EMAIL FORENSICS

Trình bày: Nguyễn Xuân Việt – FPT CIO

NỘI DUNG CHÍNH

Nội dung 01

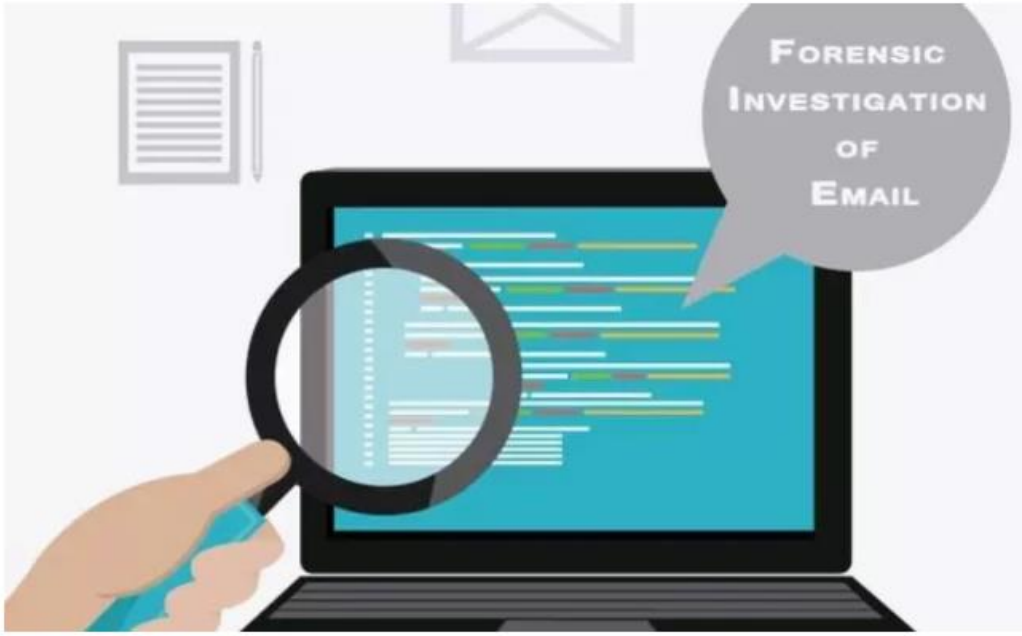
Các kỹ thuật Điều tra Email

Nội dung 02

Kỹ thuật Header Analysis

ĐIỀU TRA SỐ EMAIL (EMAIL FORENSICS)

Trong điều tra số, email được coi là một loại bằng chứng có giá trị và công việc phân tích tiêu đề email là một điều quan trọng vì từ đây điều tra viên có thể thu thập bằng chứng, củng cố hồ sơ phạm tội.



CÁC KỸ THUẬT ĐIỀU TRA EMAIL

1. Header Analysis

Điều tra thông tin có trong header của email nhằm xác định các thông tin IP, địa chỉ gửi mail hoặc xác định các thông tin giả mạo bị che dấu

2. Server Investigation

Điều tra log gửi mail trên server mail trong trường hợp truy cập được vào server. Trên server sẽ lưu log trong một thời gian nhất định, ta có thể sử dụng log này để điều tra các thông tin IP, đia chỉ, thời gian gửi nhận thậm chí cả nội dung mail

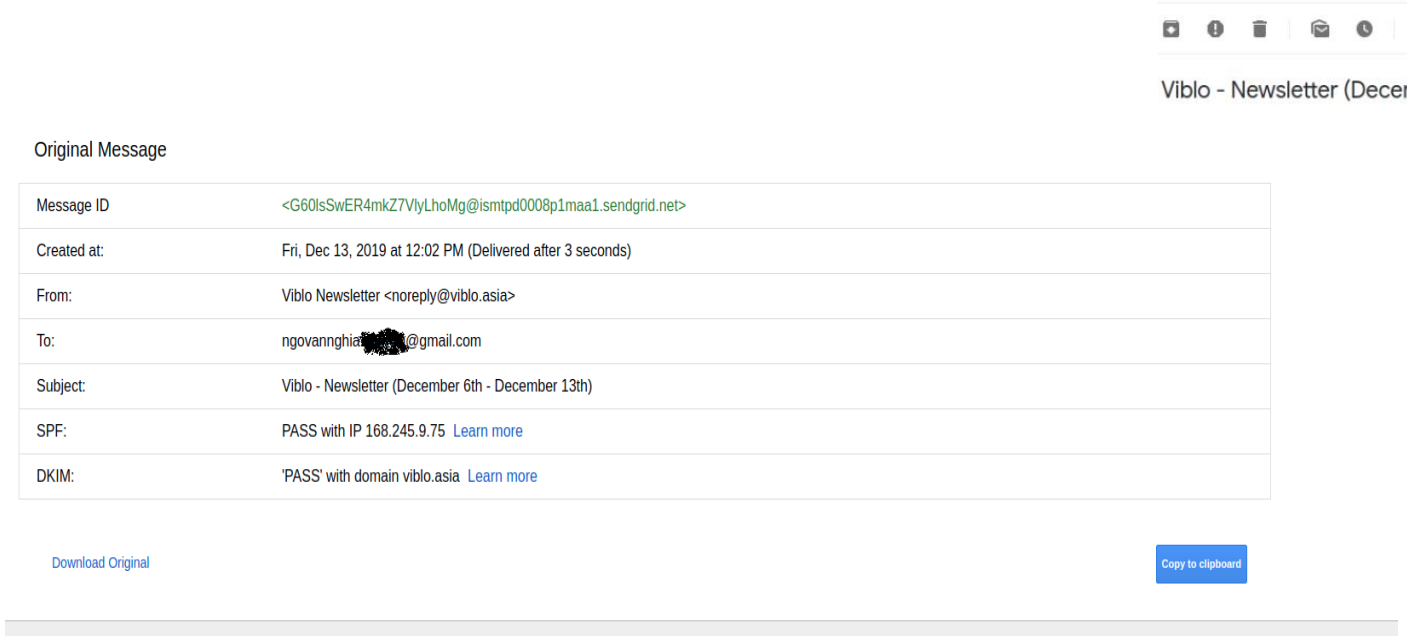
3. Software Embedded Identifiers

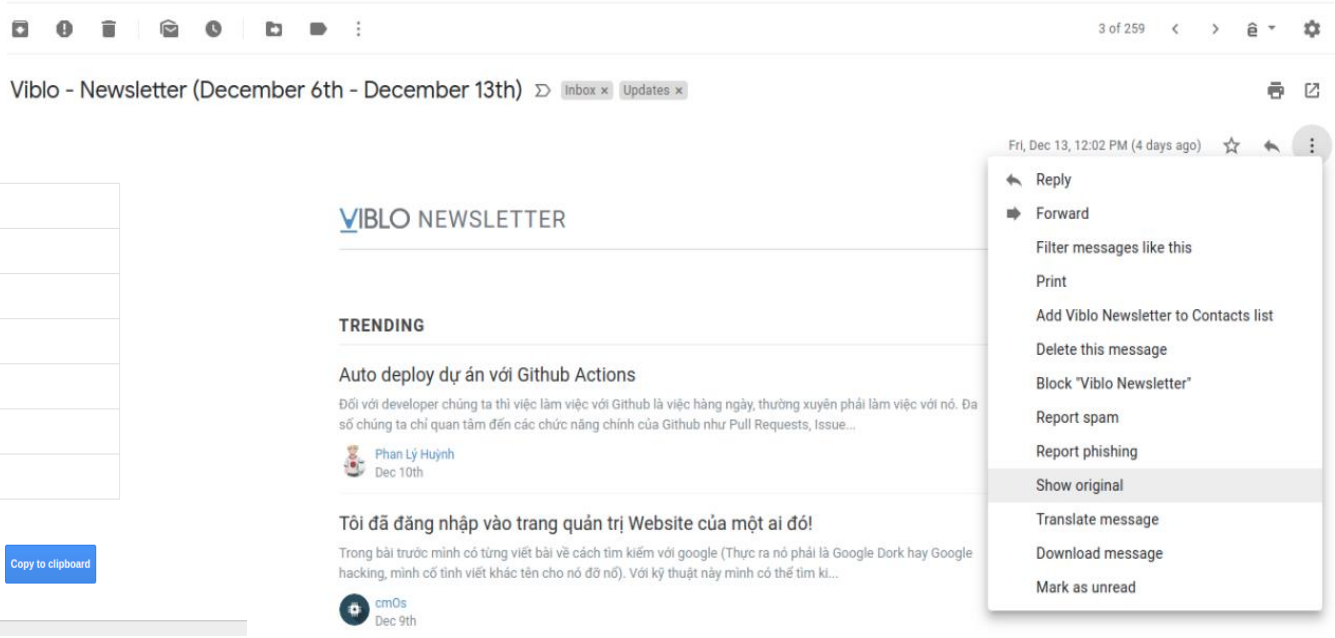
Điều tra file đính kèm trong email, trong các file đínhh kèm sẽ có thể có các thông tin, tài khoản tao file, tên máy và thời gian tạo file, từ đó có thể thu thập thông tin

KỸ THUẬT HEADER ANALYSIS

Truy Xuất Nguồn Gốc Email Bằng Header

- Truy xuất địa chỉ email bằng cách phân tích kỹ tiêu đề đầy đủ của email.
- Để xem tiêu đề email đầy đủ **trong Gmail**: Mở tài khoản Gmail của bạn, sau đó mở email bạn muốn truy xuất nguồn gốc. Di chuyển đến thanh menu cuộn ở góc trên cùng bên phải, sau đó chọn mục hiển thị bản gốc (*Show original*).





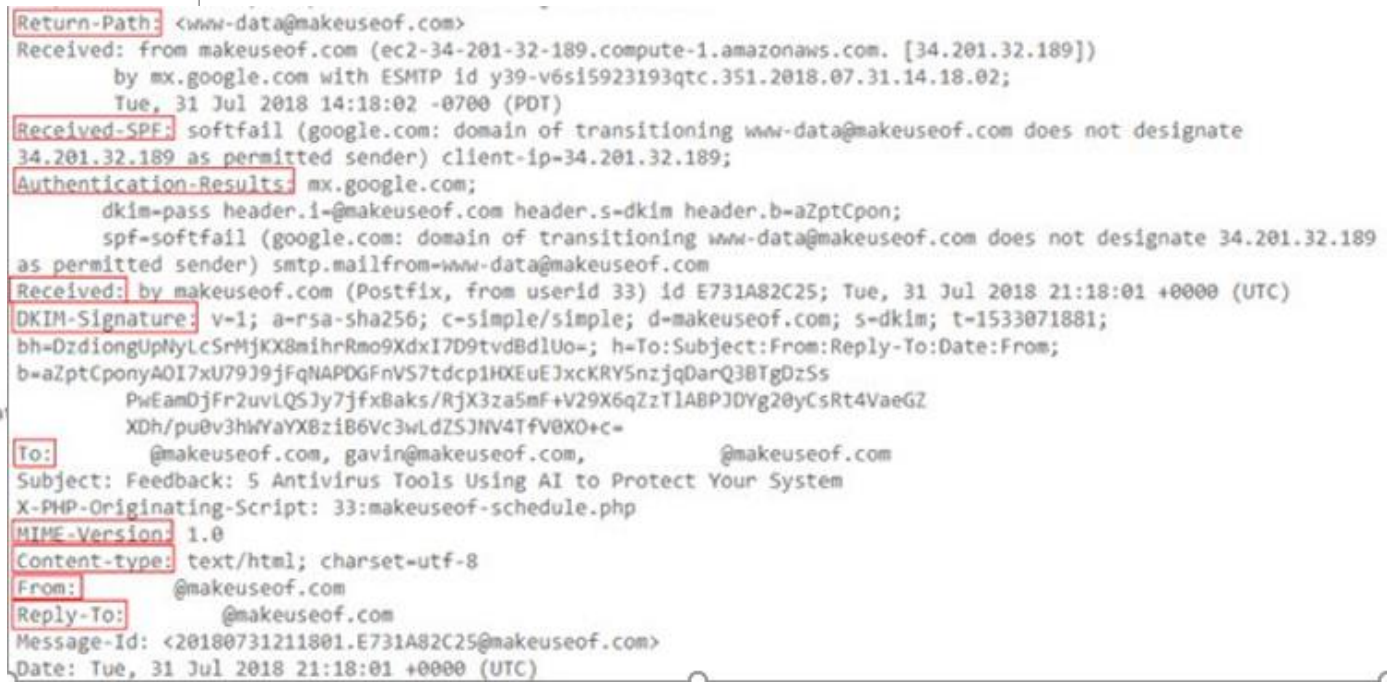
ĐIỀU TRA SỐ EMAIL (EMAIL FORENSICS)

- Xem tiêu đề email đầy đủ trong **Outlook**: Nhấp đúp vào email bạn muốn truy xuất nguồn gốc, sau đó vào **File** chọn **Properties**. Thông tin xuất hiện trong tiêu đề internet **(internet headers)**.
- Xem tiêu đề email đầy đủ trong **Apple Mail:** Mở email bạn muốn theo dõi, sau đó di chuyển chuyển đến **View > Message > Raw Source**.
- Có rất nhiều thông tin được hiển thị trong một tiêu đề email đầy đủ, nhưng cần chú ý: đọc theo trình tự từ dưới lên trên, từ thông tin cũ đến thông tin mới (có nghĩa là thông tin cũ nhất sẽ ở dưới cùng

ĐIỀU TRA SỐ EMAIL (EMAIL FORENSICS)

Ví dụ: một tiêu đề email mẫu lấy từ tài khoản Gmail

```
Delivered-To: gavin@makeuseof.com
Received: by 2002:a02:b574:0:0:0:0:0 with SMTP id z49-v6csp82209jaj;
        Tue, 31 Jul 2018 14:18:02 -0700 (PDT)
X-Google-Smtp-Source: AAOMgpdAEK/jlAcUfevVReR0HJuHe+/wNPAsgzcd3QkU8B/By4vrGg90vR8O6xskNSJ4bhyfGkj4
X-Received: by 2002:a37:5d02:: with SMTP id r2-v6mr21648702qkb.22.1533071882522;
        Tue, 31 Jul 2018 14:18:02 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1533071882; cv=none;
        d=google.com; s=arc-20160816;
        b=LLgUgxUzyukDKiqv/13MKDk+ZQJiCBFi3OHljAA1j8O8xPTaNjKneV8umkIVScHY8D
         FQQIdjkeFC2xUON16TvBi+mhDx7+bSQ0mUSehh/LfNAoIRQSAU4s8mdiBdkqnZOYEsFb
         BGRf9GU+M5axX9vH3GyRywpUpm9GkaesA4WwUZhOeinzokpXFGzFDLp0KNDweP6UmGVF
         BrqfGBqgrmQY2VLHIeNklG4Glk48BxSqPjSX1Nmmlkm47AZ/7jYTMEUy7qCr2bEmFaTU
         THWSwsviwkWgW9iofUEBAS361GMpuE0Mb7pxxnAY2iLyvD2dZNgY2y8IhX/Xhp89NKDp
         oyhw==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=date:message-id:reply-to:from:mime-version:subject:to
         :dkim-signature:arc-authentication-results;
        bh=DzdiongUpNyLcSrMjKX8mihrRmo9XdxI7D9tvdBdlUo=;
        b=hTjE4Ch8xuoTVbAofybKlNjJ1YTgZ56E7hpPOhW9WLBUhZp5bROwZwHF7SCR1rzddN
         OneLCj3VKOmdVu4v3qDGvupH8gB1rNUAKn2fWcTa9SdawoI417dehA8IGYqwKcRPhWos
         NHoXlX53NX4JmuIPs1N7TzpsCmziTyhd93KM/I/5NBtF3M+5brle6X47fFgcu+HC1CP3
         6A8GKaQZTEtEF06DB9Yxb4Qtjz0i1X6TDJpxD3gqMFWHWtRNMGKFaXKicCH0lTsmsqGT
         n9UaJGh9F8sDcLOBjN72XGvHo76pwkOEsUbkmTyYURDTz7WXtYGm5LmTu2VYLSOrznH0
         FFMQ==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@makeuseof.com header.s=dkim header.b=aZptCpon;
       spf=softfail (google.com: domain of transitioning www-data@makeuseof.com does not designa
as permitted sender) smtp.mailfrom=www-data@makeuseof.com
```



```
Return-Path: <www-data@makeuseof.com>
Received: from makeuseof.com (ec2-34-201-32-189.compute-1.amazonaws.com. [34.201.32.189])
        by mx.google.com with ESMTP id y39-v6si5923193qtc.351.2018.07.31.14.18.02;
        Tue, 31 Jul 2018 14:18:02 -0700 (PDT)
Received-SPF: softfail (google.com: domain of transitioning www-data@makeuseof.com does not designate
34.201.32.189 as permitted sender) client-ip=34.201.32.189;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@makeuseof.com header.s=dkim header.b=aZptCpon;
       spf=softfail (google.com: domain of transitioning www-data@makeuseof.com does not designate 34.201.32.189
as permitted sender) smtp.mailfrom=www-data@makeuseof.com
Received: by makeuseof.com (Postfix, from userid 33) id E731A82C25; Tue, 31 Jul 2018 21:18:01 +0000 (UTC)
DKIM-Signature: v=1; a=rsa-sha256; c=simple/simple; d=makeuseof.com; s=dkim; t=1533071881;
bh=DzdiongUpNyLcSrMjKX8mihrRmo9XdxI7D9tvdBdlUo=; h=To:Subject:From:Reply-To:Date:From;
b=aZptCponyAOI7xU79J9jFqNAPDGFnVS7tdcp1HXEuEJxcKRY5nzjqDarQ3BTgDzSs
         PwEamDjFr2uvLQSJy7jfxBaks/RjX3za5mF+V29X6qZzTlABPJDYg20yCsRt4VaeGZ
         XDh/pu0v3hWYaYXBziB6Vc3wLdZSJNV4TfV0XO+c=
To:        @makeuseof.com, gavin@makeuseof.com,          @makeuseof.com
Subject: Feedback: 5 Antivirus Tools Using AI to Protect Your System
X-PHP-Originating-Script: 33:makeuseof-schedule.php
MIME-Version: 1.0
Content-type: text/html; charset=utf-8
From:       @makeuseof.com
Reply-To:       @makeuseof.com
Message-Id: <20180731211801.E731A82C25@makeuseof.com>
Date: Tue, 31 Jul 2018 21:18:01 +0000 (UTC)
```

ĐIỀU TRA SỐ EMAIL (EMAIL FORENSICS)

Các thành phần trong header

- **Reply-To**: Địa chỉ email bạn gửi phản hồi tới.
- **From**: Hiển thị người gửi tin nhắn, thông tin này rất dễ bị giả mạo.
- **Subject**: Chủ đề của nội dung email.
- **To**: Người dự định sẽ nhận email, có thể hiển thị thêm các địa chỉ người nhận khác nữa.
- **Received**: Dòng “Received” liệt kê từng máy chủ mà email di chuyển qua trước khi được gửi tới hộp thư đến của bạn. Bạn đọc dòng “Received” từ dưới lên trên; dòng dưới cùng là người khởi tạo email.
- **Delivered-To**: Người nhận cuối cùng của email này.

ĐIỀU TRA SỐ EMAIL (EMAIL FORENSICS)

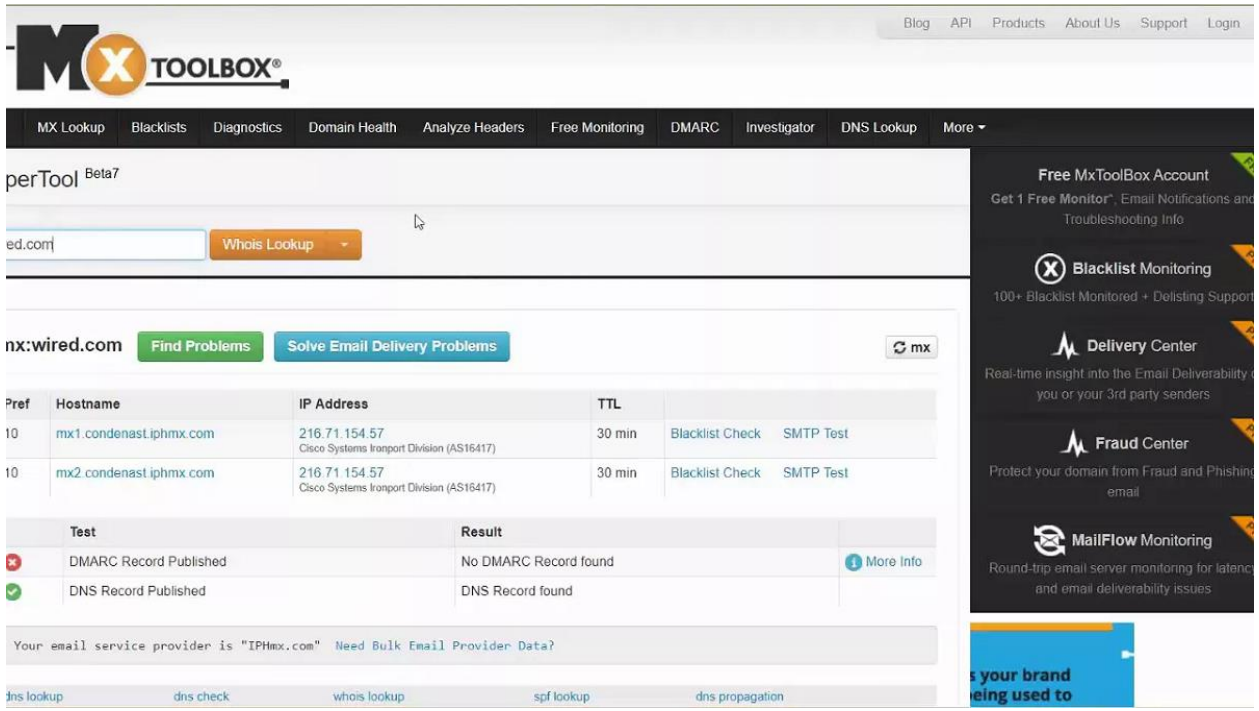
Truy xuất Địa chỉ IP gốc nơi email được gửi đi

- Hãy chú ý đến “Received” đầu tiên trong tiêu đề email đầy đủ. Bên cạnh dòng “Received” đầu tiên chính là địa chỉ IP của máy chủ đã gửi email. Đôi khi, nội dung này hiển thị dưới dạng X-Originating-IP hoặc Original-IP.

ĐIỀU TRA SỐ EMAIL (EMAIL FORENSICS)

Truy xuất Địa chỉ IP gốc nơi email được gửi đi

- Tìm địa chỉ IP, sau đó di chuyển đến trang **MX Toolbox**. Nhập địa chỉ IP này vào trong hộp thoại, thay đổi phương thức tìm kiếm thành **Reverse Lookup**, sau đó nhấn Enter.



ĐIỀU TRA SỐ EMAIL (EMAIL FORENSICS)

Truy xuất Địa chỉ IP gốc nơi email được gửi đi

- Trừ khi địa chỉ IP gốc là một địa chỉ IP riêng tư, còn không, bạn sẽ nhận được thông báo sau:

- **Miền IP 10.0.0.0-10.255.255.255, 172.16.00-172.31.255.255, 192.168.0.0-192.168.255.255 và 224.0.0.0-239.255.255.255** là các miền IP riêng tư. Sẽ không có bất kỳ kết quả nào được trả về khi bạn tra cứu các địa chỉ IP này.

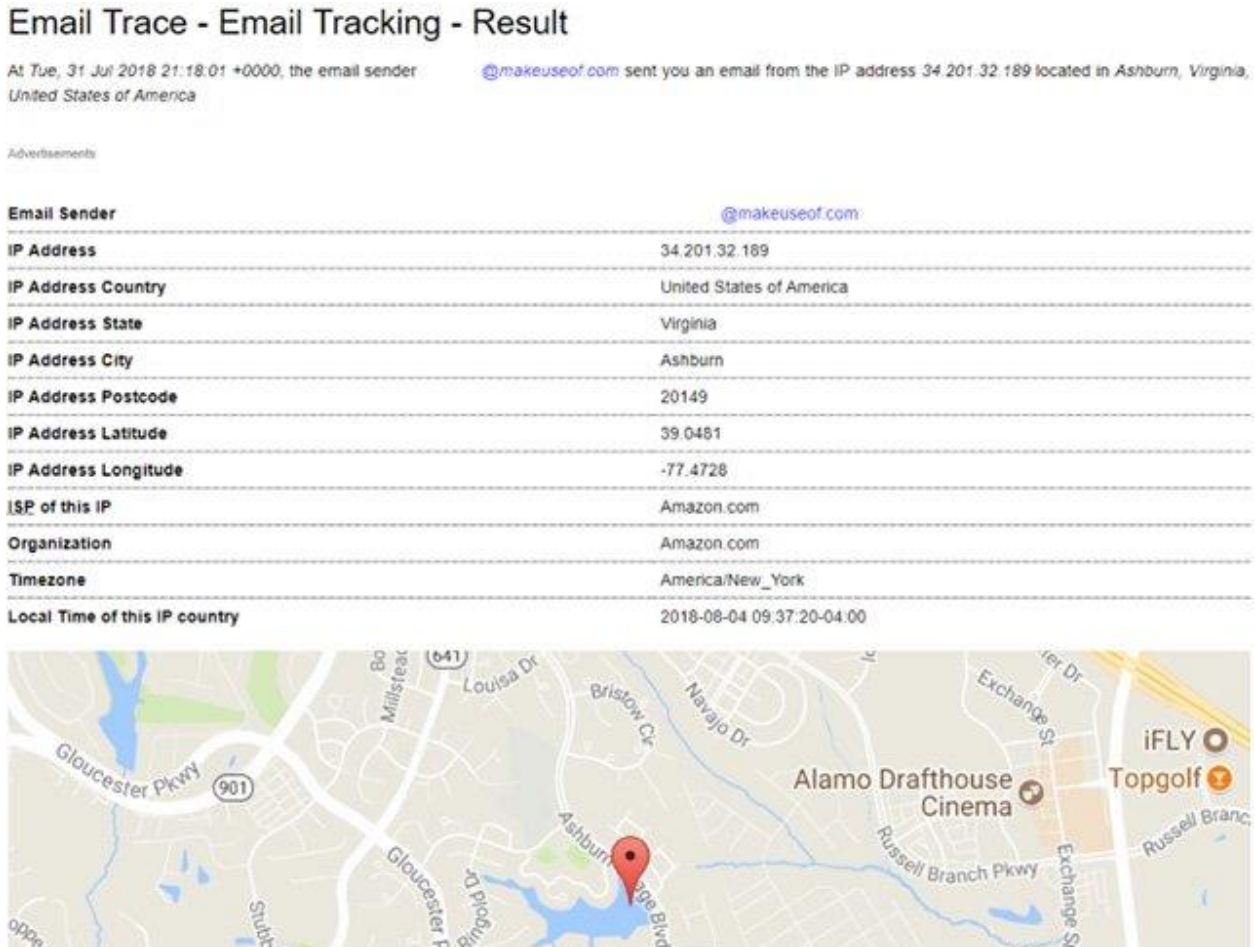
ĐIỀU TRA SỐ EMAIL (EMAIL FORENSICS)

Các công cụ hữu ích trong phân tích header email và truy xuất địa chỉ IP: Bạn có thể sử dụng một số công cụ sau để phân tích tiêu đề email:

- **GSuite Toolbox Messageheader**
- **MX Toolbox Email Header Analyzer**
- **IP-Address Email Header Trace** (phân tích được cả tiêu đề email lẫn truy xuất địa chỉ IP gửi email)

ĐIỀU TRA SỐ EMAIL (EMAIL FORENSICS)

Tuy nhiên đôi khi kết quả trả về không phải lúc nào cũng phù hợp. Trong ví dụ dưới đây, người gửi không ở gần vị trí được trả về là Ashburn, Virginia



Email Trace - Email Tracking - Result

At Tue, 31 Jul 2018 21:18:01 +0000, the email sender @makeuseof.com sent you an email from the IP address 34.201.32.189 located in Ashburn, Virginia, United States of America

Advertisements

Email Sender	@makeuseof.com
IP Address	34.201.32.189
IP Address Country	United States of America
IP Address State	Virginia
IP Address City	Ashburn
IP Address Postcode	20149
IP Address Latitude	39.0481
IP Address Longitude	-77.4728
ISP of this IP	Amazon.com
Organization	Amazon.com
Timezone	America/New_York
Local Time of this IP country	2018-08-04 09:37:20-04:00

Thank You !