Email: DMARC/SPF/DKIM

or: How I Learned to Start Worrying and Hate the Borg

A MUUG Presentation

About Trevor Cordes

- **UNIX-head since 1992 (SunOS > AIX > RH > Fedora)**
- **Fedora, PHP & Perl fan (wanna fight?)**
- **MUUG Vice-President**
- **STUG Past-President (defunct Atari ST club)**
- **Owner, Tecnopolis Enterprises**
  - Celebrating 25 years in business

April 1, 2024: Email Doomsday

- Why are we here?
- Google (“Borg”) Gmail ramping up “anti-spam” measures the last year or so
- Accelerating
- Full nuclear “Slim Pickens” on April 1, 2024
- Best practices change to requirements
- Not done yet

Who Cares?

- If you manage email flow/servers in any way
- Even if you use a third party sender
- If you manage (external-facing) DNS
- Especially: managers of email flow that can exceed 5000 emails a day

Who Doesn’t Care

- No impact on:
- Home users using their ISP’s email servers
- Gmail/Yahoomail users without their own domain
- But stay put! The tech and topic is interesting

Resistance Is Futile

- What if I don’t want to?
- Gmail and Yahoomail and maybe others
- Will demote, put in spambox, block, bounce or drop your email
- Gmail is 53% of USA email
- Gmail is 75% of all “email openings”

Partway There?

- Many administrators will already have some of the following in place already

What Do You Need To Do? (Everyone)

- Everyone:

* probably done already

- Setup SPF*
- Setup DKIM*
- PTR records*
- TLS connections*
- Don’t impersonate gmail From:’s

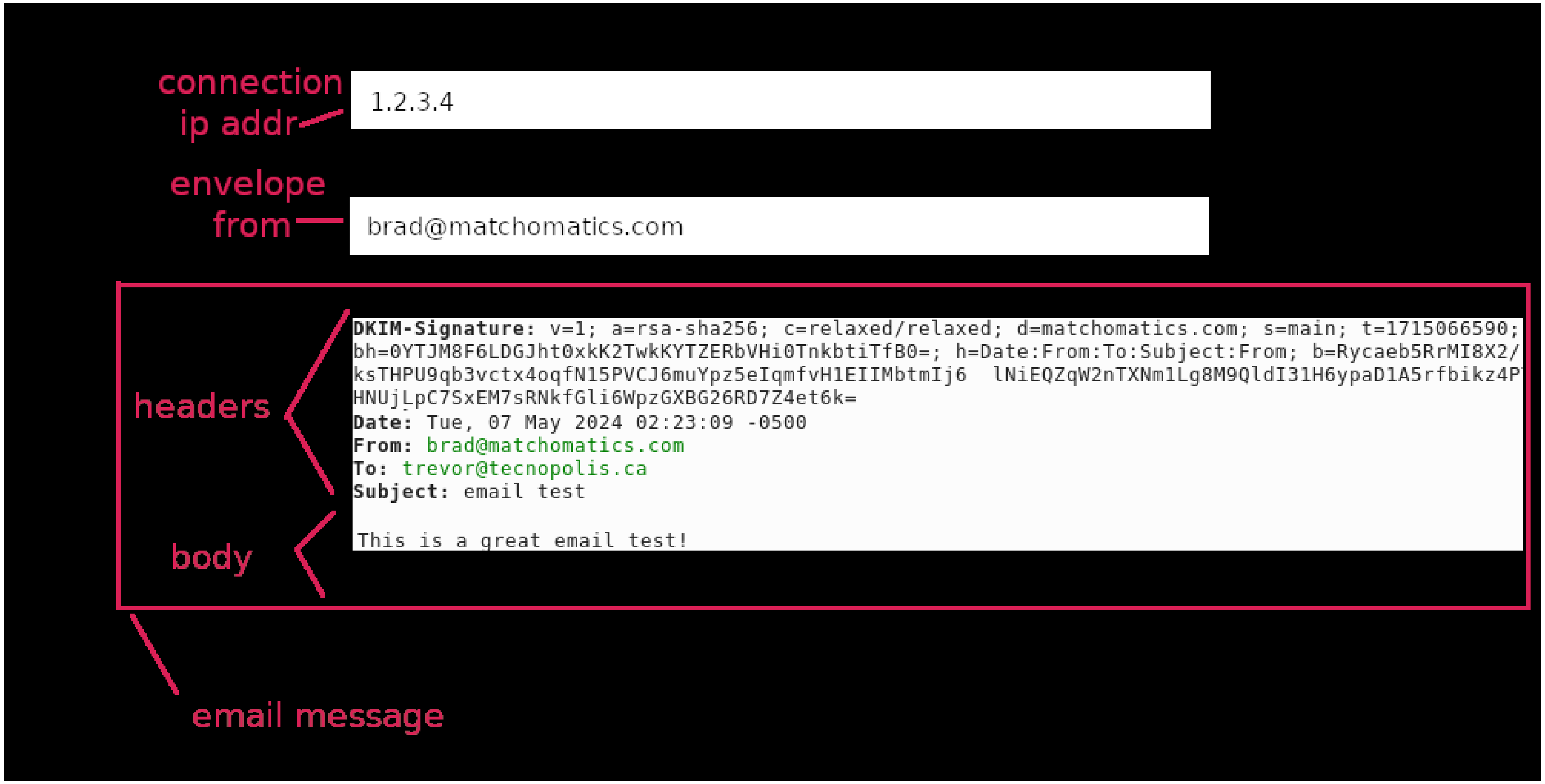
What Do You Need To Do? (Bulk)

- Bulk senders: (5000+ a day)
- Setup DMARC
- Align From: for DMARC to SPF or DKIM
- Implement one-click unsubscribe

English? What Do I Do?

- New DNS records (SPF/DKIM/DMARC)
- New daemons (opendkim)
- Rejigging your From:’s
- New custom programming (one-click unsub)

Help Me Grok



```
1.2.3.4
```

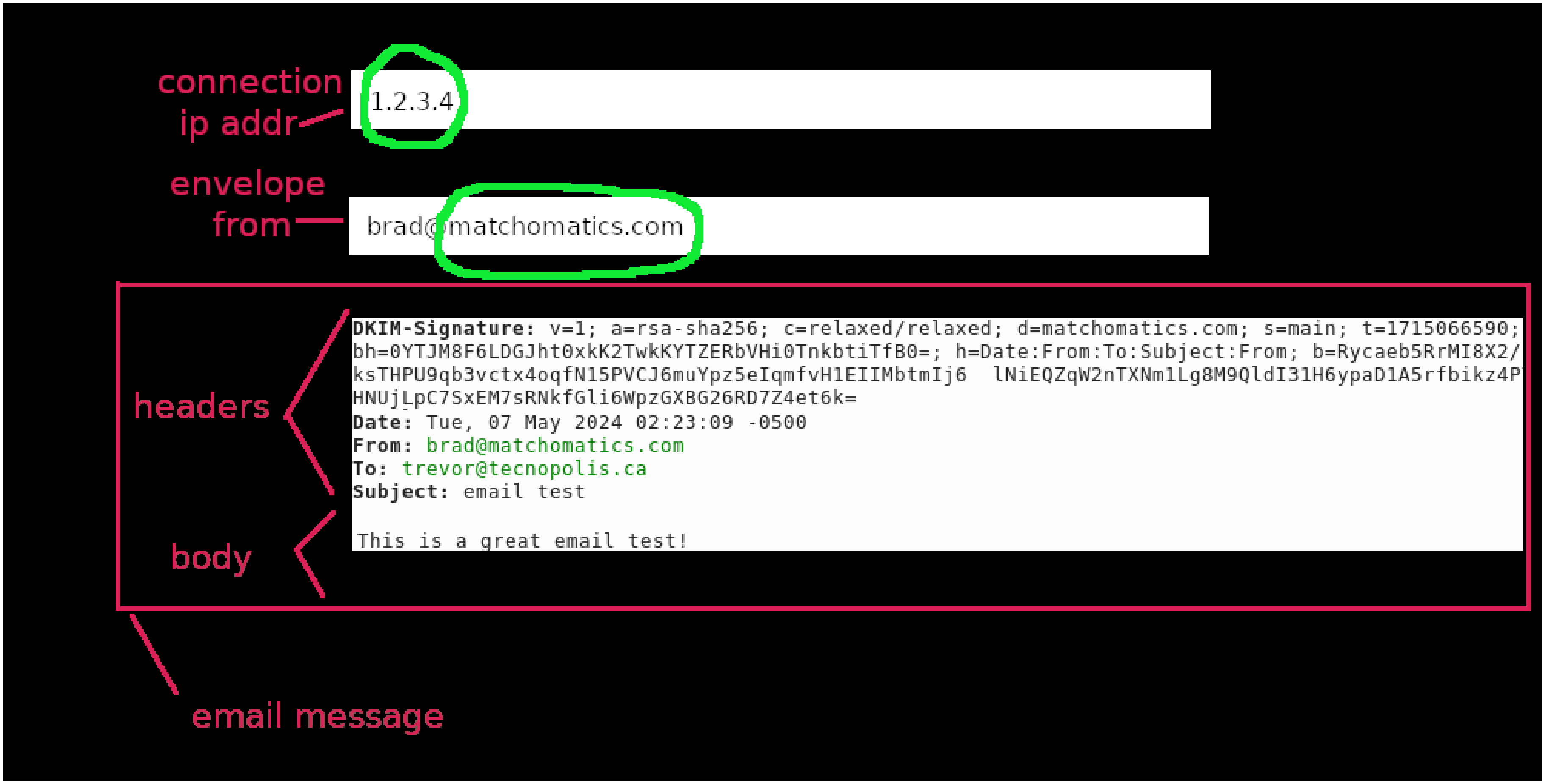
```
brad@matchomatics.com
```

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=matchomatics.com; s=main; t=1715066590;
bh=0YTJM8F6LDGJht0xkK2TwkKYTZERbVHi0TnkbtiTfB0=; h=Date:From:To:Subject:From; b=Rycaeb5RrMI8X2/
ksTHPU9qb3vctx4oqfN15PVCJ6muYpz5eIqmfvH1EIIMbtmIj6  lNiEQZqW2nTXNm1Lg8M9QldI31H6ypaD1A5rfbikz4P
HNUjLpC7SxEM7sRNkfGli6WpzGXBG26RD7Z4et6k=
Date: Tue, 07 May 2024 02:23:09 -0500
From: brad@matchomatics.com
To: trevor@tecnopolis.ca
Subject: email test

This is a great email test!
```

SPF

- Ties envelope-from to connection-ip



```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=matchomatics.com; s=main; t=1715066590;
bh=0YTJM8F6LDGJht0xkK2TwkKYTZERbVHi0TnkbtiTfB0=; h=Date:From:To:Subject:From; b=Rycaeb5RrMI8X2/
ksTHPU9qb3vctx4oqfN15PVCJ6muYpz5eIqmfvH1EIIMbtmIj6  lNiEQZqW2nTXNm1Lg8M9QldI31H6ypaD1A5rfbikz4P
HNUjLpC7SxEM7sRNkfGli6WpzGXBG26RD7Z4et6k=
Date: Tue, 07 May 2024 02:23:09 -0500
From: brad@matchomatics.com
To: trevor@tecnopolis.ca
Subject: email test

 This is a great email test!
```

SPF

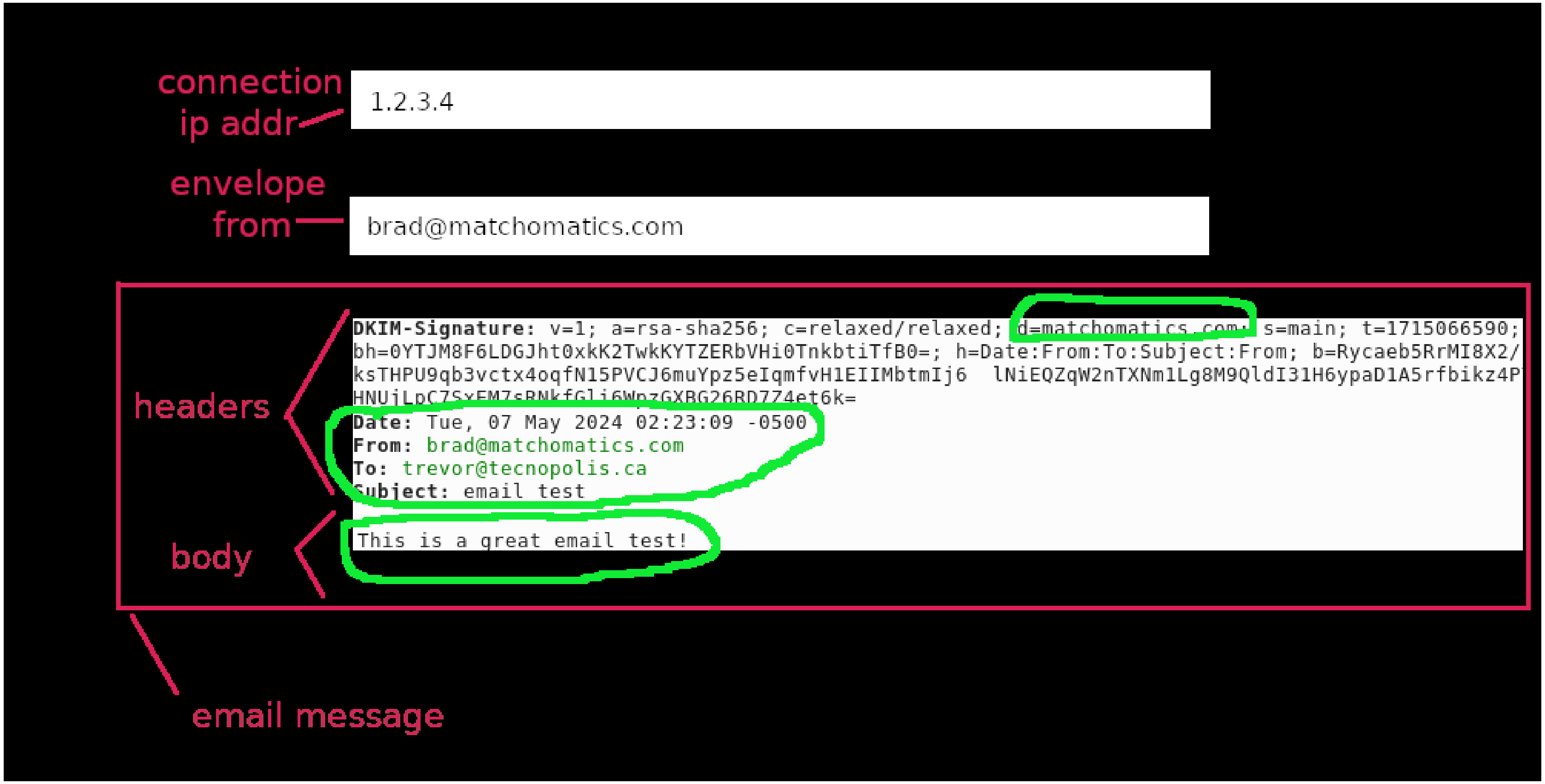
- Ties envelope-from to connection-ip
- Uses the fact only the true domain owner can create a DNS SPF record
- DNS TXT lookup on envelope-from
- dig -tTXT foo.com
- v=spf1 ip4:1.2.3.4 a mx -all
- foo.com says 1.2.3.4 can send email for it

SPF Weaknesses

- No user sees or cares about envelope-from
- Has nothing to do with header-from
- Thus doesn’t stop spoofing or phishing
- Only useful for admins investigating abuse

DKIM

- Signed hash on key headers and body with public key from DNS TXT for DKIM d= domain



1.2.3.4

brad@matchomatics.com

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=matchomatics.com; s=main; t=1715066590;
bh=0YTJM8F6LDGJht0xkK2TwkKYTZERbVHi0TnkbtiTfB0=; h=Date:From:To:Subject:From; b=Rycaeb5RrMI8X2/
ksTHPU9qb3vctx4oqfN15PVCJ6muYpz5eIqmfvH1EIIMbtmIj6  lNiEQZqW2nTXNm1Lg8M9QldI31H6ypaD1A5rfbikz4P
HNUjLpC7SxFM7sRNkfGli6WpzGXBG26RD7Z4et6k=
Date: Tue, 07 May 2024 02:23:09 -0500
From: brad@matchomatics.com
To: trevor@tecnopolis.ca
Subject: email test

This is a great email test!
```

DKIM

- Signed hash on key headers and body with public key from DNS TXT for DKIM d= domain
- Uses the fact only the true domain owner can create a DNS DKIM record, and has the corresponding private key
- DNS TXT lookup on DKIM header d= domain and s= key selector
- dig -tTXT main._domainkey.foo.com
- main._domainkey.matchomatics.com. 86400 IN TXT "v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAU..."
- p= is the public key

DKIM

- Must run a new daemon (opendkim)
- Create a new private/public key pair
- Configure conf and signing/key files

DKIM Weaknesses

- Can still spoof header-from
- All it does is say the d= domain had permission to sign the email
- Helps to confirm email was not altered in transit

PTR Records

- Reverse DNS
- Ancient tech
- Ties your connection-ip to your domain
- Only your upstream internet provider can do this
- Can still lie in some cases
- Only really eliminates home users with dynamic IP
- Evil in some senses

TLS Connections

- Forces encrypted TCP channel between mail servers
- Forces every server to have a cert (free or pay)
- Just like google “forced” every www to use SSL
- Easy

Gmail From Impersonation

- Forbidden from setting header-from to @gmail
- Unless it really goes through/from gmail
- Alignment has the same effect

Juicy Bits

- Strap in!

DMARC

- Add one new DNS TXT record
- _dmarc.matchomatics.com. 86400 IN TXT "v=DMARC1; p=none; pct=100; adkim=r; aspf=r;"
- Tells email servers what to do with emails that fail SPF or DKIM with p=
- none(accept), quarantine, reject
- rua= allows success/failure reports

DMARC

- Doesn’t do much on its own other than the reports
- And policy
- Relies solely on SPF/DKIM
- No new daemons, no IP settings, no encryption keys

DMARC Report Sample (XML)

```
<row>
  <source_ip>23.83.223.167</source_ip>
  <count>1</count>
  <policy_evaluated>
    <disposition>none</disposition>
    <dkim>pass</dkim>
    <spf>fail</spf>
```

DMARC

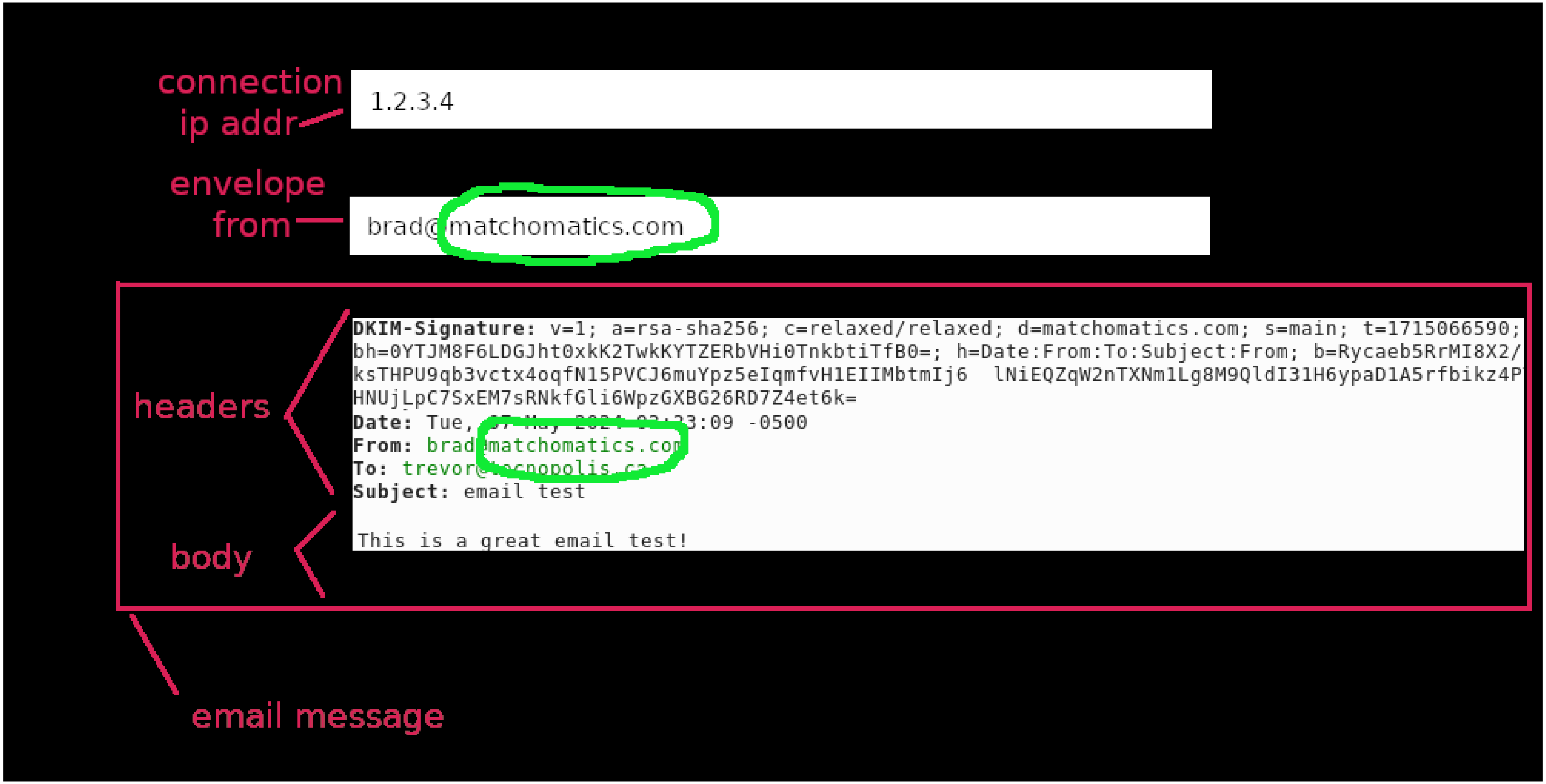
- So what’s the big deal?

DMARC Alignment

- Therein lies the rub…
- The only part of everything here that stops header-from spoofing
- Demands that header-from domain matches either:
  - d= DKIM domain (and DKIM passes)
  - envelope-from domain (and SPF passes)

DMARC Alignment: SPF

- SPF passes and env-from matches header-from



```
1.2.3.4
```

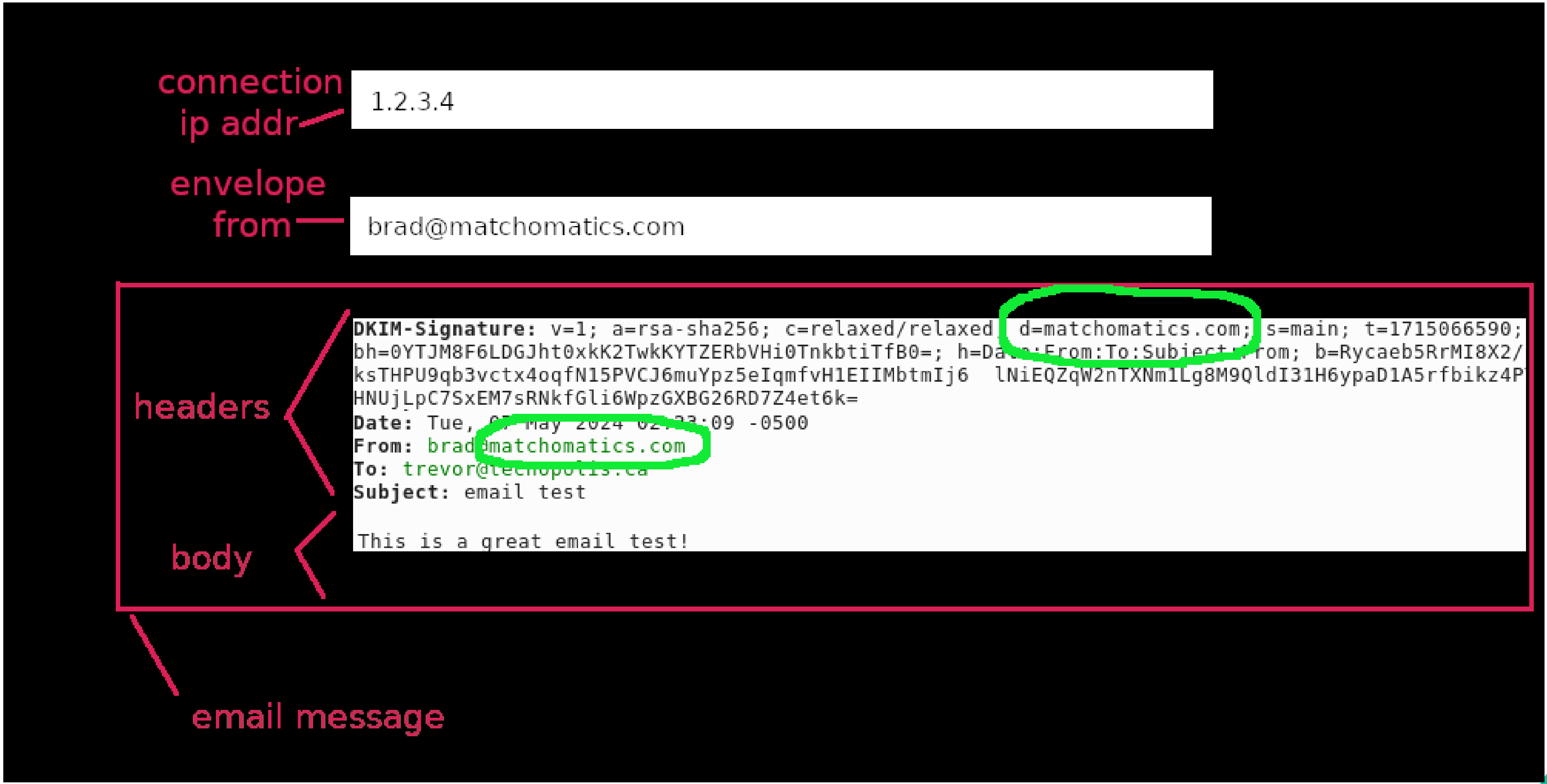
```
brad@matchomatics.com
```

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=matchomatics.com; s=main; t=1715066590;
bh=0YTJM8F6LDGJht0xkK2TwkKYTZERbVHi0TnkbtiTfB0=; h=Date:From:To:Subject:From; b=Rycaeb5RrMI8X2/
ksTHPU9qb3vctx4oqfN15PVCJ6muYpz5eIqmfvH1EIIMbtmIj6  lNiEQZqW2nTXNm1Lg8M9QldI31H6ypaD1A5rfbikz4P
HNUjLpC7SxEM7sRNkfGli6WpzGXBG26RD7Z4et6k=
Date: Tue, 07 May 2024 02:23:09 -0500
From: brad@matchomatics.com
To: trevor@tecnopolis.ca
Subject: email test

This is a great email test!
```

DMARC Alignment: DKIM

- DKIM passes and d= matches header-from



```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=matchomatics.com; s=main; t=1715066590;
bh=0YTJM8F6LDGJht0xkK2TwkKYTZERbVHi0TnkbtiTfB0=; h=Date:From:To:Subject:From; b=Rycaeb5RrMI8X2/
ksTHPU9qb3vctx4oqfN15PVCJ6muYpz5eIqmfvH1EIIMbtmIj6  lNiEQZqW2nTXNm1Lg8M9QldI31H6ypaD1A5rfbikz4P
HNUjLpC7SxEM7sRNkfGli6WpzGXBG26RD7Z4et6k=
Date: Tue, 07 May 2024 02:23:09 -0500
From: brad@matchomatics.com
To: trevor@techopolis.ca
Subject: email test

This is a great email test!
```

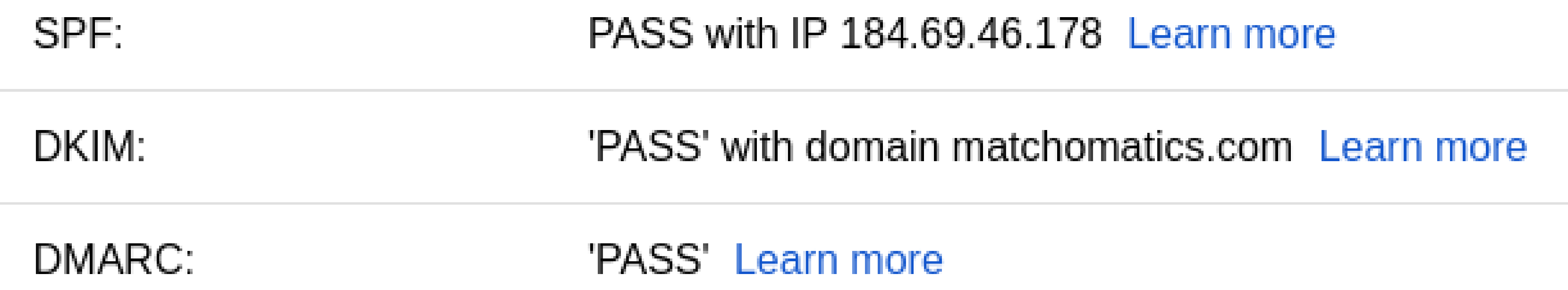
DMARC Alignment

- User can be assured the From: header they see is legit
- Someone who controls the domain shown allowed it
- A good thing and worthy goal for all mail admins

DMARC Alignment Headaches

- For third party email providers
- Mass mail senders legit businesses contract with
- Ask me how I know…

Gmail Demo



SPF:	PASS with IP 184.69.46.178 Learn more
DKIM:	'PASS' with domain matchomatics.com Learn more
DMARC:	'PASS' Learn more

Third Party Senders

- Easiest to align with DKIM (ignore SPF alignment)
- Common paradigm is provider will have you create a DNS TXT CNAME record pointing to a DKIM TXT record they host
- No need for companies to mess around with PKI keys of any type
- But they still have to know how to get their DNS edited

Real World Results

- Third party mass email sender:
- CNAME method
- Email open rate pre-April 1: 31-34%
- post-April 1: 21-25%
- Oddly, clicks are unchanged
- May be muddied by 1-pixel blocking
- business@3rdpartysender.com even worse

One-Click Unsubscribe

- Doesn’t mean you provide a link in the email body that will unsubscribe users with one click
- Does mean that you provide List-Unsubscribe headers that Gmail parses to provide a new button
- List-Unsusbscribe-Post: List-Unsubscribe=One-Click
- List-Unsubscribe: <https://z.ca/unsub?u=Jk33lJM>

One-Click Unsubscribe

- Custom built web sites / senders will need custom programming
- Framework-based sites may have plugins?
- Third party bulk email senders will do it for you

One-Click Unsubscribe

- Gmail will (probably) show a new Unsubscribe button
- They say it will sometimes show up, and sometimes not (black box)
- Makes testing difficult
- No re-subscribe ability
- Can be abused just like in-body links

One-Click Unsubscribe

- Uses POST instead of GET
- No confirmation
- No response
- URL in header must contain all identifying info
- Solves the overzealous infosec accidental unsub

One-Click Unsubscribe

- Not enforced (yet?)
- Email score demotion?
- Marketing vs transactional email
- Much is unknown / black box
- Far from perfect

One-Click Unsubscribe

- Demo
- (hopefully!)
- Maybe not!
- Thanks google & yahoo!

Scenarios: Normal Home User

- Do nothing!

Scenarios: SMB

- Small business with static IP sending their own email on their own server (Brad)
- SPF: DNS record
- DKIM: DNS record, opendkim daemon
- optional (if ever over 5000):
- DMARC: DNS record
- Alignment, one-click unsub(?)

Scenarios: Home User With Domain

- Home user with own domain and self-controlled external mail host or cloud instance (Wyatt?)
- Under 5000
- SPF: DNS record
- DKIM: DNS record, opendkim daemon

Scenarios: Home User With 3rd Party Host

- Home user with own domain and 3rd party email “smart host”
- SPF: ignore! or DNS record with smarthost’s IPs
- DKIM: DNS record with CNAME to smarthost’s DNS DKIM records
- Or they provide full DKIM record with pubkey for you to put in your DNS

Scenarios: Big Business/Gov With 3rd Party

- Same as home user with 3rd party smart host
- But add (because of 5000+):
- DMARC: DNS record
- Must ensure header-from alignment
- Difficult as every user/client can set their own!
- If bulk emailing: one-click unsub

Scenarios: Business Marketing Using 3rd Party

- Business using 3rd party mass-emailing systems for marketing, transactions, loyalty, etc.
- SPF: ignore!
- DKIM: DNS record with CNAME to 3rd party’s DNS DKIM records
- DMARC: DNS record
- Alignment & one-click: 3rd party’s problem

Scenario: You Are the 3rd Party!

- Ask me how I know!
- SPF: DNS record
- DKIM: DNS record, opendkim daemon, keys/rules for every business client, records they must paste into their DNS
- DMARC: provide business clients with copy pasta
- Alignment: must match domains
- One-click unsub: make a new POST page

Weirdness

- Mass-mailing
- DKIM passed when testing with mail-merge placeholders
- DKIM failed when actual mass mailing sent

Weirdness

- Mail-merge put a single HTML line over ~500 characters
- opendkim silently cuts off lines ~500 chars
- Gmail did something else: body hash mismatch
- No warning, no error
- Solution: Base64 encode all MIME parts
- Or check and reject long lines

Debugging

- Very hard to debug DKIM
- Very little helpful output from Gmail
- Try to narrow it down to: key/dns, body hash, header hash
- opendkim provides some tools in opendkim-tools package