**Lab Experiment 02**

**B. Tech CSF-CSE Semester III Course: Physical and IT Security**

**By: Dr. Gopal Singh Rawat**

**Lab Objective: Trace Email Sender Location, Date/Time, IP Address**

When someone sends an email message to you, the IP address of the sender computer is included in the header of the outgoing (sent) email message. The receiver can then perform a simple geo-lookup against that IP address to find the approximate geographic location of the message sender’s, date/time email was sent and other details.

1. **Finding Sender’s details in MS Outlook:**

Step 1: Open the email received in MS Outlook 🡪 Click on File 🡪 Properties

|  |
| --- |
|  |

Step 2: Select All and Copy the Internet Headers contents

Step 3: Paste them to <https://mxtoolbox.com/EmailHeaders.aspx> and Analyze

|  |
| --- |
|  |

While both Yahoo! Mail and Hotmail include IP addresses in outgoing message headers but when using Gmail web interface or Gmail for Google Apps, the sender’s IP address [won’t be included](http://support.google.com/mail/bin/answer.py?hl=en&answer=26903) in the message. Our Lab experiment is to determine the sender’s details when using Gmail.

**Tools:**

* Windows/Linux OS
* Microsoft Outlook
* <http://whois.domaintools.com>
* <https://who.is/>

**Steps to perform:**

1. **Finding Sender’s IP Address:**

Step 1: Open the message in Gmail App 🡪 Click on More 🡪 Show Original

|  |
| --- |
|  |

* + Search for the line “Received: from “ 🡪 this would be the sender’s Email Domain / IP
  + Use <http://whois.domaintools.com/> to find more information about the sender’s domain

|  |
| --- |
|  |

* Use <https://who.is/> to find and confirm the sender’s domain information

1. **Finding Sender’s Time Zone:**
   * When the IP address is not available, you can determine the sender’s very-approximate location from the time-zone of the originating computer.

Old Gmail Feature ---->

* + Go your [Gmail Labs](https://mail.google.com/mail/u/0/?shva=1#settings/labs) page and enable the “Sender Time Zone” feature.
  + Now open any message in Gmail and click on the down arrow that says “Show details”.
  + The message will display the current time in the sender’s time zone as shown in the following screenshot.

|  |
| --- |
|  |

Next you can use this [time zone map](http://www.timeanddate.com/time/map/) to determine countries where the current time is the same as the time displayed in the Gmail message.

Alternate Option

[*https://toolbox.googleapps.com/apps/messageheader/*](https://toolbox.googleapps.com/apps/messageheader/)

**Lab #02 File Work:**

1. Perform this Experiment and find out sender’s details from at least 5 different emails from different domains
2. List the details gathered as per the below table.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sender’s domain** | **Email Protocol** | **Date/Time sent** | **Time Zone** | **Geolocation** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |