

ANALISA PENERAPAN DMARC YANG DIINTEGRASIKAN DENGAN ANTI SPAM DAN ANTI VIRUS UNTUK PENGAMANAN MAIL SERVER

Rudi Kurniawan¹, Khairan Marzuki², Lilik Widyawati³

^{1,2,3} Universitas Bumigora Mataram

Artikel Info

Kata Kunci

Dmarc Anti
Spam Dan Anti
Virus Untuk
Pengamanan
Mail Server

ABSTRAK

Email spam, email spoofing, dan virus yang didistribusikan melalui email merupakan hal yang tidak diinginkan oleh pengguna email. Email spam, email spoofing, dan email yang mengandung virus dapat menimbulkan kerugian yang sangat besar baik bagi penyedia layanan maupun bagi pengguna email. Berdasarkan latar belakang tersebut maka mendorong penulis untuk menerapkan protocol DMARC, 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 Protocol DMARC, anti spam, dan anti virus ini menggunakan metodologi NDLC, yaitu metode pengembangan jaringan komputer. Yang diawali dengan 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.

Article Info

Keywords

Dmarc Anti
Spam And Anti
Virus For Mail
Server Security

ABSTRACT

Email spam, email spoofing, and viruses that are distributed via e-mail are unwanted by e-mail users. Spam e-mail, spoofing e-mail, and e-mail that contain viruses can cause enormous harm to both service providers and email users. Based on this background, it encourages the author to apply the DMARC, Anti Spam, and Anti Virus protocols so that the mail server can avoid spam e-mail, viruses and e-mail users can avoid spoofing activities.

The design and analysis of the implementation of the DMARC, anti-spam, and anti-virus protocol uses the NDLC methodology, which is a computer network development method. Which starts with designing a spam, spoofing, and virus email filtering system, simulating installation and configuration. The next stage is implementation where at this stage the system that has been previously designed is implemented and tested on the spam, spoofing, and virus email filtering system. The last stage is the monitoring stage where supervision will be carried out on the system that has been made to determine the level of success of the system that has been created.

The results or outputs to be achieved are that the mail server can avoid spam emails, email spoofing, and viruses to ensure the security and comfort of email users and avoid the impact of losses that can be caused by email spam, email spoofing, and viruses.

1. PENDAHULUAN

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.

Mengingat betapa pentingnya media komunikasi di zaman sekarang ini maka beberapa orang melakukan penelitian terutama di bidang keamanan jaringan. 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 penggunaannya, 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 [1]. penerapan protokol DomainKeys Identified Mail dapat mencegah email spoofing dengan cara melakukan otentikasi 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. Hasil atau keluaran yang 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 [2]. pendeteksi spoofing pada email menggunakan penerapan *DKIM*, *SPF* dan *DMARC* yang pada penelitian di gunakan Sebuah metode untuk melakukan deteksi diperlukan untuk melihat apakah sebuah email terindikasi sebagai *spoof* atau tidak[3]. Forensik email dengan metode Header Analysis dianggap efektif untuk melacak alamat IP pengirim email, namun hal ini tidak dapat melacak posisi pengirim email secara akurat. Mengintegrasikan email forensik klasik dengan data mining dari Twitter data stream telah terbukti efektif untuk mendapatkan informasi geografis dan memperkecil luas dari seluas kota menjadi seluas lingkungan, yang sangat berharga bagi pihak berwajib dalam menghemat waktu dan juga usaha untuk mengadili pelaku tindak kejahatan cyber[4].

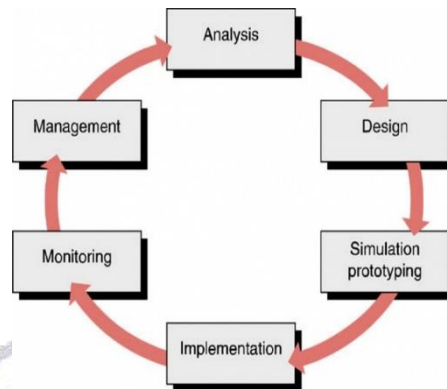
Dari kutipan di atas ada beberapa kekurangan seperti *DKIM* memiliki masalah yang tidak dapat menentukan apakah tanda tangan itu sah dan juga tidak dapat memberi laporan apabila terjadi pemalsuan email. Pertimbangan ini lah yang membuat penulis untuk menerapkan *Protocol DMARC* yang berfungsi untuk mendeteksi email palsu dan memberi tahu pengguna tanpa *DKIM* tanda tangan dengan memanfaatkan *DMARC* dan menerapkan sistem itu mengirimkan hasil verifikasi *DMARC* ke penerima, *ClamAV* sebagai tools *anti spam* dan *spoofing* yang dapat melakukan otorisasi bukan hanya melalui alamat IP saja namu juga dapat melalui URL dan antivirus *ClamAV* untuk mengatasi virus yang sangat tidak diinginkan oleh pengguna maupun penyedia layanan email. Sistem pencegahan *email spam*, *spoofing*, dan *virus* diharapkan dapat mengurangi dampak kerugian yang diakibatkan oleh email spam, spoofing, dan virus.

DMARC (*Domain-based Message Authentication, Reporting and Conformance*) dapat digunakan sebagai otentikasi dan otorisasi email sehingga email client akan terbebas dari tindakan *spoofing*. Penerapan Anti Spam dan Anti Virus *ClamAV* juga diperlukan agar email server terhindar dari email spam dan virus, metode yang diterapkan oleh Anti Spam dan Anti Virus *ClamAV* yaitu dengan melakukan pengecekan header, body, dan attachment email kemudian di sampaikan ke pengguna.

Manfaat dari penerapan *DMARC*, Anti *Spam* dan Anti *Virus ClamAV* adalah untuk mengoptimalkan system keamanan jaringan server mail, dengan cara memblokir surat elektronik yang dianggap sebagai spam atau virus, meningkatkan kualitas keamanan surat elektronik sehingga pengguna dapat terhindar dari aktifitas spoofing dan virus yang disisipkan melalui surat elektronik[2].

2. METODOLOGI PENELITIAN

Metode NDLC (*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[5]. *NDLC* mempunyai enam fase, keenam fase tersebut dapat dilihat seperti pada gambar 1.1 berikut.



Gambar 1. 1 Fase NDLC
Sumber: Nurfajar, Kurniawan, dan Yunan, 2015

2.1. Tahap Analisa

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

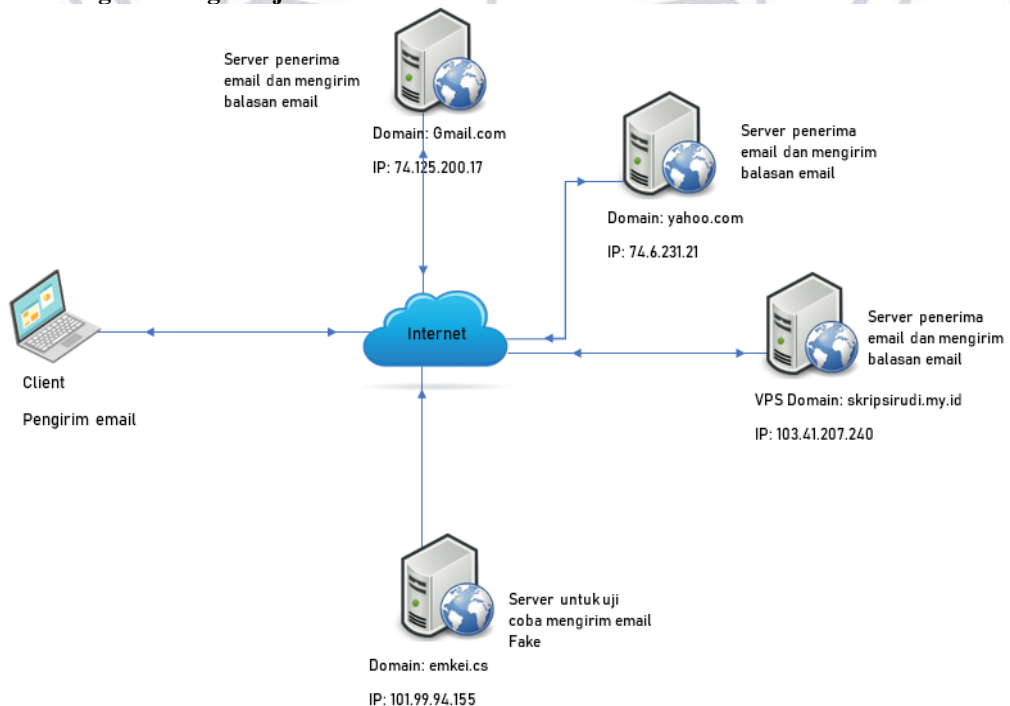
2.2. Tahap Desain

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

2.3. Tahap Simulation Prototyping

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

2.3.1. Rancangan Jaringan Uji Coba

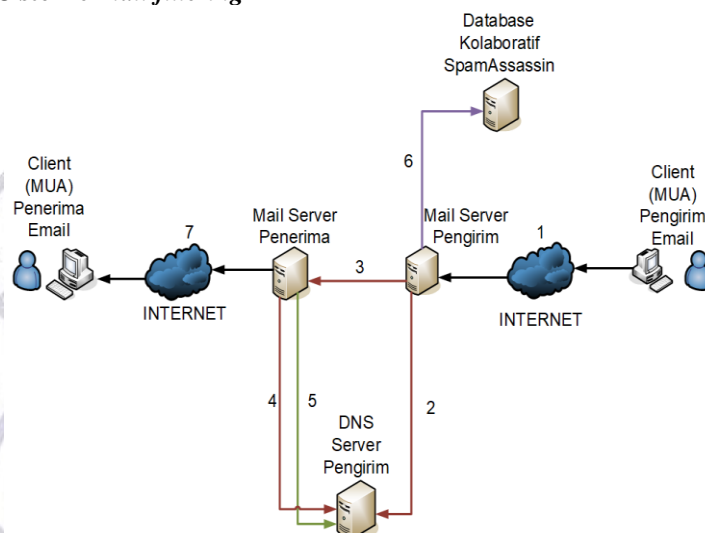


Gambar 2.2 Rancangan Jaringan Uji Coba

Rancangan ini diimplementasikan menggunakan *VPS* yang disewa pada penyedia layanan *VPS* dan pada *VPS* telah terinstal sistem operasi *CentOS Linux release 7*, *VPS* yang telah disewa diberikan satu alamat

IP public oleh penyedia layanan *VPS* yaitu 103.41.207.240. Pada *VPS* akan dilakukan instalasi *CentOS Web Panel*, konfigurasi *DNS server*, konfigurasi *Mail server*, dan pada komputer *client* telah terinstal system operasi windows 10 dan aplikasi browser Google Chrome untuk mengakses *Mail User Agent* berbasis web (*Roundcube*).

2.3.2. Rancangan Sistem *e-mail filtering*



Gambar 2.3 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.

- Langkah 1 user mengirim *email* dengan menggunakan *Mail User Agent* berbasis web (*Roundcube*), user mengakses *Roundcube* menggunakan browser.
- Langkah 2 *Mail server* pengirim meneruskan *email* ke *mail server* penerima dengan menambahkan *private key* pada *header email*.
- Langkah 3 *Mail server* pengirim mempublish *public key* pada *DNS server*nya.
- Langkah 4 *Mail server* penerima mengambil *public key* yang ada pada *DNS server* pengirim *email* untuk dicocokkan dengan *private key* yang ada pada *header email*, jika *private key* tidak cocok dengan *public key* maka *email* akan dianggap sebagai *email spam* dan akan di report oleh *DMARC* berlaku langkah 8, jika *private key* cocok dengan *public key* maka proses akan berlanjut pada langkah ke 5.
- Langkah 5 *Mail server* penerima mencocokkan 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.
- Langkah 6 *Mail server* penerima melakukan pengecekan pada *database* kolaboratif *SpamAssassin*.
- 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*.
- Proses report *email* dari *DMARC* yang dikirim ke folder spam, kemudian proses 9 yang mengirim balik *email spam* ke pengirim semula.

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), (no 8 dan 9) garis biru mewakili *protocol DMARC*.

2.3.3. Rancangan Pengalamatan IP

Tabel 2.1 Rancangan Pengalamatan IP

No	Perangkat	IP Address	Network	Interface
1	DNS Server, HTTP Server, SMTP Server, POP3/IMAP Server (VPS)	192.168.43.24/25	192.168.43.1	eth0
2	Client	DHCP	DHCP	-

2.3.4. Rancangan Akun e-mail

Tabel 2.2 Kebutuhan Akun e-mail

NO	Alamat e-mail	Domain
1	Rudi.masterqq3@gmail.com	gmail.com
2	Rudi.masterqq3@yahoo.com	yahoo.com
3	Root@Skripsirudi.my.id	Skripsirudi.my.id
4	admin@ Skripsirudi.my.id	Skripsirudi.my.id

2.3.5. Kebutuhan Perangkat Keras

Tabel 2.3 Spesifikasi Laptop

Komponen	Spesifikasi
CPU	Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz 1.80 GHz
RAM	12 GB
Hard Drive	TB

Tabel 3.1 Spesifikasi VPS

Komponen	Spesifikasi
CPU	Virtual CPU 2 Core
RAM	2 GB
Hard Drive	40 GB

2.3.6. Adapun kebutuhan perangkat lunak yang dibutuhkan adalah sebagai berikut :

- Linux CentOS 7
- Bind-chroot sebagai *DNS server daemon*
- Postfix sebagai *Mail Transfer Agent* (MTA)
- Dovecot sebagai *Mail Delivery Agent* (MDA)
- Claws Mail sebagai *Mail User Agent* (MUA)
- Chrome untuk mengakses Webadmin Sophos UTM dari Client2
- VMware Workstation
- GNS3 Network Simulator
- Tiny Core Linux
- QEMU

3. HASIL DAN PEMBAHASAN

3.1. Hasil Uji Coba

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

3.2. Header Email pada Gmail

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

```
ARC-Authentication-Results: i=1; mx.google.com;
dkim=tempererror (no key for signature) header.i=@skripsirudi.my.id header.s=default header.b=X5TPJCmt;
dkim=tempererror (no key for signature) header.i=@skripsirudi.my.id header.s=default header.b=iqCe0FXw;
spf=neutral (google.com: 103.41.207.240 is neither permitted nor denied by best guess record for domain of
admin@skripsirudi.my.id) smtp.mailfrom=admin@skripsirudi.my.id
Return-Path: <admin@skripsirudi.my.id>
Received: from srv1.skripsirudi.my.id ([103.41.207.240])
by mx.google.com with ESMTPS id 1175i293887pjz.83.2021.08.12.10.40.21
for <rudi.masterqq3@gmail.com>
(version=TLS1_2 cipher=ECDSA-AES128-GCM-SHA256 bits=128/128);
Thu, 12 Aug 2021 10:40:21 -0700 (PDT)

Received-SPF: neutral (google.com: 103.41.207.240 is neither permitted nor denied by best guess record for domain of
admin@skripsirudi.my.id) client-ip=103.41.207.240;
Authentication-Results: mx.google.com;
dkim=tempererror (no key for signature) header.i=@skripsirudi.my.id header.s=default header.b=X5TPJCmt;
dkim=tempererror (no key for signature) header.i=@skripsirudi.my.id header.s=default header.b=iqCe0FXw;
spf=neutral (google.com: 103.41.207.240 is neither permitted nor denied by best guess record for domain of
admin@skripsirudi.my.id) smtp.mailfrom=admin@skripsirudi.my.id
```

Gambar 4. 1 Cuplikan Header Email pada Gmail Sebelum Penerapan

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

```
Authentication-Results: mx.google.com;
dkim=pass header.i=@skripsirudi.my.id header.s=default header.b=rflDG5ip;
dkim=pass header.i=@skripsirudi.my.id header.s=default header.b="m0n/OfEf";
spf=pass (google.com: domain of admin@skripsirudi.my.id designates 103.41.207.240 as permitted sender)
smtp.mailfrom=admin@skripsirudi.my.id;
dmarc=pass (p=QUARANTINE sp=QUARANTINE dis=NONE) header.from=skripsirudi.my.id
Received: from localhost (unknown [127.0.0.1]) by srv1.skripsirudi.my.id (Postfix) with ESMTP id E550C0778 for
<rudi.masterqq3@gmail.com>; Sun, 27 Jun 2021 06:59:38 +0000 (UTC)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=skripsirudi.my.id; s=default; t=1624777178;
bh=0nLVXWl0LbC9inyoGwFCTTHs5+Kc/F/uvToZ4sZEsQ=; h=Date:From:To:Subject;
b=rflDG5ipTJdm5ClzZUco0tLAjzV8K1BzboLSegHnF6n/GCbninyC8e/t8mb0Nk8tP
TCWjACPNDDJMJnJa5RpNkzBjmTKmhaWc93eBZH8pozme6hIFQITt0zGLeP0qaQyHa
YUddrY0zVq5Qz0Riab9LDBxpluNj/rJWJ3KCTLi0=
X-Virus-Scanned: amavisd-new at skripsirudi.my.id
```

Gambar 4. 2 Cuplikan Header Email pada Gmail Setelah Penerapan

3.3. Header Email pada Yahoo! Mail

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

```
Received: from 10.222.142.149
by atlas301.free.mail.ne1.yahoo.com with HTTPS; Thu, 12 Aug 2021 18:17:56 +0000
Return-Path: <root@skripsirudi.my.id>
X-Originating-IP: [103.41.207.240]
Received-SPF: none (domain of skripsirudi.my.id does not designate permitted sender hosts)
Authentication-Results: atlas301.free.mail.ne1.yahoo.com;
dkim=perm_fail header.i=@skripsirudi.my.id header.s=default;
dkim=perm_fail header.i=@skripsirudi.my.id header.s=default;
spf=none smtp.mailfrom=skripsirudi.my.id;
dmarc=unknown header.from=skripsirudi.my.id;
X-Apparently-To: rudi.masterqq3@yahoo.com; Thu, 12 Aug 2021 18:17:56 +0000
X-YMail-IsGz: 5X-D70KwLpT-30YpC74qA1-5uu7+bbvze77UgMoJy1EdXUg
```

Gambar 4. 3 Cuplikan Header Email pada Yahoo! Mail Sebelum Penerapan

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

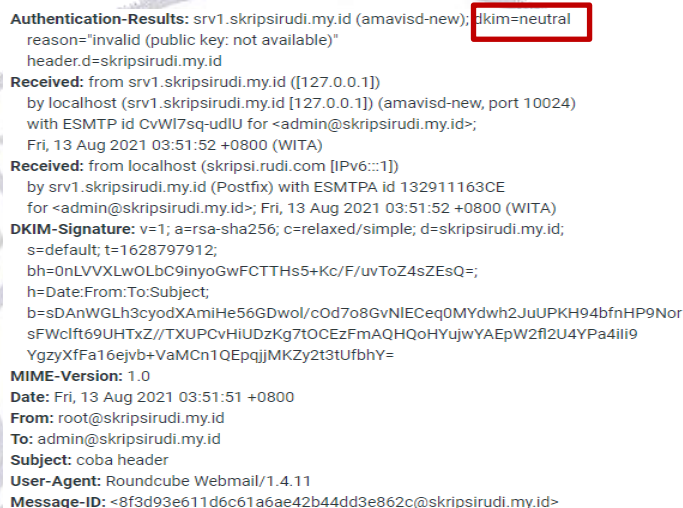
```
Received-SPF: pass (domain of skripsirudi.my.id designates 103.41.207.240 as permitted sender)
Authentication-Results: atlas310.free.mail.bf1.yahoo.com;
dkim=pass header.i=@skripsirudi.my.id header.s=default;
dkim=pass header.i=@skripsirudi.my.id header.s=default;
spf=pass smtp.mailfrom=skripsirudi.my.id;
dmarc=pass (p=QUARANTINE) header.from=skripsirudi.my.id;
X-Apparently-To: rudi.masterqq3@yahoo.com; Sat, 26 Jun 2021 09:45:19 +0000
X-YMail-IsGz: zTAGvATWLDtOvncCvnp08J_ukVwluirMtA5sCth78leCRCMg
_KT8VBfW5q16ccKam1NVkcXz7m1HV7INz0Fes_WR2bXYtf9SXXmxFCUYVY
c09JnBmZVLmPFOZcu6X8c5710i1itEQvQbRGU8xH1E0uWjvZoHfpjB1diSI
WXB8e58mdoZ7KxZgBLTOaff8aKrud2v5kxV3KmNKNu0LZig4Jc9IKsSmsNc0F4
7hIQwtZ1R47Qt4qXejM66FW7KSjvX.zFmTYIcnlrdRkohl_rIsrqlvjRPok
.HHInABsg9a_eLeiaTBWOXGJ2IZTI2oSCb6FhhXx6Nk9E8xLD2yEdGjPGZN
vVAu1ltN8RL4ct1Ch2wWuEDQm3Hkma7XB030aXw8IPwZ_f_p4k6Mk3ysWKjh
oSryh6cIW3_b_cX1fXWZDL3KxNEP_m8vCIBGw0JA5k3Edz5Cvfng.p3DuTal
XB50Q33VEAB.LV_nzzTe.fCcFCwbQIuqWMCMBET1oenkXMTc3iEJncjBMRg
pcSsz2.03Ixo2p0pggtQYDMpErYwlpANDYKdEROAwet9906cpYf2nD._giGnyr
zV1Wvw6cdqsd__bsI3gvLmhWZ14chJK95nCHFC_3wk51fEPVH8hLnadI1x7t
oQ8rR1LpCCs72qQfXqmd.yTcrGFbpTF_ArvIPBQd98zuhG2v6dXMS2Zgd6hn
oydFEb79pHJ2Nvj5kcGBPKzeLjv7JL1EWeTT2c0NnIZZU0t0d06QFC1V4L9w
Woy2amilyJXdqv7M4KmOo12GXgleOexaeJNGUmus4zbhijnjJ43Z1gPQPqEHg
1qjuRqCqEV.h2UMtr9KN8eDGBYbCy7tE7TtWLUprJDVnIigu1vCTBdrdzZc9n
irbekyqtp76vTA1kgsbkAiZHGCUq9bhI1CdNL_90d00ZDZGY3RidBusmdI
q_Gz.7nw.M0g5a6idxCCSkP.WuS3718mJ3XFLTd8tuXsxwHpZpXayYHovMb
qHPE7WwQajvuF0p8YHFV2OSZMIL8ssVug7u1af.EF7sAaP_zU0crCYHxamB
OFU309TM8CnHrePBvtx6mId33Zraw--
Received: from 103.41.207.240 (EHLO srv1.skripsirudi.my.id)
by 10.197.39.201 with SMTPs
(version=TLS1_2 cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256);
Sat, 26 Jun 2021 09:45:18 +0000
Received: from localhost (unknown [127.0.0.1])
by srv1.skripsirudi.my.id (Postfix) with ESMTP id 58D87C0778
for <rudi.masterqq3@yahoo.com>; Sat, 26 Jun 2021 09:45:16 +0000 (UTC)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=skripsirudi.my.id;
s=default; t=1624700716;
bh=Sa2S8055UoJrVdFrDhMTAzoFieSwi3d9s1+ux1tMzVQ=;
h=Date:From:To:Subject;
b=XbIK1SckWjaJAtc9UQTUSGZQT0709rhSka312DxwerJLuq9zN949hap/TSRHynfy2
ATcT0aUGbU6Wh+b0Y3skk0EtoFY0VPY587aUTNGR0xc2Yk3J0U1F0EyK8oDhew3Zgz
LW9C2/xNvhSeeac96YzZMMZPOTRlqptOe8mUQs0=
X-Virus-Scanned: amavisd-new at skripsirudi.my.id
```

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

Pada gambar 4.53 terlihat perbedaan *header email* setelah penerapan protocol *DMARC*, *DKIM*, *SPF*, *anti spam*, dan *anti virus* yaitu nilai dari parameter *Received-SPF* yang awalnya *none* menjadi *pass*, parameter *dkim* yang awalnya *neutral* menjadi *pass*, parameter *dmARC* yang menjadi *pass* dan terdapat tambahan parameter *DKIM-Signature* dan *X-Virus-Scanned* [2].

3.4. Header Email pada skripsirudi.my.id

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



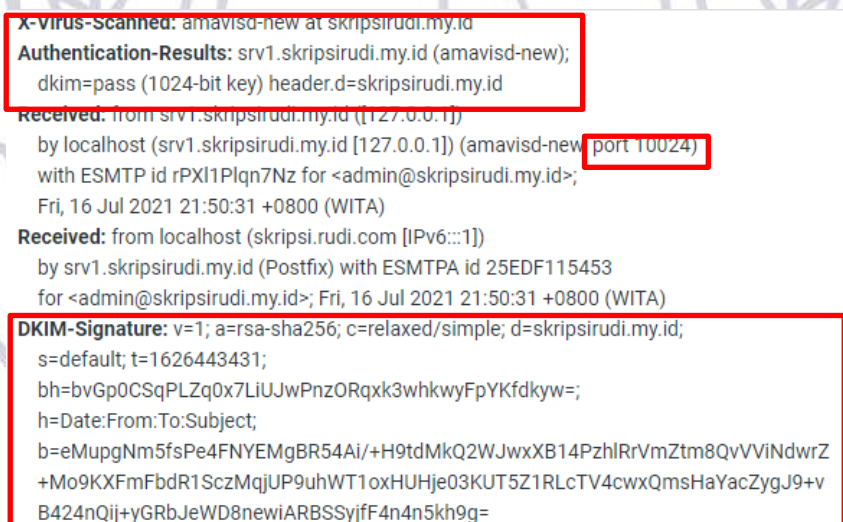
```

Authentication-Results: srv1.skripsirudi.my.id (amavisd-new); dkim=neutral
reason="invalid (public key: not available)"
header.d=skripsirudi.my.id
Received: from srv1.skripsirudi.my.id ([127.0.0.1])
by localhost (srv1.skripsirudi.my.id [127.0.0.1]) (amavisd-new, port 10024)
with ESMTP id CvWl7sq-udIU for <admin@skripsirudi.my.id>;
Fri, 13 Aug 2021 03:51:52 +0800 (WITA)
Received: from localhost (skripsi.rudi.com [IPv6:::1])
by srv1.skripsirudi.my.id (Postfix) with ESMTPA id 132911163CE
for <admin@skripsirudi.my.id>; Fri, 13 Aug 2021 03:51:52 +0800 (WITA)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=skripsirudi.my.id;
s=default; t=1628797912;
bh=0nLVVXLwOLbC9inyoGwFCTTHs5+Kc/F/uvToZ4sZEsQ=;
h=Date:From:To:Subject;
b=sDAnWGLh3cyodXAmiHe56GDw0l/cOd7o8GvNIECeq0MYdwh2JuUPKH94bfnHP9Nor
sFWclft69UHTxZ//TXUPCvHiUDzKg7tOCEzFmAQHqoHYUjwYAEpW2f2U4YPa4iil9
YgzyXfFa16ejvb+VaMcN1QEppjMKZy2t3tUfbhY=
MIME-Version: 1.0
Date: Fri, 13 Aug 2021 03:51:51 +0800
From: root@skripsirudi.my.id
To: admin@skripsirudi.my.id
Subject: coba header
User-Agent: Roundcube Webmail/1.4.11
Message-ID: <8f3d93e611d6c61a6ae42b44dd3e862c@skripsirudi.my.id>

```

Gambar 4. 5 Cuplikan Header Email pada skripsian Sebelum Penerapan

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



```

X-Virus-Scanned: amavisd-new at skripsirudi.my.id
Authentication-Results: srv1.skripsirudi.my.id (amavisd-new);
dkim=pass (1024-bit key) header.d=skripsirudi.my.id
Received: from srv1.skripsirudi.my.id ([127.0.0.1])
by localhost (srv1.skripsirudi.my.id [127.0.0.1]) (amavisd-new, port 10024)
with ESMTP id rPXl1Plqn7Nz for <admin@skripsirudi.my.id>;
Fri, 16 Jul 2021 21:50:31 +0800 (WITA)
Received: from localhost (skripsi.rudi.com [IPv6:::1])
by srv1.skripsirudi.my.id (Postfix) with ESMTPA id 25EDF115453
for <admin@skripsirudi.my.id>; Fri, 16 Jul 2021 21:50:31 +0800 (WITA)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=skripsirudi.my.id;
s=default; t=1626443431;
bh=bvGp0CSqPLZq0x7LiUJwPnzORqxk3whkwyFpYKfdkyw=;
h=Date:From:To:Subject;
b=eMupgNm5fsPe4FNYEMgBR54Ai/+H9tdMkQ2WJwxXB14PzhlRrVmZtm8QvVViNdwrZ
+Mo9KXFmFbdr1SczMqjUP9uhWT1oxHUHje03KUT5Z1RLcTV4cwxQmsHaYacZygJ9+v
B424nQij+yGRbJeWD8newiARBSSyjfF4n4n5kh9g=

```

Gambar 4. 6 Cuplikan Header Email skripsirudi.my.id Setelah Penerapan

3.5. Hasil Analisa

Pada tahap ini akan dilakukan analisa hasil uji coba yang telah di lakukan sebelumnya. Pada analisa hasil uji coba akan di tampilkan analisa hasil uji coba pengiriman *email spoofing* sebelum dan setelah penerapan protocol *DMARC*, *DKIM* dan *SPF*, pengiriman *email spam* sebelum dan setelah penerapan *anti spam*, pengiriman *email* yang mengandung *virus* sebelum dan setelah penerapan *anti virus*, dan pengecekan *header email* sebelum dan setelah penerapan protocol *DMARC*, *DKIM*, *SPF*, *anti spam*, dan *anti virus*[2].

3.5.1. Analisa Hasil Uji Coba Pengiriman Email Spoofing

Cara yang dapat digunakan untuk mengetahui apakah sudah dilakukan proses otorisasi dan otentikasi oleh protocol *DMARC*, *DKIM* dan *SPF* adalah dengan melakukan pengiriman *email spoofing*

menggunakan *Emkei's Fake Mailer* dengan mengatasmakan salah satu *user email* pada *mail server* skripsirudi.my.id, kemudian *email* tersebut dikirim ke layanan *email Gmail, Yahoo! Mail*, dan skripsirudi.my.id. Berikut Analisa hasil ujicoba perbandingan sebelum diterapkan protokol *DMARC, DKIM* dan *SPF* dan setelah diterapkan protokol *DMARC, DKIM* dan *SPF* yang dilakukan pada uji coba sebelumnya, seperti terlihat pada tabel 4.1 berikut[2].

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

NO	Fake Mailer	Layanan Email yang diatasmakan	Layanan Email Penerima	Sebelum Penerapan	Setelah Penerapan
1	<i>Emkei's Fake Mailer</i>	Skripsirudi.my.id	<i>Gmail</i>	Masuk <i>Folder Inbox</i>	Diblokir Dan di report oleh DMARC
2	<i>Emkei's Fake Mailer</i>	Skripsirudi.my.id	<i>Yahoo! Mail</i>	Masuk <i>Folder Inbox</i>	Masuk <i>Folder Spam</i>
3	<i>Emkei's Fake Mailer</i>	Skripsirudi.my.id	Skripsirudi.my.id	Masuk <i>Folder Inbox</i>	Masuk <i>Folder Inbox</i>

Berdasarkan tabel 4.1 perbandingan sebelum dan setelah penerapan protokol *DMARC, DKIM* dan *SPF* dengan melakukan pengiriman *email spoofing* yang dikirim menggunakan *Emkei's Fake Mailer* ke layanan *email Gmail, Yahoo! Mail*, dan skripsirudi.my.id sebelum penerapan protokol *DMARC, DKIM* dan *SPF* yaitu *email spoofing* berhasil masuk ke *folder inbox* penerima *email* yang berada pada *mail server Gmail, Yahoo! Mail*, dan skripsirudi.my.id sedangkan setelah penerapan protokol *DMARC, DKIM* dan *SPF*, *email spoofing* tersebut diblokir dan *dmarc* mereport email, dimasukan ke *folder spam* oleh layanan *email Yahoo! Mail* dan dimasukan ke *folder inbox* oleh layanan *email skripsirudi.my.id*[2].

3.5.2. Analisa Hasil Uji Coba Pengiriman Email Spam

Analisa penerapan *anti spam* dilakukan dengan mengirim *email spam* dengan menggunakan layanan *email skripsirudi.my.id, Yahoo! Mail*, dan *Gmail* ke layanan *email skripsirudi.my.id* untuk menguji kinerja *anti spam* sebelum dan setelah penerapan *anti spam* seperti terlihat pada tabel 4.2 berikut[2].

Tabel 4.2 Perbandingan Sebelum dan Setelah Penerapan Anti Spam

NO	Layanan Email Pengirim	Layanan Email Penerima	Sebelum Penerapan	Setelah Penerapan
1	<i>Yahoo! Mail</i>	Skripsirudi.my.id	Masuk <i>Folder Inbox</i>	Diblokir
2	<i>Gmail</i>	Skripsirudi.my.id	Masuk <i>Folder Inbox</i>	Diblokir
3	Skripsirudi.my.id	Skripsirudi.my.id	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 skripsirudi.my.id*, sedangkan setelah penerapan *anti spam*, terjadi proses pemblokiran *email spam* oleh *Amavisd-New* sehingga *email* yang terindikasi sebagai *spam* langsung diblokir sebelum sampai pada *folder penerima email*[2].

3.5.3. Analisa Hasil Uji Coba Mengirim Email Mengandung Virus

Analisa penerapan *anti virus* dilakukan dengan mengirim *email spam* dengan menggunakan layanan *email skripsirudi.my.id, Yahoo! Mail*, dan *Gmail* ke layanan *email skripsirudi.my.id* untuk menguji kinerja *anti spam* sebelum dan setelah penerapan *anti spam* seperti terlihat pada tabel 4.3[2].

Tabel 4.3 Perbandingan Sebelum Penerapan Anti virus

NO	Layanan Email Pengirim	Layanan Email Penerima	Sebelum Penerapan	Setelah Penerapan
1	<i>Yahoo! Mail</i>	Skripsirudi.my.id	Masuk <i>Folder Inbox</i>	Diblokir dan di report oleh dmarc
2	<i>Gmail</i>	Skripsirudi.my.id	Masuk <i>Folder Inbox</i>	Diblokir dan di report oleh dmarc
3	Skripsirudi.my.id	Skripsirudi.my.id	Masuk <i>Folder Inbox</i>	Diblokir dan di report oleh dmarc

Berdasarkan tabel 4.3, dapat disimpulkan bahwa sebelum penerapan *anti virus*, tidak terjadi proses pemblokiran *email* yang mengandung *virus* oleh *Amavisd-New* sehingga *email* yang mengandung *virus* dapat masuk pada *folder inbox* pengguna *email* yang berada pada *mail server skripsirudi.my.id*, sedangkan

setelah penerapan *anti virus*, tidak terjadi pemblokiran *email* namun ada report *DMARC* yang mereport *email* yang mengandung *virus* sehingga *email* yang terindikasi mengandung *virus* langsung di report[2].

3.5.6. Analisa Hasil Uji Coba Pengecekan Header Email

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

Tabel 4.4 Perbandingan Header Email Sebelum dan Setelah Penerapan

NO	Uji Coba	Layanan Email	DKIM-Signature	DMARC	X-Virus-Scanned	Nilai Received-SPF
1	Sebelum Penerapan	Gmail	<i>DKIM =temperror</i>	-	-	neutral
		Yahoo! Mail	<i>dkim=perm_fail</i>	-	-	none
		Skripsirudi.my.id	<i>dkim=neutral</i>	-	-	-
2	Setelah Penerapan	Gmail	Pass	Pass	Ada	Pass
		Yahoo! Mail	Pass	Pass	Ada	Pass
		Skripsirudi.my.id	Pass	-	Ada	-

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

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

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

Sebelum penerapan protocol *DMARC*, *DKIM*, *SPF*, *anti spam*, dan *anti virus* terdapat parameter *DKIM-Signature* yang bernilai *neutral* dan tidak ada parameter *X-Virus-Scanned*, sedangkan parameter *SPF-Received* juga tidak ada pada header email di skripsirudi.my.id, sedangkan setelah penerapan protocol *DMARC*, *DKIM*, *SPF*, *anti spam*, dan *anti virus* terdapat parameter *DKIM-Signature* yang bernilai *Pass* dan *X-Virus-Scanned*, namun tetap tidak terdapat parameter *Received-SPF* dan *DMARC* pada header email di skripsirudi.my.id[2].

4. KESIMPULAN

Berdasarkan hasil ujicoba penerapan protocol *DMARC* 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 protocol *DMARC* dapat mencegah *email spoofing* dan memberikan sebuah laporan kepada email pengguna asli dengan cara melakukan otentikasi pencocokan alamat *IP server* dan header email.
4. Penerapan *SpamAssassin*, *ClamAV*, dan *Amavisd-New* dapat mencegah masuknya *email spam* dan *virus* dengan cara melakukan pengecekan *header*, *body*, dan *attachment email*.

UCAPAN TERIMAKASIH

Dengan selesainya skripsi ini, penulis ingin mengucapkan terima kasih kepada pihak-pihak yang telah banyak membantu dalam penyelesaian skripsi ini. Dalam kesempatan ini penulis menyampaikan ucapan terima kasih kepada:

1. Kedua Orang Tua yang telah memberikan dukungan berupa Bimbingan, Materi dan Doa. Tidak Terlupakan Keluarga Besar yang telah Memberikan Semangat dan Doa untuk menyelesaikan Tugas Akhir ini.
2. Bapak Dr.Ir. Anthony Anggrawan, MT., Ph.D. selaku Rektor Universitas Bumigora.
3. Ibu Ni Gusti Ayu Dasriani, M.Kom, selaku Wakil Rektor I Universitas Bumigora.
4. Bapak Ahmat Adil, M.Sc, selaku Dekan Fakultas Teknik dan Desain.
5. Ibu Lilik Widyawati., M.Kom selaku Ketua Program Studi S1 Ilmu Komputer dan Selaku Pembimbing Kedua dalam membantu mengerjakan Skripsi ini.
6. Bapak Khairan Marzuki S.T, M.Kom, selaku dosen pembimbing pertama dalam membantu mengerjakan Skripsi ini.
7. Bapak/Ibu dosen yang telah memberikan ilmu selama dalam masa perkuliahan.
8. Special thanks kepada Fauji Ferdiansyah dan Sutrisno yang telah memberikan bantuan yang sangat membantu penulis dalam menyelesaikan penelitian dan sidang skripsi
9. Teman-teman sahabat seperjuangan Universitas Bumigora. Terima kasih atas segala kerja samanya dan segala bentuk bantuannya selama perkuliahan berlangsung.

10.

REFERENSI

- [1] Hoiriyah, Bambang Sugiantoro, and Yudi Prayudi. 2016. "Investigasi Forensik Pada E-Mail Spoofing Menggunakan Metode Header Analysis." *jurnal ilmiah dasi* 17(4): 20–25.
- [2] Hanif, Naufal. 2018. "Analisa Penerapan Domainkeys Identified Mail (Dkim), Sender Policy Framework (Spf), Anti Spam , Dan Anti Virus Pada Mail Server".
- [3] Nadzifan, Andrian Maftuh, Farih Nazihullah, and . Syaifuddin . 2018. "Aplikasi Untuk Deteksi Adanya Spoof Pada Email." *Sistemasi* 7(3): 268.
- [4] Ardhi, Naufal Herdyputra. 2020. "Pelacakan Geolocation Pada Forensik Email Terintegrasi Dengan Twitter Geo-Social Network." *jakarta*. [https://repository.uinjkt.ac.id/dspace/bitstream/123456789/53623/1/NAUFAL HERDYPUTRA ARDHI-FST.pdf](https://repository.uinjkt.ac.id/dspace/bitstream/123456789/53623/1/NAUFAL%20HERDYPUTRA%20ARDHI-FST.pdf).
- [5] Puspita, Okta, Dwi Anggorowati, M Teguh Kurniawan, and Umar Yunan K S H. 2015. "Desain Dan Analisa Infrastruktur Jaringan Wireless Di Pdii-Lipi Jakarta Dengan Menggunakan Metode Network Development Life Cycle (Ndlc) Design and Analysis of Infrastructure Wireless Network in Pdii-Lipi Jakarta Using Network Development Life Cycle (Nd." *Telkom University* 2(2): 5811–19.
- [6]