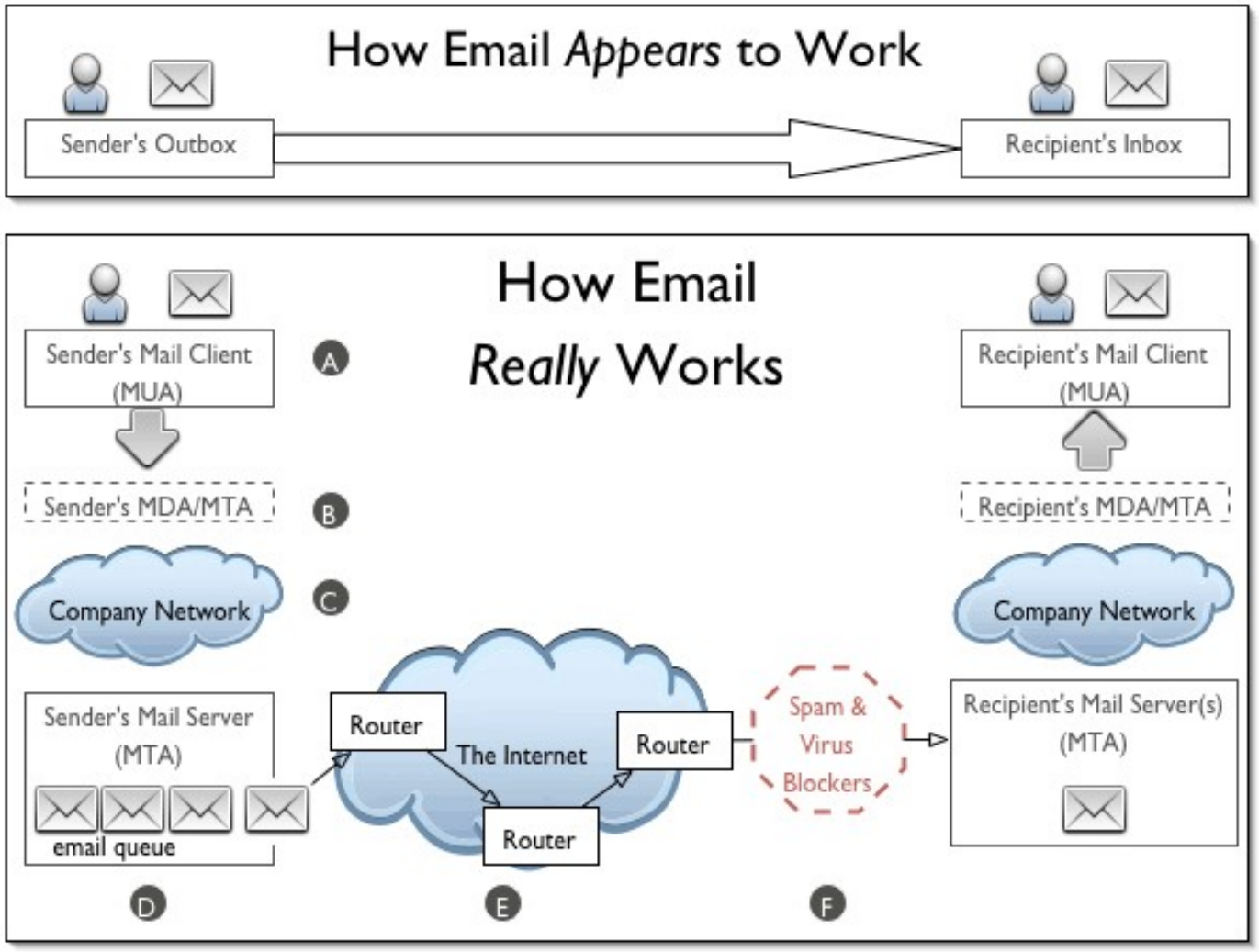
Email Headers

digital forensic needs

How email works



How email works

- **Mail User Agent (MUA)** merupakan client yang dapat berbicara dengan protokol tertentu (SMTP, POP3) kepada sebuah **Mail Transfer Agent (MTA)**,
- MTA berfungsi meneruskan email kepada MTA lain, atau langsung kepada MUA (dengan protokol IMAP).
- contoh MUA antara lain Thunderbird, Ms. Outlook.
- contoh sebuah MTA adalah Ms. Exchange, Sendmail, Postfix.

Headers

Delivered-To: [disembunyikan]@gmail.com

Received: by 10.229.84.10 with SMTP id h10cs128890qcl;

Fri, 4 Dec 2009 05:31:43 -0800 (PST)

Received: by 10.150.87.2 with SMTP id k2mr5425632ybb.267.1259933502490;

Fri, 04 Dec 2009 05:31:42 -0800 (PST)

Return-Path: <[disembunyikan]@info.paypal.com>

Received: from om-paypal-apac.rsys4.com (om-paypal-apac.rsys4.com [12.130.139.51])

by mx.google.com with ESMTP id 22si6368786gxk.17.2009.12.04.05.31.39;

Fri, 04 Dec 2009 05:31:41 -0800 (PST)

Headers

Date: Fri, 4 Dec 2009 05:18:36 -0800

From: "PayPal" <[disembunyikan]@info.paypal.com>

Reply-To: "PayPal" <[disembunyikan]info.paypal.com>

Subject: <ADV> [disembunyikan], win over US$60K when you start shopping with PayPal

x-headers

x-headers adalah headers custom yang memiliki standar yang beragam. digunakan untuk berbagai hal mulai dari melacak user id, atau advertising id dari penerima email, karena minimnya standar dari x-headers, terdapat begitu banyak jenisnya.

Headers: SPF

Received-SPF: pass (google.com: domain of [disembuyikan]@info.paypal.com designates 12.130.139.51 as permitted sender) client-ip=12.130.139.51;

Authentication-Results: mx.google.com; spf=pass (google.com: domain of [disembunyikan]@info.paypal.com designates 12.130.139.51 as permitted sender) smtp.mail=[disembunyikan]@info.paypal.com;

Sender Policy Framework (SPF) adalah sebuah **DNS record** (TXT record) berisi informasi alamat IP yang diperbolehkan mengirim email atas nama domain tertentu.

SPF berfungsi memberikan kepercayaan bahwa sebuah email yang dikirimkan dari IP tertentu memang berhak mengirimkan email tersebut.

contoh: MTA mx.google.com memverifikasi apakah IP address 12.130.139.51 (pengirim email) memang merupakan IP yang diperbolehkan mengirimkan email atas nama domain paypal.com.

spfchecklink

Headers: DKIM

DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; s=responsys;
d=info.paypal.com; h=MIME-Version:Content-Type:Date:From:Reply-
To:Subject:List-Unsubscribe:To:Message-Id; i=[disembunyikan]@info.paypal.com;
bh=gsI3Bb5slkuo+p/q6yjixbNU3mw=;
b=D3rOkUdQ2clZdSo8DRNHL/dhCp2CWRmHpdF141GVzoULBmU04wArvKBaRKNsT
0BN1fiMRCNXRJYm
ypaEUzkvIonQoin9dHv25b1wbBZqURL203V4QVOIOGtaoe4AuZPh83X7lYwhh2nNc
o1j365UQZnqlOjmprcf9lOni+cxBq0

DKIMverify

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=gmail.com; s=20161025;
        h=mime-version:from:date:message-id:subject:to;
        bh=f6o6k9LY4eyBAD+MiJllJpRd7oW4+hjPaEbLa3gSQRU=;
        b=UVaGn190LS9PrRTToK9FpNBjuk3jfSfgyzjXh1PlwF2k+g1a1AVOzFpZqz+e3gAG2d
         xtqiIGxLReDUwyLm4l2sjXRpd7SSd2f5SoM/Jmwy6R+Y8RYlUbIR2d5l0/DR8tLoNEHv
         Bq+FwLHibVRyj/wM6yxv3y3SJp8OfFbYP2PlwHlSbhtCL318142S82eXllRCKllNPNcP
         55aa2DWNUZyqb4w+JZCu0E/st4Mzp4ar1pXvRXqD3SXngxLn+XcFIF38YaJB/ZNKYl7R
         FXCqWg1W+FN5zfzFVAoBjk5w9XszySlefRgAJ77ikk9ecOHTMiz6lAeMdPssrIJe97gL
         2l4g==
```

```
From: [redacted]@gmail.com>
Date: Thu, 11 Jun 2020 10:17:39 +0700
Message-ID: <CADK2mnChPCErHdHpvnF[redacted]5_6WPyw@mail.gmail.com>
Subject: tes
To: [redacted]@gmail.com>
Content-Type: text/plain; charset="UTF-8"

pesan tes!
```

```
From: [redacted]@gmail.com>
Date: Thu, 11 Jun 2020 10:17:39 +0700
Message-ID: <CADK2mnChPCErHdHpvnF[redacted]Pyw@mail.gmail.com>
Subject: tes
To: [redacted]@gmail.com>
Content-Type: text/plain; charset="UTF-8"

pesan tes
```

```
root@osboxes:/home/osboxes/.local/bin# cat tes.eml | dkimverify
signature ok
root@osboxes:/home/osboxes/.local/bin# cat tes2.eml | dkimverify
signature verification failed
```

pip install dkimpy

cat filename.eml | dkimverify

or use [mxtoolbox]

Forensic needs

1. Sender
2. Sender MUA, MTA
3. Email Integrity

Terima Kasih