E-mails

- Email has become a primary means of communication.
- Email can easily be forged
- Email can be abused
  - Spam
  - Aid in committing a crime …
  - Threatening email, …
Challenges to E-mail Authenticity

- Origin & Sender of the E-Mail
- Party refutes the emails, allege forgery
- IP Address of sender matches, still the party refute the emails
- Sender accept the mail but challenge attachments
- Email coming from Proxy Server
E-mail tracing…

- **Study of Email:**
  - *Identifying the source system domain, IP Address*
  - *Tracing the sender*
  - *Date/time of sending email*
  - *Message / contents*

- **Locate the source of e-mail & its sender**
Email Protocols:

- Email program such as outlook is a **client application**.

- Needs to interact with an email server:
  - Post Office Protocol (POP)
  - Internet Message Access Protocol (IMAP)
  - Simple Mail Transfer Protocol: SMTP
## Email Protocols:

<table>
<thead>
<tr>
<th>Post Office Service</th>
<th>Protocol</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stores only incoming messages.</td>
<td>POP</td>
<td>Investigation must be at the workstation.</td>
</tr>
<tr>
<td>Stores all messages</td>
<td>IMAP, MS’ MAPI, Lotus Notes</td>
<td>Copies of incoming and outgoing messages might be stored on the workstation or on the server or on both.</td>
</tr>
<tr>
<td>Web-based send and receive.</td>
<td>HTTP</td>
<td>Incoming and outgoing messages are stored on the server, but there might be archived or copied messages on the workstation. Easy to spoof identity.</td>
</tr>
</tbody>
</table>
Client based Emails

Sending and Receiving Email On Internet Using Desktop Email Clients
Web based Emails

Sending and Receiving Email Using Web Based Clients
Naresh (naresh3151@rediffmail.com) sending mail to Ram (cyber.nk@gmail.com)
POP3/IMAP Architecture
Email Protocol Architecture

HYD  Lucknow  Jaipur  Delhi
Rediff Mail  SMTP Server 2  SMTP Server 3  Gmail

HCU  CBI
Naresh  Ram
Click on Show Original

Window Showing Full Header Appears

http://cyberforensics.in/OnlineEmailTracer/Header.aspx
This mail is for testing purpose only.

Hi

This mail is for testing purpose only.
Delivered-To: cyber.nk@gmail.com

Received: by 10.79.9.7 with SMTP id 7csp649857ivj;
  Tue, 5 Jul 2016 23:09:18 -0700 (PDT)
X-Received: by 10.98.68.152 with SMTP id m24mr38873398pfi.35.1467785358556;
  Tue, 05 Jul 2016 23:09:18 -0700 (PDT)
Return-Path: <naresh3151@rediffmail.com>

Received: from rediffmail.com (f4mail-235-198.rediffmail.com.
by mx.google.com with ESMTPS id 15si2283824pfx.153.2016.07.05.23.09.17
for <cyber.nk@gmail.com>
(version=TLS1_2 cipher=AES128-GCM-SHA256 bits=128/128);
  Tue, 05 Jul 2016 23:09:18 -0700 (PDT)
Received-SPF: pass (google.com: domain of naresh3151@rediffmail.com designates 202.137.235.198 as permitted sender)
  client-ip=202.137.235.198;
Authentication-Results: mx.google.com;
  spf=pass (google.com: domain of naresh3151@rediffmail.com designates 202.137.235.198 as permitted sender)
  smtp.mailfrom=naresh3151@rediffmail.com
Received: (qmail 25568 invoked by uid 510); 6 Jul 2016 06:09:16 -0000
Comment: DomainKeys? See http://antispam.yahoo.com/domainkeys
DomainKey-Signature: a=rsa-sha1; q=dns; c=nofws;
  s=redf; d=rediffmail.com;
  b=JoWWDTsl1llu/9TOhON/WLScR8zlPXrmyrMaekYHoTuauoBLWt9kLuTUijoSVJ4zCeziD8YoL5qwQZJilQotYas5aozk974gh3UjWh5QPJoZsbx9+e8h6IAJJUwgpOw85s+YEUVbXyaBsotwzUjxkYZWLEKWTGTTBerxqZaaPPl= ;
x-m-msg: asd54d564ad7aa6sd5as6d5; a6da7d6asas6dasd77; 5dad65ad5sd;
**Analysis of Important Parts of Gmail Header**

In this example, we have sent an e-mail from ‘naresh3151@rediffmail.com’ to ‘cyber.nk@gmail.com’

1. **Sender:** naresh3151@rediffmail.com
   
   This represent the name and email address of the person who send the email.

2. **Received:** from unknown 171.50.146.253 by rediffmail.com via HTTP; 06 Jul 2016 06:09:15 -0000
   
   This is probably the most vital part of the email header from investigation point of view. It represents us that -
   
   - The email was sent from a computer having IP address **171.50.146.253**
   - The email was sent on **06 Jul 2016 06:09:15 (GMT)**.
3. To: "cyber.nk@gmail.com" <cyber.nk@gmail.com>
   This represent the name and email address of the receiver.

4. Message-ID: <20160706060915.25557.qmail@f4mail-235-198.rediffmail.com>
   Message ID can be broken into the following parts:
   - 20160706060915: Represent the time stamp of the email in yyyymmdhhmmss format.
   - 25557: This number is the reference number that represents the corresponding email which is unique.
Analysis of Important Parts of Gmail Header

5. Received: from rediffmail.com (f4mail-235-198.rediffmail.com. [202.137.235.198])
   by mx.google.com with ESMTPS id 15si2283824pfx.153.2016.07.05.23.09.17
   for <cyber.nk@gmail.com>
   (version=TLS1_2 cipher=AES128-GCM-SHA256 bits=128/128);
   Tue, 05 Jul 2016 23:09:18 -0700 (PDT)

This represents that the email was received by an SMTP server at Google
Called **mx.google.com** from Rediffmail server at the given date and time
that has the IP Address **202.137.235.198**.
6. Delivered-To: cyber.nk@gmail.com

This shows that the email was delivered to the account cyber.nk@gmail.com.

You have noticed that time and date in the above examples have been mentioned as –

- 06 Jul 2016 06:09:15-0000
- It means that the time mentioned above i.e. 06:09:15 is in GMT which is 0000 hours.
- IST time is 05:30 hours ahead of GMT.
- To calculate time in IST, add 05:30 hours to make it IST.
What are we looking for?

- 171.50.146.253?
- Verification of IP addresses:
  - Regional Internet Registry
    - APNIC (Asia Pacific Network Information Centre).
    - ARIN (American Registry of Internet Numbers).
    - LACNIC Latin American and Caribbean IP address Regional Registry.
    - RIPE NCC (Réseau IP Européens Network Coordination Centre).
  - Whois (whois.apnic.net) The best
  - www.samspade.org
  - Numerous other websites.
Whois IP 171.50.146.253
% [whois.apnic.net]
% Whois data copyright terms http://www.apnic.net/db/dbcopyright.html
% Information related to '171.50.128.0 - 171.50.191.255'
inetnum: 171.50.128.0 - 171.50.191.255
netname: BHARTI-IN
_descr: Bharti Airtel Limited
descr: Transport Network Group
descr: 234, Okhla Phase III
country: IN
admin-c: NA40-AP
tech-c: NA40-AP
status: ALLOCATED NON-PORTABLE
mnt-by: MAINT-IN-BBIL
mnt-irt: IRT-BHARTI-IN
changed: @apnic.net 20160108
source: APNIC
Fake mails

- We have seen a general flow
- How do you identify fake mails
Delivered-To: cyber.nk@gmail.com
Received: by 10.79.9.7 with SMTP id 7csp651524ivj;
    Tue, 5 Jul 2016 23:14:48 -0700 (PDT)
X-Received: by 10.194.114.106 with SMTP id jf10mr21445216wjb.48.1467785688255;
    Tue, 05 Jul 2016 23:14:48 -0700 (PDT)
Return-Path: <naresh3151@rediffmail.com>
Received: from emkei.cz ([2a01:5e0:36:5001::20])
    by mx.google.com with ESMTP id uy1si1916593wjb.36.2016.07.05.23.14.48
    for <cyber.nk@gmail.com>;
    Tue, 05 Jul 2016 23:14:48 -0700 (PDT)
Received-SPF: softfail (google.com: domain of transitioning naresh3151@rediffmail.com does not designate 2a01:5e0:36:5001::20 as permitted sender) client-ip=2a01:5e0:36:5001::20;
Authentication-Results: mx.google.com;
    spf-softfail (google.com: domain of transitioning naresh3151@rediffmail.com does not designate 2a01:5e0:36:5001::20 as permitted sender) smtp.mailfrom=naresh3151@rediffmail.com
Received: by emkei.cz (Postfix, from userid 33)
    id 026D8D60BE; Wed, 6 Jul 2016 08:18:09 +0200 (CEST)
To: cyber.nk@gmail.com
Subject: Mail for Header Analysis
From: "Naresh Kumar" <naresh3151@rediffmail.com>
X-Priority: 3 (Normal)
Importance: Normal
Errors-To: naresh3151@rediffmail.com
Reply-To: naresh3151@rediffmail.com
Content-Type: text/plain; charset=utf-8
Message-Id: <20160706061810.026D8D60BE@emkei.cz>
Date: Wed, 6 Jul 2016 08:18:09 +0200 (CEST)
Analysis of Fake E-mail Header

1. From: "Naresh Kumar" <naresh3151@rediffmail.com>
2. Received: from emkei.cz ([2a01:5e0:36:5001::20]) by mx.google.com with ESMTP id uy1si1916593wjb.36.2016.07.05.23.14.48 for <cyber.nk@gmail.com>; Tue, 05 Jul 2016 23:14:48 -0700 (PDT)
3. Delivered-To: cyber.nk@gmail.com
4. Message-Id: <20160706061810.026D8D60BE@emkei.cz> Date: Wed, 6 Jul 2016 08:18:09 +0200 (CEST)

Server of Rediffmail is Missing
Spoofed Emails

- They are sent using –
  - Open relays
  - Compromised systems
  - Self owned email servers
  - Proxy Server
  - Hijacked accounts
Proxy Server

Naresh -> Internet -> Proxy -> Internet -> Rediff

Proxy -> Internet -> Gmail

Gmail -> Internet -> Ram
Tools To Trace The Source Of An E-mail

- **NeoTracePro**
  
  [http://neotrace-pro.en.softonic.com/download](http://neotrace-pro.en.softonic.com/download)

- **Visual IP Trace**
  
  [http://www.visualiptrace.com/download.html](http://www.visualiptrace.com/download.html)

- **Visual Route**
  
  [http://www.visualroute.com/download.html](http://www.visualroute.com/download.html)

- **Email Tracker Pro**
  
  [http://www.emailtrackerpro.com/download.html](http://www.emailtrackerpro.com/download.html)

- **Email tracer (from CDAC, India)**
  
  [http://cyberforensics.in/OnlineEmailTracer/index.aspx](http://cyberforensics.in/OnlineEmailTracer/index.aspx)