4/8/2023

Email Header Analysis

Computer Networks Assignment # 1

EMAIL HEADER ANALYSIS Sardar Muhammad Zeeshan khan
27969 TEACHER: SIR AHMED NAWAZ

CONTENTS

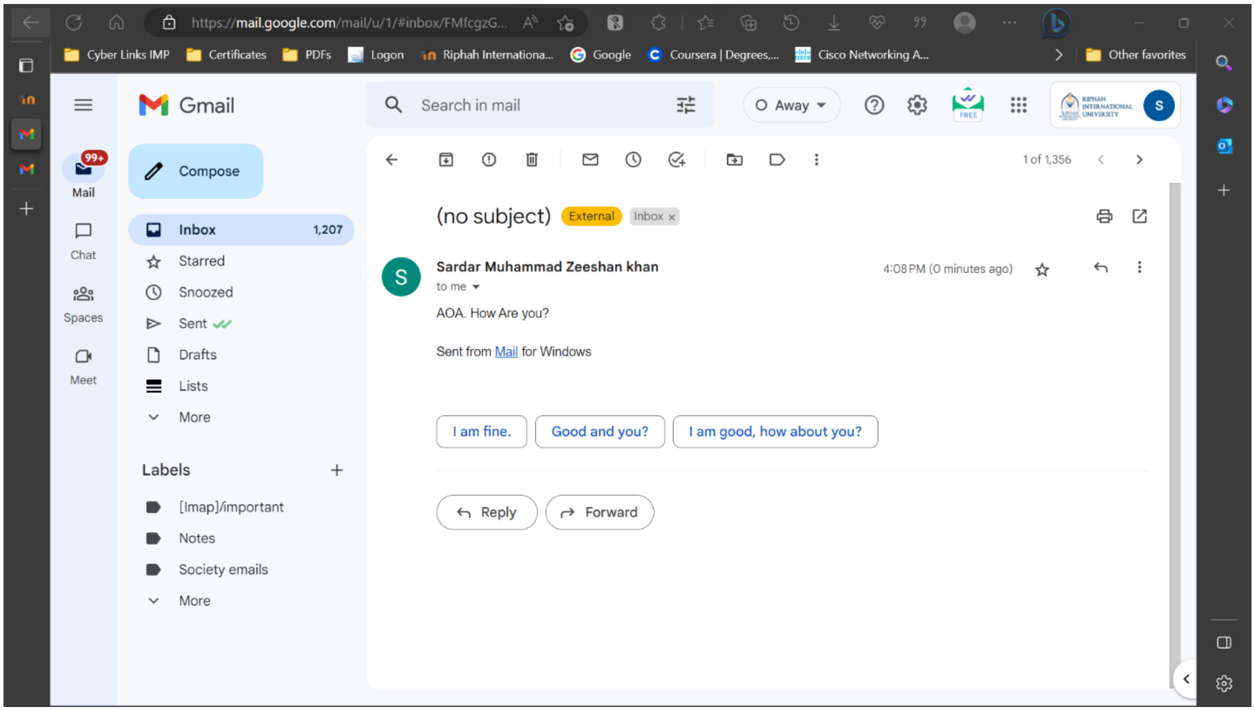
EMAIL HEADER PARTS

An email header typically contains the following parts:

1. **From:** The email address of the sender.
2. **To:** The email address of the recipient.
3. **Cc:** The email addresses of any additional recipients who are being copied on the email.
4. **Bcc:** The email addresses of any additional recipients who are being blind copied on the email (i.e., their email address is hidden from other recipients).
5. **Subject:** A brief description of the topic of the email.
6. **Date:** The date and time the email was sent.
7. **Reply-To:** The email address to which the recipient should send a reply.
8. **Message ID:** A unique identifier assigned to the email by the email server.
9. **MIME-Version:** The version of the Multipurpose Internet Mail Extensions (MIME) standard used for email.
10. **Content-Type:** The type of content included in the email (e.g., text, HTML, images, attachments).
11. **Content-Transfer-Encoding:** The method used to encode the email content (e.g., Base64, Quoted-Printable).
12. **X-Mailer:** The email client or software used to send the email.

EMAIL HEADER ANALYSIS BY MX TOOL

First of all for the analysis I received an email from my other email address



(no subject)

Sardar Muhammad Zeeshan khan

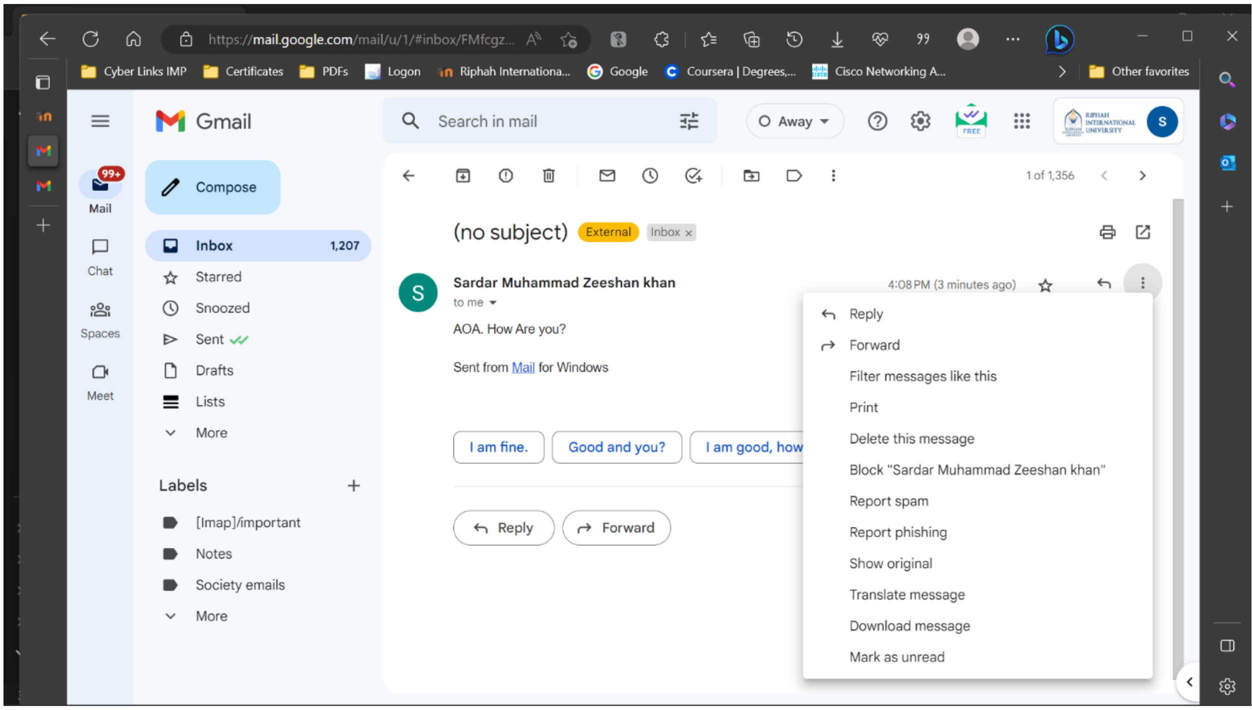
to me

4:08 PM (0 minutes ago)

AOA. How Are you?

Sent from Mail for Windows

Then I tapped on the 3 dots on the right and click on the show original option.



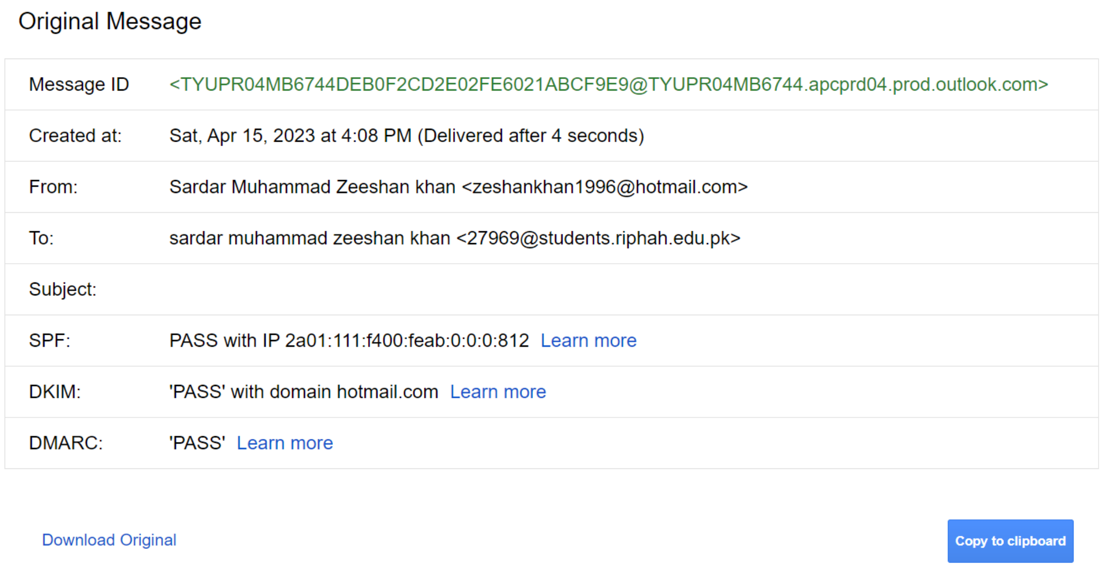
(no subject) External Inbox ×

Sardar Muhammad Zeeshan khan
to me
4:08 PM (3 minutes ago)

AOA. How Are you?

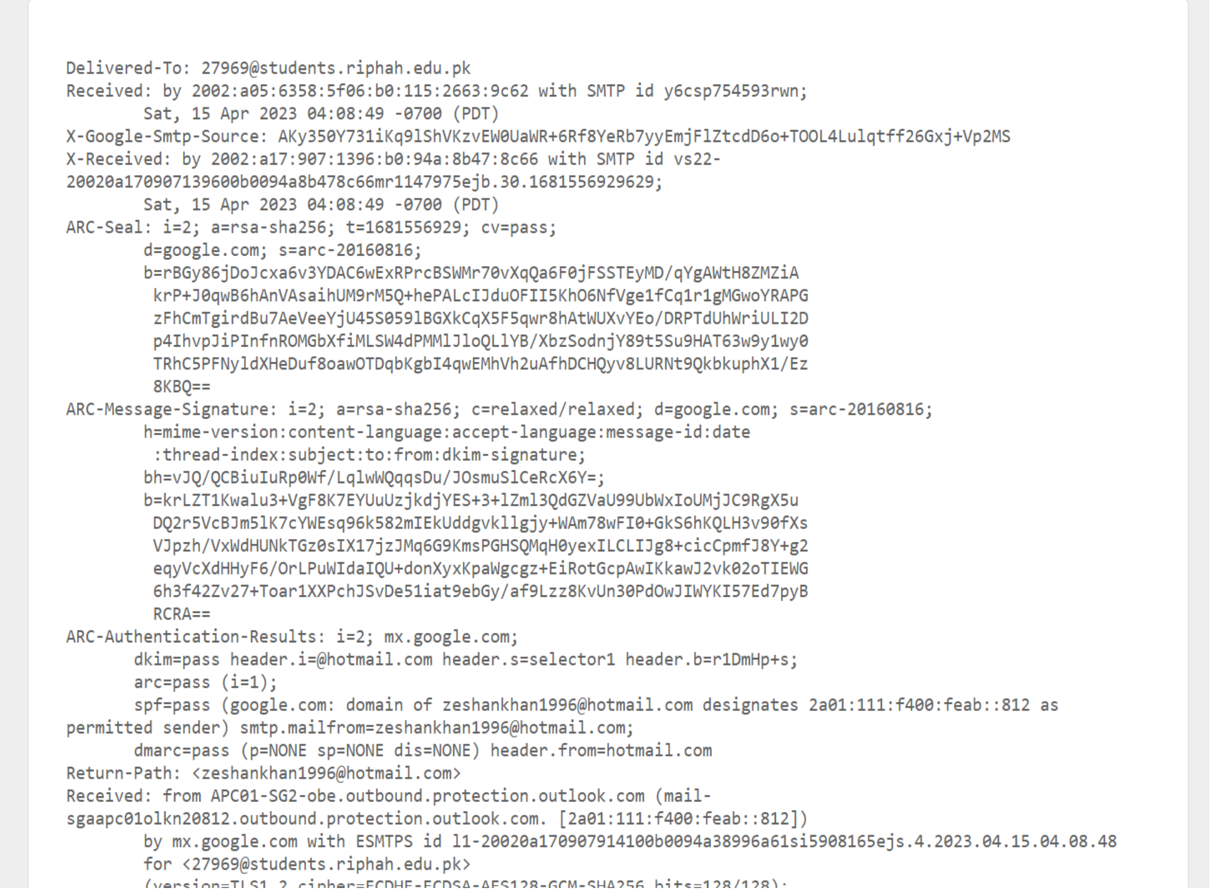
Sent from Mail for Windows

It will open up an email header in the new tab as shown in the figure.



Original Message

Message ID	<TYUPR04MB6744DEB0F2CD2E02FE6021ABCF9E9@TYUPR04MB6744.apcprd04.prod.outlook.com>
Created at:	Sat, Apr 15, 2023 at 4:08 PM (Delivered after 4 seconds)
From:	Sardar Muhammad Zeeshan khan <zeshankhan1996@hotmail.com>
To:	sardar muhammad zeeshan khan <27969@students.riphah.edu.pk>
Subject:	
SPF:	PASS with IP 2a01:111:f400:feab:0:0:0:812 Learn more
DKIM:	'PASS' with domain hotmail.com Learn more
DMARC:	'PASS' Learn more

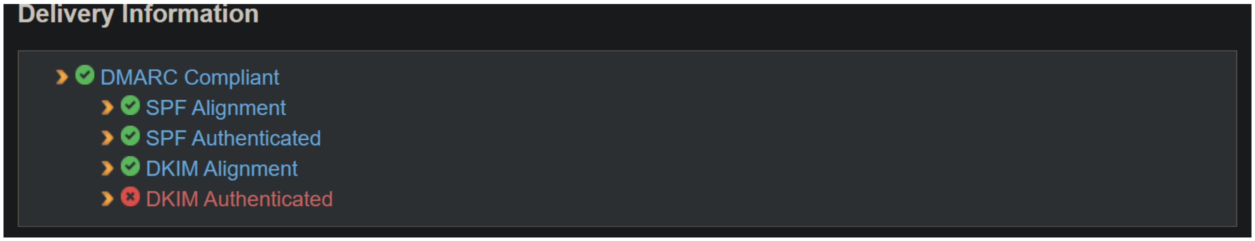


```
Delivered-To: 27969@students.riphah.edu.pk
Received: by 2002:a05:6358:5f06:b0:115:2663:9c62 with SMTP id y6csp754593rwn;
        Sat, 15 Apr 2023 04:08:49 -0700 (PDT)
X-Google-Smtp-Source: AKy350Y731iKq9lShVKzvEW0UaWR+6Rf8YeRb7yyEmjFlZtcdD6o+TOOL4Lulqtff26Gxj+Vp2MS
X-Received: by 2002:a17:907:1396:b0:94a:8b47:8c66 with SMTP id vs22-
20020a170907139600b0094a8b478c66mr1147975ejb.30.1681556929629;
        Sat, 15 Apr 2023 04:08:49 -0700 (PDT)
ARC-Seal: i=2; a=rsa-sha256; t=1681556929; cv=pass;
        d=google.com; s=arc-20160816;
        b=rBGy86jDoJcxa6v3YDAC6wExRPrcBSWMr70vXqQa6F0jFSSTEyMD/qYgAWtH8ZMZiA
         krP+J0qwB6hAnVAsaihUM9rM5Q+hePALcIJduOFII5KhO6NfVge1fCq1r1gMGwoYRAPG
         zFhCmTgirdBu7AeVeeYjU45S059lBGXkCqX5F5qwr8hAtWUXvYEo/DRPTdUhWriULI2D
         p4IhvpJiPInfnROMGbXfiMLSW4dPMMlJloQLlYB/XbzSodnjY89t5Su9HAT63w9y1wy0
         TRhC5PFNyldXHeDuf8oawOTDqbKgbI4qwEMhVh2uAfhDCHQyv8LURNt9QkbkuphX1/Ez
         8KBQ==
ARC-Message-Signature: i=2; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=mime-version:content-language:accept-language:message-id:date
         :thread-index:subject:to:from:dkim-signature;
        bh=vJQ/QCBiuIuRp0Wf/LqlwWQqqsDu/JOsmuSlCeRcX6Y=;
        b=krLZT1Kwalu3+VgF8K7EYUuUzjkdjYES+3+lZml3QdGZVaU99UbWxIoUMjJC9RgX5u
         DQ2r5VcBJm5lK7cYWEsq96k582mIEkUddgvkllgjy+WAm78wFI0+GkS6hKQLH3v90fXs
         VJpzh/VxWdHUNkTGz0sIX17jzJMq6G9KmsPGHSQMqH0yexILCLIJg8+cicCpmfJ8Y+g2
         eqyVcXdHHyF6/OrLPuWIdaIQU+donXyxKpaWgcgz+EiRotGcpAwIKkawJ2vk02oTIEWG
         6h3f42Zv27+Toar1XXPchJSvDe51iat9ebGy/af9Lzz8KvUn30PdOwJIWYKI57Ed7pyB
         RCRA==
ARC-Authentication-Results: i=2; mx.google.com;
       dkim=pass header.i=@hotmail.com header.s=selector1 header.b=r1DmHp+s;
       arc=pass (i=1);
       spf=pass (google.com: domain of zeshankhan1996@hotmail.com designates 2a01:111:f400:feab::812 as
permitted sender) smtp.mailfrom=zeshankhan1996@hotmail.com;
       dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=hotmail.com
Return-Path: <zeshankhan1996@hotmail.com>
Received: from APC01-SG2-obe.outbound.protection.outlook.com (mail-
sgaapc01olkn20812.outbound.protection.outlook.com. [2a01:111:f400:feab::812])
        by mx.google.com with ESMTPS id l1-20020a170907914100b0094a38996a61si5908165ejs.4.2023.04.15.04.08.48
        for <27969@students.riphah.edu.pk>
        (version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128);
```

Then I copied the Email header for analysis of the email.

Then I opened up the MX Tool for the Analysis of the Email header and paste the header there.

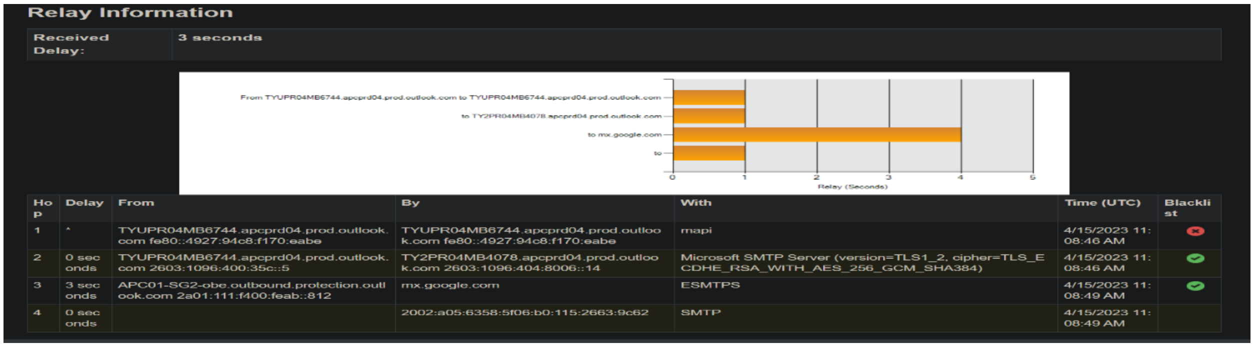
DELIVERY INFORMATION



Delivery Information

- › ✓ DMARC Compliant
    - › ✓ SPF Alignment
    - › ✓ SPF Authenticated
    - › ✓ DKIM Alignment
    - › ✗ DKIM Authenticated

RELAY INFORMATION



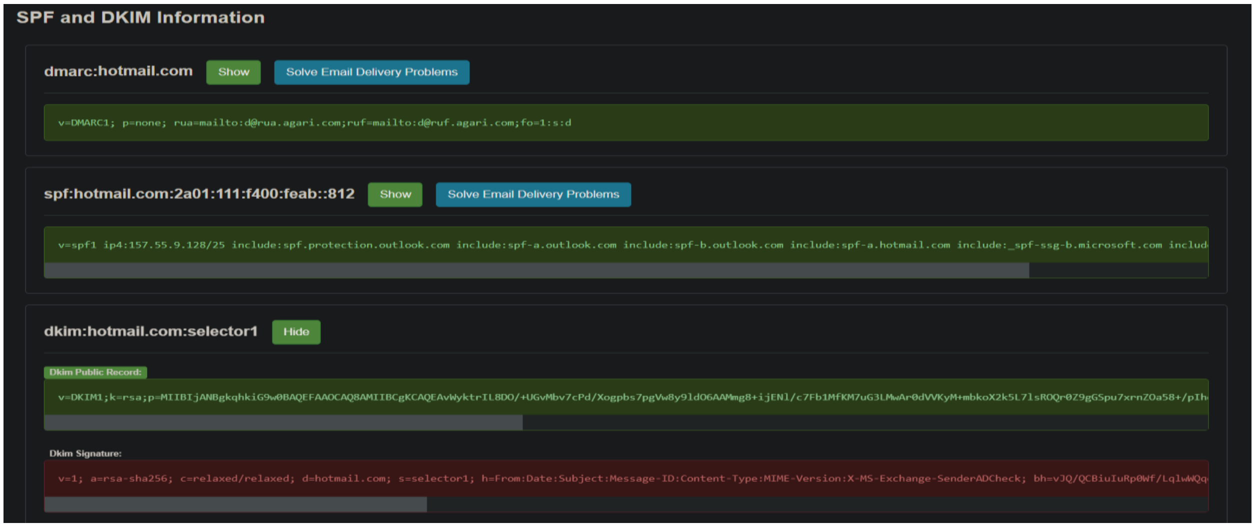
Relay Information

Received Delay:	3 seconds

From TYUPR04MB6744.apcprd04.prod.outlook.com to TYUPR04MB6744.apcprd04.prod.outlook.com
to TY2PR04MB4078.apcprd04.prod.outlook.com
to mx.google.com
to
0
1
2
3
4
5
Relay (Seconds)

Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	TYUPR04MB6744.apcprd04.prod.outlook.com fe80::4927:94c8:f170:eabe	TYUPR04MB6744.apcprd04.prod.outlook.com fe80::4927:94c8:f170:eabe	mapi	4/15/2023 11:08:46 AM	✗
2	0 seconds	TYUPR04MB6744.apcprd04.prod.outlook.com 2603:1096:400:35c::5	TY2PR04MB4078.apcprd04.prod.outlook.com 2603:1096:404:8006::14	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	4/15/2023 11:08:46 AM	✓
3	3 seconds	APC01-SG2-obe.outbound.protection.outlook.com 2a01:111:f400:feab::812	mx.google.com	ESMTPS	4/15/2023 11:08:49 AM	✓
4	0 seconds		2002:a05:6358:5f06:b0:115:2663:9c62	SMTP	4/15/2023 11:08:49 AM	

SPF & and DKIM INFORMATION



SPF and DKIM Information

dmarc:hotmail.com

```
v=DMARC1; p=none; rua=mailto:d@rua.agari.com;ruf=mailto:d@ruf.agari.com;fo=1:s:d
```

spf:hotmail.com:2a01:111:f400:feab::812

```
v=spf1 ip4:157.55.9.128/25 include:spf.protection.outlook.com include:spf-a.outlook.com include:spf-b.outlook.com include:spf-a.hotmail.com include:_spf-ssg-b.microsoft.com includ
```

dkim:hotmail.com:selector1

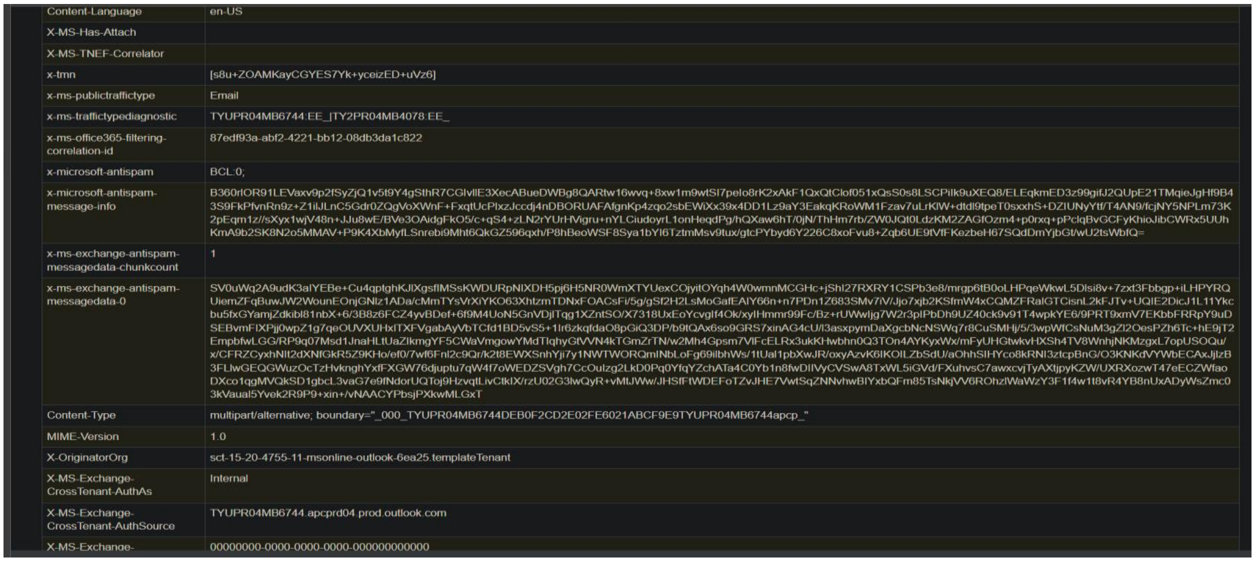
Dkim Public Record:

```
v=DKIM1;k=rsa;p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvWyktrIL8DO/+UGvMbv7cPd/Xogpbs7pgVw8y91dO6AAMmg8+ijENl/c7Fb1MfKM7uG3LMwAr0dVVKyM+mbkoX2k5L71sROQr0Z9gGSpu7xrnZOa58+/pIh
```

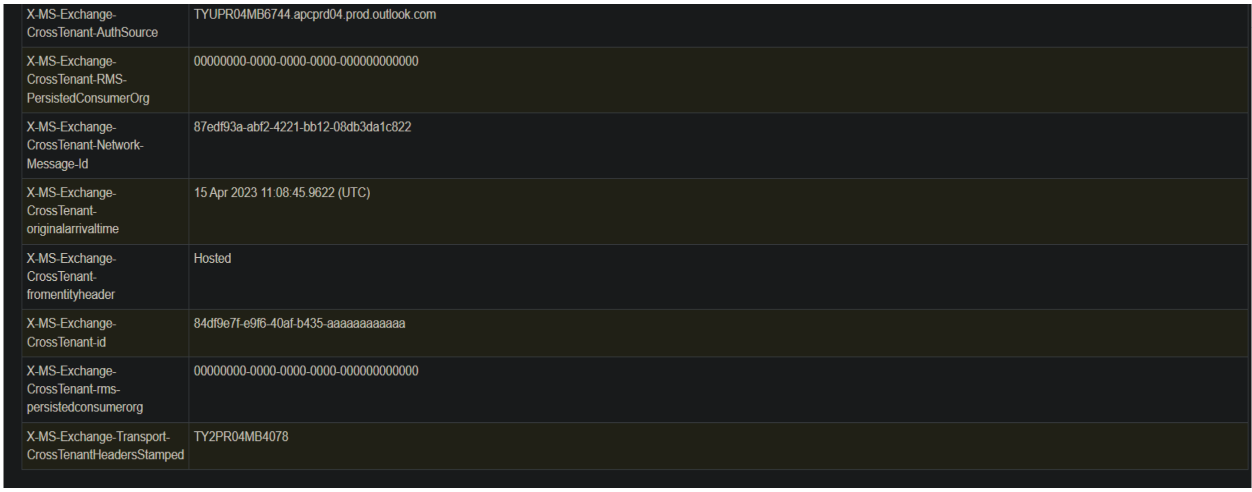
Dkim Signature:

```
v=1; a=rsa-sha256; c=relaxed/relaxed; d=hotmail.com; s=selector1; h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-SenderADCheck; bh=vJQ/QCBiuIuRp0Wf/LqlwWQq
```

HEADERS FOUND



Content-Language	en-US
X-MS-Has-Attach	
X-MS-TNEF-Correlator	
x-tmn	[s8u+ZOAMKayCGYES7Yk+yceizED+uVz6]
x-ms-publictraffictype	Email
x-ms-traffictypediagnostic	TYUPR04MB6744:EE_|TY2PR04MB4078:EE_
x-ms-office365-filtering-correlation-id	87edf93a-abf2-4221-bb12-08db3da1c822
x-microsoft-antispam	BCL:0;
x-microsoft-antispam-message-info	B360rIOR91LEVaxv9p2fSyZjQ1v5t9Y4gSthR7CGIvlIE3XecABueDWBg8QARtw16wvq+8xw1m9wtSI7pelo8rK2xAkF1QxQtClof051xQsS0s8LSCPilk9uXEQ8/ELEqkmED3z99gifJ2QUpE21TMqieJgHf9B43S9FkPfvnRn9z+Z1ilJLnC5Gdr0ZQgVoXWnF+FxqtUcPlxzJccdj4nDBORUAFAfgnKp4zqo2sbEWiXx39x4DD1Lz9aY3EakqKRoWM1Fzav7uLrKlW+dtdl9tpeT0sxxhS+DZIUNyYtf/T4AN9/fcjNY5NPLm73K2pEqm1z//sXyx1wjV48n+JJu8wE/BVe3OAidgFkO5/c+qS4+zLN2rYUrHVigru+nYLCiudoyrL1onHeqdPg/hQXaw6hT/0jN/ThHm7rb/ZW0JQt0LdzKM2ZAGfOzm4+p0rxq+pPclqBvGCFyKhioJibCWRx5UUhKmA9b2SK8N2o5MMAV+P9K4XbMyfLSnrebi9Mht6QkGZ596qxh/P8hBeoWSF8Sya1bYI6TztmMsv9tux/gtcPYbyd6Y226C8xoFvu8+Zqb6UE9tVfFKezbeH67SQdDmYjbGt/wU2tsWbfQ=
x-ms-exchange-antispam-messagedata-chunkcount	1
x-ms-exchange-antispam-messagedata-0	SV0uWq2A9udK3alYEBe+Cu4qptghKJlXgsflMSsKWDURpNIXDH5pj6H5NR0WmXTYUexCOjyitOYqh4W0wmnMCGHc+jShI27RXRY1CSPb3e8/mrgp6tB0oLHPqeWkwL5Dlsi8v+7zxt3Fbbgp+iLHPYRQUiemZFqBuwJW2WounEOnjGNlz1ADa/cMmTYsVrXiYKO63XhtzmTDNxFOACsFi/5g/gSf2H2LsMoGafEAIY66n+n7PDn1Z683SMv7iV/Jjo7xjb2KSfmW4xCQMZFRalGTCisnL2kFJTv+UQIE2DicJ1L11Ykcbu5fxGYamjZdkibl81nbX+6/3B8z6FCZ4yvBDef+6f9M4UoN5GnVDjlTqg1XZntSO/X7318UxEoYcvglf4Ok/xylHmmr99Fc/Bz+rUWwljg7W2r3pIPbDh9UZ40ck9v91T4wpkYE6/9PRT9xmV7EKbbFRRpY9uDSEBvmFIXPjj0wpZ1g7qeOUVXUHxITXFVgabAyVbTCfd1BD5vS5+1Ir6zkqfdaO8pGiQ3DP/b9tQAx6so9GRS7xinAG4cU/l3asxpymDaXgcbNcNSWq7r8CuSMHj/5/3wpWfCsNuM3gZl2OesPZh6Tc+hE9jT2EmpbfwLGG/RP9q07Msd1JnaHLtUaZlkmgYF5CWaVmgowYMdTlqhyGtVVN4kTGmZrTN/w2Mh4Gpsm7VlFcELRx3ukKHwbhn0Q3TOn4AYKyxWx/mFyUHGtwkvHXSh4TV8WnhjNKMzgxL7opUSOQu/x/CFRZCyxhNlt2dXNfGkR5Z9KHo/ef0/7wf6Fnl2c9Qr/k2t8EWXSnhYji7y1NWTWORQmINbLoFg69ilbhWs/1tUal1pbXwJR/oxyAzvK6IKOILZbSdU/aOhhSIHYco8kRNI3ztcpBnG/O3KNKdVYWbECAxJjlzB3FLlwGEQGWuzOcTzHvknghYxfFXGW76djuptu7qW4f7oWEDZSVgh7CcOulzg2LkD0Pq0YfqYZchATa4C0Yb1n8fwDIlVyCVSwA8TxWL5iGVd/FXuhvsC7awxcvjTyAXtjpyKZW/UXRXozwT47eECZWfaoDXco1qgMVQkSD1gbcL3vaG7e9fNdorUQToj9HzvqtLivCtkIX/rzU02G3lwQyR+vMlJWw/JHSfFtWDEFoTZvJHE7VwtSqZNNvhwBIYxbQFm85TsNkjVV6ROhzlWaWzY3F1f4w1t8vR4YB8nUxADyWsZmc03kVaual5Yvek2R9P9+xin+/vNAACYPbsjPXkwMLGxT
Content-Type	multipart/alternative; boundary="_000_TYUPR04MB6744DEB0F2CD2E02FE6021ABCF9E9TYUPR04MB6744apcp_"
MIME-Version	1.0
X-OriginatorOrg	sct-15-20-4755-11-msonline-outlook-6ea25.templateTenant
X-MS-Exchange-CrossTenant-AuthAs	Internal
X-MS-Exchange-CrossTenant-AuthSource	TYUPR04MB6744.apcprd04.prod.outlook.com
X-MS-Exchange-	00000000-0000-0000-0000-000000000000



X-MS-Exchange-CrossTenant-AuthSource	TYUPR04MB6744.apcprd04.prod.outlook.com
X-MS-Exchange-CrossTenant-RMS-PersistedConsumerOrg	00000000-0000-0000-0000-000000000000
X-MS-Exchange-CrossTenant-Network-Message-Id	87edf93a-abf2-4221-bb12-08db3da1c822
X-MS-Exchange-CrossTenant-originalarrivaltime	15 Apr 2023 11:08:45.9622 (UTC)
X-MS-Exchange-CrossTenant-fromentityheader	Hosted
X-MS-Exchange-CrossTenant-id	84df9e7f-e9f6-40af-b435-aaaaaaaaaaaa
X-MS-Exchange-CrossTenant-rms-persistedconsumerorg	00000000-0000-0000-0000-000000000000
X-MS-Exchange-Transport-CrossTenantHeadersStamped	TY2PR04MB4078

As you can see, All the information regarding the email is shown above.