یافتن مکان فرستنده ایمیل

شناسنامه کتاب		
نام کتاب : **یافتن مکان فرستنده ایمیل توسط IP**		
محقق : **آرش یوسف دوست**	سطح آموزش: **متوسط-حرفه ای**	تعداد صفحات : **۱۰**
ناشر : **مقصد (www.Maghsad.com)**	نوع آموزش : **امنیت و هک**	تاریخ انتشار : **۲۸ مرداد ۱۳۸۸**
کلیه حقوق مادی و معنوی اثر برای نویسنده و ناشر محفوظ است.		قیمت : **رایگان**

بعضی مواقع ممکن است بخواهید بدانید فرستنده Email ارسالی به شما از کدام شهر و کشور است.

ممکن است افراد و گروه های مختلف به دلایلی مانند مزاحمت،کارهای تبلیغاتی و ... اقدام به شناسایی مکان فرستنده Email کنند؛ این کار را نمی توان خلاف حقوق شهروندی دانست، چون همانطور که در سایر کتاب های من (آرش یوسف دوست) نیز مطرح شد، همه چیز در اینترنت نشانی و شناسه منحصر به فرد خود را دارد و با هر فرایند ارتباطی، نشانی و مشخصات دوطرف ارتباط رد و بدل می شود. از سوی دیگر این حق شماست بدانید نامه ای که به دست شما رسیده از کجا و از طرف چه کسی است.

حداقل کمکی که انتشار این مطلب به کاربر می کند، اینست که :

۱. پیشگیری از ارتکاب جرم : کاربرانی که قصد سو استفاده از سرویس Eamil را دارند، بدانند قابل ره گیری هستند.

۲. اطمینان نسبی از صحت Email های دریافتی : به عنوان نمونه،غیر منطقی است Email ای از طرف دانشگاه شریف به دست شما رسیده باشد و کشور ارسال کننده آن، کشوری غیر ایران باشد. در این حالت باید به صحت Email شک کرد و بیشتر در باره آن تحقیق کرد.

IP چیست؟

IP شماره ایست که به هر کامپیوتر متصل به اینترنت داده میشود تا بتوان به کمک آن شماره به آن کامپیوترها دسترسی داشت و مانند اثر انگشت انسان، هر کامپیوتر را در شبکه منحصر به فرد و قابل شناسایی مب کند. این عدد برای کامپیوترهایی که حالت سرور دارند و نیز کامپیوترهای Client ای که معمولا به روشی غیر از (Dial Up) به اینترنت وصل هستند، عددی ثابت و برای دیگران عددی متغیر است. در هر بار وصل شدن به اینترنت IP شما عوض می شود؛ یعنی هر بار که شما با شرکت ISP خود تماس گرفته و به اینترنت وصل میشوید، عددی جدید به شما نسبت داده میشود.

IP یک عدد ۳۲ بیتی است و برای راحتی به صورت زیر نوشته می شود:

xxx.xxx.**xxx**.xxx

منظور از xxx عددی بین ۰ تا ۲۵۵ است (البته بعضی شماره ها قابل استفاده نیست). مثلا ممکن است آدرس شما به صورت ۱۹۵.۲۱۹.۱۷۶.۶۹ باشد. حتی اسم هایی مثل www.Maghsad.com که برای اتصال به یک سایت استفاده می کنید، در نهایت باید به یک IP تبدیل شود، تا شما سایت مقصد را ببینید.

در IP معمولا xxx اولی معنای خاصی دارد. مثلا اگر به روش شماره گیری یا همان Dial Up به اینترنت وصل شوید، معمولا عددی که به عنوان xxx اول می گیرید، مابین ۱۹۲ تا ۲۲۳ خواهد بود.این توضیح برای تشخیص کامپیوترهای کلاینت از سرور (حداقل در ایران) بسیار میتواند مفید باشد.

بعد از اتصال به اینترنت برای به دست آوردن IP خود، از دستور IPCONFIG یا در command prompt استفاده کنید.

یافتن آدرس IP :

هر بار که یک کامپیوتر به کامپیوتر دیگری متصل می شود، حداقل اطلاعاتی که باید به آن بدهد آدرس IP خود است؛ **بنابراین یافتن IP کسی که به دلیلی قصد اتصال به رایانه شما را داشته است نه تنها غیر قانونی نیست بلکه یک حق کاملاً طبیعی است.**

در زیر چند روش مناسب یافتن IP فرستنده Email را برای شما توضیح می دهیم، اما قبل از آن، نکته مهمی را یادآوری می کنیم:

اگر کسی از اینترنت قطع شود، IP او عوض می شود! پس اگر شما امروز IP کسی را به دست آورید که با خط تلفن و مودم به اینترنت وصل می شود، ممکن است ۳۰ ثانیه بعد او Disconnect کند و دوباره Connect شود که در این شرایط قاعدتاً IP دیگری خواهد داشت که این موضوع اطلاع قبلی شما را بی فایده می کند!

اگر کسی به هردلیل قصد حمله و تجاوز به حریم شخصی شما را داشت، بلافاصله IP او را به دست آورید و تمامی مدارک را نگه دارید تا از طریق آن بتوانید به طور قانونی از وی شکایت کنید.

یافتن IP ارسال کننده Email در سرویس Yahoo :

وارد ایمیل خود شوید و از طریق قسمت Options به General Preferences بروید. در قسمت Messages بخش Headers را بیابید.

در حالت پیش فرض ، عبارت Show brief headers on incoming messages انتخاب شده است. اما شما عبارت دیگر را انتخاب کنید : Show all headers on incoming messages و در پائین یا بالای صفحه ایمیل خود دکمه Save را کلیک کنید.

اکنون اگر به ایمیلی که هر شخص برای شما فرستاده است وارد شوید متوجه می شوید لیست کاملی از اطلاعات فرستنده نمایش داده شده و شما می توانید IP فرستنده را در قسمت X-Originating-IP ملاحظه کنید.

یافتن محل ارسال کننده Email :

برای اینکه Location یا موقعیت سکونت فرستنده را متوجه بشوید IP آن را در یکی از سایت های سرویس دهنده خدمات IP وارد کنید. به عنوان مثال سایت :

http://www.ip-adress.com/ipaddresstolocation

این موقعیت جغرافیایی شرکت ارائه کننده خدمات اینترنت به شخص فرستنده ایمیل نمایش داده می شود . بدیهی است در سراسر جهان همه افراد از شهر خودشان خدمات اینترنت می گیرند ، بنابراین شهر ارائه کننده خدمات

اینترنت همان شهر فرستنده ایمیل نیز می باشد. مگر آنکه شخص فرستنده ایمیل از VPN یا Proxy برای ارسال ایمیل استفاده کرده باشد.(VPN سرویسی است کهIP شخصی به افراد تعلق می دهد و IP واقعی آن ها را پنهان می کند.)

همچنین می توانید با مراجعه به این سایت :

http://www.ripe.net/perl/whois

و وارد کردن IP بدست آمده در قسمت Search، مشخصات ISP ارسال کننده را بدست آورید.

به عنوان مثال این سایت به ما می گوید آی پی ۲۱۷.۲۱۹.۱۳۶.۱۱۱ ظاهرا مربوط به دانشگاه آزاد میانه است :

netname: Mianehazuni

descr: Mianeh Azad University

country: IRAN

person: aurang kavoosi

address: Mianeh Azad University , Mianeh , East azarbaidjan , Iran

phone: +۲۲۳۷۰۴۰ ۴۲۳ ۹۸

fax-no: +۲۱۲۷۲۹۰ ۴۲۳ ۹۸

e-mail: aurang_k۲۱@hotmail.com

برای دیدن نقشه ماهواره ای کشور ان نیز می توانید از این سایت استفاده کنید :

http://www.seomoz.org/ip۲loc/ip۲loc.php

البته توجه کنید در ادرس دوم یعنی :

http://www.seomoz.org/ip۲loc/ip۲loc.php

صرفا نقشه کشور شما نشان داده می شود نه شهر صاحب IP

برای پیدا کردن شهر باید IP مورد نظر خود را در سایت اول یعنی :

http://www.ripe.net/perl/whois

جستجو کنید تامشخصات کامل ISP و به دنبال ان شهری را که از ان کانکت میشوید را با اطلاعات کامل ISP شما از جمله تلفن و ادرس انISP را نشان می دهد.

یافتن IP ایمیل سایر سرویس های Email (روش عمومی) :

هنگامی که شما یک ایمیل از فردی می گیرید، معمولاً آدرس IP وی در آن نامه وجود دارد. ابتدا باید با رفتن به قسمت تنظیمات ایمیل خود آن را در حالتی قرار دهید که تمامی Header نامه را به شما نشان دهد که با کمی گردش در قسمت تنظیمات ایمیل خود آن را پیدا خواهید کرد.

حال به بالای ایمیل دقت کنید و به دنبال عبارت Received: from باشید. شما معمولاً دو یا چند بار عبارت "Received: from" را در بالای ایمیل خواهید دید که ما فقط با پایینی کار داریم که معمولاً کمی با بالاییها فاصله دارد و بعد از Message ID قرار می گیرد. آدرس IP فرستنده ایمیل درست در ابتدای این عبارت قرار می گیرد.

اما معمولاً همانطور که اشاره شد، در پایینترین قسمت Received باید به دنبال IP باشید. با این حال در شرایطی که فقط در بالاترین قسمت Received عددی شبیه IP مشاهده کنید، IP همان است.

بسیاری از میزبانان ایمیل، راه آسانتری هم برای کمک به شما در نظر می گیرند به این صورت که قسمتی با نامی شبیه به X-Originating-IP برای شما قرار می دهند و IP فرستنده نامه را در آن می نویسند. به مثالهای زیر توجه کنید که IP فرستنده به رنگ قرمز مشخص شده است:

مثال ۱ :

Received: from yechizi@yechizi.com [۶۲.۱۴۵.۶۱.۱] by server۴PFS

(SMTPD ۷.۱۲-۳۲) id A۹۰۳۱۳۰۱۸E; Mon, ۳۰Jun ۰۰۴۳ ۲۰۰۳-۰۷۰۰

Message-Id: ;۲۰۰۳۰۶۳۰۰۱۰۴۵۰۰.SM۰۱۲۱۲@yechizi@yechizi.com<

From: yechizi@yechizi.com

Date: Mon, ۳۰Jun ۰۱:۰۶:۳۸ ۲۰۰۳-۰۷۰۰

X-RCPT-TO: yechizi@yechizi.com

Status: U

X-UIDL: ۳۴۷۷۳۱۲۳۷

مثال ۲ :

Received: from spf۱.us.outblaze.com [۲۰۵.۱۵۸.۶۲.۱۵۸] by server۴pfs

(SMTPD ۷.۱۲-۳۲) id AC۹E۵۴۰۰EA; Sat, ۰۷Jun ۰۹:۰۲:۳۸ ۲۰۰۳-۰۷۰۰

Received: (Gmail ۳۱۰۶۸invoked from network); ۷Jun ۱۶:۰۳:۳۹ ۲۰۰۳-۰۰۰۰

Received: from unknown (۲۰۵.۱۵۸.۶۲.۶۸)

by spf۱.us.outblaze.com with QMQP; ۷Jun ۱۶:۰۳:۳۹ ۲۰۰۳-۰۰۰۰

Received: (Gmail ۶۱۶۱۱invoked from network); ۷Jun ۱۶:۰۳:۳۷ ۲۰۰۳-۰۰۰۰

Received: from unknown (HELO ws۷-۱.us۴.outblaze.com) ((۲۰۵.۱۵۸.۶۲.۵۷

by ۱۵۳-۶۲-۱۵۸-۲۰۵.outblaze.com with SMTP; ۷Jun ۱۶:۰۳:۳۷ ۲۰۰۳-۰۰۰۰

مثال ۳ :

Received: (Gmail ۵۴۸۹۱invoked by uid ۱۰۰۱); ۷Jun ۱۶:۰۳:۳۵ ۲۰۰۳-۰۰۰۰

Message-ID: ;۲۰۰۳۰۶۰۷۱۶۰۳۳۵.۵۴۸۸۹.qmail@mail.com<

Content-Type: multipart/mixed; boundary="----------=_"۰-۵۴۳۷۰-۱۰۵۵۰۰۱۸۰۹

Content-Transfer-Encoding: ۷bit

MIME-Version: ۱.۰

X-Mailer: MIME-tools ۵.۴۱(Entity ۵.۴۰۴)

Received: from [۲۱۷.۲۱۸.۵۷.۵۵] by ws۷-۱.us۴.outblaze.com with http for

yechizi@yechizi.com; Sat, ۰۷Jun ۱۱:۰۳:۲۹ ۲۰۰۳-۰۵۰۰

From: "Reza "

To: yechizi@yechizi.com

Date: Sat, ۰۷Jun ۱۱:۰۳:۲۹ ۲۰۰۳-۰۵۰۰

Subject: The Interactive Matrix

X-Originating-Ip: ۲۱۷.۲۱۸.۵۷.۵۵

X-Originating-Server: ws۷-۱.us۴.outblaze.com

X-RCPT-TO :

Status: U

X-UIDL: ۳۴۴۳۹۳۳۵۰

یک استثنا:

اگر فرد برای فرستادن ایمیل از فرمهای موجود در برخی سایتها مانند سایتهایی که اجازه ارسال یک خبر یا کارت را می دهند یا سایتهایی که ادعای ارسال ایمیل فارسی را دارند (هرچند واقعاً فارسی تایپ کردن در یاهو از اکثر آنها بهتر است) یا فرمهای "تماس با ما" در سایتها استفاده کنند، بعید است IP آنها در ایمیل شما باشد و معمولاً IP سرور خود سایت را در آن می بینید. در مثال زیر که ایمیلی است که با استفاده از فرم "تماس با ما" سایت همسفر برای مدیر آن ارسال شده بوده است، فقط IP خود همسفر را مشاهده می کنید:

Received: from server۴pfs [۳۸.۱۱۸.۱۴۳.۹۸] by hamsafar.com with ESMTP

(SMTPD ۷.۱۲-۳۲) id A۵C۵۴۴۰۰DC; Sat, ۰۷Jun ۰۶۵۳ ۲۰۰۳-۰۷۰۰

From :

To :

Subject: hadirayaneh

Date: Sat, ۷Jun ۰۶۵۳ ۲۰۰۳-۰۷۰۰

Message-ID: ;۰۰۰۳۰۱c۳۲cf۱۰۴۶$۷b۶۲۸$۷۴۰f۷۶۲۶@server۴pfs<

MIME-Version: ۱.۰

Content-Type: text/plain;

charset="iso-"۱-۸۸۵۹

Content-Transfer-Encoding: ۷bit

X-Mailer: Microsoft CDO for Windows ۲۰۰۰

Thread-Index: AcMs۹xBGKda۵j۵B/RZms۱WTby۶vhkQ==

Content-Class: urn:content-classes:message

X-MimeOLE: Produced By Microsoft MimeOLE V۶.۰۰.۲۸۰۰.۱۱۶۵

X-RCPT-TO :

Status: U

X-UIDL: ۳۴۷۷۳۰۷۵۳

برای دریافت رایگان سایر کتاب های آموزش گام به گام و تصویری منتشر شده توسط انتشارات مقصد، به نشانی www.Book.Maghsad.com یا www.Maghsad.ws مراجعه فرمایید.

صاحب نظران،نویسندگان و محققین محترم می توانند نظرات، مقالات و آموزش های تالیفی و ترجمه ای خود، از طریق نشانی Book.Maghsad@Gmail.com مطرح و ارسال نمایند.