

Term Project:

Paper Review

Kush Patel and Nick Austin

11/20/2022

Computer & Network Forensics

Professor Fu

Paper Review

QUESTIONS

1. Review state-of-the-art email tracking techniques. Students may Google for related papers. Here is a list of academic and industry conferences. At least 4 academic papers by academic researchers (not articles at websites) shall be reviewed. The paper can use either IEEE or ACM format as shown below. Either Word or Latex can be used to edit your paper/report. (8 points)
 - a. IEEE Manuscript Templates for Conference Proceedings.
<https://www.ieee.org/conferences/publishing/templates.html>
 - b. ACM Primary Article Template: <https://www.acm.org/publications/proceedings-template>
 - c. Review of each of the first four papers shall be put into your report/paper and each review is worth 2 points. Each paper review shall have at least 5 sentences and summarizes what the paper talks about in your own language.

Identification of Spam Email Based on Information from Email Header

This paper talks about several features contained in the email header that can be used to identify and classify spam messages efficiently. Email communication brings attention of attackers especially spam. Spam can cause network traffic problems and economic loss.

According to the paper, spammers have been using many email header features to evade existing mail filtering techniques. The contents in the body of the email can be used to detect spam. The author talks about how a header-message-based spam detector has a high accuracy in detecting

spam. The paper then talks about the common features in email headers of three big email providers: Hotmail, Yahoo, and Gmail. Features like Message-ID, Received, DKIM-Sig, and many more. The paper also talks about work done by other authors about how these features can be used to detect spam email. The received field involves transporting the email message. Spam has small number of hops, spam have non-existent domain address, and more things are explained. The authors then go on to talk about features that can be used in a system. Received field records all email messages from one SMTP server to another and could eliminate 25% of spam. From field could be used as well because the domain in From should match the domain in Hello command, otherwise there is a good chance it's spam. This paper talks about other features as well to help detect and trace back on spam email.

Analysis of Email Header for Forensics Purpose

This paper discusses the use of email headers in forensic analysis. The paper starts off with pros and cons about emails. Emails are a carrier of criminal evidence. Email headers provide detailed technical information about the sender, software used to compose email, and the email server through recipient to the arrival. Then the authors talk about some general information about email like the structure of them and how they work. Then the paper goes on to talk about the email headers. Explains how the Received field is best read bottom to top. First received is your mail server and the last one is where the email was sent from. The authors do say that the email could be tampered during the delivery process. Each email has its own unique Message-ID. The paper then gives an example of how forensics could be used. Three conditions if an email could be used as evidence or not: Sender/receiver do not admit to sending/receiving the email, both parties have a disagreement on the time of sending and receiving the email, both parties have a disagreement on the contents of the email. The authors

talks about how using POP3, IMAP, and HTTP can identify the authenticity and integrity of the email. This helps identify forged content and rule out false information. The paper then gives an example situation of the defendant saying the mail received by the plaintiff was forged. One thing they touch on is if you assume the email is not forged then you analyze the time and time zone of the email. They compared the time zone from the start to the end and found a time dislocation. Meaning the timing of sending the receiving didn't add up to where the email was delivered. This means either there is a server error or the email header was forged. Can double check this by converting the Message-ID to find the times and if it is similar then either the Message-ID or header is forged. Overall, the paper is about the usage of email header can ensure evidence and provide clues for cases.

Detection of Spoofed Mails

This paper discusses methods to detect spoofing by looking at the email header. The paper starts off by giving an introduction about cyber forensics and email. Says the main purpose of cyber forensics is to perform an investigation by recreating the event. Authors talk about other forensics as well. Gives examples of attacks that emails are vulnerable to such as spoofing, DOS, Replay and more. Spoofing is the sending of email messages with forged senders address. The paper talks about different crimes done on email such as cyber bullying, phishing, sending viruses and more. Authors then explain how to analyze an email header. The Received and Message-ID field are the most important for integrity and authenticity. In the Message-ID, left of the @ is the date and time, right of the @ is the domain name of the local host. Paper then explains how to detect spoofed email. Can be analyzed multiple ways. One way is analyzing date and time. Some way that shows the email could be spoofed is that there is junk information in the Received field or any other field or if the email takes longer to be received. More specifically,

convert the time in the header to UTC. The difference between senders time and intermediate servers and time between senders time and receivers time is calculated. This helps know the know the actual time mail was sent, if they are not in range, the email could be spoofed. You could also do a DNS lookup where if the domain in Message-ID is different from the Received field, than email could be spoofed. These tactics are helpful if the email header is available and a good solution if spoofing is suspected.

Email forensic tools: A roadmap to email header analysis through a cybercrime use case

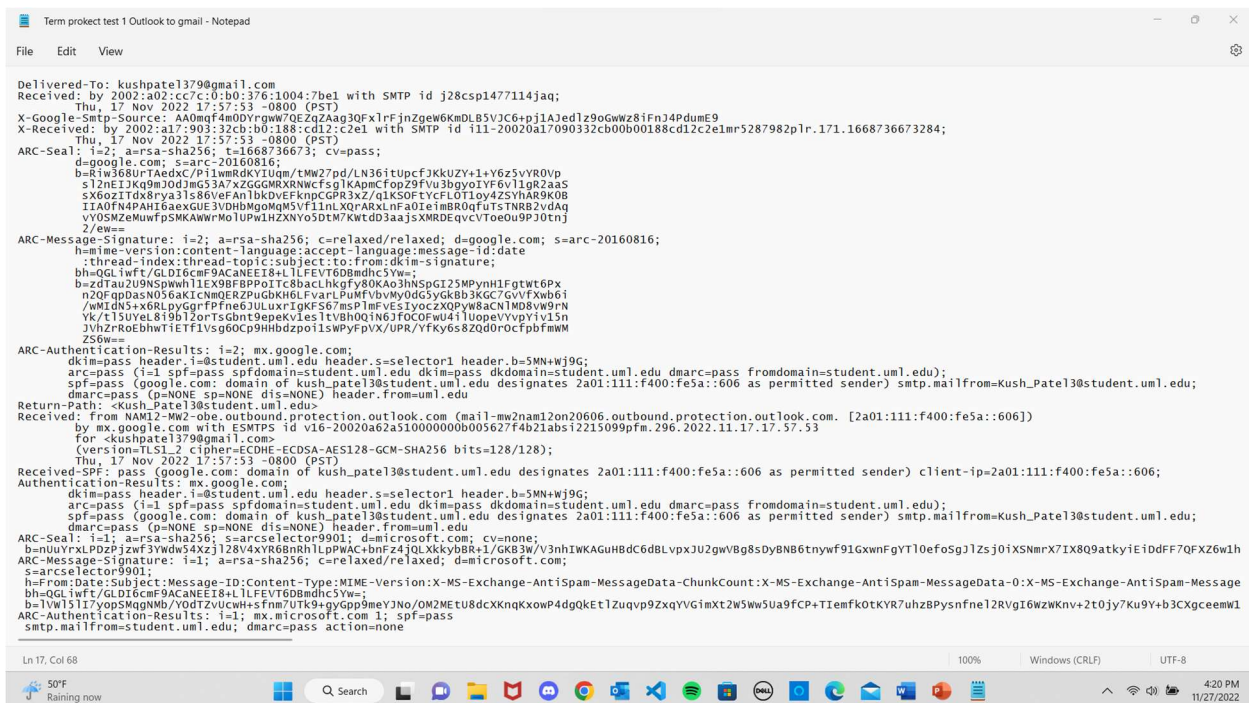
This paper reviews existing forensics tools for email header analysis, as part of their investigation. The papers start off with a basic talk about emails like how the number of crimes have increased over emails. This is because rarely any encryption at the sender's end and no integrity checks at the recipient's end. SMTP doesn't have a source authentication mechanism. Talks about uses of spam, phishing, and more like in previous papers. Authors than talk about email forensics. It is the analysis of the source and content of email message as evidence. It than explains about investigation techniques like metadata, keyword searching, and more. You can also analyze SMTP server for logs and email copies but this is time consuming and these are also only maintained limited period of time. You can also analyze software embedded identities by looking for information related to the sender of the email. It is time consuming but can reveal Windows username and MAC address. After than the paper talks about email structure and email header tracing similar to the previous papers. Than examples of forensic tools are given. One tool is EmailTracer, which traces the originating IP address and other header details and than creates a report of the sender, the path the email took, and the geographic location of the email. Email header analysis can help investigators find links and start a criminal investigation.

2. Pick up 4 email services such as Gmail, Yahoo email, Outlook and our cs.uml.edu email, and show how to track emails sent from those services. (8 points)
- If an email can be tracked, show how.
 - If an email cannot be tracked, discuss why.
 - Document the findings in your paper/report.
- Investigation of each email service is worth 2 points.

Email Tracking Services

Email sent from Outlook to Gmail and Yahoo:

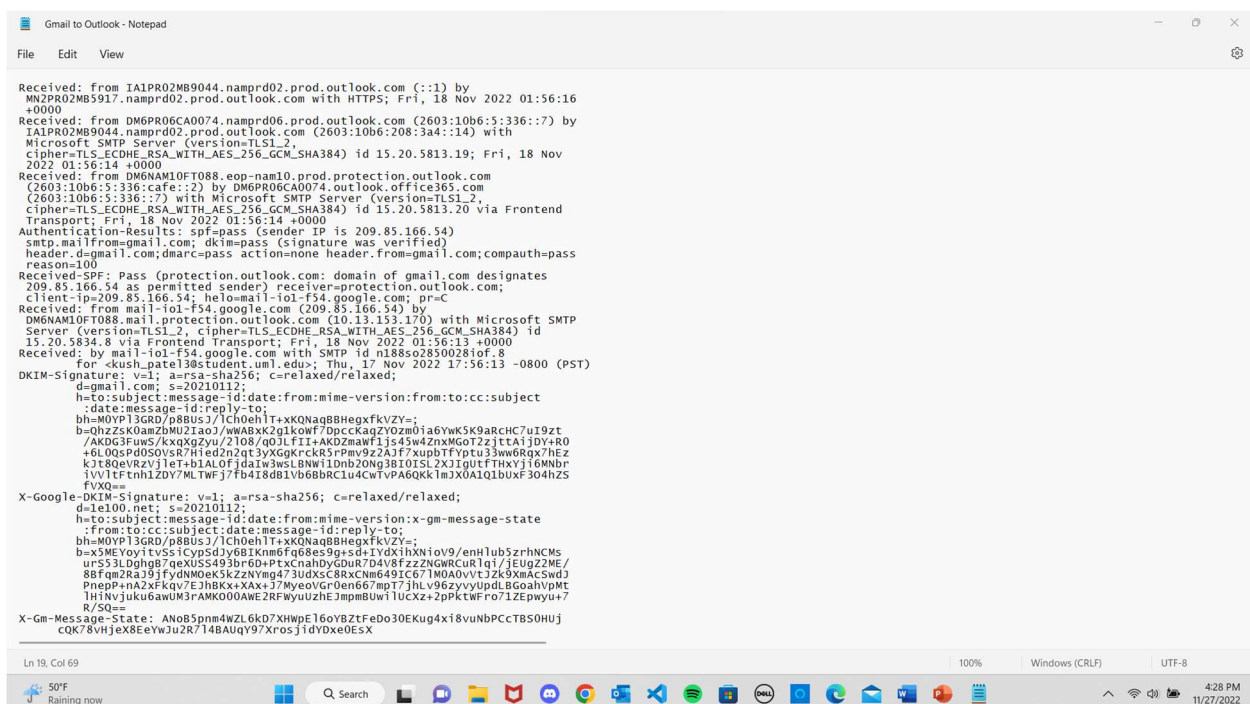
The email can be tracked when sent from Outlook. I sent an email from Outlook to Gmail and then tracked that email on Gmail. Click on the email then click the three dots on the right side and then click “show original”. It shows you the message ID and date/time it was received. Also gives you the SPF, DKIM, DMARC, this information tells you that its authenticated. Unlike Outlook, Gmail headers also shows HTML/CSS content.



I also sent an email from Outlook to Yahoo to check if the email can be track by Yahoo. It can be tracked by click on the email then the three dots at the bottom, and then clicking “View Raw Message”. This will show all the information similar to headers in Outlook and Gmail. Similar to the Outlook and Gmail headers, it shows you servers it went through, date/time, authentication, and more. Unlike Outlook, Yahoo headers also shows HTML/CSS content and is the same as Gmail headers. The screenshot for the Yahoo header is the same as the Gmail screenshot

Email sent from Gmail to Outlook:

The email can be tracked when sent from Gmail. I sent an email from Gmail to Outlook and then track that email on Outlook. Double click the email and then click properties. This will show you the internet headers information. It consists of all the servers the email went through, the time the email was sent and received, DKIM signature, and much more. Very similar to the Gmail header email.



```
Received: from IAPR02MB9044.namprd02.prod.outlook.com (::1) by
MN2PR02MB5917.namprd02.prod.outlook.com with HTTPS; Fri, 18 Nov 2022 01:56:16
+0000
Received: from DM6PR06CA0074.namprd06.prod.outlook.com (2603:10b6:5:336::7) by
IAPR02MB9044.namprd02.prod.outlook.com (2603:10b6:208:3a4::14) with
Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.5813.19; Fri, 18 Nov
2022 01:56:14 +0000
Received: from DM6NAM10FT088.eop-nam10.prod.protection.outlook.com
(2603:10b6:5:336:cafe::2) by DM6PR06CA0074.outlook.office365.com
(2603:10b6:5:336::7) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.5813.20 via Frontend
Transport; Fri, 18 Nov 2022 01:56:14 +0000
Authentication-Results: spf=pass (sender IP is 209.85.166.54)
smtp.mailfrom=gmail.com; dkim=pass (signature was verified)
header.d=gmail.com; dmarc=pass action=none header.from=gmail.com; compauth=pass
reason=100
Received-SPF: Pass (protection.outlook.com: domain of gmail.com designates
209.85.166.54 as permitted sender) receiver=protection.outlook.com;
Client-ip=209.85.166.54; helo=mail-lol-f54.google.com; pr=C
Received: from mail-lol-f54.google.com (209.85.166.54) by
DM6NAM10FT088.mail.protection.outlook.com (10.13.153.170) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
15.20.5834.8 via Frontend Transport; Fri, 18 Nov 2022 01:56:13 +0000
Received: by mail-lol-f54.google.com with SMTP id n188so2850028iof.8
for <kush_pate13@student.uml.edu>; Thu, 17 Nov 2022 17:56:13 -0800 (PST)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=gmail.com; s=20210112;
h=to:subject:message-id:date:from:mime-version:from:to:cc:subject
:date:message-id:reply-to;
bh=M0YP13GRD/p8BUSj/1Ch0eh1t+xxQNaqBBHegxfkVZY=;
b=QhZzK0amZbmU2IaoJ/wwABxK2g1kwf7DpccKagZY0zm0ia6yWk5K9aRCHC7uI9zt
/AKD3Fuws/kxXg2yu/2108/q0Jf1I+AKDZmawf1js45w4znxMGoT2zj1tAIjDy+R0
+6L0osP0DS0vsR7Hied2nzt3yXopckrcK8rPmv9z2AJf7xubtF7vptu33w6Rq7heZ
k3T8qeVRzvj1et+b1ALOfjdaIw3wslBNW1Dnb20ng3BIOISL2XJ1qutFTHxyji6MnBr
jV1tFtnh1ZDY7MLTWFj7fb4I8db1Vb6bRCLu4CwtvPA6QK1mJX0A1Q1bUxf304hZS
FVWQ=
X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=le100.net; s=20210112;
h=to:subject:message-id:date:from:mime-version:x-gm-message-state
:from:to:cc:subject:date:message-id:reply-to;
bh=M0YP13GRD/p8BUSj/1Ch0eh1t+xxQNaqBBHegxfkVZY=;
b=x5MEYoyitvS5IcypSdJy6bEKnmf6q8es9g5d+1YdixhNwioV9/enH1ub5zrhNCMs
urS53LDghgB7qexU55493br6D+PtxCnahDyGduR704v8fzzzNGWRcuR1qi/1EugZ2ME/
88fqm2Ra3jfyfndM0ek5kZzNymg473udxsC8RxCNm649IC671M0A0vvtJ2K9xmAcSwdJ
PnepP+nA2cFkqv7EJh8KsXAXsJ7myeoVGr0en667mp17JhLv96zyvUpdLBGoahVpMt
1HivJukuGawU3rAMQ00AME2R7WyuuzhEJm0Buwi1ucXz+2pPktwFro7JZepmy+/
R/SQ=
X-Gm-Message-State: ANoB5pnm4WZL6kD7XHWpE16oY8ZTFeDo30EKug4x18vuNBpCctB50Huj
CQK78vHj8EeYw2uZR/14BAuqY9/XrosjiDYDxeUeSX
```

I also sent an email from Gmail to AOL. The email can tracked, click on the three dots than “View Raw Message”. The header information is the same as if you were tracking on Yahoo and Gmail.

Email sent from Yahoo to Outlook:

The email can be tracked when sent from Yahoo. Just like viewing the internet header when sent from Gmail to Outlook. All the same information is given in the header. Something different is that “yahoo.com” is mentioned in the header for Outlook, but not in the Gmail header when from Yahoo.

```
Outlook to Yahoo - Notepad
File Edit View

Received: from PH0PR02MB7429.namprd02.prod.outlook.com (2603:10b6:510:9::21)
by MN2PR02MB5917.namprd02.prod.outlook.com with HTTPS; Sat, 19 Nov 2022
18:06:28 +0000
Received: from MW4PR04CA0387.namprd04.prod.outlook.com (2603:10b6:303:81::32)
by PH0PR02MB7429.namprd02.prod.outlook.com (2603:10b6:510:9::21) with
Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.5834.9; Sat, 19 Nov
2022 18:06:25 +0000
Received: from MW2NAM10FT086.eop-nam10.prod.protection.outlook.com
(2603:10b6:303:81:cafe::ee) by MW4PR04CA0387.outlook.office365.com
(2603:10b6:303:81::32) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.5834.9 via Frontend
Transport; Sat, 19 Nov 2022 18:06:25 +0000
Authentication-Results: spf=pass (sender IP is 209.85.219.46)
smtp.mailfrom=gmail.com; dkim=pass (signature was verified)
header.d=gmail.com; dmarc=pass action=none header.from=gmail.com; compauth=pass
reasons=100
Received-SPF: Pass (protection.outlook.com: domain of gmail.com designates
209.85.219.46 as permitted sender) receiver=protection.outlook.com;
Client-ip=209.85.219.46; helo=mail-qv1-f46.google.com; pr=C
Received: from mail-qv1-f46.google.com (209.85.219.46) by
MW2NAM10FT086.mail.protection.outlook.com (10.13.154.113) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
15.20.5834.8 via Frontend Transport; Sat, 19 Nov 2022 18:06:25 +0000
Received: by mail-qv1-f46.google.com with SMTP id h7so4892514qvs.3
for <kush_pate130@student.uml.edu>; Sat, 19 Nov 2022 10:06:25 -0800 (PST)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=gmail.com; s=20210112;
h=references:mime-version:subject:message-id:to:reply-to:from:date
:from:to:cc:subject:date:message-id:reply-to;
bh=GIB7wu3nkb0pXxwJCC9e5Td5kuJdGobupNgl8VC5To=;
b=D2emgoi5Ulgys9mL+p4c50dgg66f1YvGnlX006r-dcw4M5/r0XcH8YjgAz1JaT0/
+T69uSR8yc5mh0x1LILMBUSi101jvuEcanSJe1GwPRF4TS9DeTY+w9+Xg45IoDrgzIPJ
kMugIX7MQR5ecnpYqd6yFzYLiwuF1xaeWAuNBt7+df5xOQhupfngz7xwMt8gl3ncJRFw
s7M6lyhAFCDP1CWAE8HjgLI1h+uks90dG5Wpklwu0XWQmK+zzREbyGYgtorMEZGn9x/
8EqxtAW0Zb8S3q8tEjnyUC2lh4YzP6cpwuv1UeRVBqlnwFg8/g+R4yCqqdPzhZJF8a
BwRQ==
X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=1e100.net; s=20210112;
h=references:mime-version:subject:message-id:to:reply-to:from:date
:x-gm-message-state:from:to:cc:subject:date:message-id:reply-to;
bh=GIB7wu3nkb0pXxwJCC9e5Td5kuJdGobupNgl8VC5To=;
b=YF430bBZECkzUF7MDa9885ITU9qf5sHrvDyqsHQcW4K5Lts0SVIwzh14FgLU
P31hgpOKPC3Ca09f9yc+R3CeNigqfG0HFc1s1ev1IqW993h9oduy+ZRVybdYtpzQw6m0
4XZKvYwAotopJkmp/ShohJW75ukz5sau9zagiP0j1lmm10tqhlMRhd74tQBkFY
FohyxK0aF3UG55yQrZiWb6gxcdVTz2ZN03240dfdxNdzqyZyQcdzRHCKXgYodh8q12s
1Ih+EKsb3aYf1IEFQkqNaR0lkvF1XLDk1a6rJFY05eh3gnTAACXhrAC3AaSMXIXhwZY
hs1A=
X-Gm-Message-State: ANoB5pnamHUjnpHKEYogZmpZUwa+RCRRSNFDPWff7WGF81/yPYFC7Q0e
96NAaVZRYKZzxWP8xdzqAD8TTU/77XE=

Ln 21, Col 58
100% Windows (CRLF) UTF-8
50°F Raining now 4:31 PM 11/27/2022
```

Email sent from AOL to Gmail:

The email can be tracked from AOL. The header information is the same as with tracking other email providers to Gmail.

Other ways to track Email:

There are other ways to find information about a sender using their email address. You can use paid websites such as [spokeo.com](https://www.spokeo.com) that will find and search for social media and other accounts that are associated with the same email address. Things such as their current and past addresses, family members names and contact information, their cell phone numbers, and much more can be found using such software. This, however, doesn't always yield results. Sometimes searches of emails don't provide any results. This means that someone using an email account specifically for sending spam and nothing else will easily be able to avoid detection from someone using methods such as this.

Links to the papers:

- <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6920762&tag=1>
- <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6524415&tag=1>
- <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7435764>
- <https://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-bc8cc4d5-03c2-4ba8-b73d-c3809c54458a>