How does email work?

PART 1

Is it secure?

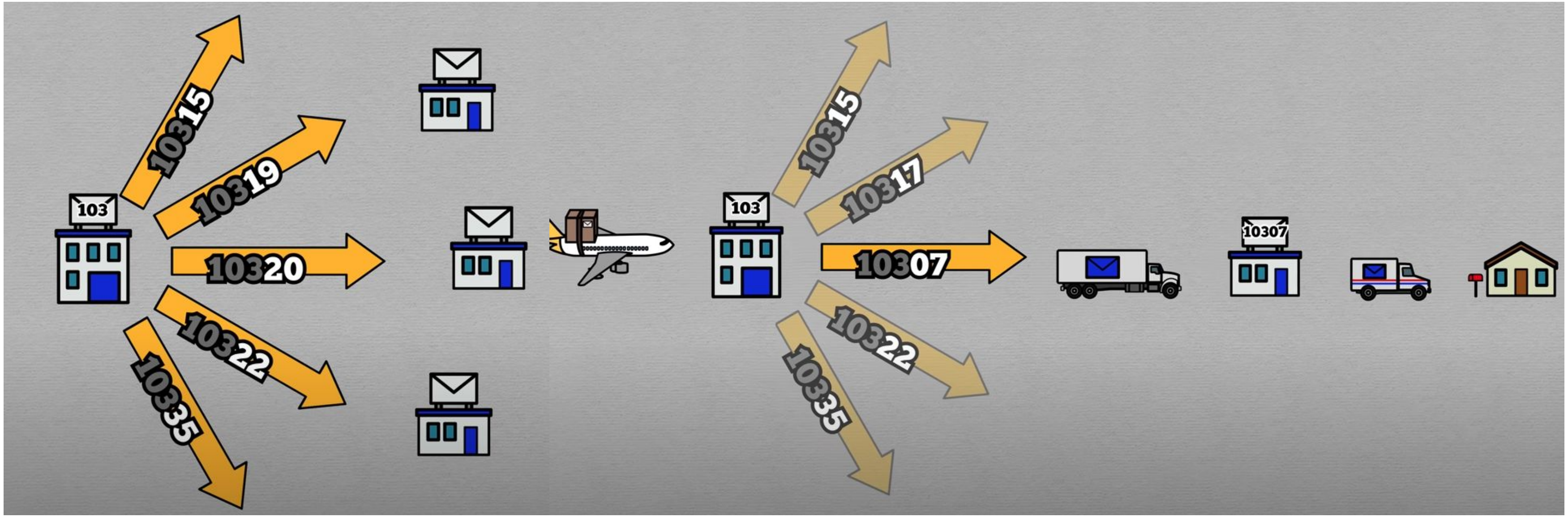
an overview of

SMTP, SPF, DKIM, DMARC

CYBER SECURITY CLUB AT UC DAVIS

24 FEB 2025

How does good old fashion *mail* work?



Zip Codes: https://youtu.be/1K5oDtVAYzk
CGP Grey, *The Hidden Pattern in Post Codes*

Simple Mail Transfer Protocol

- Application Layer Protocol
- Transfers (sends) mail on the internet
- *Simple* by design
- Takes mail and forwards to mail server

[username]@[address]

- Sends mail to server at [address]
- Internet abstracts middleman
- Final server sorts mail to users [username]

IMAP & POP3

Internet Mail Access Protocol

- Modern email
- Email server retains all copies
- Suited for *online* clients and multi-access

Post Office Protocol

- Works like real-world mail
- Once retrieved, server’s copy is removed
- Legacy: when servers had storage limits

What happens if I *pretend* to be someone else?

What happens in the real world if someone pretends to be a different sender?
What’s the difference between the real world and the internet?

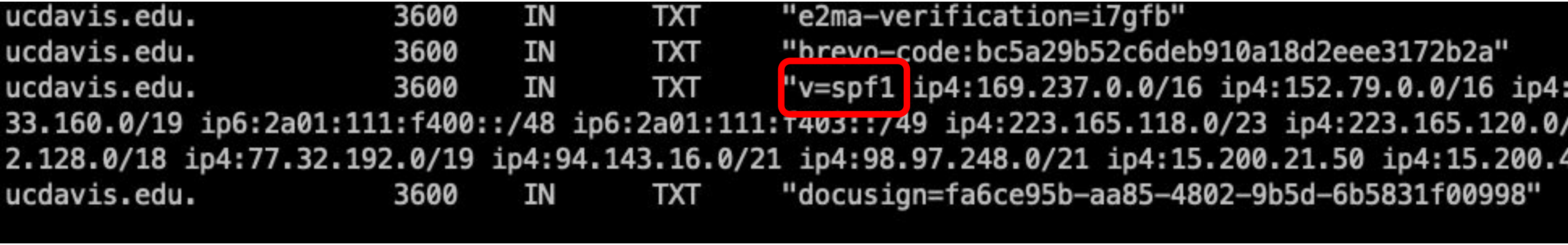
Sender Policy Framework

List of trusted sender IP addresses

- Exists in DNS TXT records
- Verifies (PASS/FAIL) based on list

Problems:

- Email “forwarding”



```
ucdavis.edu.            3600    IN      TXT     "e2ma-verification=i7gfb"
ucdavis.edu.            3600    IN      TXT     "brevo-code:bc5a29b52c6deb910a18d2eee3172b2a"
ucdavis.edu.            3600    IN      TXT     "v=spf1 ip4:169.237.0.0/16 ip4:152.79.0.0/16 ip4:
33.160.0/19 ip6:2a01:111:f400::/48 ip6:2a01:111:f403::/49 ip4:223.165.118.0/23 ip4:223.165.120.0/
2.128.0/18 ip4:77.32.192.0/19 ip4:94.143.16.0/21 ip4:98.97.248.0/21 ip4:15.200.21.50 ip4:15.200.4
ucdavis.edu.            3600    IN      TXT     "docusign=fa6ce95b-aa85-4802-9b5d-6b5831f00998"
```

Sender Rewriting Scheme (“bypassing SPF”)

- “Rewrites” SENDER FROM address
- Retains original path(s)
- SPF is continued to be used for all intermediate paths

SPF still relies on verifying the origin IP address

How do we check and confirm that?

Common SMTP Header Fields:

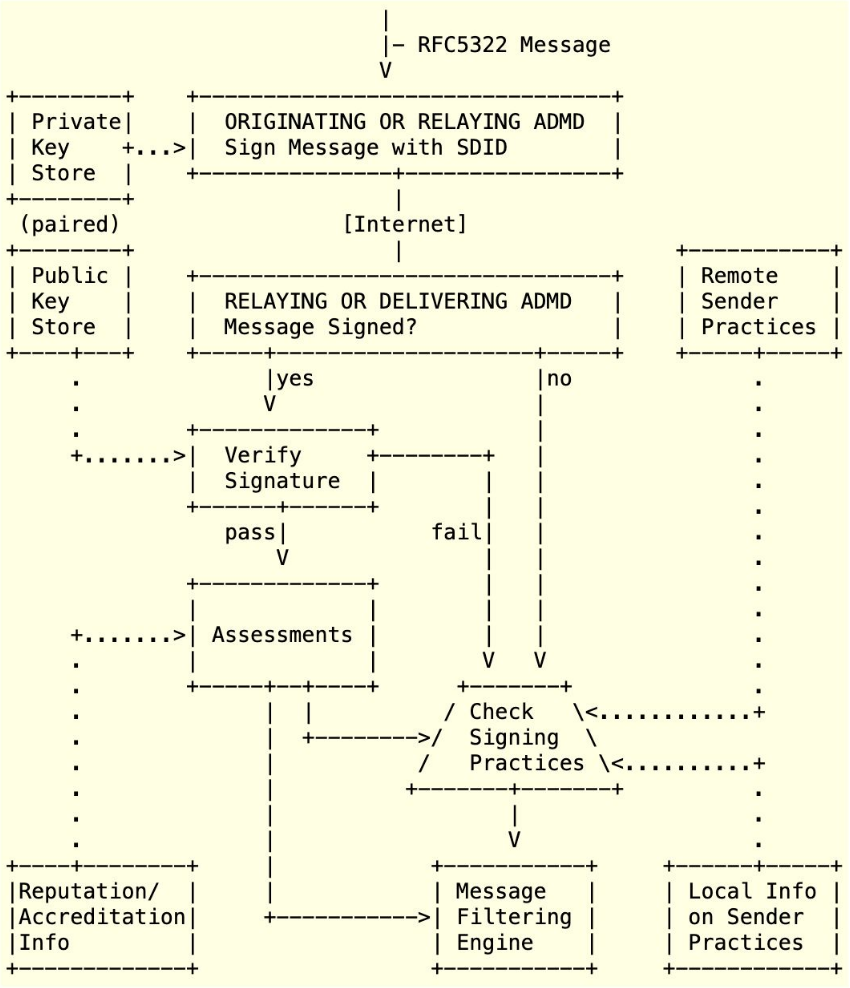
☆ SENDER (*ENVELOPE* FROM)
- FROM
- RETURN-PATH
- RCPT TO
- LIST ID
- Subject/Date/…

DKIM

DomainKeys Identified Mail

- Signs all outgoing mail
- Records in DNS
- Verifies that the message did *originate* from the domain
- Helps mitigate SPF spoofing

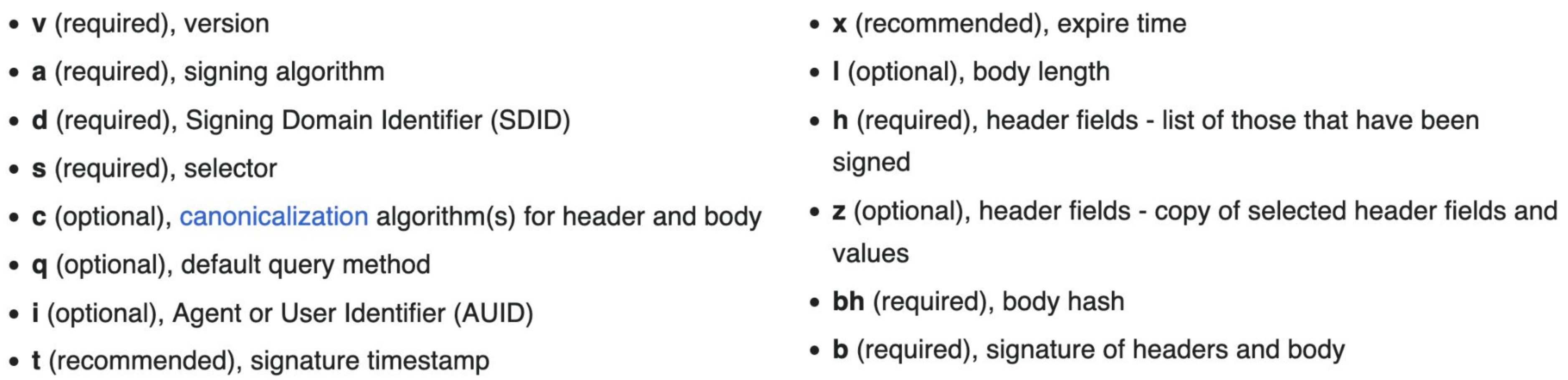
http://dkim.org/specs/rfc5585.html



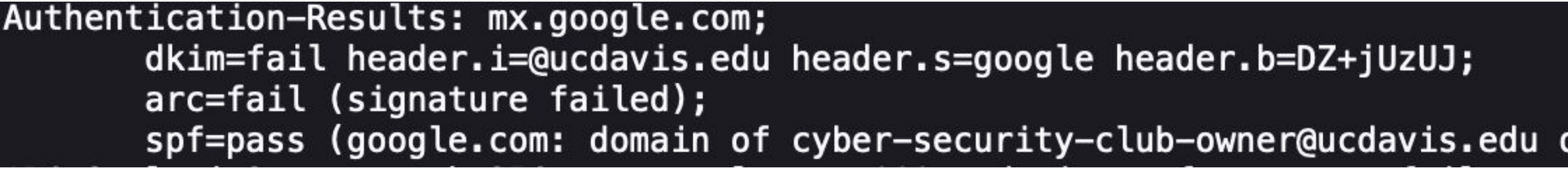
```
                             |
                             |- RFC5322 Message
                             V
+--------+    +--------------------------------+
| Private|    |  ORIGINATING OR RELAYING ADMD  |
| Key    +...>|  Sign Message with SDID        |
| Store  |    +---------------+----------------+
+--------+                    |
 (paired)                 [Internet]
+--------+                    |                     +-----------+
| Public |    +--------------------------------+    | Remote    |
| Key    |    |  RELAYING OR DELIVERING ADMD   |    | Sender    |
| Store  |    |  Message Signed?               |    | Practices |
+----+---+    +-----+--------------------+-----+    +-----+-----+
     .              |yes                 |no              .
     .              V                    |                .
     .        +-------------+            |                .
     +.......>|  Verify     +--------+   |                .
              |  Signature  |        |   |                .
              +------+------+        |   |                .
                 pass|           fail|   |                .
                     V               |   |                .
              +-------------+        |   |                .
              |             |        |   |                .
     +.......>| Assessments |        |   |                .
     .        |             |        V   V                .
     .        +-----+--+----+      +--------+             .
     .              |  |          / Check   \<............+
     .              |  +-------->/  Signing  \
     .              |           /   Practices \<..........+
     .              |          +-------+-------+          .
     .              |                  |                  .
     .              |                  V                  .
+----+--------+     |            +-----------+     +------+-----+
|Reputation/  |     |            | Message   |     | Local Info |
|Accreditation|     +----------->| Filtering |     | on Sender  |
|Info         |                  | Engine    |     | Practices  |
+-------------+                  +-----------+     +------------+
```

Figure 1: DKIM Service Architecture

DKIM con’t



- **v** (required), version
- **a** (required), signing algorithm
- **d** (required), Signing Domain Identifier (SDID)
- **s** (required), selector
- **c** (optional), canonicalization algorithm(s) for header and body
- **q** (optional), default query method
- **i** (optional), Agent or User Identifier (AUID)
- **t** (recommended), signature timestamp
- **x** (recommended), expire time
- **l** (optional), body length
- **h** (required), header fields - list of those that have been signed
- **z** (optional), header fields - copy of selected header fields and values
- **bh** (required), body hash
- **b** (required), signature of headers and body

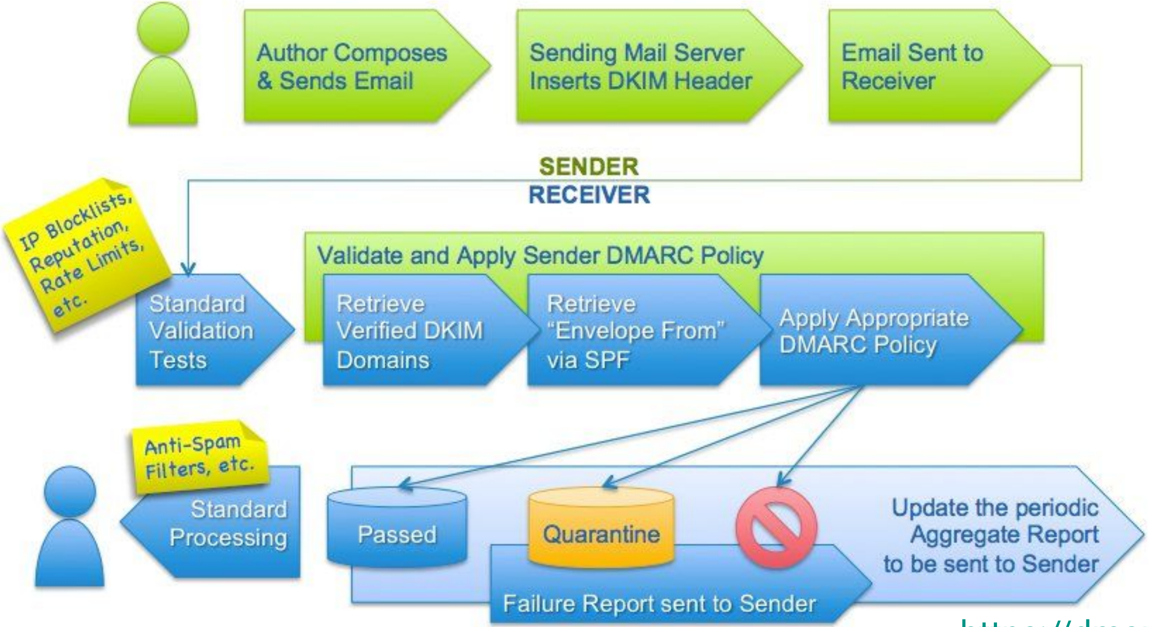


```
Authentication-Results: mx.google.com;
       dkim=fail header.i=@ucdavis.edu header.s=google header.b=DZ+jUzUJ;
       arc=fail (signature failed);
       spf=pass (google.com: domain of cyber-security-club-owner@ucdavis.edu
```

DMARC

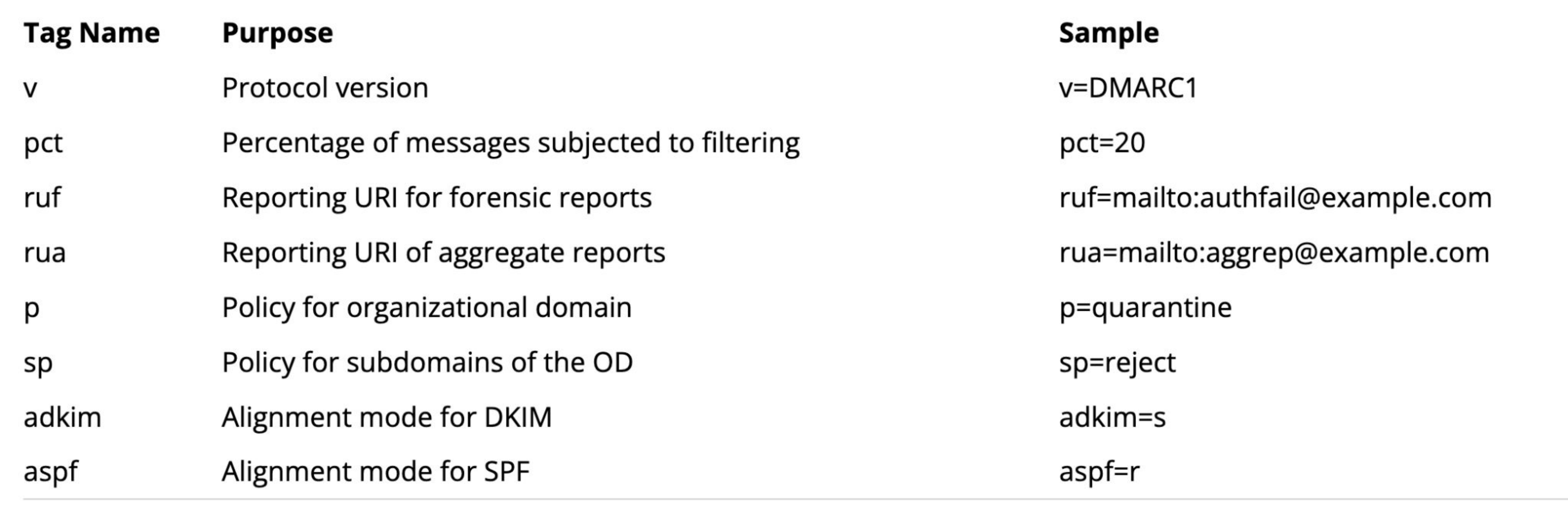
Domain-based Message Authentication, Reporting and Conformance

- Extension of SPF & DKIM
- Allows sender & receiver to communicate

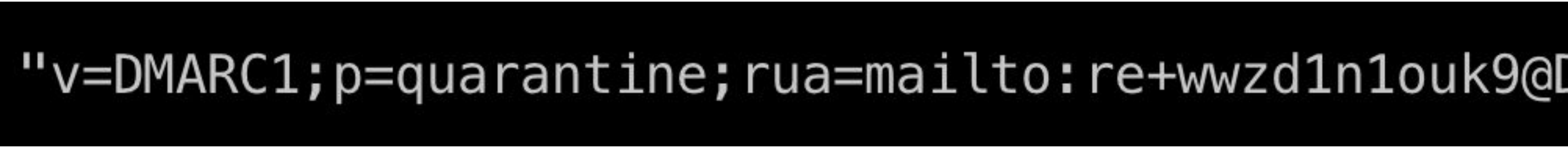

Author Composes & Sends Email
Sending Mail Server Inserts DKIM Header
Email Sent to Receiver
SENDER
RECEIVER
IP Blocklists, Reputation, Rate Limits, etc.
Standard Validation Tests
Validate and Apply Sender DMARC Policy
Retrieve Verified DKIM Domains
Retrieve "Envelope From" via SPF
Apply Appropriate DMARC Policy
Anti-Spam Filters, etc.
Standard Processing
Passed
Quarantine
Update the periodic Aggregate Report to be sent to Sender
Failure Report sent to Sender

https://dmarc.org/

DMARC con’t

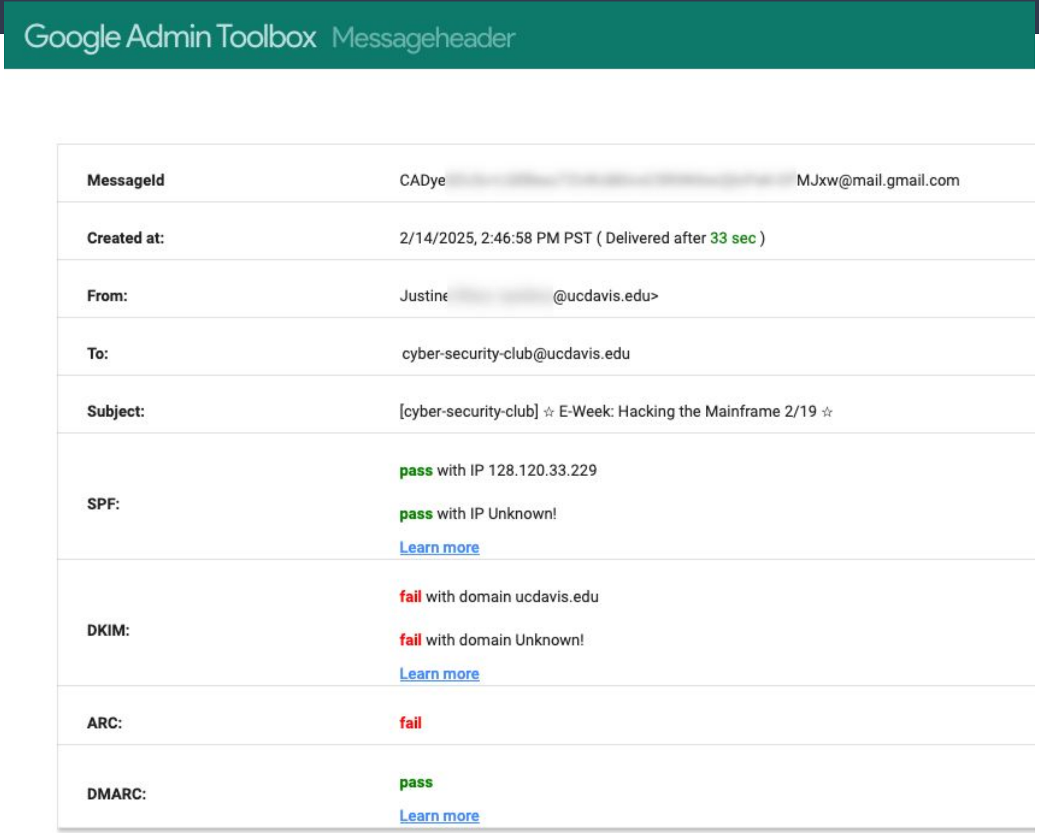


Tag Name	Purpose	Sample
v	Protocol version	v=DMARC1
pct	Percentage of messages subjected to filtering	pct=20
ruf	Reporting URI for forensic reports	ruf=mailto:authfail@example.com
rua	Reporting URI of aggregate reports	rua=mailto:aggrep@example.com
p	Policy for organizational domain	p=quarantine
sp	Policy for subdomains of the OD	sp=reject
adkim	Alignment mode for DKIM	adkim=s
aspf	Alignment mode for SPF	aspf=r



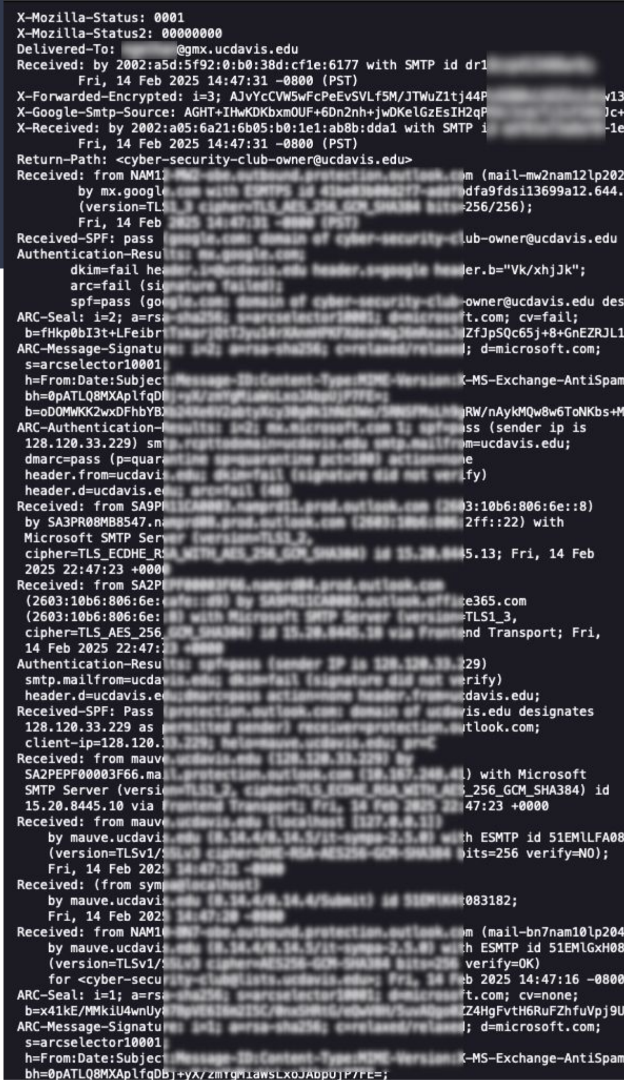
```
"v=DMARC1;p=quarantine;rua=mailto:re+wwzd1n1ouk9@D
```

How it comes together



Google Admin Toolbox Messageheader

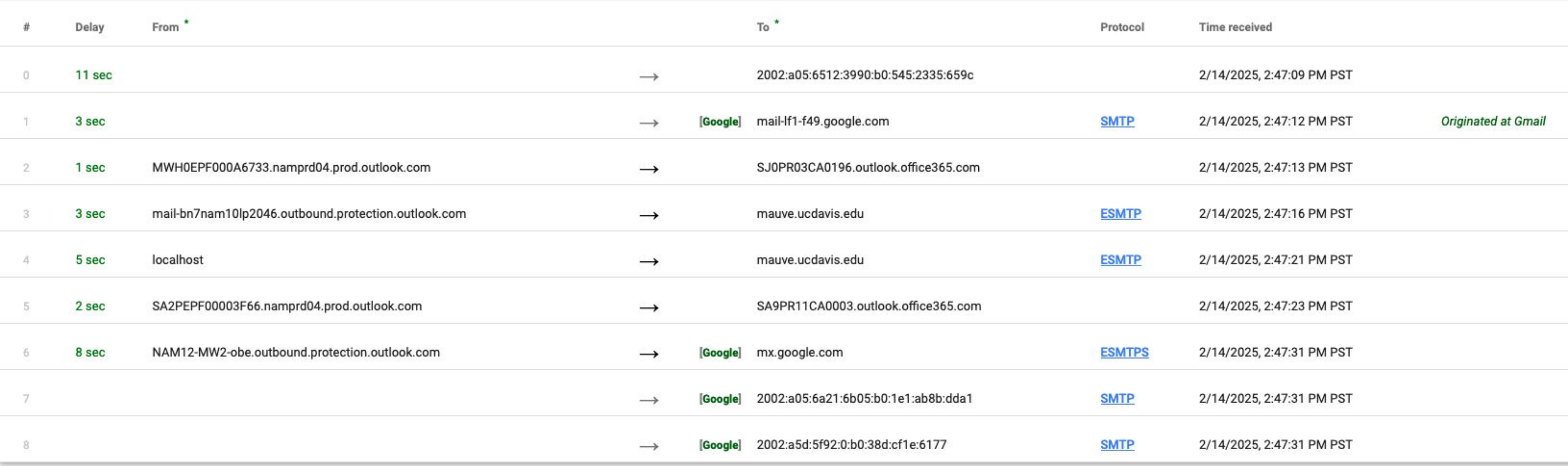
MessageId	CADye[redacted]MJxw@mail.gmail.com
Created at:	2/14/2025, 2:46:58 PM PST (Delivered after 33 sec)
From:	Justine [redacted]@ucdavis.edu>
To:	cyber-security-club@ucdavis.edu
Subject:	[cyber-security-club] ☆ E-Week: Hacking the Mainframe 2/19 ☆
SPF:	pass with IP 128.120.33.229 pass with IP Unknown! Learn more
DKIM:	fail with domain ucdavis.edu fail with domain Unknown! Learn more
ARC:	fail
DMARC:	pass Learn more



```
X-Mozilla-Status: 0001
X-Mozilla-Status2: 00000000
Delivered-To: [redacted]@gmx.ucdavis.edu
Received: by 2002:a5d:5f92:0:b0:38d:cf1e:6177 with SMTP id dr1[redacted]
        Fri, 14 Feb 2025 14:47:31 -0800 (PST)
X-Forwarded-Encrypted: i=3; AJvYcCVW5wFcPeEvSVLf5M/JTWuZ1tj44P[redacted]v13
X-Google-Smtp-Source: AGHT+IHwKDKbxmOUF+6Dn2nh+jwDKelGzEsIH2qP[redacted]Jc+
X-Received: by 2002:a05:6a21:6b05:b0:1e1:ab8b:dda1 with SMTP i[redacted]-1e
        Fri, 14 Feb 2025 14:47:31 -0800 (PST)
Return-Path: <cyber-security-club-owner@ucdavis.edu>
Received: from NAM1[redacted]m (mail-mw2nam12lp202
        by mx.googl[redacted]dfa9fdsi13699a12.644.
        (version=TL[redacted]256/256);
        Fri, 14 Feb [redacted]
Received-SPF: pass [redacted]lub-owner@ucdavis.edu
Authentication-Resu[redacted]
       dkim=fail he[redacted]er.b="Vk/xhjJk";
       arc=fail (si[redacted]
       spf=pass (go[redacted]-owner@ucdavis.edu des
ARC-Seal: i=2; a=rs[redacted]t.com; cv=fail;
 b=fHkp0bI3t+LFeibr[redacted]ZfJpSQc65j+8+GnEZRJL1
ARC-Message-Signatu[redacted]; d=microsoft.com;
 s=arcselector10001[redacted]
 h=From:Date:Subjec[redacted]X-MS-Exchange-AntiSpam
 bh=0pATLQ8MXAplfqD[redacted]
 b=oDOMWKK2wxDFhbYB[redacted]RW/nAykMQw8w6ToNKbs+M
ARC-Authentication-[redacted]ss (sender ip is
 128.120.33.229) sm[redacted]m=ucdavis.edu;
 dmarc=pass (p=quar[redacted]e
 header.from=ucdavi[redacted]fy)
 header.d=ucdavis.e[redacted]
Received: from SA9P[redacted]3:10b6:806:6e::8)
 by SA3PR08MB8547.n[redacted]2ff::22) with
 Microsoft SMTP Ser[redacted]
 cipher=TLS_ECDHE_R[redacted]5.13; Fri, 14 Feb
 2025 22:47:23 +000[redacted]
Received: from SA2P[redacted]
 (2603:10b6:806:6e:[redacted]e365.com
 (2603:10b6:806:6e:[redacted]TLS1_3,
 cipher=TLS_AES_256[redacted]nd Transport; Fri,
 14 Feb 2025 22:47:[redacted]
Authentication-Resu[redacted]29)
 smtp.mailfrom=ucda[redacted]rify)
 header.d=ucdavis.e[redacted]davis.edu;
Received-SPF: Pass [redacted]is.edu designates
 128.120.33.229 as [redacted]tlook.com;
 client-ip=128.120.[redacted]
Received: from mauv[redacted]
 SA2PEPF00003F66.ma[redacted]) with Microsoft
 SMTP Server (versi[redacted]_256_GCM_SHA384) id
 15.20.8445.10 via [redacted]47:23 +0000
Received: from mauv[redacted]
    by mauve.ucdavi[redacted]h ESMTP id 51EMlLFA08
    (version=TLSv1/[redacted]bits=256 verify=NO);
    Fri, 14 Feb 202[redacted]
Received: (from sym[redacted]
    by mauve.ucdavi[redacted]083182;
    Fri, 14 Feb 202[redacted]
Received: from NAM1[redacted]m (mail-bn7nam10lp204
    by mauve.ucdavi[redacted]h ESMTP id 51EMlGxH08
    (version=TLSv1/[redacted] verify=OK)
    for <cyber-secu[redacted]b 2025 14:47:16 -0800
ARC-Seal: i=1; a=rs[redacted]t.com; cv=none;
 b=x41kE/MMkiU4wnUy[redacted]Z4HgFvtH6RuFZhfuVpj9U
ARC-Message-Signatu[redacted]; d=microsoft.com;
 s=arcselector10001[redacted]
 h=From:Date:Subjec[redacted]X-MS-Exchange-AntiSpam
 bh=0pATLQ8MXAplfqDBj+yX/zmYgMiawsLxoJAbpUjP7FE=;
```

con’t

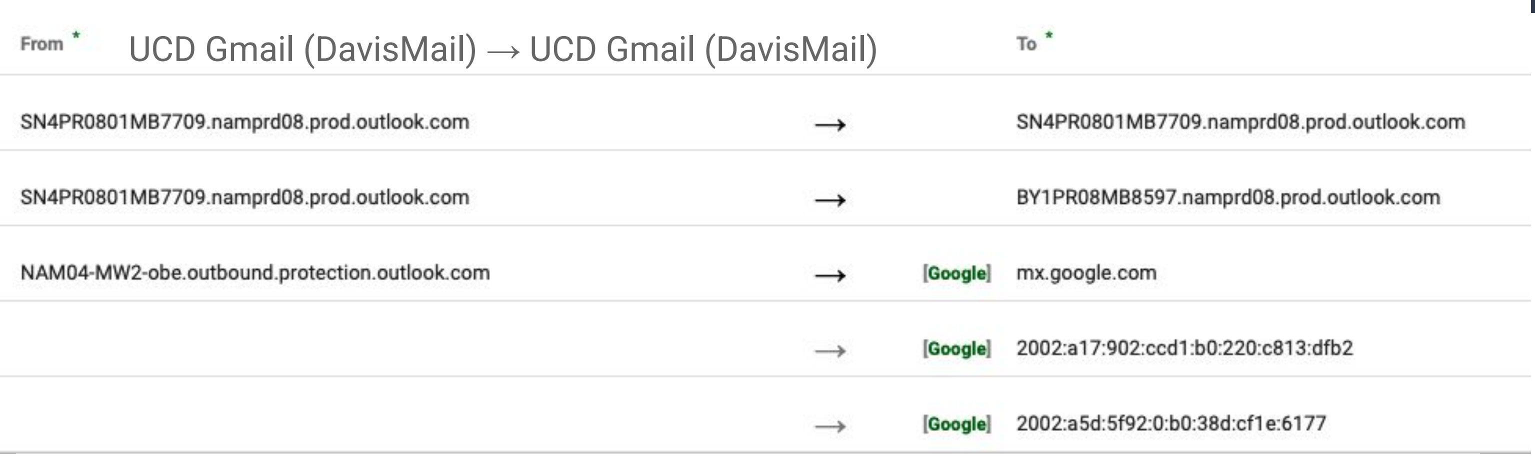
UCD Gmail (DavisMail) → UCD Sympa (Mailing list) → UCD Gmail (DavisMail)



#	Delay	From *			To *	Protocol	Time received	
0	11 sec		→		2002:a05:6512:3990:b0:545:2335:659c		2/14/2025, 2:47:09 PM PST	
1	3 sec		→	[Google]	mail-lf1-f49.google.com	SMTP	2/14/2025, 2:47:12 PM PST	*Originated at Gmail*
2	1 sec	MWH0EPF000A6733.namprd04.prod.outlook.com	→		SJ0PR03CA0196.outlook.office365.com		2/14/2025, 2:47:13 PM PST	
3	3 sec	mail-bn7nam10lp2046.outbound.protection.outlook.com	→		mauve.ucdavis.edu	ESMTP	2/14/2025, 2:47:16 PM PST	
4	5 sec	localhost	→		mauve.ucdavis.edu	ESMTP	2/14/2025, 2:47:21 PM PST	
5	2 sec	SA2PEPF00003F66.namprd04.prod.outlook.com	→		SA9PR11CA0003.outlook.office365.com		2/14/2025, 2:47:23 PM PST	
6	8 sec	NAM12-MW2-obe.outbound.protection.outlook.com	→	[Google]	mx.google.com	ESMTPS	2/14/2025, 2:47:31 PM PST	
7			→	[Google]	2002:a05:6a21:6b05:b0:1e1:ab8b:dda1	SMTP	2/14/2025, 2:47:31 PM PST	
8			→	[Google]	2002:a5d:5f92:0:b0:38d:cf1e:6177	SMTP	2/14/2025, 2:47:31 PM PST	

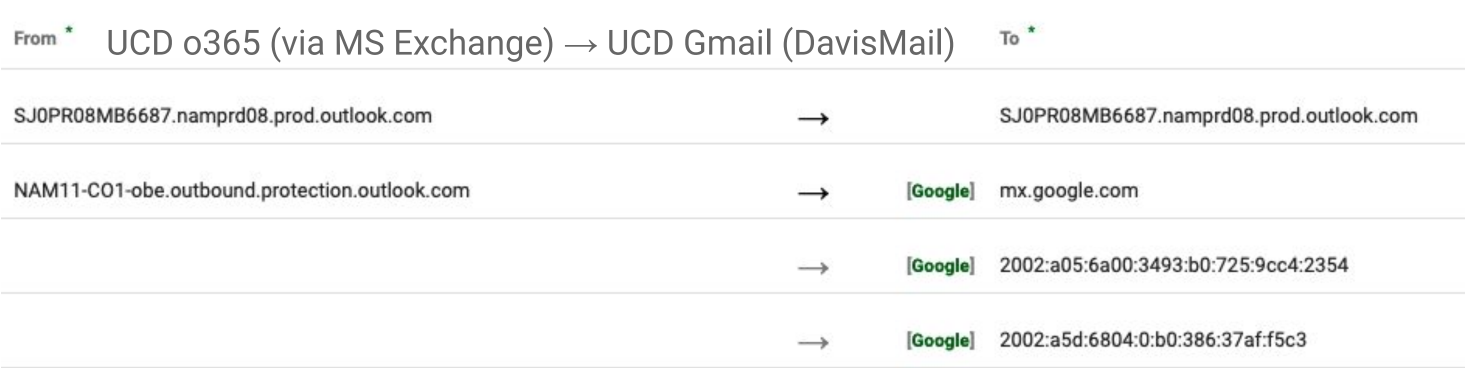
"v=DMARC1;p=quarantine;rua=mailto:re+wwzd1n1ouk9@DMARC.postmarkapp.com,mailto:dmarc_agg@valigov.email;rf=afrf;sp=quarantine;fo=1;pct=100;aspf=r"

More examples



UCD Gmail (DavisMail) → UCD Gmail (DavisMail)

From *			To *
SN4PR0801MB7709.namprd08.prod.outlook.com	→		SN4PR0801MB7709.namprd08.prod.outlook.com
SN4PR0801MB7709.namprd08.prod.outlook.com	→		BY1PR08MB8597.namprd08.prod.outlook.com
NAM04-MW2-obe.outbound.protection.outlook.com	→	[Google]	mx.google.com
	→	[Google]	2002:a17:902:ccd1:b0:220:c813:dfb2
	→	[Google]	2002:a5d:5f92:0:b0:38d:cf1e:6177



UCD o365 (via MS Exchange) → UCD Gmail (DavisMail)

From *			To *
SJ0PR08MB6687.namprd08.prod.outlook.com	→		SJ0PR08MB6687.namprd08.prod.outlook.com
NAM11-CO1-obe.outbound.protection.outlook.com	→	[Google]	mx.google.com
	→	[Google]	2002:a05:6a00:3493:b0:725:9cc4:2354
	→	[Google]	2002:a5d:6804:0:b0:386:37af:f5c3

Thank you

Part 2: How to ensure messages are not *tampered with* in transit?

A look into *SMIME* (PKI), PGP/GPG, and SSL/TLS in email.

https://daviscybersec.org

CYBER SECURITY CLUB AT UC DAVIS