

LAB MANUAL

MODERN EDUCATION SOCIETY'S WADIA COLLEGE OF ENGINEERING, PUNE

Fourth Year of Computer Engineering (2019 Course)

410247: Laboratory Practice IV

410244(C): Cyber Security and Digital Forensics

NAME OF STUDENT:	CLASS: BE
SEMESTER/YEAR: VII	ROLL NO:
DATE OF PERFORMANCE:	DATE OF SUBMISSION:
EXAMINED BY:	EXPERIMENT NO:

TITLE: Email Header Analyzer

AIM/PROBLEM STATEMENT: Write a program for Tracking Emails and Investigating Email Crimes. i.e. Write a program to analyze e-mail header

OBJECTIVES:

- To understand various vulnerabilities and use of various tools for assessment of vulnerabilities

OUTCOMES:

- Identify various vulnerabilities and demonstrate using various tools.

PRE-REQUISITES:

1. Knowledge of C, C++, python programming
2. Basic knowledge of computer, network and security information

THEORY:

The email header is a code snippet in an HTML email, that contains information about the sender, recipient, email's route to get to the inbox and various authentication details. The email header always precedes the email body.

What purpose do email headers serve

Providing information about the sender and recipient :

An email header tells who sent the email and where it arrived. Some markers indicate this information, like "From:" — sender's name and email address, "To:" — the recipient's name and email address, and "Date:" — the time and date of when the email was sent. All of these are mandatory indicators. Other parts of the email header are optional and differ among email service providers.

Preventing spam:

The information displayed in the email header helps email service providers troubleshoot potential spam issues. Encapsulating Security Payload (ESPs) analyzes the email header, the "Received:" tag, in particular, to decide whether to deliver an email or not.

Identifying the email route:

Identifying the email route. When an email is sent from one computer to another, it transfers through the Mail Transfer Agent which automatically “stamps” the email with information about the recipient, time and date in the email header.

How to Find an Email Header

Viewing an email header in Gmail:

Open an email. Find “More” (three vertical dots), choose “Show original.”

Viewing an email header in Outlook:

Open an email. Find “More actions” (three horizontal dots), choose “View message source.”

Viewing an email header in Yahoo:

Open an email. Find “More actions” (three horizontal dots), choose “View raw message.”

All ESPs allow curious users to see how the email looks from the inside, in HTML code. This function looks and works the same way with every ESP. Let’s take a closer look at it.

Analyzing an Email Header

The appearance of the email header differs between ESPs. To analyze it, you need to find the email header and examine the lines of interest to you. All the code from the beginning, until the <body> tag, represents the header. Here is the list of what you can find in the email header:

“Received:” lines. They show the address of the computer that received the email, as well as other computers’ addresses that an email may have been transferred through. Unlike other email header elements, “Received:” lines can’t be forged.

```
Received: from mxfront60.mail.yandex.net ([127.0.0.1])
  by mxfront60.mail.yandex.net with SMTP id 461ygpzt
  for <rtkachev@sendpulse.com>; Thu, 18 Apr 2019 01:11:51 +0300
Received: from mail5694.archdigest.mkt6293.com (mail5694.archdigest.mkt6293.com [74.112.65.117])
  by mxfront60.mail.yandex.net (nsmtp/Yandex) with ESMTPS id 9Qh05rPcph-81ZqvW9e;
  Thu, 18 Apr 2019 01:11:48 +0300
  (using TLSv1.2 with cipher ECDHE-RSA-AES128-GCM-SHA256 (128/128 bits))
  (Client certificate not present)
Return-Path: v-omega_fchliniafm_gakaioci_gakaioci_a@bounce.newsletters.archdigest.com
X-Yandex-Front: mxfront60.mail.yandex.net
X-Yandex-TimeMark: 1555539108.502
Authentication-Results: mxfront60.mail.yandex.net; spf=pass (mxfront60.mail.yandex.net: domain of bounce.newsletters.archdigest.com designates 74.112.65.117 a
smtp.mail=v-omega_fchliniafm_gakaioci_gakaioci_a@bounce.newsletters.archdigest.com; dkim=pass header.i=email@archdigest.messages2.com
X-Yandex-Spam: 2
X-Yandex-Fwd: NTK3NDMx0Nz4NzQx0Jjc4NzKzYw2HjMSNDY4NTIzNzK4NzI4NTQ3
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; s=spop1024; d=archdigest.messages2.com;
h=Date:From:Reply-To:To:Message-ID:Subject:MIME-Version:Content-Type:List-Unsubscribe; i=email@archdigest.messages2.com;
bh=NVISouVy5DXhQCaTLKXeUx9mGas=;
b=aXLbd2hyUN94z8LAHirD6wAa71P357e5FsJ1Ajrw/gkZMpxfwF7vuJCPB1oLaXQeZ8CR2D4k85YB
```

MIME-version. Multipurpose Internet Mail Extensions are an Internet standard that extends the format of email by supporting text and non-text attachments like audio, video, images, message bodies with multiple parts, etc.

```

Date: Wed, 17 Apr 2019 22:11:41 +0000 (GMT)
From: Architectural Digest <email@archdigest.messages2.com>
Reply-To: email@archdigest.messages2.com
To: rtkachev@sendpulse.com
Message-ID: <763600385.13061421155539101049.JavaMail.app@rbg23.atlisl>
Subject: Debate Over How Notre-Dame Will Be Rebuilt
MIME-Version: 1.0
Content-Type: multipart/alternative;
    boundary="-----_Part_35741_1805585129.155539069133"
x-mid: 15488096
X-CSA-Complaints: whitelist-complaints@eco.de
x-rpcampaign: sp15488096
Feedback-ID: pod2_21948_15488096_1621134888:pod2_21948:ibmsilverpop
x-job: 15488096
x-orgId: 21948
List-Unsubscribe: <mailto:v-omega_fchliniafm_gakaioci_gakaioci_a@bounce.newsletters.archdigest.com?subject=Unsubscribe>
X-Yandex-Forward: b01a1c6487a67e98038c94dfff0bc5e09

```

Message-ID. The message-ID is a globally unique identifier used in email. Message-IDs have a specific format that is generated for a specific email address and message, thus, no two messages have the same Message-ID.

```

Received: by mail15694.archdigest.mkt6293.com id hmuia819if4o for <rtkachev@sendpulse.com>; Wed, 17 Apr 2019 22:11:41 +0000 (envelope-from <v-omega_fchliniafm_gakaioci_gakaioci_a@bounce.newsletters.archdigest.com>)
Date: Wed, 17 Apr 2019 22:11:41 +0000 (GMT)
From: Architectural Digest <email@archdigest.messages2.com>
Reply-To: email@archdigest.messages2.com
To: rtkachev@sendpulse.com
Message-ID: <763600385.13061421155539101049.JavaMail.app@rbg23.atlisl>
Subject: Debate Over How Notre-Dame Will Be Rebuilt
MIME-Version: 1.0
Content-Type: multipart/alternative;
    boundary="-----_Part_35741_1805585129.155539069133"
x-mid: 15488096
X-CSA-Complaints: whitelist-complaints@eco.de
x-rpcampaign: sp15488096
Feedback-ID: pod2_21948_15488096_1621134888:pod2_21948:ibmsilverpop
x-job: 15488096
x-orgId: 21948
List-Unsubscribe: <mailto:v-omega_fchliniafm_gakaioci_gakaioci_a@bounce.newsletters.archdigest.com?subject=Unsubscribe>
X-Yandex-Forward: b01a1c6487a67e98038c94dfff0bc5e09

-----_Part_35741_1805585129.155539069133
Content-Type: text/plain; charset="utf-8"

```

DKIM Signatures. DomainKeys Identified Mail confirms the sender's authenticity by connecting the domain name with the email. DKIM is the technology that helps to reduce spam and phishing and allows companies to guarantee for their email messages.

```

Authentication-Results: mxtr@n00.mail.yandex.net; spf=pass (mxtr@n00.mail.yandex.net: domain of bounce.newsletters.archdigest.com designates 74.112.65.117
smtp.mail=v-omfega_fchliniafm_gakaioci_gakaioci_a@bounce.newsletters.archdigest.com; dkim=pass header.i=email@archdigest.messages2.com
X-Yandex-Spam: 2
X-Yandex-Fwd: NTK3NDMxNzMNzQxNjc4NzgzMjYwZmYjM5NDY4NTIzNzk4NzI4NTQ3
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; s=spop1024; d=archdigest.messages2.com;
h=Date:From:Reply-To:To:Message-ID:Subject:MIME-Version:Content-Type:List-Unsubscribe; i=email@archdigest.messages2.com;
bh=WiSouVy5DXhQCaTLkXeUx9mGas=;
b=aXLbd2hyUN94z8LAHirDGwAa7iP357e5FsJ1AjrW/gkZMpxfiw7vuJCPB1oLaXQeZ8CR2D4k8SYB
s5RKD8vh4W8YGoEaia/iwLZtZl7VsKvnuSebpHllyZnziY8PL/h77mmBofJFhtXg5FgaqptjN/k4
Xa01I8IyUTrkaxOKjJo=
DomainKey-Signature: a=rsa-sha1; c=noews; q=dns; s=spop1024; d=archdigest.messages2.com;
b=H746rBH301kImHBUs8kQxZOnT+0u6c5HwTb961+Dd46taTuHETXeZMbrabT02HsOGVLZ5KK2Ila
RyS+jQYpdgsBARobSCYNmTRWLJ24o1Z3y8S7/8ClvtmI4VbQYXh7V2/GDQ+8CIm3YS8rKhdQgJ4ub
DGg2vowJjYs42ebdnQc=;
Received: by mail5694.archdigest.mkt6293.com id hmuia819if4o for <rtkachev@sendpulse.com>; Wed, 17 Apr 2019 22:11:41 +0000 (envelope-from <v-
omfega_fchliniafm_gakaioci_gakaioci_a@bounce.newsletters.archdigest.com>)
Date: Wed, 17 Apr 2019 22:11:41 +0000 (GMT)

```

CONCLUSION: Thus, implementation of email header program is performed successfully.

QUESTIONS:

1. Why are email headers so important in computer forensics ?
2. How can an email header analysis be used in the legal process ?
3. How the use of email header information could be used by a digital forensic professional in an investigation ?