Task -2

Objective: Identify phishing characteristics in a suspicious email sample.

Sol. - To help you identify phishing characteristics in a suspicious email sample, I need you to provide me with the email sample. Please include as much detail as possible, such as:

- **Sender's email address:**
- **Subject line:**
- **Content of the email:** (text, images, links - please be careful not to click on any links)
- **Any attachments:** (if applicable, but *do not open them*)
- **Any unusual formatting or grammar errors:**
- **Suspicious Sender:** Does the sender's email address look legitimate? Is it a common domain or a misspelled one?
- **Urgent or Threatening Language:** Does the email create a sense of urgency, fear, or a demand for immediate action?
- **Generic Greetings:** Does it use a generic greeting like "Dear Customer" instead of your name?
- **Requests for Personal Information:** Does it ask for sensitive data like passwords, bank account numbers, or social security numbers?
- **Suspicious Links:** Do the links in the email point to an unexpected or illegitimate website? (Hovering over links without clicking can reveal the true URL).
- **Grammar and Spelling Errors:** Are there numerous typos or grammatical mistakes?
- **Unusual Attachments:** Are there unexpected attachments, especially executables (.exe) or zip files?
- **Inconsistencies:** Does the email's branding, logo, or tone seem inconsistent with the supposed sender?
- **Sense of Authority:** Does it impersonate a known organization (bank, government agency, tech support)?

Some samples below :

Phishing emails often try to trick you into revealing personal information or clicking on malicious links. They come in many forms, but here are some common categories and samples:

1. Impersonating a Financial Institution (Bank, PayPal, Credit Card Company)

- **Goal:** To get your login credentials or financial details.
- **Characteristics:** Urgent tone, fake security alerts, requests to "verify" your account, links to fake login pages.

Sample 1 (Fake Security Alert):

Subject: Urgent: Your Bank Account Has Been Limited!

From: service@[yourbankname].com

(but the actual email address might be support@yourbanksecurity.xyz or similar upon inspection)

Dear Customer,

We regret to inform you that we have temporarily limited your online banking access due to unusual activity detected on your account. For your protection, we recommend that you immediately verify your account details to restore full access.

Failure to complete this verification within 24 hours will result in permanent suspension of your account.

Click here to verify your account: [Malicious Link - e.g., http://yourbank.secure-login.com/verify (but the real destination is http://phishing-site.ru/banklogin)]

Thank you for your cooperation.

Sincerely, [Your Bank Name] Security Team

Sample 2 (Fake Invoice/Payment Confirmation):

Subject: PayPal: Payment Confirmation for Order #987654321

From: service@paypal.com (

but the actual email address might be noreply@paypall-support.info)

Dear Valued Customer,

Thank you for your recent purchase. Your payment of $499.99 for "Apple MacBook Pro" has been processed successfully.

If you did not authorize this transaction, please click the link below to dispute the charge:

[Malicious Link - e.g., https://www.paypal.com/dispute-transaction (but the real destination is http://fakepaypal.biz/dispute)]

This transaction will appear on your statement within 2-3 business days.

Sincerely, The PayPal Team

Some online header analyzer tools

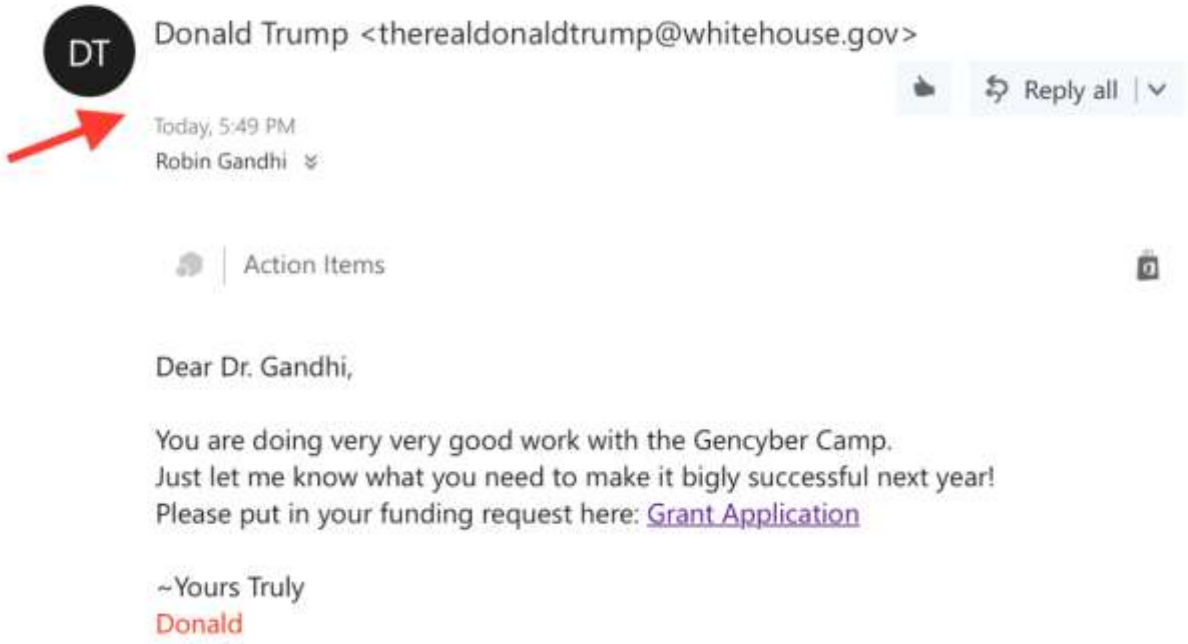
Analyzing email headers is crucial for identifying phishing attempts and understanding the true origin and path of an email. While the raw headers can look like a jumble of technical terms, online header analyzer tools make them much more readable and easier to interpret.

Here are some popular and reliable online email header analyzer tools:

1. **Google Admin Toolbox Messageheader:**
   - **Link:** https://toolbox.googleapps.com/apps/messageheader/
   - **Why it's good:** This is a very popular and straightforward tool, especially useful for Gmail users. It parses the header into an easily digestible format, highlighting key information like SPF, DKIM, and DMARC authentication results, which are vital for checking email legitimacy. It also helps identify delivery delays and the approximate source of the delay.
2. **MXToolbox Email Header Analyzer:**
   - **Link:** https://mxtoolbox.com/EmailHeaderAnalyzer.aspx
   - **Why it's good:** MXToolbox is a well-known resource for various email and domain-related diagnostics. Their header analyzer provides a clear breakdown of the header fields, including server hops, timestamps, and authentication results (SPF, DKIM, DMARC). It's generally very user-friendly.
3. **Zoho Mail Email Header Analyzer:**
   - **Link:** https://www.zoho.com/toolkit/email-header-analyzer.html
   - **Why it's good:** Zoho's tool is part of their broader toolkit. It offers a clean interface and categorizes the information into "message details," "hop

details," and "other details," making it easy to navigate and understand the email's journey and authentication status.

4. **Mailheader.org:**
   - **Link:** https://mailheader.org/
   - **Why it's good:** This tool is very simple and to the point. You paste your header, and it parses it into a readable format. It also emphasizes that it does not store or forward any information provided, which is good for privacy concerns.
5. **WhatIsMyIP.com Email Header Analyzer:**
   - **Link:** https://www.whatismyip.com/email-header-analyzer/
   - **Why it's good:** Another straightforward analyzer that helps you quickly get the originating IP address and other key details from the email header, which can be useful for tracing the source of a suspicious email.
6. **DNS Checker - Email Header Analyzer:**
   - **Link:** https://dnschecker.org/email-header-analyzer.php
   - **Why it's good:** Similar to other tools, it provides a breakdown of the email header information, focusing on details like sender's IP address, server hops, and authentication results.



Donald Trump <therealdonaldtrump@whitehouse.gov>

Today, 5:49 PM

Robin Gandhi

Action Items

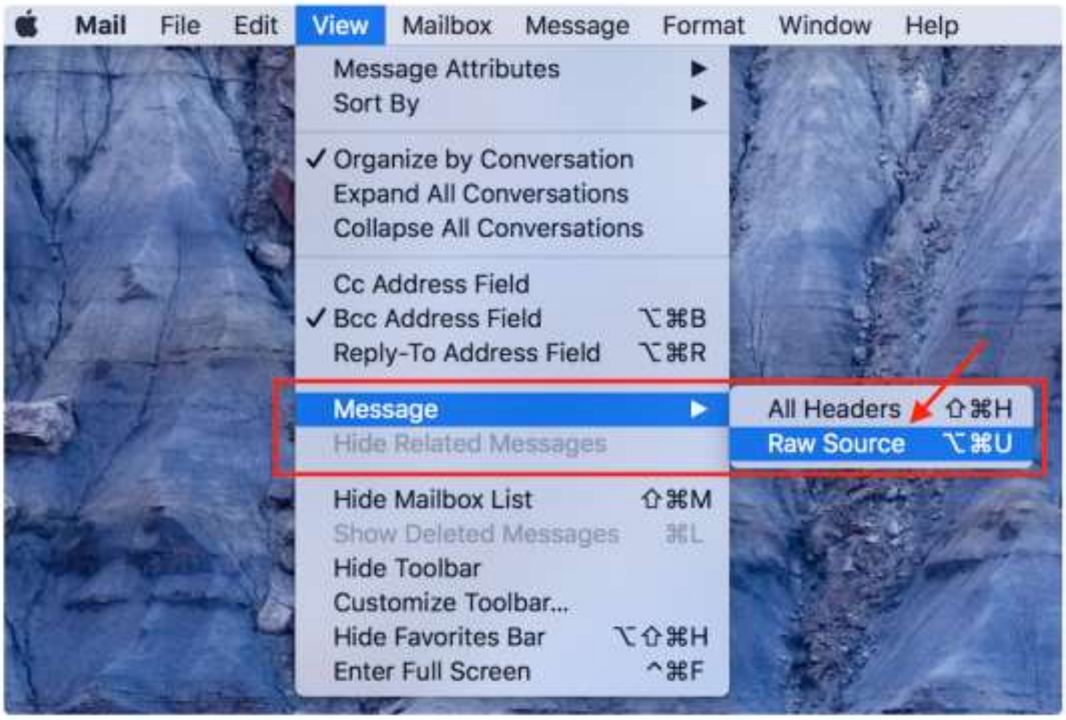
Dear Dr. Gandhi,

You are doing very very good work with the Gencyber Camp.
Just let me know what you need to make it bigly successful next year!
Please put in your funding request here: Grant Application

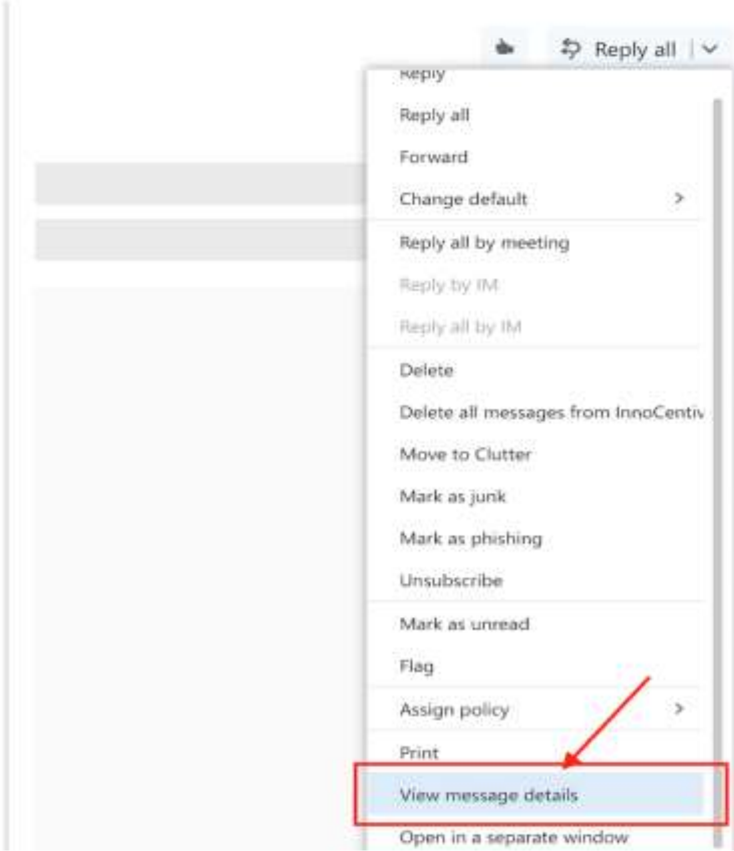
~Yours Truly
Donald

Next step :

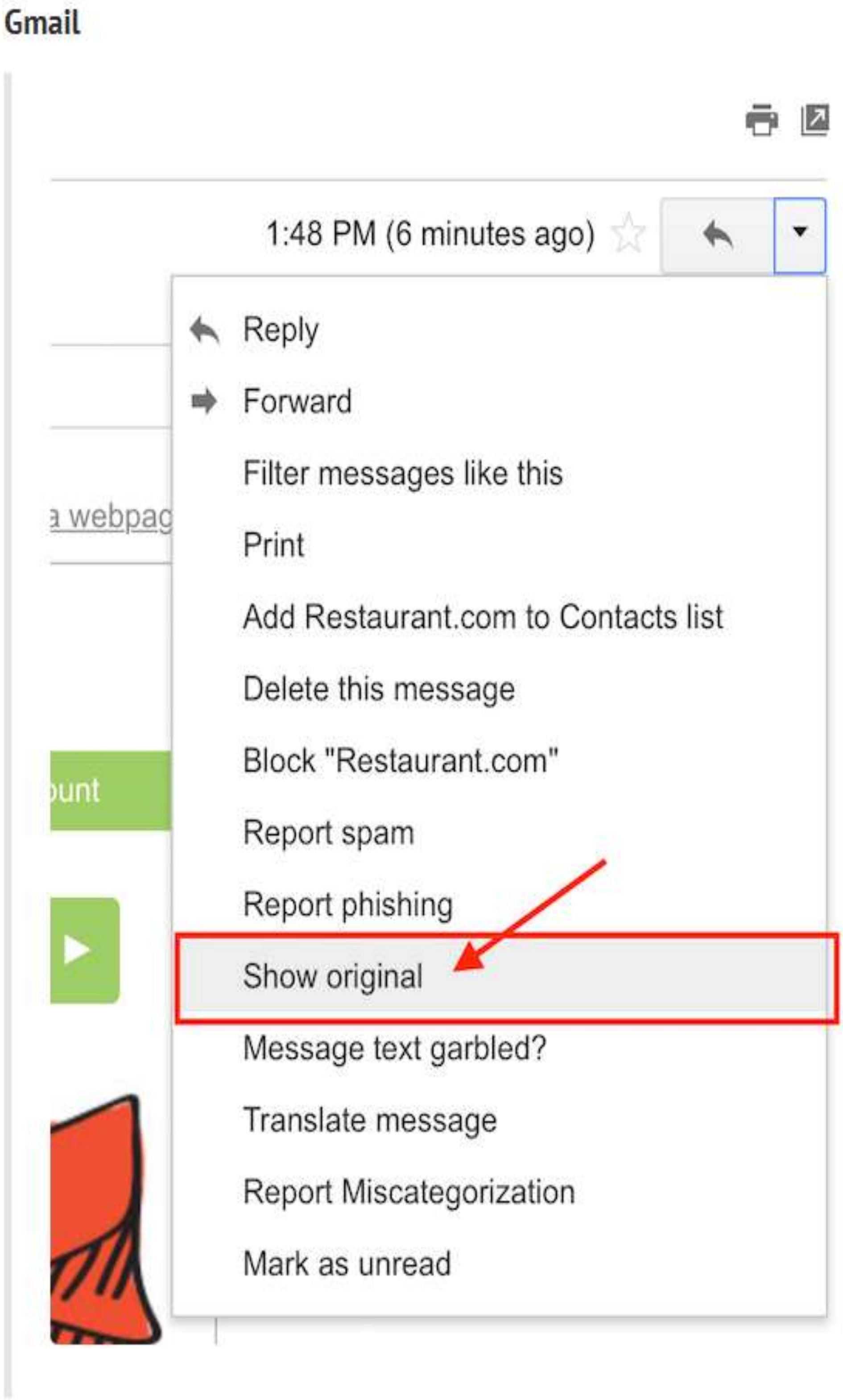
Find the view source of the email



Outlook Web Client



For Gmail need to click on show original



Below is the email header :

Email Header

```
================================================================================
=

Received: from BL2PRD0711HT001.namprd07.prod.outlook.com (10.255.104.164) by
 BY2PRD0711HT003.namprd07.prod.outlook.com (10.255.88.166) with Microsoft SMTP
 Server (TLS) id 14.16.257.4; Thu, 17 Jan 2013 23:35:35 +0000
Received: from BL2PRD0711HT002.namprd07.prod.outlook.com (10.255.104.165) by
 BL2PRD0711HT001.namprd07.prod.outlook.com (10.255.104.164) with Microsoft
 SMTP Server (TLS) id 14.16.257.4; Thu, 17 Jan 2013 23:35:34 +0000
Received: from mail240-tx2-R.bigfish.com (65.55.88.116) by
 BL2PRD0711HT002.namprd07.prod.outlook.com (10.255.104.165) with Microsoft
 SMTP Server (TLS) id 14.16.257.4; Thu, 17 Jan 2013 23:35:34 +0000
Received: from mail240-tx2 (localhost [127.0.0.1]) by mail240-tx2-R.bigfish.com (Postfix)
with ESMTP id A05C032025F for <jerryp@mail.unomaha.edu>; Thu, 17 Jan 2013 23:35:33
+0000 (UTC)
X-Forefront-Antispam-Report:
CIP:59.125.100.113;KIP:(null);UIP:(null);IPV:NLI;H:bf.shako.com.tw;RD:59-125-100-
113.HINET-IP.hinet.net;EFVD:NLI
X-BigFish:
ps73(zz7f52hd926hzz1ee6h1de0h1ce5h1202h1e76h1d1ah1d2ahz58hz8275bhz2ei2a8h668h
839h940h10d2h1177h1288h12a5h12a9h12bdh137ah139eh13b6h13eah1441h1537h162dh
1631h1758h17f1h184fh1898h300k503k953iwa7jk)
X-FOSE-spam: This message appears to be spam.
X-SpamScore: 73
Received-SPF: neutral (mail240-tx2: 59.125.100.113 is neither permitted nor denied by
domain of aol.com) client-ip=59.125.100.113; envelope-from=vieria@aol.com;
helo=bf.shako.com.tw ;shako.com.tw ;
Received: from mail240-tx2 (localhost.localdomain [127.0.0.1]) by mail240-tx2
```

```
 (MessageSwitch) id 1358465731454940_30539; Thu, 17 Jan 2013 23:35:31 +0000

 (UTC)

Received: from TX2EHSMHS007.bigfish.com (unknown [10.9.14.242]) by mail240-
tx2.bigfish.com (Postfix) with ESMTP id 675424200E7 for <jerryp@mail.unomaha.edu>; Thu,
17 Jan 2013 23:35:31 +0000 (UTC)

Received: from bf.shako.com.tw (59.125.100.113) by TX2EHSMHS007.bigfish.com

 (10.9.99.107) with Microsoft SMTP Server (TLS) id 14.1.225.23; Thu, 17 Jan

 2013 23:35:28 +0000

Received: from mail.shako.com.tw (59-125-100-112.HINET-IP.hinet.net

 [59.125.100.112]) by bf.shako.com.tw (8.14.3/8.14.3) with ESMTP id

 r0HNYCgA013928; Fri, 18 Jan 2013 07:34:12 +0800

X-Authentication-Warning: bf.shako.com.tw: Host 59-125-100-112.HINET-IP.hinet.net
[59.125.100.112] claimed to be mail.shako.com.tw

Authenticated-By: nobody

X-SpamFilter-By: BOX Solutions SpamTrap 3.5 with qID r0HNXZSI028539, This message is
passed by code: ctdos35128

Received: from User (85-250-54-29.bb.netvision.net.il[85.250.54.29])

(authenticated bits=0)

by mail.shako.com.tw (8.14.3/8.14.3/4.90) with ESMTP

 id r0HNXZSI028539; Fri, 18 Jan 2013 07:33:38 +0800

X-BOX-Message-Id: r0HNXZSI028539

Message-ID: <201301172333.r0HNXZSI028539@mail.shako.com.tw>

X-Authentication-Warning: mail.shako.com.tw: Host 85-250-54-
29.bb.netvision.net.il[85.250.54.29] claimed to be User

Reply-To: <carrr444@yahoo.com>

From: JOSEPH CAMARAH VIEIRA <vieria@aol.com>

Subject: [Spam-Mail] Dear Sir/Madam. (This message should be blocked: ctdos35128)

Date: Fri, 18 Jan 2013 01:46:07 +0200

Content-Type: text/plain; charset="Windows-1251"
```

Content-Transfer-Encoding: 7bit

X-Mailer: Microsoft Outlook Express 6.00.2600.0000

X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2600.0000

To: Undisclosed recipients:;

Return-Path: vieria@aol.com

X-MS-Exchange-Organization-SCL: 7

X-MS-Exchange-Organization-AVStamp-Mailbox: MSFTFF;1;0;0 0 0

X-MS-Exchange-Organization-AuthSource: BL2PRD0711HT002.namprd07.prod.outlook.com

X-MS-Exchange-Organization-AuthAs: Anonymous

MIME-Version: 1.0

Dear Sir/Madam,

my name is Joseph Camarah Vieira, i am from Guinea Bissau, my late father was the former minister of mines in my country Guinea Bissau, he was short dead by the rebels in my country, before his death he deposited $60 million Dollars with Global Trust Security Company Accra Ghana, i want you to help me receive this money in your country for investment in your country i will give you 30% of the total sum when the funds arrive your country.

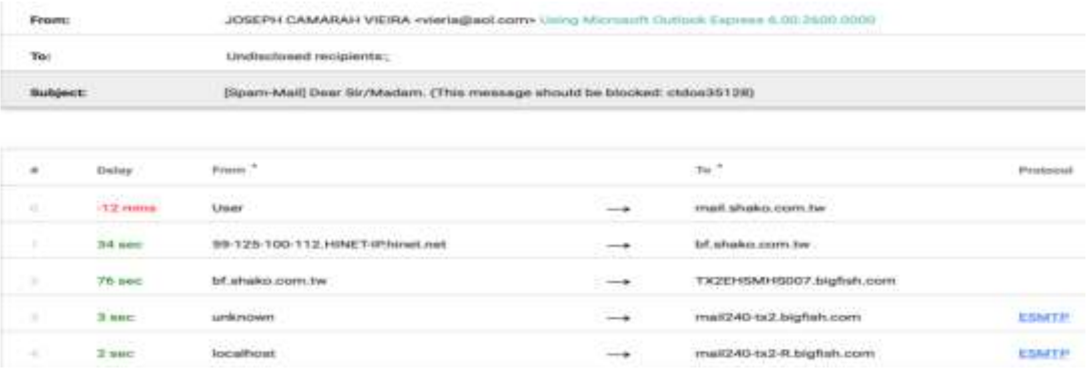
Regards.

Mr Joseph Camarah Vieira

00233 244 617 863

my email:carrr444@yahoo.com

Here above we can find the email fake links and also send ip address further investigate.



From:	JOSEPH CAMARAH VIEIRA <vieria@aol.com> Using Microsoft Outlook Express 6.00.2600.0000
To:	Undisclosed recipients:;
Subject:	[Spam-Mail] Dear Sir/Madam. (This message should be blocked: ctdos35138)

#	Delay	From *		To *	Protocol
0	-12 mins	User	→	mail.shako.com.tw	
1	34 sec	59-125-100-112.HINET-IP.hinet.net	→	bf.shako.com.tw	
2	76 sec	bf.shako.com.tw	→	TX2EHSMHS007.bigfish.com	
3	3 sec	unknown	→	mail240-tx2.bigfish.com	ESMTP
4	2 sec	localhost	→	mail240-tx2-R.bigfish.com	ESMTP