalhanif@skripsi.ononline>, relay=127.0.0.1[127.0.0.1]:10024, delay=3.7, delays=0.49/0.21/0.08/3, dsn=2.7.0, status=sent (250 2.7.0 Ok, discarded, id=19909-05 - spam)
```

Gambar 4.64 *Email* dari skripsi.ononline Terindikasi *Spam*

4.2.2.2.2. Uji Coba Mengirim *Email Spam* dari *Yahoo! Mail*

Uji coba mengirim *email spam* dari layanan *email Yahoo! Mail* ke skripsi.ononline adalah dengan mengirim *email spam* menggunakan layanan *email Yahoo! Mail* ke layanan *email* skripsi.ononline, 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 4.65 berikut.



Gambar 4.65 Mengirim Email *Spam* dari *Yahoo! Mail* Setelah Penerapan

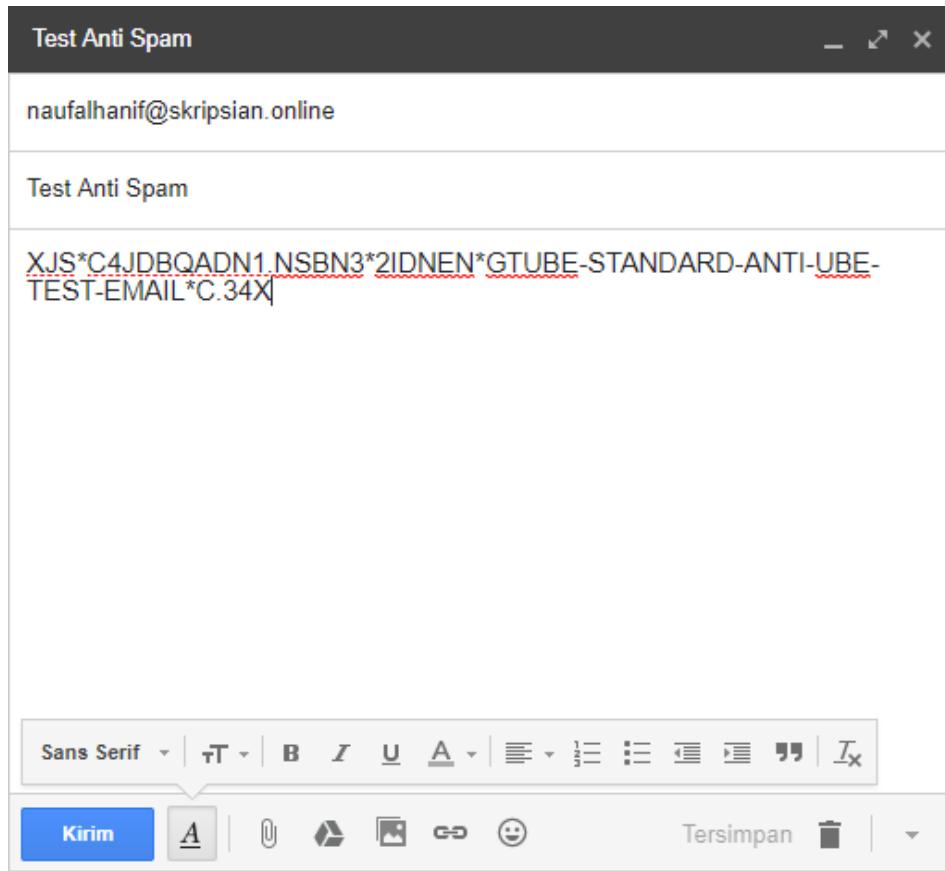
Email spam tersebut diatas diblokir oleh *Amavisd-New* karena terindikasi sebagai *email spam* oleh *SpamAssassin*, hasil pemfilteran *email spam* dapat dilihat pada *mail log* dengan menggunakan perintah `#cat /var/log/maillog` seperti terlihat pada gambar 4.66 berikut.

```
Jul  8 15:31:41 ns1 amavis[19908]: (19908-05) Blocked SPAM {DiscardedInbound,Quarantine}, [66.163.184.47]:36414 [66.163.184.47] <naufalhanif74@yahoo.com> -> <naufalhanif@skripsi.online>, Queue-ID: 9BD6D303682F, Message-ID: <221199817.819059.1531038692831@mail.yahoo.com>, mail_id: Rr2EVJNQ44A1, Hits: 1000.151, size: 3606, dkim_sd=s2048@yahoo.com, 12707 ms
Jul  8 15:31:41 ns1 postfix/smtp[23615]: 9BD6D303682F: to=<naufalhanif@skripsi.online>, relay=127.0.0.1[127.0.0.1]:10024, delay=15, delays=2.3/0.02/0.12/13, dsn=2.7.0, status=sent (250 2.7.0 Ok, discarded, id=19908-05 - spam)
```

Gambar 4.66 Email dari *Yahoo! Mail* Terindikasi *Spam*

4.2.2.2.3. Uji Coba Mengirim Email *Spam* dari *Gmail*

Uji coba mengirim *email spam* dari layanan *email Gmail* ke layanan *email skripsi.online* adalah dengan mengirim *email spam* menggunakan layanan *email Gmail* ke layanan *email skripsi.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 4.67 berikut.



Gambar 4.67 Mengirim *Email Spam* dari *Gmail* Setalah 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 4.68 berikut.

```
Jul  8 15:30:33 nsl amavis[19909]: (19909-04) Blocked SPAM {DiscardedInbound, Quarantined}, [209.85.218.53]:46514 [209.85.218.53] <naufalhanif1477.nh@gmail.com> -> <naufalhanif@skripsian.online>, Queue-ID: 6E2B2303682F, Message-ID: <CAEOh3LHNVUQUf7hbnjEYy_fmokQ9g_P7+LwC+2pPh-JzF8NgoQ@mail.gmail.com>, mail_id: lhXXt-2IKN-h, Hits: 999.881, size: 3824, dkim_sd=20161025:gmail.com, 33589 ms
Jul  8 15:30:33 nsl postfix/smtp[23615]: 6E2B2303682F: to=<naufalhanif@skripsian.online>, relay=127.0.0.1[127.0.0.1]:10024, delay=37, delays=1.2/0.03/6.1/30, dsn=2.7.0, status=sent (250 2.7.0 Ok, discarded, id=19909-04 - spam)
```

Gambar 4.68 *Email* dari *Gmail* Terindikasi *Spam*

4.2.2.2.4. Uji Coba Mengirim *Email Spam* Tanpa *GTUBE Test*

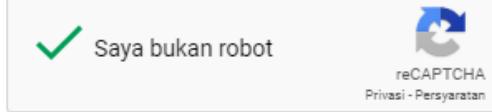
Uji coba mengirim *email* yang terindikasi *spam* oleh *Yahoo! Mail* adalah dengan mengirim *email* melalui *Emkei's Fake Mailer* dengan format

email spam yang berisi penipuan atau promosi suatu produk seperti terlihat pada gambar 4.69 berikut.

From Name: Hendarto
From E-mail: hendarto@skripsi.online
To: naufalhanif74@yahoo.com
Subject: Coba
Attachment: Pilih File Tidak ada file yang dipilih
Attach another file
[Advanced Settings](#)

Content-Type: text/plain text/html Editor

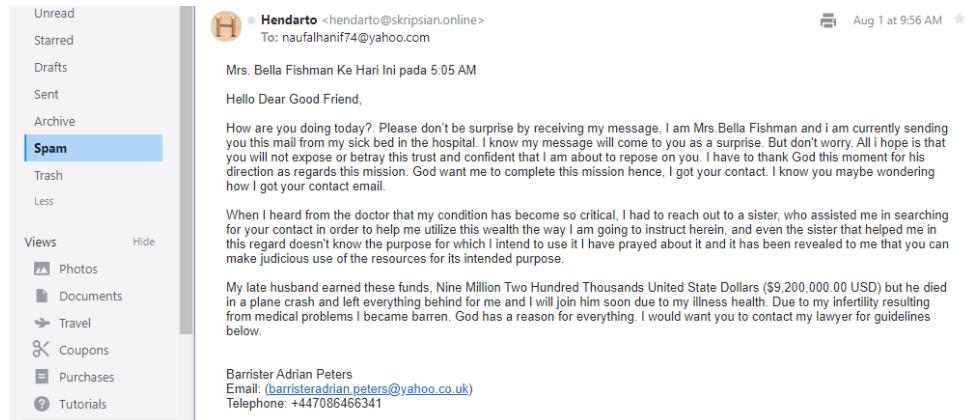
Text: Mrs. Bella Fishman Ke Hari Ini pada 5:05 AM
Hello Dear Good Friend,
How are you doing today?. Please don't be surprise by receiving my message, I am Mrs.Bella Fishman and i am currently sending you this mail from my sick bed in the hospital. I know my message will come to you as a surprise. But don't worry. All i hope is that you will not expose or betray this trust and confident that I am about to repose on you. I have to thank God this moment for his direction as regards this mission. God want me to complete this mission hence, I got your contact. I know you maybe wondering how I got your contact email.

Captcha: 
reCAPTCHA
Privasi - Persyaratan

Send **Clear**

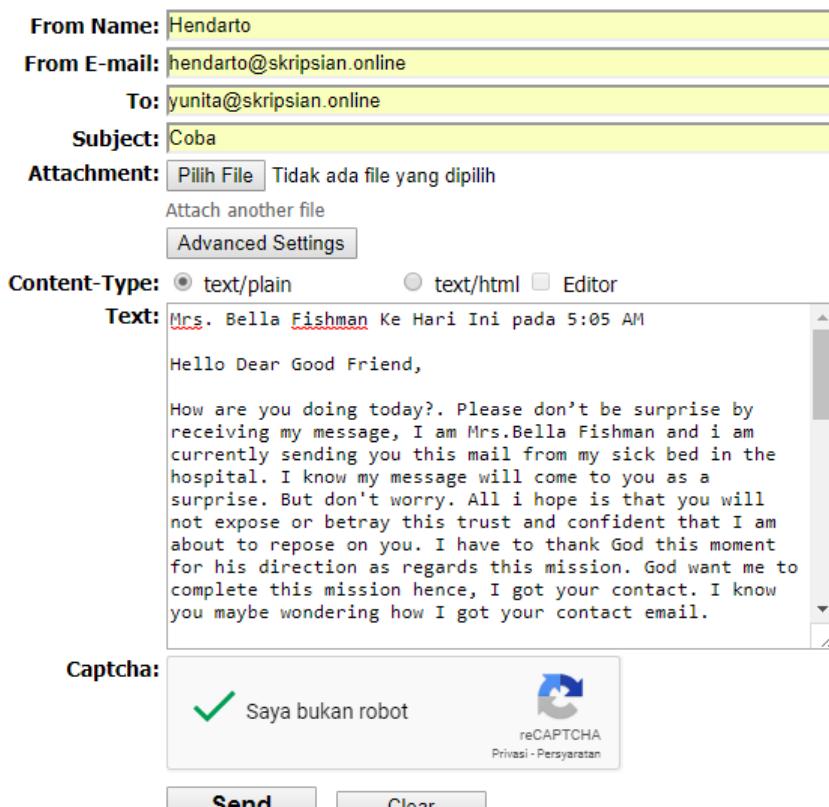
Gambar 4.69 Email Dengan Format Spam

Email dengan *format spam* tersebut terkirim ke *Yahoo! Mail* dan masuk ke dalam *folder spam* seperti terlihat pada gambar 4.70 berikut.



Gambar 4.70 Email Terindikasi Sebagai Spam oleh Yahoo! Mail

Yahoo! Mail mengindikasi bahwa *email* tersebut diatas merupakan *spam* sehingga *format email* tersebut diatas dapat dijadikan acuan untuk melakukan uji coba mengirim *email spam* tanpa *GTUBE test* dengan cara mengirim *email* seperti *format email* tersebut diatas dari *Emkei's Fake Mailer* ke salah satu *user* yang ada pada layanan *email* skripsi.ononline seperti terlihat pada gambar 4.71 berikut.



Gambar 4.71 Mengirim Email Spam Tanpa Format GTUBE Test

Email spam tanpa format GTUBE Test tersebut terindikasi sebagai *spam* oleh *mail server* skripsi.ononline karena memiliki skor 7,502, sedangkan skor yang dapat ditoleransi oleh *SpamAssassin* adalah 5,0 (*default score*) sehingga *email* yang memiliki skor lebih besar atau sama dengan 5,0 akan langsung diblokir karena terindikasi sebagai *spam* dan *email* yang memiliki skor lebih rendah dari 5,0 akan masuk pada kotak masuk karena dianggap sebagai *email ham* seperti terlihat pada gambar 4.72 dan 4.73 berikut.

```
# Set the threshold at which a message is considered spam (default: 5.0)
#
required_score 5.0
```

Gambar 4.72 Default Score SpamAssassin

```

Aug  1 08:59:19 nsl amavis[20182]: (20182-07) Blocked SPAM (DiscardedInbound,Quarantined), [46.167.245.206]:35806 [46.167.245.206] <hendarto@skripsi.online> -> <yunita@skripsi.online>, Queue-ID: 8DE0F303688B, Message-ID: <20180801015908.C317BD62E4@emkei.cz>, mail_id: 3jtzqVY6YSVjF, Hits: 7.502, size: 2596, 10973 ms
Aug  1 08:59:19 nsl postfix/smtp[32150]: 8DE0F303688B: to=<yunita@skripsi.online>, relay=127.0.0.1[127.0.0.1]:10024, delay=13, delays=2/0.06/0.02/11, dsn=2.7.0, status=sent (250 2.7.0 Ok, discarded, id=20182-07 - spam)

```

Gambar 4.73 Skor *Email* yang Terindikasi Sebagai *Spam*

4.2.2.2.3. Uji Coba Mengirim *Email* yang Mengandung *Virus*

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

4.2.2.2.3.1. Uji Coba Mengirim *Email* yang Mengandung *Virus* dari skripsi.online

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* skripsi.online ke layanan *email* skripsi.online, seperti pada gambar 4.74 berikut.



Gambar 4.74 *EICAR Test* dari skripsi.online Setelah Penerapan

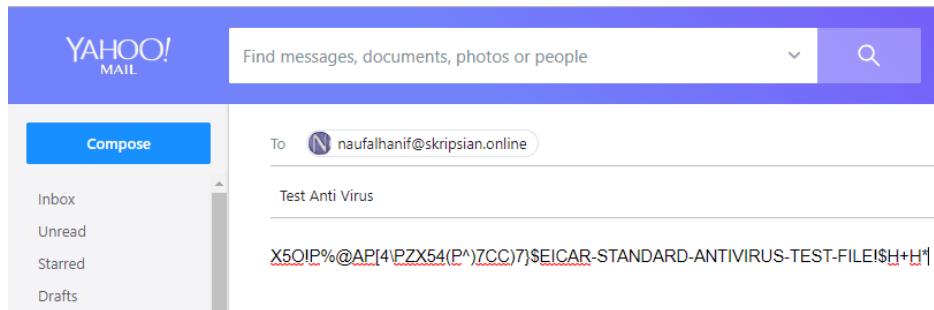
Setelah *email* yang mengandung *virus* tersebut dikirim ke salah satu *user email* yang ada pada *mail server* skripsi.ononline maka *email* tersebut akan *diblock* oleh *Amavisd-New* karena *email* tersebut telah terdeteksi mengandung *virus* oleh *ClamAV* yang merupakan *anti virus mail server* skripsi.ononline. cara untuk mengecek bahwa *email* tersebut telah terblok adalah dengan membuka *mail log server* dengan perintah `#cat /var/log/maillog`, seperti terlihat pada gambar 4.75 berikut.

```
Jul  8 12:08:55 ns1 clamd[24191]: /var/spool/amavisd/tmp/amavis-20180708T120037-19909-VQym_s8x/parts/p002: Eicar-Test-Signature FOUND
Jul  8 12:08:55 ns1 clamd[24191]: /var/spool/amavisd/tmp/amavis-20180708T120037-19909-VQym_s8x/parts/p001: Eicar-Test-Signature FOUND
Jul  8 12:08:55 ns1 amavis[19909]: (19909-02) Blocked INFECTED (Eicar-Test-Signature) {DiscardedInternal,Quarantined}, MYNETS LOCAL [:1]:55726 <naufalhanif@skripsi.ononline> -> <yunita@skripsi.ononline>, Queue-ID: 7E1B4303682F, Message-ID: <9809faf37ca5e673ele6e42074f9749f@skripsi.ononline>, mail_id: PYBqCtqDQwAL, Hits: -, size: 1004, dkim_sd=default:skripsi.ononline, 675 ms
Jul  8 12:08:55 ns1 postfix/smtp[21537]: 7E1B4303682F: to=<yunita@skripsi.ononline>, relay=127.0.0.1[127.0.0.1]:10024, delay=1, delays=0.21/0.08/0.08/0.65, dsn=2.7.0, status=sent (250 2.7.0 Ok, discarded, id=19909-02 - INFECTED: Eicar-Test-Signature)
```

Gambar 4.75 *Email* dari skripsi.ononline Terblok

4.2.2.2.3.2. 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* skripsi.ononline, seperti pada gambar 4.76 berikut.



Gambar 4.76 EICAR Test dari Yahoo! Mail Setelah Penerapan

Setelah *email* yang mengandung *virus* tersebut di kirim pada salah satu *user email* yang ada pada *mail server* skripsi.online maka *email* tersebut akan *diblock* oleh *Amavisd-New* karena *email* tersebut telah terdeteksi mengandung *virus* oleh *ClamAV* yang merupakan *anti virus mail server* skripsi.online. cara untuk mengecek bahwa *email* tersebut telah terblok adalah dengan membuka *mail log server* dengan perintah `#cat /var/log/maillog`, seperti terlihat pada gambar 4.77 berikut.

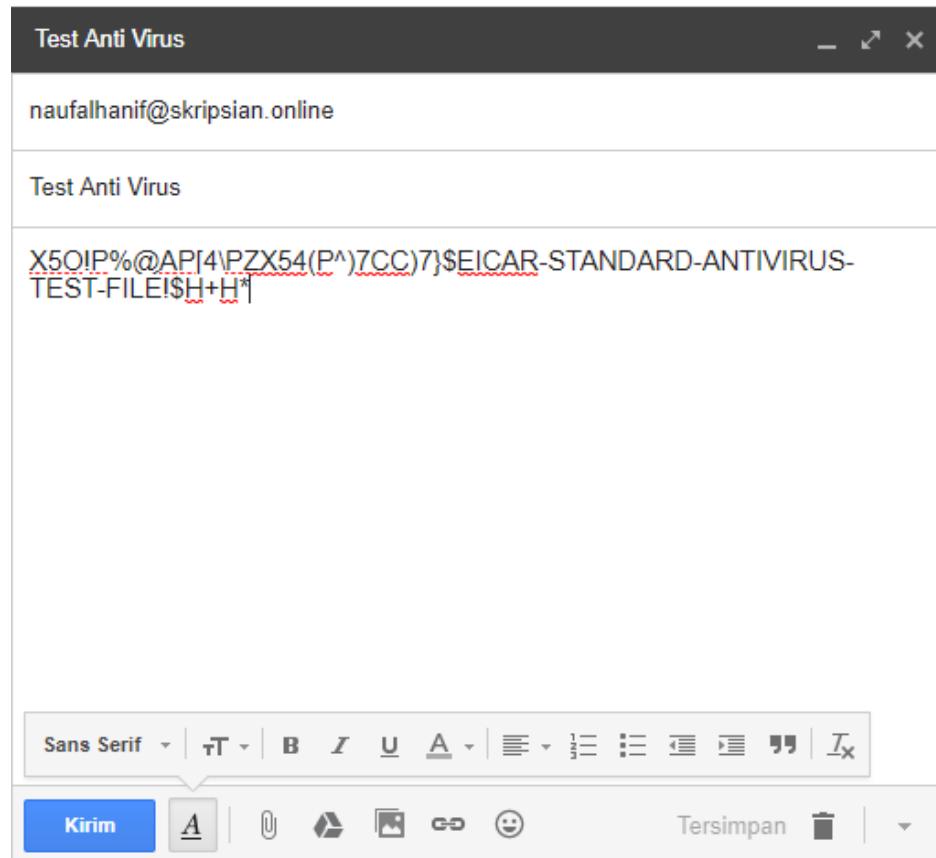
```
Jul  8 12:00:53 nsl clamd[24191]: /var/spool/amavisd/tmp/amavis-20180708T120037-19909-VQym_s8x/parts/p004: Eicar-Test-Signature FOUND
Jul  8 12:00:53 nsl clamd[24191]: /var/spool/amavisd/tmp/amavis-20180708T120037-19909-VQym_s8x/parts/p001: Eicar-Test-Signature FOUND
Jul  8 12:01:01 nsl amavis[19909]: (19909-01) Blocked INFECTED (Eicar-Test-Signature) (DiscardedInbound,Quarantined), [66.163.186.146]:35658 [66.163.186.146] <naufalhanif74@yahoo.com> -> <naufalhanif@skripsi.online>, Queue-ID: 9F71E303682F, Message-ID: <1351379827.788337.1531026026282@mail.yahoo.com>, mail_id: W4z4xU15k1I, Hits: -, size: 3559, dkim_sd=s2048@yahoo.com, 31746 ms
Jul  8 12:01:02 nsl postfix/smtp[21361]: 9F71E303682F: to=<naufalhanif@skripsi.online>, relay=127.0.0.1[127.0.0.1]:10024, delay=41, delays=6/0.01/9.9/25, dsn=2.7.0, status=sent (250 2.7.0 Ok, discarded, id=19909-01 - INFECTED: Eicar-Test-Signature)
```

Gambar 4.77 Email dari Yahoo! Mail Terblok

4.2.2.2.3. 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 skripsi.ononline, seperti pada gambar 4.78 berikut.



Gambar 4.78 EICAR Test dari Gmail Setelah Penerapan

Setelah email yang mengandung virus tersebut di kirim pada salah satu user email yang ada pada mail server skripsi.ononline maka email tersebut akan diblock oleh Amavisd-New karena email tersebut telah terdeteksi mengandung virus oleh ClamAV yang merupakan anti virus mail server skripsi.ononline. cara untuk mengecek bahwa email tersebut telah terblok adalah dengan membuka mail log server dengan perintah #cat /var/log/maillog, seperti terlihat pada gambar 4.79 berikut.

```

Jul  8 12:23:06 ns1 clamd[24191]: /var/spool/amavisd/tmp/amavis-20180708T120037-
19909-VQym_s8x/parts/p004: Eicar-Test-Signature FOUND
Jul  8 12:23:06 ns1 clamd[24191]: /var/spool/amavisd/tmp/amavis-20180708T120037-
19909-VQym_s8x/parts/p001: Eicar-Test-Signature FOUND
Jul  8 12:23:07 ns1 amavis[19909]: (19909-03) Blocked INFECTED (Eicar-Test-Signa-
ture) {DiscardedInbound,Quarantined}, [209.85.218.43]:44624 [209.85.218.43] <naufalhanif1477.nh@gmail.com> -> <naufalhanif@skripsian.online>, Queue-ID: F1B14303
682F, Message-ID: <CAEOh3LFoXBYtXNErFq_FAnhvRPAgW8nMS8vCdApBiDzzwlvPA@mail.gmai
l.com>, mail_id: xELLAfPNT2UQ, Hits: -, size: 3357, dkim_sd=20161025@gmail.com,
1380 ms
Jul  8 12:23:07 ns1 postfix/smtp[21727]: F1B14303682F: to=<naufalhanif@skripsian
.online>, relay=127.0.0.1[127.0.0.1]:10024, delay=4.6, delays=3.1/0.08/0.02/1.4,
dsn=2.7.0, status=sent (250 2.7.0 Ok, discarded, id=19909-03 - INFECTED: Eicar-
Test-Signature)

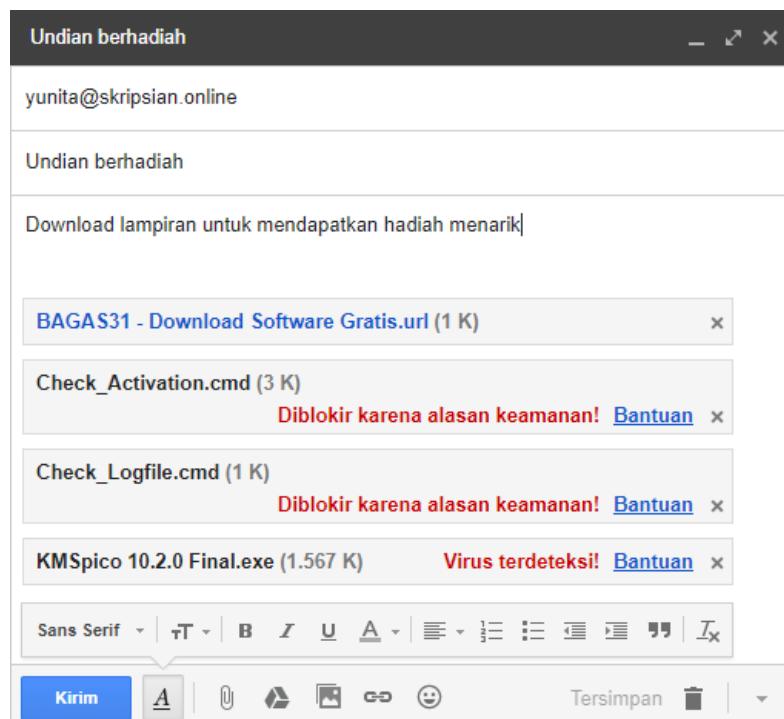
```

Gambar 4.79 Email dari Gmail Terblok

4.2.2.2.3.4. Uji Coba Mengirim Email Virus Tanpa Menggunakan

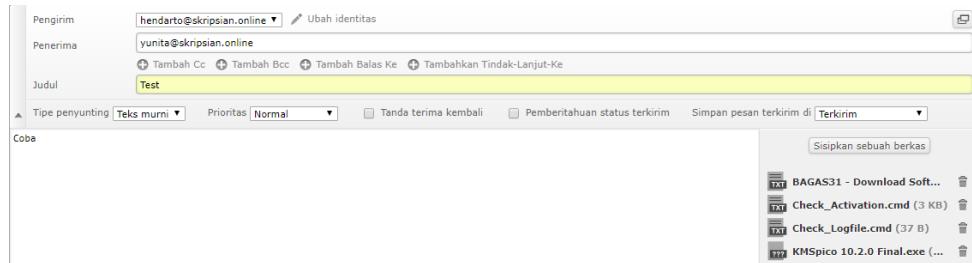
EICAR Test

Uji coba mengirim *email* yang mengandung *virus* dilakukan dengan mengirim *email* dari layanan *email gmail*, *email* yang dikirim diberi lampiran berupa program *crack* dengan ekstensi .exe yang akan terdeteksi sebagai *virus* oleh *gmail* seperti terlihat pada gambar 4.80 berikut.



Gambar 4.80 Lampiran Terdeteksi Sebagai Virus

Lampiran yang telah terdeteksi sebagai *virus* oleh layanan *email* *gmail* akan dikirim ke layanan *email* skripsi.ononline untuk menguji layanan *email* skripsi.ononline sebelum penerapan *anti virus* seperti terlihat pada gambar 4.81 berikut.



Gambar 4.81 Mengirim Virus Setelah Penerapan Anti Virus

Email yang mengandung *virus* tersebut diblokir oleh *Amavisd-New* karena terdeteksi mengandung *virus*. seperti terlihat pada gambar 4.82 berikut.

```
Aug  3 19:52:56 ns1 clamd[17546]: /var/spool/amavisd/tmp/amavis-20180803T194946-17584-bcV27luA/parts/p007: Win.Trojan.Agent-5420570-0 FOUND
Aug  3 19:52:57 ns1 clamd[17546]: /var/spool/amavisd/tmp/amavis-20180803T194946-17584-bcV27luA/parts/p005: Win.Trojan.Agent-5420570-0 FOUND
Aug  3 19:53:07 ns1 amavis[17584]: (17584-01) Blocked INFECTED (Win.Trojan.Agent-5420570-0) {DiscardedInternal,Quarantined}, MYNETS LOCAL [:1]:56688 <hendarto@skripsi.ononline> -> <yunita@skripsi.ononline>, Queue-ID: A60B5303682B, Message-ID: <b5b9dcaa557f532f61e2494b694091c@skripsi.ononline>, mail_id: PrbMSj80p-WE, Hits: -, size: 2201148, dkim_sd=default:skripsi.ononline, 209013 ms
Aug  3 19:53:07 ns1 postfix/smtp[26804]: A60B5303682B: to=<yunita@skripsi.ononline>, relay=127.0.0.1[127.0.0.1]:10024, delay=216, delays=2.3/0.27/12/202, dsn=2.7.0, status=sent (250 2.7.0 Ok, discarded, id=17584-01 - INFECTED: Win.Trojan.Agent-5420570-0)
```

Gambar 4.82 Email Terdeteksi Mengandung Virus

4.2.2.2.4. Uji coba pengecekan *header email*

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

4.2.2.2.4.1. Header Email pada Gmail

Uji coba ini dilakukan dengan mengirim *email* menggunakan salah satu *user email* yang ada pada layanan *email* skripsi.ononline ke salah satu *user email* yang ada pada layanan *email* *Gmail* kemudian melakukan pengecekan *header email* tersebut dan melakukan perbandingan terhadap *header email* sebelum dan setelah penerapan *DKIM*, *SPF*, *anti spam*, dan *anti virus*, *header email* setelah diterapkannya *DKIM*, *SPF*, *anti spam*, dan *anti virus* terlihat seperti gambar 4.83 berikut.

```
Authentication-Results: mx.google.com;
dkim=pass header.i=@skripsi.ononline header.s=default header.b=Gw8y7ydm;
dkim=pass header.i=@skripsi.ononline header.s=default header.b=c+ULa20;
spf=pass (google.com: domain of naufalhanif@skripsi.ononline designates 103.112.162.228 as permitted sender)
smtp.mailfrom=naufalhanif@skripsi.ononline
Received: from localhost ([unKnown [127.0.0.1]]) by ns1.skripsi.ononline (Postfix) with ESMTP id 71F03306AF72; Wed, 27 Jun 2018
07:26:30 +0000 (UTC)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=skripsi.ononline; s=default; t=1530084390;
bh=7EE6rR/7Lj10C1YzWMPGgbVc1Myf6gczz4HUIXpvg8; h=Date:From:To:Subject;
b=Gw8y7ydm3jcx6QnlpGs2+j1lY09djfhCemt8n+XL8hfJZk2R3U3FAIHfKKcj06B2
ZUSGeByEc0bYkp6bKF4RX0dZeqCKsu2jAS4nLXkCEauPVFB1sf0eUzDRYq5Yyt0x/
OS13FIntzniu2UMKFD4MbfAu2Rfu1qjYHwUY1m8=
X-Virus-Scanned: amavisd-new at skripsi.ononline
Received: from ns1.skripsi.ononline ([127.0.0.1]) by localhost (ns1.skripsi.ononline [127.0.0.1]) (amavisd-new, port 10024) with
ESMTP id dhMOADmqIz77; Wed, 27 Jun 2018 14:24:41 +0700 (WIB)
Received: from localhost ([localhost [IPV6::1]]) by ns1.skripsi.ononline (Postfix) with ESMTPA id 6EF283069687; Wed, 27 Jun 2018
14:24:34 +0700 (WIB)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=skripsi.ononline; s=default; t=1530084274;
bh=7EE6rR/7Lj10C1YzWMPGgbVc1Myf6gczz4HUIXpvg8; h=Date:From:To:Subject;
b=c+ULa20kPPWbj2U0Bgfs0F8/mPYySS/1J50A25XGzq3zyFT/bduhu88902
aizTY7Cw18o/H2aq3jXjd+18vDBjsTOjtTsxlFHVmfeoFXQIS//1feZ20CqIVDp
cIPkVrxrmXvJVS/es8DBHukv1pSrgV1d4psycq+M=
```

Gambar 4.83 Cuplikan Header Email pada Gmail Setelah Penerapan

Pada gambar 4.62 terlihat perbedaan *header email* setelah penerapan *DKIM*, *SPF*, dan *anti virus* yaitu terdapat tambahan parameter *X-Virus-Scanned*, dan *DKIM-Signature*.

4.2.2.2.4.2. Header Email pada Yahoo! Mail

Uji coba ini dilakukan dengan mengirim *email* menggunakan salah satu *user email* yang ada pada layanan *email* skripsi.ononline ke salah satu *user* yang ada pada layanan *email* *Yahoo! Mail* kemudian melakukan pengecekan *header email* tersebut dan melakukan perbandingan terhadap *header email* sebelum dan setelah penerapan *DKIM*, *SPF*, *anti spam*, dan

anti virus, header email setelah diterapkannya *DKIM, SPF, anti spam, dan anti virus* terlihat seperti gambar 4.84 berikut.

```

Received-SPF: pass (domain of skripsi.ononline designates 103.112.162.228 as permitted sender)
X-YMailISG: Jy3jTxwvLd6z2VzPt1w89_X0XpN_ReRvOjVsDfMv14yqHvo
SPDj0dL04U4wDxx1rOeup897N5wf7nFaP_ePmXry_9EF92iYGLL_52tguehZ6
jQeDQmzeIE5e01bmvyx71__Pc8c0pRkXhXUgaUeUGBVVL1B55A5eZ9ud60u
701s5231kj24mrFaFkY1d8vTmxE246P7Q21pmgD61Ec1FLa1zrk4aS
CVj193B2h2XrCbQH9y15Gnqy95Fnf1VjAdhBzoyX01w8uGFIk5kbpKY_IaJ0
c8d0Y6wlu4Ccs_t1lMoze5vgyfb65nCLpuqjvxpx2Uhzv62rqueb_WsH3
y9kdofuuhTcvw8y90khfQVK217o4vsj50UThapQdIYRybkdMVGKokf8pWlo
oQKRUEEQs3nyt3wEyay0Vg33EVy25o1z_uhxh_EltcdKruDzYka71EOQb6
7_nHjZxyIJUJUFBkpl20nqj1HfEylScxa_FtrolkL61Tvb5n10^jRJd15
2cnHh1k_e9voZ6unATSK/2R4_71c1PQwct08A01G3mxnU-MEZm_bCG9Rbkch
catYXXZDFzNvQg_2mSuSx45f5x5xRtu2Qa1wKNSKuidH9E1EuVmRnSy4v871
Xnun80lw19WkzQxaErQgFQIAvw891qBnsGTgxYYtb7tmmnPFLw61PBZQ1
_73m0i0ET_dh1o3Jefp1ntzvRLRkRehAK6L8j1XmJ02nCVspvOp1bw1
QLA_1x-BcQ5nFxkz311npfxsq_hGoUfXca15D1RUWk4w4d6rhFOqc@N
ZhypEy7RCUqgJKiwdhcgPMNqJgiwFunC2K_ko13extYTx12YemEqbnMcx
7003bo7bX0atkYObkvu1Bq_9t681XTDGZ9esBn1VGDCL25hN7gE5w71wA
np2A+V741wqYeIQ047yp5V9dK0KN1rLXQgbocGejnjmn5_NsRMMJ3duF
_F37dayZQMLBHE2gsahCNhAYtYbX95_Nsce1oP8c3z8PXxhknzP7I7xUa
Co6_bvOJXPNB-
X-Originating-IP: [103.112.162.228]
Authentication-Results: mta4270.mail.bf1.yahoo.com from=skripsi.ononline; domainkeys=neutral (no sig); from=skripsi.ononline; dkim=pass (ok)
Received: from 127.0.0.1 (EHLO ns1.skripsi.ononline) (103.112.162.228)
by mta4270.mail.bf1.yahoo.com with SMTP; Wed, 27 Jun 2018 07:26:31 +0000
Received: from localhost (UnKnown [127.0.0.1])
by ns1.skripsi.ononline (Postfix) with ESMTP id 71F03306AF72;
Wed, 27 June 2018 07:26:30 +0000 (UTC)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=skripsi.ononline;
s=default; t=1530084390;
bh=EE66R/7Lj10CYzWfFG6bVc1Myf6gzCzz4HU1Xpvpg8=;
h=Date:From:To:Subject;
b=Q08j7ydm3jCx5QoWNgzAjl1v0djfhEmT8nXL8hF3Z3k2R3U3F41HfkKcj06B2
ZUSGeByEce0bykp6bKF4RX0dZ0qCksu2jAS4nLXkCEauPVFB15f0eUzdRYq5YtoX
OS13FIntIniu2Ulkf4Dlbfau2Rfu1qjYHuUv1m8=
X-Virus-Scanned: amavisd-new at skripsi.ononline

```

Gambar 4. 84 Cuplikan Header Email pada Yahoo! Mail Setelah Penerapan

Pada gambar 4.84 terlihat perbedaan *header email* setelah penerapan *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 (OK)* dan terdapat tambahan parameter *DKIM-Signature* dan *X-Virus-Scanned*.

4.2.2.2.4.3. Header Email pada skripsi.ononline

Uji coba ini dilakukan dengan mengirim *email* menggunakan salah satu *user email* yang ada pada layanan *email* skripsi.ononline ke salah satu *user email* yang ada pada layanan *email* skripsi.ononline kemudian melakukan pengecekan *header email* tersebut dan melakukan perbandingan terhadap *header email* sebelum dan setelah penerapan *DKIM, SPF, anti spam, dan anti virus, header email* setelah diterapkannya *DKIM, SPF, anti spam, dan anti virus* terlihat seperti gambar 4.85 berikut.

```

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=skripsi.online;
s=default; t=1530239492;
bh=5jtrnNw9RJpLzzBAVfY5dy+L5y+H+RNH4s8DSbVA2Ek=;
h=Date:From:To:Subject;
b=asreqFSmSoOwAmABCcP5PyLZmrQZbv7rg0UoRQn0/S48QmzuHioDB7iFbWLWHIN2K
JPrZDqaCb+GSoYBvoFjyWAUVdtOEWA6PlIV+x0+JK10ZgMuJA/K78twCZQXQFlXU
13cb1vw42pR9jClwigDRuVdTnoEHkIviXZEZWpY=
X-Virus-Scanned: amavisd-new at skripsi.online
Authentication-Results: ns1.skripsi.online (amavisd-new);
dkim=pass (1024-bit key) header.d=skripsi.online
Received: from ns1.skripsi.online ([127.0.0.1])
by localhost (ns1.skripsi.online [127.0.0.1]) (amavisd-new, port 10024)

```

Gambar 4.85 Cuplikan Header Email skripsi.online Setelah Penerapan

Pada gambar 4.85 terlihat perbedaan *header email* setelah penerapan *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*.

4.3. Analisa Hasil Uji Coba

Pada tahap ini akan dilakukan analisa hasil uji coba yang telah dilakukan sebelumnya. Pada analisa hasil uji coba akan di tampilkan analisa hasil uji coba pengiriman *email spoofing* sebelum dan setelah penerapan *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 *DKIM*, *SPF*, *anti spam*, dan *anti virus*.

4.3.1. Analisa Hasil Uji Coba Pengiriman *Email Spoofing*

Cara yang dapat digunakan untuk mengetahui apakah sudah dilakukan proses otorisasi dan otentikasi oleh protokol *DKIM* dan *SPF* adalah dengan melakukan pengiriman *email spoofing* menggunakan *Emkei's Fake Mailer* dengan mengatasnamakan salah satu *user email* pada *mail server* *skripsi.online*, kemudian *email* tersebut dikirim ke layanan *email Gmail*, *Yahoo! Mail*, dan *skripsi.online*. Berikut analisa

hasil ujicoba perbandingan sebelum diterapkan *DKIM* dan *SPF* dan setelah diterapkan *DKIM* dan *SPF* yang dilakukan pada uji coba sebelumnya, seperti terlihat pada tabel 4.1 berikut.

Tabel 4.1 Perbandingan Sebelum dan Setelah Penerapan *DKIM* dan *SPF*

NO	Fake Mailer	Layanan Email yang diatasnamakan	Layanan Email Penerima	Sebelum Penerapan	Setelah Penerapan
1	<i>Emkei's Fake Mailer</i>	skripsi.ononline	Gmail	Masuk Folder Inbox	Diblokir
2	<i>Emkei's Fake Mailer</i>	skripsi.ononline	Yahoo! Mail	Masuk Folder Inbox	Masuk Folder Spam
3	<i>Emkei's Fake Mailer</i>	skripsi.ononline	skripsi.ononline	Masuk Folder Inbox	Masuk Folder Inbox

Berdasarkan tabel 4.1 perbandingan sebelum dan setelah penerapan *DKIM* dan *SPF* dengan melakukan pengiriman *email spoofing* yang dikirim menggunakan *Emkei's Fake Mailer* ke layanan *email Gmail*, *Yahoo! Mail*, dan skripsi.ononline sebelum penerapan *DKIM* dan *SPF* yaitu *email spoofing* berhasil masuk ke *folder inbox* penerima *email* yang berada pada *mail server Gmail*, *Yahoo! Mail*, dan skripsi.ononline sedangkan setelah penerapan *DKIM* dan *SPF*, *email spoofing* tersebut diblokir oleh layanan *email Gmail*, dimasukan ke *folder spam* oleh layanan *email Yahoo!* *Mail* dan dimasukan ke *folder inbox* oleh layanan *email* skripsi.ononline.

4.3.2 Analisa Hasil Uji Coba Pengiriman *Email Spam*

Analisa penerapan *anti spam* dilakukan dengan mengirim *email spam* dengan menggunakan layanan *email* skripsi.ononline, *Yahoo! Mail*, dan *Gmail* ke layanan *email* skripsi.ononline untuk menguji kinerja *anti*

spam sebelum dan setelah penerapan *anti spam* seperti terlihat pada tabel 4.2 berikut.

Tabel 4.2 Perbandingan Sebelum dan Setelah Penerapan *Anti Spam*

NO	Layanan <i>Email</i> Pengirim	Layanan <i>Email</i> Penerima	Sebelum Penerapan	Setelah Penerapan
1	<i>Yahoo! Mail</i>	skripsi.ononline	Masuk <i>Folder Inbox</i>	Diblokir
2	<i>Gmail</i>	skripsi.ononline	Masuk <i>Folder Inbox</i>	Diblokir
3	skripsi.ononline	skripsi.ononline	Masuk <i>Folder Inbox</i>	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* skripsi.ononline, 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*.

4.3.3 Analisa Hasil Uji Coba Mengirim *Email* Mengandung

Virus

Analisa penerapan *anti virus* dilakukan dengan mengirim *email* *spam* dengan menggunakan layanan *email* skripsi.ononline, *Yahoo! Mail*, dan *Gmail* ke layanan *email* skripsi.ononline untuk menguji kinerja *anti spam* sebelum dan setelah penerapan *anti spam* seperti terlihat pada tabel 4.3.

Tabel 4.3 Perbandingan Sebelum Penerapan *Anti virus*

NO	Layanan <i>Email</i> Pengirim	Layanan <i>Email</i> Penerima	Sebelum Penerapan	Setelah Penerapan
----	-------------------------------	-------------------------------	-------------------	-------------------

1	<i>Yahoo! Mail</i>	skripsi.ononline	Masuk <i>Folder Inbox</i>	Diblokir
2	<i>Gmail</i>	skripsi.ononline	Masuk <i>Folder Inbox</i>	Diblokir
3	skripsi.ononline	skripsi.ononline	Masuk <i>Folder Inbox</i>	Diblokir

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* skripsi.ononline, sedangkan setelah penerapan *anti virus*, terjadi pemblokiran *email* yang mengandung *virus* oleh *Amavisd-New* sehingga *email* yang terindikasi mengandung *virus* langsung diblokir sebelum sampai pada *folder* penerima *email*.

4.3.4 Analisa Hasil Uji Coba Pengecekan *Header Email*

Analisa pengecekan *header email* dilakukan dengan melihat *header email* sebelum dan setelah penerapan *DKIM*, *SPF*, *anti spam*, dan *anti virus*. Perbedaan *header email* sebelum dan setelah diterapkan *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	X-Virus-Scanned	Received-SPF
1	Sebelum Penerapan	Gmail	Tidak Ada	Tidak Ada	Pass
		Yahoo! Mail	Tidak Ada	Tidak Ada	None
		skripsi.ononline	Tidak Ada	Tidak Ada	Tidak Ada
2	Setelah Penerapan	Gmail	Ada	Ada	Pass
		Yahoo! Mail	Ada	Ada	Pass
		skripsi.ononline	Ada	Ada	Tidak Ada

Berdasarkan tabel 4.4, sebelum penerapan *DKIM, SPF, anti spam*, dan *anti virus* tidak terdapat parameter *DKIM-Signature* dan *X-Virus-Scanned*, namun *Received-SPF* sudah bernilai *Pass* pada *header email* di *Gmail*, sedangkan setelah penerapan *DKIM, SPF, anti spam*, dan *anti virus* terdapat parameter *DKIM-Signature* dan *X-Virus-Scanned*, serta *Received-SPF* bernilai *Pass* pada *header email* di *Gmail*.

Sebelum penerapan *DKIM, SPF, anti spam*, dan *anti virus* tidak terdapat parameter *DKIM-Signature* dan *X-Virus-Scanned*, serta *Received-SPF* bernilai *none* pada *header email* di *Yahoo! Mail*, sedangkan setelah penerapan *DKIM, SPF, anti spam*, dan *anti virus* terdapat parameter *DKIM-Signature* dan *X-Virus-Scanned*, serta *Received-SPF* bernilai *Pass* pada *header email* di *Yahoo! Mail*.

Sebelum penerapan *DKIM, SPF, anti spam*, dan *anti virus* tidak terdapat parameter *DKIM-Signature*, *X-Virus-Scanned*, dan *SPF-Received* pada *header email* di *skripsiian.online*, sedangkan setelah penerapan *DKIM, SPF, anti spam*, dan *anti virus* terdapat parameter *DKIM-Signature* dan *X-Virus-Scanned*, namun tetap tidak terdapat parameter *Received-SPF* pada *header email* di *skripsiian.online*.

BAB V

PENUTUP

5.1. Kesimpulan

Berdasarkan hasil ujicoba yang telah dilakukan maka dapat diperoleh kesimpulan sebagai berikut:

1. Penerapan protokol *DomainKeys Identified Mail* dapat mencegah *email spoofing* dengan cara melakukan otentikasi menggunakan metode pencocokan *private key* dan *public key* (*Asymmetric keys*).
2. Penerapan protokol *Sender Policy Framework* dapat mencegah *email spoofing* dengan cara melakukan otorisasi menggunakan metode pencocokan alamat *IP server pengirim*.
3. Penerapan *SpamAssassin*, *ClamAV*, dan *Amavisd-New* dapat mencegah masuknya *email spam* dan *virus* dengan cara melakukan pengecekan *header*, *body*, dan *attachment email*.

5.2. Saran

Adapun saran-saran untuk pengembangan penelitian ini lebih lanjut adalah sebagai berikut:

1. Mengembangkan sistem otentikasi dan otorisasi *email spoofing* dengan menambahkan protokol *DMARC*.
2. Mengembangkan sistem *anti spam* dengan menggunakan *database kolaboratif SpamAssassin* yaitu Pyzor, Razor2, dan DCC serta menggunakan fitur *blacklist* dan *whitelist* *SpamAssassin* untuk memaksimalkan kinerja *SpamAssassin*.

3. Mengembangkan sistem *anti spam* dengan menambahkan *tools anti spam* lainnya seperti *Barracuda Central*, *Spamhaus*, *SpamCop*, *SORBS*, dan lain-lain.

DAFTAR REFERENSI

- Ardiantoro, T., Triyono, J., Fatkhiyah, E. (2016). Optimalisasi rancangan jaringan komputer menggunakan *google sketchup*. *Jurnal JARKOM*, 4, 81-88.
- Arrington, M. (2006), Internet. *Single Ajax Interface for Yahoo Mail & IM Coming*. Diperoleh Juli 22, 2018, dari <https://www.techcrunch.com/2006/11/09/single-ajax-interface-for-yahoo-mail-im-coming/>
- Barovih, G. (2011). Desain dan implementasi *mail server* berbasis *web* beserta pengamannya pada PT. PLN (persero) sektor pembangkitan bukit asam tanjung enim. Sekolah Tinggi Manajemen Informatika dan Komputer PalComTech Palembang. 1-10.
- Chandra, W. N., Indrawan, G., Sukajaya, I. N. (2016). *Spam filtering* dengan metode *pos tagger* dan klasifikasi *naïve bayes*. *Jurnal Ilmiah Teknologi dan Informasi ASIA*, 10, 47-55.
- CentOS Web Panel. (n.d.), Internet. *Control Web Panel*. Diperoleh 30 Juni, 2018, dari <http://centos-webpanel.com/>
- Crocker, D. (2009). *Internet Mail Architecture. Request for Comments: 5598*, 1-39.
- Desmira., Sumarto, D., Yuliani, R. (2017). Rancang bangun *mail server* berbasis *squirrelmail* menggunakan MTA (*Mail Transfer Agent*) pada PT. Teras Inti Media. *Jurnal PROSISKO*, 4, 55-59.
- Emkei's Mailer, Internet. *Free Online Fake Mailer with Attachments, Encryption, HTML Editor and Advanced Settings*. Diperoleh Juni 20, 2018, dari <https://emkei.cz/>
- Fitriani, R. E., Riyono, A. (2015). Mendesain keamanan sistem jaringan. *Jurnal Ilmiah*, 1-21.
- Google. (n.d.), Internet. Gmail. Diperoleh 21 Juni, 2018, dari <https://www.google.com/gmail/>
- Hansen, T., Crocker, D., Baker, P. H. (2009). *DomainKeys Identified Mail (DKIM) Service Overview. Request for Comments: 5585*, 1-24.
- Harjono, E. B. (2016). Analisa dan implementasi dalam membangun sistem operasi *linux* menggunakan metode *LSF* dan *remaster*. *Jurnal & Penelitian Teknik Informatika*, 1, 30-35.
- Haryanto, M. D., Riadi, I. (2014). Analisis dan optimalisasi jaringan menggunakan teknik *load balancing* (studi kasus: jaringan UAD kampus 3). *Jurnal Sarjana Teknik Informatika*, 2, 1370-1378.
- Hayuningtyas, R. Y. (2017). Aplikasi *filtering of spam email* menggunakan *naïve bayes*. *Indonesian Journal on Computer and Information Technology*, 2, 53-60.

- Hidayat, W. N., Pangera, A. A. (2010). Membangun *mail server* berbasis linux menggunakan *postfix* dengan *client squirrelmail*. Sekolah Tinggi Manajemen Informatika dan Komputer Amikom Yogyakarta.
- Hoiriyah., Sugiantoro, B., Prayudi, Y. (2016). Investigasi forensik pada *e-mail spoofing* menggunakan metode *header analysis*. *Jurnal Ilmiah DASI*, 17, 20-25.
- Kader, D. P., Najoan, M. E. I., Sinsuw, A. A. E. (2014). Analisa performansi algoritma *routing* di jaringan komputer UNSRAT. *E-journal Teknik Elektro dan Komputer*, 28-39.
- Kusmaya. (2016). Implementasi *mail server* menggunakan *postfix*. *Jurnal Informasi*, 8, 49-69.
- Martinec, M. (2016), Internet. Amavisd-New. Diperoleh Juni 20, 2018, dari <https://amavis.org/#intro>
- Masero, A. P., Triyono, J., Andayati, D. (2013). Perancangan pengelolaan jaringan *IT* pada institut sains & teknologi AKPRIND menggunakan teknologi *VPN* (*Virtual Private Network*). *Jurnal JARKOM*, 1, 20-30.
- Mawarsih, A. (2014). Pengaruh *electronic mail* sebagai media komunikasi terhadap mengerjakan tugas kuliah mahasiswa. *Ejournal Ilmu Komunikasi*, 2, 334-348.
- Muarif, M. I., Irwan, D. (2017). Sistem *auto backup* elektronik *mail* pada *mail server* menggunakan *cron job*. *Jurnal Penelitian Ilmu Komputer*, 5, 79-90.
- Nurfajar, A., Kurniawan, M. T., Hediyan, U. Y. K. S. (2015). Desain dan analisa infrastruktur jaringan *wired* di PDII-LIPI jakarta dengan menggunakan metode *Network Development Life Cycle (NDLC)*. *e-Proceeding of Engineering*, 2, 5359-5365.
- Nurlina., Irmayana. (2014). Studi banding *spam-assassin mail server* dengan dan tanpa *filter* di sisi *mail client*. *Citec Journal*, 1, 77-88.
- Pratama, A. M. R. (2008). Perancangan dan implementasi *mail server* berbasis *qmail* pada *jcpnel web hosting control panel*. Seminar Nasional Aplikasi Teknologi Informasi 2008, 1-7.
- Riadi, I. (2011). Optimalisasi keamanan jaringan menggunakan *pemfilteran* aplikasi berbasis mikrotik. *JUSI*, 1, 71-80.
- Sadikin, N. (2014). Implementasi *e-mail server* terdistribusi pada jaringan *Local Area Network (LAN)* dan *Wide Area Network (WAN)*. Seminar Nasional Teknologi Informasi dan Multimedia 2014, 7-12.
- Saputra, A., Syafrizal, M. (2012). Perancangan dan implementasi *mail server* pada CV. Sanjaya Anugerah Sejahtera (ISP Jogjaringan) berbasis *open source*. *Jurnal DASI*, 13, 1-6.
- Sujana, A. P. (2014). Perangkat pendukung forensik lalu lintas jaringan. *Jurnal Teknik Komputer Unikom*, 3, 31-37.

- Suryana, A. L., Akbar, R. R. E., Widiyasono, N. (2016). Investigasi *email spoofing* dengan metode *Digital Forensics Research Workshop (DFRWS)*. Jurnal Edukasi dan Penelitian Informatika, 2, 112-117.
- The Roundcube Team. (n.d.), Internet. *About the Roundcube webmail project*. Diperoleh 30 Juni, 2018, dari <https://roundcube.net/about/>
- Valsecchi, P. (2013), Internet. *Secure Postfix with Amavisd, ClamAV, SpamAssassin*. Diperoleh Juni 20, 2018, dari <https://nolabnoparty.com/en/secure-postfix-amavisd-clamav-spamassassin/>
- Wardoyo, S., Ryadi, T., Fahrizal, R. (2014). Analisis performa *file transport protocol* pada perbandingan metode IPv4 murni, IPv6 murni dan *tunneling 6to4* berbasis router mikrotik. Jurnal Nasional Teknik Elektro, 3, 106-117.
- Wicitra, A., Utomo, D., Wardana, H. K. (2014). Membangun infrastruktur komputasi awan privat *single cluster* dan *multi cluster* dengan menggunakan *linux CentOS*. Techné Jurnal Ilmiah Elektroteknika, 13, 185-194.
- Zabar, A. A., Novianto, F. (2015). Keamanan *HTTP* dan *HTTPS* berbasis web menggunakan sistem operasi kali linux. Jurnal Ilmiah Komputer dan Informatika, 4, 69-74.
- Zimbra a Synacor Product. (2005), Internet. *Best Practices on Email Protection: SPF, DKIM and DMARC*. Diperoleh 22 Juni, 2018, dari https://wiki.zimbra.com/wiki/Best_Practices_on_Email_Protection:_SPF,_DKIM_and_DMARC

LAMPIRAN A

HEADER EMAIL

Header Email pada Gmail Sebelum Penerapan

Delivered-To: naufalhanif1477.nh@gmail.com

Received: by 2002:a9d:1b90:0:0:0:0:0:0 with SMTP id z16-v6csp2930798otd; Thu, 24 May 2018 20:14:27 -0700 (PDT)

X-Google-Smtp-Source: AB8JxZrCk7AjzJqbCSSgEp+7rgOmLXunmoGj1lvVEo1FspoHrtYpNYELxf18LaWU6ok+6R73tPiL

X-Received: by 2002:a63:77c9:: with SMTP id s192-v6mr563891pgc.140.1527218067862; Thu, 24 May 2018 20:14:27 -0700 (PDT)

ARC-Seal: i=1; a=rsa-sha256; t=1527218067; cv=none; d=google.com; s=arc-20160816; b=e5850DLYx1AK4rT1EGJsT68AAAYr8whzBt/hsWmU2e1V5FCUbhEmHYrWQjpdetXuHL1771GuPOYu1DLo21wmwu81fNMmFWtyZXzeQiKgil/xeAPSb0p1mk6wwYI2j0tOagA6VTkrDD4S0tdPMY3aiDXE1Ar7J5vAxO3JFgzxBdpMxPG9/uXvaytGItmBovM4qPH8wNBSv5hpxcxBvAkmtpbDlpShGfeKTMFHGQU6FIIn1WqAdqIJEd0WUhgSoDC+CelRcqrlOlgrdFzOLFRMHqru/g6Yan/CUtnvDofpeJeBXrOaWOQfMdPIr8w==

ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816; h=user-agent:message-id:subject:to:from:date:content-transfer-encoding:mime-version:arc-authentication-results; bh=5JtrnNw9RJpLz-zAyfY5dy+L5y+H+RNH4s8DSbVA2Ek=; b=gP0Me9Pz98ZG2UgGIwWWzPGpiRuMB410sm99JEpviu9f+u1d3UX6kUVcK6Ktgt2ka21xUOq1ynPm5ujsmTtUL1JYp1gADT5etLH8Zd0JLeqXGAIxNWg0Pl0Hg5FmvHzX5jSzBzvRevKfLlK18aYrnr3sKQyzo+L3RuSnplzTmiTPoqjqDefB4ZFjQ6Y27SU1deG6szzPtO/t+kfUKb39M81yOgiAYEZuoUWsSopcep80X5+F6nvySKR67AgjPSIw9jZC0Lt6AD1Earq6oyb7FQbOwujs9ztMT0Isct7WbqhsCPucin4ct9XXHxz8Hxic3z1yJPbYBPNpMhBTCHCOQ==

ARC-Authentication-Results: i=1; mx.google.com; spf=pass (google.com: best guess record for domain of hendarto@skripsian.online designates 103.112.162.164 as permitted sender)

Return-Path: <hendarto@skripsian.online>

Received: from ns1.skripsian.online (ns1.skripsian.online. [103.112.162.164]) by mx.google.com with ESMTPS id 13-v6si22345139pld.96.2018.05.24.20.14.26 for <naufalhanif1477.nh@gmail.com> (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128); Thu, 24 May 2018 20:14:27 -0700 (PDT)

Received-SPF: pass (google.com: best guess record for domain of hendarto@skripsian.online designates 103.112.162.164 as permitted sender) client-ip=103.112.162.164; Authentication-Results: mx.google.com; spf=pass (google.com: best guess record for domain of hendarto@skripsian.online designates 103.112.162.164 as permitted sender) smtp.mailfrom=hendarto@skripsian.online

Received: from localhost (localhost [IPv6:::1]) by ns1.skripsian.online (Postfix) with ESMTPA id 77ED630535C8 for

<naufalhanif1477.nh@gmail.com>; Fri, 25 May 2018 10:13:57 +0700
(WIB)

MIME-Version: 1.0

Content-Type: text/plain; charset=US-ASCII; format=flowed

Content-Transfer-Encoding: 7bit

From: hendarto@skripsian.online

To: naufalhanif1477.nh@gmail.com

Subject: Cek Header Email

Message-ID: 4af09547044f1ef8842fd8e66b388f48@skripsian.online

X-Sender: hendarto@skripsian.online

User-Agent: Roundcube Webmail/1.2.3

Melakukan pengecekan header email

Header Email pada Gmail Setelah Penerapan

Delivered-To: naufalhanif1477.nh@gmail.com

Received: by 2002:a9d:2005:0:0:0:0:0:0 with SMTP id n5-v6csp3905089ota; Wed, 27 Jun 2018 00:26:30 -0700 (PDT)

X-Google-Smtp-Source: ADUXVKLvb8NK4fhnsz+IQuVVVM8h1geLLx16dzztNDSdcpEEzvt056eVbwLd9ZOI6MbNWTD/fwZ

X-Received: by 2002:a65:418b:: with SMTP id a11-v6mr4169890pgq.118.1530084390645; Wed, 27 Jun 2018 00:26:30 -0700 (PDT)

ARC-Seal: i=1; a=rsa-sha256; d=google.com; s=arc-20160816; b=pMob8JnJiBb78YxyRnTeyk/s9WoS/aJ3am7K0qR8UY+hiaBt/aCcHnhYZt/2yjq6ZJFdh+M5VA4QBGksqcWF2M5nXTK7YbUtB1C5go9X26DX8cEqtb91JDjBpcfG4WG3Oc6xdj1td2UGMQPhqh50QjE6OkId0Jhknirr4NT3qEQekAfSD1MNOA5u9COIzCatFWU+1SsJT4AzA6GwjPx0gnIz1PwkAtDgamu01OoxvvdMh518W9+IRVynSVal+aioDz2IQ51emhVvuPO2gYe0777sAlH3dE3Ek05UaInr9VJsLdbBk3aZ5F7ltz/hInrooIBnLwqBhFySoedM s/pw==

ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816; h=user-agent:message-id:subject:to:from:date:content-transfer-encoding:mime-version:dkim-signature:dkim-signature:arc-authentication-results; bh=7EE6rR/7Llj0C1YZwMFG6bVc1Myf6gzCzz4HU1Xpvq8=; b=xuhJWKfGtNgte5iUxg197I0jEZrqQzjVQb7+XDJZ10xw86wnOzpDpWgGkscTE0Ve eEQtaZqJ8jxhMphJswy81aeLliKfUgBVnERMtgh5d2dSIFdGxvmLG1Ne66q0UZM/J+uy7Yxrak7ww/Wk3XKZlaAa+Htca4HYlo7eyxXFR1PoF3TNnVaSr8DxK7nR/90XDefLVCE2Z1joW+Zurlcxoswclugwe0dtboDxbdlWo8gD0y+zK8zxXjTPUxq7S6VTYfKbX/W/sy22sQ11Myw507pNqP4TAbS+KoU2n6hj57DtsJAana2fdd11Gm8zT9Wpj02pI0ddh0wujgFXTM9OKA==

ARC-Authentication-Results: i=1; mx.google.com; dkim=pass
 header.i=@skripsian.online header.s=default header.b=GW8y7ydm;
 dkim=pass header.i=@skripsian.online header.s=default
 header.b=c+WLla20; spf=pass (google.com: domain of
 naufalhanif@skripsian.online designates 103.112.162.228 as
 permitted sender) smtp.mailfrom=naufalhanif@skripsian.online

Return-Path: <naufalhanif@skripsian.online>

Received: from ns1.skripsian.online (skripsian.online. [103.112.162.228]) by mx.google.com with ESMTPS id x2-v6si3356094plv.388.2018.06.27.00.26.29 for <naufalhanif1477.nh@gmail.com> (version=TLS1_2 cipher=ECDHE- Wed, 27 Jun 2018 00:26:29 -0700 (PDT))

Received-SPF: pass (google.com: domain of naufalhanif@skripsian.online designates 103.112.162.228 as permitted sender) client-ip=103.112.162.228;

Authentication-Results: mx.google.com; dkim=pass
 header.i=@skripsian.online header.s=default header.b=GW8y7ydm;
 dkim=pass header.i=@skripsian.online header.s=default
 header.b=c+WLla20; spf=pass (google.com: domain of naufalhanif@skripsian.online designates 103.112.162.228 as permitted sender) smtp.mailfrom=naufalhanif@skripsian.online

Received: from localhost (unknown [127.0.0.1]) by ns1.skripsian.online (Postfix) with ESMTP id 71F03306AF72; Wed, 27 Jun 2018 07:26:30 +0000 (UTC)

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple;
 d=skripsian.online; s=default; t=1530084390;
 bh=7EE6rR/7Llj0C1YZwMFG6bVc1Myf6gzCzz4HU1Xpvpg8=;
 h=Date:From:To:Subject;
 b=GW8y7ydm3jcX6QqNPgsZ+j1iYo9djfhcEmT8n+XL8hFJZJk2R3U3F4IHfkKcjо6B
 2ZUSGeByECe0bYkp6bKF4RX0dZ0qCKsu2jAS4nLXkCEauPVFB1Sf0eUzdRYq5YytOx
 / O5I3FIIntZnliu2UMkf4DMbfAu2RfuiqjYHwUYlm8=

X-Virus-Scanned: amavisd-new at skripsian.online

Received: from ns1.skripsian.online ([127.0.0.1]) by localhost (ns1.skripsian.online [127.0.0.1]) (amavisd-new, port 10024) with ESMTP id dhMoADmqIZ77; Wed, 27 Jun 2018 14:24:41 +0700 (WIB)

Received: from localhost (localhost [IPv6:::1]) by ns1.skripsian.online (Postfix) with ESMTPA id 6EF283069687; Wed, 27 Jun 2018 14:24:34 +0700 (WIB)

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple;
 d=skripsian.online; s=default; t=1530084274;
 bh=7EE6rR/7Llj0C1YZwMFG6bVc1Myf6gzCzz4HU1Xpvpg8=;
 h=Date:From:To:Subject;
 b=c+WLla20kPPPW1bj2U0gGbfsoF8/mPYySS/1JJ50A25XGZq3zZyFT/bDufhu889D
 2aizTY7cGwi0o/H2aq3JXVd+i8vDBJsTOjTSxgLFHVmfeoFXQIS//1feZ2J0CqIVDP
 EcIPkVrxrmXvJVS/es8DBHukv1pSrgVIId4psycq+M=

MIME-Version: 1.0

Content-Type: text/plain; charset=US-ASCII; format=flowed

Content-Transfer-Encoding: 7bit
 Date: Wed, 27 Jun 2018 14:24:32 +0700
 From: naufalhanif@skripsian.online
 To: Naufal Hanif <naufalhanif1477.nh@gmail.com>, naufalhanif74@yahoo.com, yunita@skripsian.online
 Subject: Cek Header Email
 Message-ID: <15f73f4a3d9cb5af642565d45702f46a@skripsian.online>
 X-Sender: naufalhanif@skripsian.online
 User-Agent: Roundcube Webmail/1.2.3
 Melakukan Pengecekan Header Email

Header Email pada Yahoo! Mail Sebelum Penerapan

X-Apparently-To: naufalhanif74@yahoo.com; Wed, 27 Jun 2018 05:06:51 +0000
 Return-Path: <naufalhanif@skripsian.online>
 X-YahooFilteredBulk: 103.112.162.228
 Received-SPF: none (domain of skripsian.online does not designate permitted sender hosts)
 X-IMailISG: wd_by.YWLDTGH6UaoekbpNHudL9y6gu11V2y4qcVzHnllhdw
 QKd8Y4JT01BiQS6tMpOT6cosy0UmdZ_joglaXOgjOnTFTpaLXFoZIZrgK1Qs
 z8QmIyTRGX9GkD402N4cWD38v2SZK1WmNykihxcoNR5z79memgqtRRLU_kkT
 K65FtlyjenPfNOhYMiklwhDKDI8kIT7SmNWW4c34.PtuYcw86cg1yo8IyHPw
 9ItC6279w4fdRINQD5eSqVtX6_DwpkHbK2eIM34aDTtR0sdWFPLGwd300sx
 FQiE8ewC.7N65Lvg3gOrYB8S3iLN.sdVNi1j24FRdTVEYfa30dkTL0IxmxY.Q
 ABXHmFn4vQle0xmkkIt73L9LGGH1HKeryWRqNPLIOLFpgatJbSWnWWefNCi8
 Z3MzonRvHQOAKV7qi9PpIUDD6khkklbouV9MU5PvPhQb1fAbhZrasQwRFD
 kRDeHj08g0uPDJs0mEKpuvctUEOSXQAQ6HTJwC7SBocFlpHvEeguSl.1Ng.w
 o.pWAzLPRxh4ZEqlDRTtYmyN58pDlwEM81kcnzPuZBvVwpwgFy6.Jsy4gKNT
 mzlHVL8idEzsYU4kETwiYbh8nCxVs3dVLbWhHSLVeOQZJy7UU2an0Tz.yqBp
 DRshO1F9bDRfUOZg1_M5uFDuAoJfaNgewgeYrnzE9H8YetyEAJLjQCnCSmQc
 I9PN8J.8mWzcf2BI8FUnn7bLRGtniGwDWriVFZhOvqi11kAkKJJ.vAN12pWc
 CaoGY_95J1cX7WsmqVUiZziwE13P7QKPrvyn_X_U9UY8BpnC3YiaZctJTCG
 CLaXhYvYQCoM7W3ePDLEwAFq9tBNOMI5jZ1AMhCIL9XwTWBh2iHGsatCe3Jn
 _KXq9uqhPSL3kQvhzHAMLW8MpXcRNWIjg--
 X-Originating-IP: [103.112.162.228]
 Authentication-Results: mta4243.mail.ne1.yahoo.com
 from=skripsian.online; domainkeys=neutral (no sig);
 from=skripsian.online; dkim=neutral (no sig)
 Received: from 127.0.0.1 (EHLO ns1.skripsian.online) (103.112.162.228) by mta4243.mail.ne1.yahoo.com with SMTPS; Wed, 27 Jun 2018 05:06:50 +0000
 Received: from localhost (localhost [IPv6:::1]) by ns1.skripsian.online (Postfix) with ESMTPA id 370623069661; Wed, 27 Jun 2018 12:06:51 +0700 (WIB)
 MIME-Version: 1.0
 Content-Type: text/plain; charset=US-ASCII; format=flowed
 Content-Transfer-Encoding: 7bit

Date: Wed, 27 Jun 2018 12:06:51 +0700
From: naufalhanif@skripsian.online
To: Naufal Hanif <naufalhanif1477.nh@gmail.com>, naufalhanif74@yahoo.com, yunita@skripsian.online
Subject: Cek Header Mail
Message-ID: <5a808340b5c6f19cc349b0198c116a1f@skripsian.online>
X-Sender: naufalhanif@skripsian.online
User-Agent: Roundcube Webmail/1.2.3
Content-Length: 33

Uji coba pengecekan header email

Header Email pada Yahoo! Mail Setelah Penerapan

X-Apparently-To: naufalhanif74@yahoo.com; Fri, 25 May 2018 08:53:57 +0000
Return-Path: <yunita@skripsian.online>
X-YahooFilteredBulk: 103.112.162.164
Received-SPF: pass (domain of skripsian.online designates 103.112.162.164 as permitted sender)
X-YMailISG: fffFxpsMWLDu.4FqQJaKpVVaJoFeW_P3ygeM2RLljE4o5Tr_F_Db9mnVz3MDqu4E3_m11ltQB0NTlupgKveyN0D92rG1z7nfdQJzVXzoYX4ZT_ei3pww.80HGftoYT0ykpLvaGZwkrz2UU0NUJCPXoHx5V0_cS85HKV_7sQu_1_sZKWFq21WqmiK83INbViHAQoKzySzZAKFcw5GPm9zHJdL2ACBEi9fpTf7F4K_51qunt.ZsonrFTIpnk_gUffrNHin_XaTyuc9.qquDarZ0JqZddlvaIQ480eJ_o88MBZPyfV6oG9wt6.e7G.Y15yW7_RTUQzi0M4GCvLyKC0d34Q1LnneVdMUXI_QOPMhOXAyrMeafehQRPoX22_dL227yPzcoal6CEw35XPeS9BHRaiHBjqWzY6_deWJLl.bcd5pd7MEg0P_XX9E5nvxMeLC0PCEzovUUhXvjKHQ61aI5v7oDLHm_cZRISC5RjMs.U6M3y1TesE41ptgxQ4ceqNb801E5Evt2HmjCiBgegyT6yZmE_GG6Zu9Igd5hZwfLucwAef5YGCSZCaJwpQmPqyvJ7jT7Yiso_TcOoztPAgPH0_h.w.3D9X4fPOXjd030FX27Qqh2dh9c5Btdls24_hKR6ET5WjX5ZcJrRI2maU_Mk.HTfUomATFFKmio3PTiCrEwkg1E1qJu8xZSr.PzOHluUm7PqJ_wmavYivk_glrGR9QZMGSZMJ5aOejshs5c10I14X.fxKfLuhkDK9g.LjPx7fnIdacXb5Vu_t5VJ6ijM76.46xPzyvNodrrSK3JE_2N0YSXGJ1H5jVbLc2QtYKsjeLRRDQhM_qCc.xxtDptKSbNYaVPiKYRiO_5CZGRKqylM83hf.OUj0d8K7ez9_GrV7SX1_7U0Ns67imBGtWhu6WxcEyQu.3Z8oKTePyE2D5RF6rUw9XTCcWHN5aHiNIA_u_T3LBrHovUE0Md5SQBquBckVTedrShRhGKzvgrymFyOMRUhLyLO5UiqNj1u1_lIJKvbqf0nanftQeoET2QupfgcJCUR2h1H2A0Tw101516CPIr.9838.hilCf_HBnCUtIGlsAXUw--
X-Originating-IP: [103.112.162.164]
Authentication-Results: mta4247.mail.gq1.yahoo.com from=skripsian.online; domainkeys=neutral (no sig); from=skripsian.online; dkim=pass (ok)
Received: from 127.0.0.1 (EHLO ns1.skripsian.online) (103.112.162.164) by mta4247.mail.gq1.yahoo.com with SMTPS; Fri, 25 May 2018 08:53:56 +0000
Received: from localhost (unknown [127.0.0.1]) by ns1.skripsian.online (Postfix) with ESMTP id B251D30535CB for <naufalhanif74@yahoo.com>; Fri, 25 May 2018 08:53:32 +0000 (UTC)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=skripsian.online; s=default; t=1527238412; bh=IHq60PwVrrx751B/xqUvHPs4OM1ToRpO/EFxCboljFk=; h=Date:From:Subject; b=QzXtxy5pDfeBe8Z5uPfzzvKJj5ZI+5DzUcASE1aK41YDx14MQsbz4MOogyEyYWid

avY7XMigCx1UT2Wn26eTQsA5g/4rXJmEsKwoYXHCbKidqzF8BVToj7czj71Fkd/X9a
 ag2bVxq5UBoRcF09ZGdkc7nB4jELC5HeNM74orcmA=
 X-Virus-Scanned: amavisd-new at skripsian.online
 Received: from ns1.skripsian.online ([127.0.0.1]) by localhost
 (ns1.skripsian.online [127.0.0.1]) (amavisd-new, port 10024) with
 ESMTP id kFD1twHtwkMA for <naufalhanif74@yahoo.com>; Fri, 25 May
 2018 15:53:26 +0700 (WIB)
 Received: from localhost (localhost [IPv6:::1]) by
 ns1.skripsian.online (Postfix) with ESMTPA id 6056430535C3 for
 <naufalhanif74@yahoo.com>; Fri, 25 May 2018 15:53:26 +0700 (WIB)
 DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple;
 d=skripsian.online; s=default; t=1527238406;
 bh=IHq60PwVrrx751B/xqUvHPs4OMlToRpO/EFxCboljFk=;
 h=Date:From:To:Subject;
 b=gGQZBtBRyer1QIWazoCb7vMFyelGwh6D/f3HjqHNIZ7uVAWZdnvTNqRFoXRGvwFH
 aiFuEnAAPQjfY33x9yd3/xpce9LXgRNY/zgiBKo7JtCiT6JeXJ5bYVimHp9L9VE+ih
 Mfrsz5KfPeuaWgySPK364Yw3WsOZXOEK9s3AtriK0=
 MIME-Version: 1.0
 Content-Type: text/plain; charset=US-ASCII;
 format=flowed
 Content-Transfer-Encoding: 7bit
 Date: Fri, 25 May 2018 15:53:26 +0700
 From: yunita@skripsian.online
 To: naufalhanif74@yahoo.com
 Subject: Cek Header Mail
 Message-ID: <b3ab19d7e9a37d85ba586b7ea5752241@skripsian.online>
 X-Sender: yunita@skripsian.online
 User-Agent: Roundcube Webmail/1.2.3
 Content-Length: 48

Cek header email setelah penerapan DKIM dan SPF

Header Email pada skripsian.online Sebelum Penerapan

Return-Path: <yunita@skripsian.online>
 Delivered-To: naufalhanif@skripsian.online
 Received: from localhost (localhost [IPv6:::1]) by
 ns1.skripsian.online (Postfix) with ESMTPA id 1B948306969F for
 <naufalhanif@skripsian.online>; Tue, 26 Jun 2018 16:15:08 +0700
 (WIB)
 MIME-Version: 1.0
 Content-Type: text/plain; charset=US-ASCII; format=flowed
 Content-Transfer-Encoding: 7bit
 Date: Tue, 26 Jun 2018 16:15:07 +0700
 From: yunita@skripsian.online
 To: naufalhanif@skripsian.online
 Subject: Test Anti Spam
 Message-ID: <b935648c3ce1e2a691fdd459d3454b58@skripsian.online>
 X-Sender: yunita@skripsian.online
 User-Agent: Roundcube Webmail/1.2.3

XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-
 EMAIL*C.34X

Header Email pada skripsi.ononline Setelah Penerapan

```
Return-Path: <yunita@skripsi.ononline>
Delivered-To: naufalhanif@skripsi.ononline
Received: from localhost (unknown [127.0.0.1]) by
ns1.skripsi.ononline (Postfix) with ESMTP id A89C1306969F for
<naufalhanif@skripsi.ononline>; Fri, 29 Jun 2018 02:31:32 +0000
(UTC)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple;
d=skripsi.ononline; s=default; t=1530239492;
bh=5JtrnNw9RJpLzzBAVfY5dy+L5y+H+RNH4s8DSbVA2Ek=;
h=Date:From:To:Subject;
b=asreqFSmSoOWmABCcP5PyLZmrQZbv7rg0OuoRQn0/S48QmzuHioDB7iFbWLWHIN2
KJPrZDqaCb+GSoyBvoFJyWAUVDtOENA6PlMV+x0+JK10QZeGmuJA/K78twCZQXQFlX
U13cb1vw42pR9jCWwigDRuVdTnoEHkIvWXZEZWpY=
X-Virus-Scanned: amavisd-new at skripsi.ononline
Authentication-Results: ns1.skripsi.ononline (amavisd-new);
dkim=pass (1024-bit key) header.d=skripsi.ononline
Received: from ns1.skripsi.ononline ([127.0.0.1]) by localhost
(ns1.skripsi.ononline [127.0.0.1]) (amavisd-new, port 10024) with
ESMTP id fAERE5f6jNzQ for <naufalhanif@skripsi.ononline>; Fri, 29
Jun 2018 09:31:09 +0700 (WIB)
Received: from localhost (localhost [IPv6:::1]) by
ns1.skripsi.ononline (Postfix) with ESMTPA id 22531306969D for
<naufalhanif@skripsi.ononline>; Fri, 29 Jun 2018 09:31:09 +0700
(WIB)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple;
d=skripsi.ononline; s=default; t=1530239469;
bh=5JtrnNw9RJpLzzBAVfY5dy+L5y+H+RNH4s8DSbVA2Ek=;
h=Date:From:To:Subject;
b=plum4Fjn67DX1TWaQS1fbibLTu6r+aKoAOguEhX/bU3Mf+tnape0FivcCa3reD8m
rm8OZEn0Mv2swvV9UiyN6J47gbS5YVXMUd84FMXweF5QNieTwJUjDyScK+b1PIs492
9zHUOtyQI4vNdOD8d3yEipK04LcJvZ9YFW+eMUXgQ=
MIME-Version: 1.0
Content-Type: text/plain; charset=US-ASCII; format=flowed
Content-Transfer-Encoding: 7bit
Date: Fri, 29 Jun 2018 09:31:08 +0700
From: yunita@skripsi.ononline
To: naufalhanif@skripsi.ononline
Subject: Cek Header Mail
Message-ID: <55a57f675639d913ec310d949a052be7@skripsi.ononline>
X-Sender: yunita@skripsi.ononline
User-Agent: Roundcube Webmail/1.2.3
```

Melakukan pengecekan header email