EXPERMINT: 01

Aim:

- Perform Email Header Analysis for extracting valuable information like sender IP address, email servers, and routing information.
- Conduct email address enumeration by attempting to verify the existence of email addresses within a target domain. Use tools like the Harvester or thehunter.io to search for email addresses associated with a specific domain. This can help identify valid email addresses within an organization.
- Analyze the metadata of an email, including date and time stamps, email clients used, or the originating IP address, email's origin, potential geographic

Theory:

Email header analysis

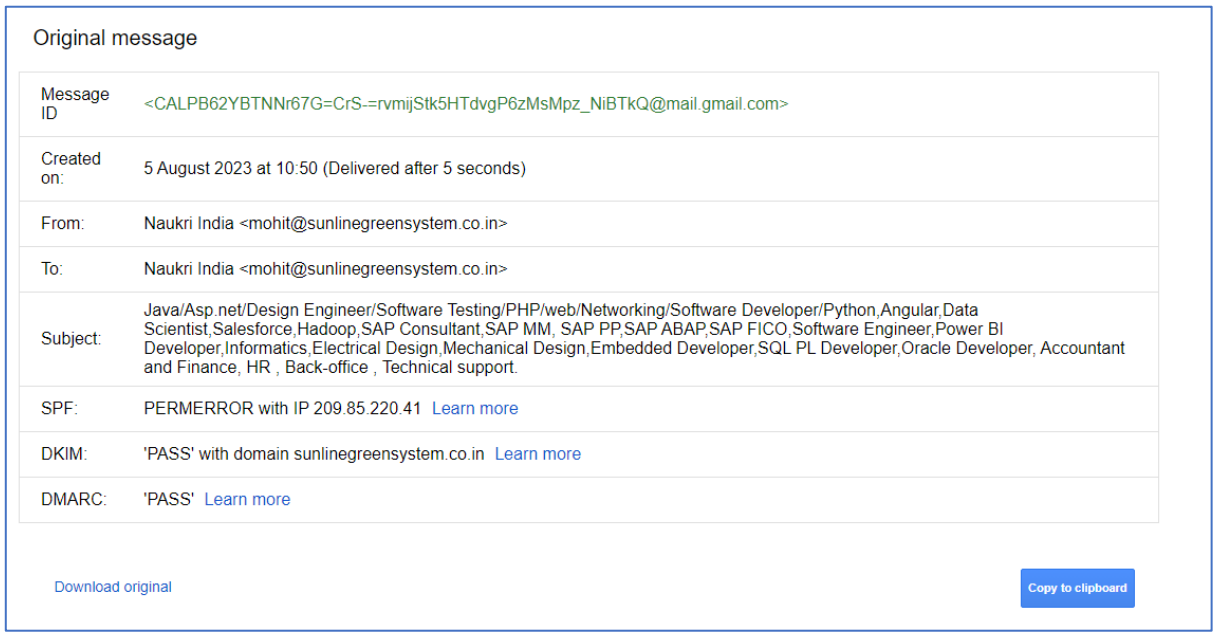
Email header analysis can reveal important information about the source and path of an email, including sender IP addresses, email servers, routing details, and more. You can perform email header analysis in most email clients or online email analysis tools. Here's a basic guide to analyze email headers:

- **Open the Email**: Open the email for which you want to analyze the header.
- **View Email Header**: The process for viewing email headers varies depending on your email client. In general, you'll want to find an option to "View Full Header," "Show Original," or "View Source." This is usually found in the email's settings or options.
- **Analyze the Header:** The email header will typically be displayed in a plain text or HTML format. Look for information such as:
- **Return-Path**: The return path can provide information about the initial sender.
- **Received:** This section will have multiple lines showing the path the email took through various email servers. Look for the "from" and "by" domains and IP addresses.
- **X-Originating-IP**: Some email services may include the sender's IP address.
- **Subject**: While not a technical detail, it can still provide context.
- **Check for Anomalies**: Look for any unusual or suspicious entries, such as unfamiliar IP addresses or domains. This can help identify potential phishing attempts or email spoofing.
- **Trace the Route**: To understand the path the email took, read the "Received" entries from bottom to top. This shows the journey of the email through different email servers.
- **IP Geolocation**: You can use online tools to perform IP geolocation to determine the approximate location of the IP addresses involved.

Email header analysis tools can help you quickly and effectively dissect and understand the information contained in email headers. These tools can assist you in uncovering details about the email's source, routing, and authenticity. Here are some email header analysis tools that you can use:

- **MXToolBox Header Analyzer**: MXToolBox offers a free online tool for email header analysis. Simply paste the email header, and it provides a detailed breakdown of the information, including sender IP addresses and server details.
- **EmailHeader.io**: EmailHeader.io is another free online tool that offers email header analysis. It breaks down the header information in a user-friendly way, making it easy to understand.

- **IPInfo.io**: While not specifically an email header analysis tool, IPInfo.io allows you to perform IP geolocation. You can use this to identify the geographic location of IP addresses mentioned in the email header.
- **Email Forensics by Agari:** Agari offers an email forensics tool that allows you to analyze email headers. This tool is particularly useful for identifying email-based threats and phishing attempts.
- **GlockApps Email Header Analyzer**: GlockApps offers a tool to analyze email headers and check for authentication details, which can help in identifying legitimate emails.

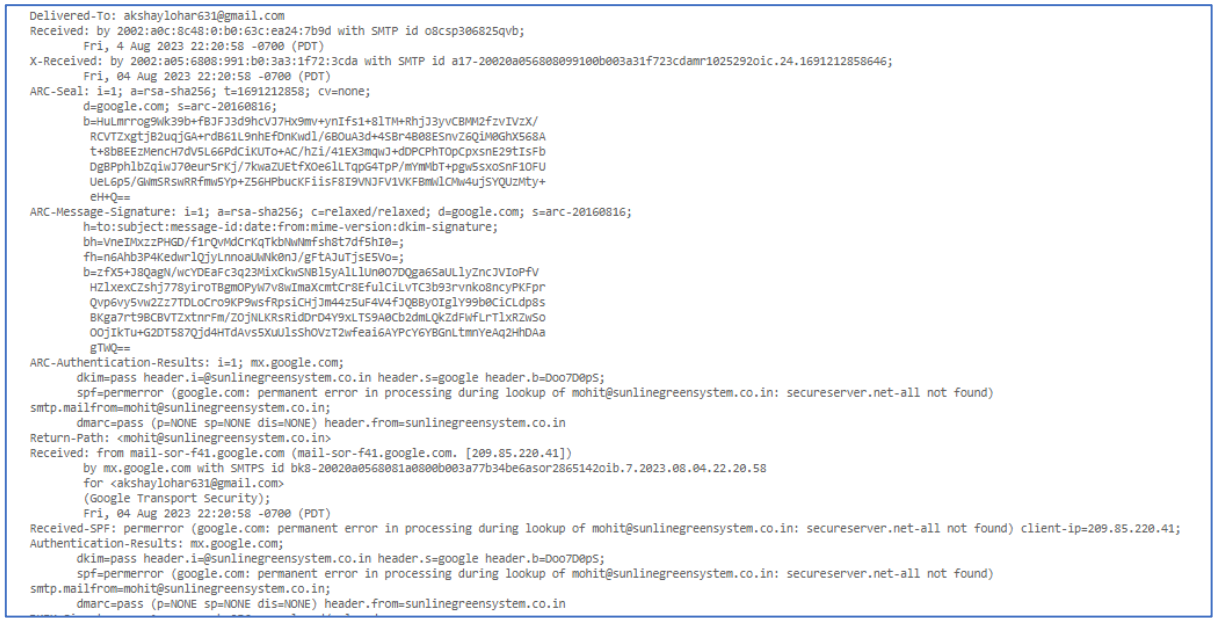


Original message

Message ID	<CALPB62YBTNNr67G=CrS-=rvmijStk5HTdvgP6zMsMpz_NiBTkQ@mail.gmail.com>
Created on:	5 August 2023 at 10:50 (Delivered after 5 seconds)
From:	Naukri India <mohit@sunlinegreensystem.co.in>
To:	Naukri India <mohit@sunlinegreensystem.co.in>
Subject:	Java/Asp.net/Design Engineer/Software Testing/PHP/web/Networking/Software Developer/Python,Angular,Data Scientist,Salesforce,Hadoop,SAP Consultant,SAP MM, SAP PP,SAP ABAP,SAP FICO,Software Engineer,Power BI Developer,Informatics,Electrical Design,Mechanical Design,Embedded Developer,SQL PL Developer,Oracle Developer, Accountant and Finance, HR , Back-office , Technical support.
SPF:	PERMERROR with IP 209.85.220.41 Learn more
DKIM:	'PASS' with domain sunlinegreensystem.co.in Learn more
DMARC:	'PASS' Learn more

Download original

Copy to clipboard



```
Delivered-To: akshaylohar631@gmail.com
Received: by 2002:a0c:8c48:0:b0:63c:ea24:7b9d with SMTP id o8csp306825qvb;
        Fri, 4 Aug 2023 22:20:58 -0700 (PDT)
X-Received: by 2002:a05:6808:991:b0:3a3:1f72:3cda with SMTP id a17-20020a056808099100b003a31f723cdamr1025292oic.24.1691212858646;
        Fri, 04 Aug 2023 22:20:58 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1691212858; cv=none;
        d=google.com; s=arc-20160816;
        b=HuLmrrog9Wk39b+fBJFJ3d9hcVJ7Hx9mv+ynIfs1+8lTM+RhjJ3yvCBMM2fzvIVzX/
         RCVTZxgtjB2uqjGA+rdB61L9nhEfDnKwd1/6BOuA3d+4SBr4B08ESnvZ6QiM0GhX568A
         t+8bBEEzMencH7dV5L66PdCiKUTo+AC/hZi/41EX3mqwJ+dDPCPhTOpCpxsnE29tIsFb
         DgBPphlbZqiwJ70eurSrKj/7kwaZUEtfXOe6lLTqpG4TpP/mYmMbT+pgw5sxoSnF1OFU
         UeL6p5/GWmSRswRRfmwSYp+Z56HPbucKFiisF8I9VNJFV1VKFBmWlCMw4ujSYQUzMty+
         eH+Q==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=to:subject:message-id:date:from:mime-version:dkim-signature;
        bh=VneIMxzzPHGD/f1rQvMdCrKqTkbNwNmfsh8t7dfShI0=;
        fh=n6Ahb3P4KedwrlQjyLnnoaUwNk0nJ/gFtAJuTjsE5Vo=;
        b=zfX5+J8QagN/wcYDEaFc3q23MixCkwSNBl5yAlLlUn0O7DQga6SaULlyZncJVIoPfV
         HZlxexCZshj778yiroTBgmOPyW7v8wImaXcmtCr8EfulCiLvTC3b93rvnko8ncyPKFpr
         Qvp6vy5vW2Zz7TDLoCro9KP9wsfRpsiCHjJm44z5uF4V4fJQBByOIglY99b0CiCLdp8s
         BKga7rt9BCBVTZxtnrFm/ZOjNLKRsRidDrD4Y9xLTS9A0Cb2dmLQkZdFWfLrTlxRZwSo
         OOjIkTu+G2DT587Qjd4HTdAvs5XuUlsShOVzT2wfea16AYPcY6YBGnLtmnYeAq2HhDAa
         gTWQ==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@sunlinegreensystem.co.in header.s=google header.b=Doo7D0pS;
       spf=permerror (google.com: permanent error in processing during lookup of mohit@sunlinegreensystem.co.in: secureserver.net-all not found)
smtp.mailfrom=mohit@sunlinegreensystem.co.in;
       dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=sunlinegreensystem.co.in
Return-Path: <mohit@sunlinegreensystem.co.in>
Received: from mail-sor-f41.google.com (mail-sor-f41.google.com. [209.85.220.41])
        by mx.google.com with SMTPS id bk8-20020a0568081a0800b003a77b34be6asor2865142oib.7.2023.08.04.22.20.58
        for <akshaylohar631@gmail.com>
        (Google Transport Security);
        Fri, 04 Aug 2023 22:20:58 -0700 (PDT)
Received-SPF: permerror (google.com: permanent error in processing during lookup of mohit@sunlinegreensystem.co.in: secureserver.net-all not found) client-ip=209.85.220.41;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@sunlinegreensystem.co.in header.s=google header.b=Doo7D0pS;
       spf=permerror (google.com: permanent error in processing during lookup of mohit@sunlinegreensystem.co.in: secureserver.net-all not found)
smtp.mailfrom=mohit@sunlinegreensystem.co.in;
       dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=sunlinegreensystem.co.in
```

Email header analysis in Gmail

Other Important Email Headers

X-BBounce: 227254537|1486804|paul.friedman@gmail.com|47|0|3605|4

X-IADB-URL: http://www.isipp.com/iadb.php

Sender: Ginger (noreply@gingersoftware.com)

Submitter: reply@activetrail.com

X-Feedback-ID: 3605:3605.1346802.0:G1:atgfbl

List-Unsubscribe:(http://trailer.web-view.net/unsubscribe/0XE838F4BC62366CBC595D7E381467599CE32C9B2368C35B4CB7315919D29140E3552835B8FF6C759D.htm),

Reply-To: Newsletter@gingersoftware.com

From: Ginger : (noreply@gingersoftware.com)

To: "paul.friedman@gmail.com" : (paul.friedman@gmail.com)

Message-ID: (c000e5f41f8f4137a30cab4g6eddcd1e@gingersoftware.com)

Date: Wed, 01 Feb 2017 10:39:06 +0200

Subject: Thank you for registering with Ginger!

MIME-Version: 1.0

Content-Type: multipart/alternative; boundary="----7308DF8A8DBB43098928C652849D6409"

------7308DF8A8DBB43098928C902849D6409

Content-type: text/plain; charset=utf-8

Content-Transfer-Encoding: quoted-printable

Email enumeration

Email enumeration is a type of brute-force attack in which a malicious actor attempts to guess or confirm users in a system by passing an email address to the API and checking the response.

In the examples that follow, email enumeration protection is disabled. Identity Platform returns information that can be used in an email enumeration attack:

- An attempt is made to sign in with an email address that doesn't exist in the system. Identity Platform returns an EMAIL_NOT_FOUND error.
- An attempt is made to sign up with an email address that already exists in the system. Identity Platform returns an EMAIL_EXISTS error.
- You can use Identity Platform's email enumeration protection feature to protect user accounts in your app from these attacks. Email enumeration protection offers the following features:
- Invalid sign-in cases return an INVALID_LOGIN_CREDENTIALS error response. Invalid sign-up cases return EMAIL_EXISTS.
- Removes error responses for email verification flows. If the email address exists, a verification email is sent. If it does not exist, a verification email is not sent. We recommend that you do not allow users to sign up without an email verification flow.
- Disables the ability for users to change their email address without first verifying the new address.
- Disables listing of sign-in methods for a specified email address when calling createAuthUri.

Step #1: Getting Started with theHarvester

- The first step is to download the Harvester. If you are using a Linux distribution other than Kali, you can get theHarvester from github.com such as;
- kali > git clone https://github.com/laramies/theHarvester
- If you are using Kali, it is built into nearly every version. If not, simply download it from the repository. Note the lower case "h" in the repository name.
- kali > sudo apt install theharvester

```
kali@kali:/etc/theHarvester$ sudo apt install theharvester
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
```

Step #2: the Harvest Syntax and help

- Let's begin by examining the help screen for the Harvester.
- kali > theHarvester -h

```
kali@kali:~$ theHarvester -h
table results already exists

*******************************************************************
*                                                                 *
*  _   _                                            _            *
*  | |_| |_ ___ /\  /\__ _ _ ____   _____  ___| |_ ___ _ __    *
*  | __| __/ _ \ /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__|   *
*  | |_| ||  __/ __  / (_| | |   \ V /  __/\__ \ ||  __/ |      *
*   \__|\__\___\/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|      *
*                                                                 *
* theHarvester 3.1.0                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************


usage: __main__.py [-h] -d DOMAIN [-l LIMIT] [-S START] [-g] [-p] [-s] [-v] [-e DNS_SERVER] [-t DNS_TLD]
                   [-n] [-c] [-f FILENAME] [-b SOURCE]

theHarvester is used to gather open source intelligence (OSINT) on a company or domain.

optional arguments:
  -h, --help            show this help message and exit
  -d DOMAIN, --domain DOMAIN
                        company name or domain to search
  -l LIMIT, --limit LIMIT
                        limit the number of search results, default=500
  -S START, --start START
                        start with result number X, default=0
  -g, --google-dork     use Google Dorks for Google search
  -p, --port-scan       scan the detected hosts and check for Takeovers (21,22,80,443,8080)
  -s, --shodan          use Shodan to query discovered hosts
  -v, --virtual-host    verify host name via DNS resolution and search for virtual hosts
  -e DNS_SERVER, --dns-server DNS_SERVER
```

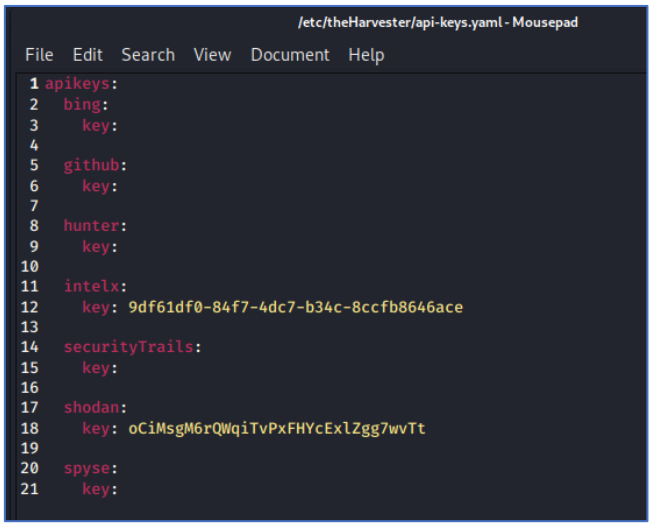
theHarvester -d <domain>

We can specify which source we want to access for data by using the -b switch, such as;

1. Baidu
2. Bing
3. Bing API
4. Certspotter
5. CRTSH
6. DNSdumpster
7. Dogpile

and many others. If you want to use all these resources, you can simply use the all switch from the command line.

In some cases, you will want to use the services API (application programming interface). To do so, open the text file in any text editor at /etc/theHarvester/api-kets.yaml like below.



Step #3: Run a Scan with theHarvester

Now, let try using theHarvester against everyone's favorite electric car manufacturer, Tesla. To scrape all this data on Tesla, we can use the following command;

kali > theHarvester -d teslas.com -b all -f /home/kali/tesla_results2

Where:

theHarvester is the command

-d tesla.com directs the tool to scape data from the domain (-d) tesla.com

-b all directs this tool to use all the sources available

-f /home/kali/tesla_results2 directs the tool to send the results to file

When the Harvester completes its work, we can view the results by opening the tesla_results2 file to view with a web browser.

kali > firefox tesla_results2

This opens our HTML file as seen below.

theHarvester Scan Report

Latest scan report

Date	Domain	Plugin	Record type	Result
2021-02-10	tesla.com	CRTsh	host	ciscoguest.tesla.com
2021-02-10	tesla.com	CRTsh	host	events.tesla.com
2021-02-10	tesla.com	CRTsh	host	api-toolbox.tesla.com toolbox.tesla.com
2021-02-10	tesla.com	CRTsh	host	gridlogic-eng.energy.tesla.com
2021-02-10	tesla.com	CRTsh	host	image.emails.tesla.com my.tesla.com serviceapp.tesla.com smarttax.tesla.com static.tesla.com warpbilling.tesla.com www.tesla.com

If we scan down a bit, we can see that theHarvester has scraped numerous emails from Bing and other search engines.

2021-02-10	tesla.com	bing	email	studio.sandbox-courses.tesla.com
2021-02-10	tesla.com	bing	email	autobidder-eng.powerhub.energy.tesla.com
2021-02-10	tesla.com	bing	email	view.emails.tesla.com
2021-02-10	tesla.com	bing	email	de.tesla.com de.tesla.com
2021-02-10	tesla.com	bing	email	sso-dec.tesla.com
2021-02-10	tesla.com	bing	email	autodiscover.tesla.com xmail.tesla.com
2021-02-10	tesla.com	bing	email	powerhub.energy.tesla.com www.powerhub.energy.tesla.com
2021-02-10	tesla.com	bing	email	image.emails.tesla.com my.tesla.com static.tesla.com www.tesla.com
2021-02-10	tesla.com	bing	email	rumipv6.tesla.com
2021-02-10	tesla.com	bing	email	factory-berlin.tesla.com factory-berlin.tesla.com
2021-02-10	tesla.com	bing	email	engage.tesla.com engage.tesla.com
2021-02-10	tesla.com	bing	email	toolbox.tesla.com www.toolbox.tesla.com
2021-02-10	tesla.com	bing	email	studio.courses.tesla.com
2021-02-10	tesla.com	bing	email	sandbox-manager.courses.tesla.com sandbox-manager.courses.tesla.com
2021-02-10	tesla.com	bing	email	sso-dev.tesla.com
2021-02-10	tesla.com	bing	email	my.tesla.com static.tesla.com www.tesla.com

● Conclusion:

Perform Email Header Analysis for extracting valuable information like sender IP address, email Use tools like the Harvester or thehunter.io to search for email addresses associated with a IP address, email's origin, potential geographic location of the sender, or possible email routing.