هدف ردیابی ایمیل ها (Email Tracing) استخراج اطلاعات مرتبط با ایمیل های دریافتی است چرا که بسیاری از مهاجمان با دستکاری سرآیند ایمیل اقدام به ارسال ایمیل‌های جعلی می‌نمایند. این اطلاعات شامل آی پی ارسال کننده ایمیل، گام‌های ارسالی از مبداء تا مقصد، اطلاعات whois دامنه ارسالی و ISP می‌باشد. در طول انجام این آزمایش و تدوین این نوشتار سعی شده است تا به سوالات مطرح شده در CEH Lab Manual فصل ۲ (آزمایش ۷) نیز پاسخ داده شود.

Questions

1. What is the difference between tracing an email address and tracing an email message?
2. What are email Internet headers?
3. What does "unknown" mean in the route table of the identification report?
4. Does eMailTrackerPro work with email messages that have been forwarded?
5. Evaluate whether an email message can be traced regardless of when it was sent.

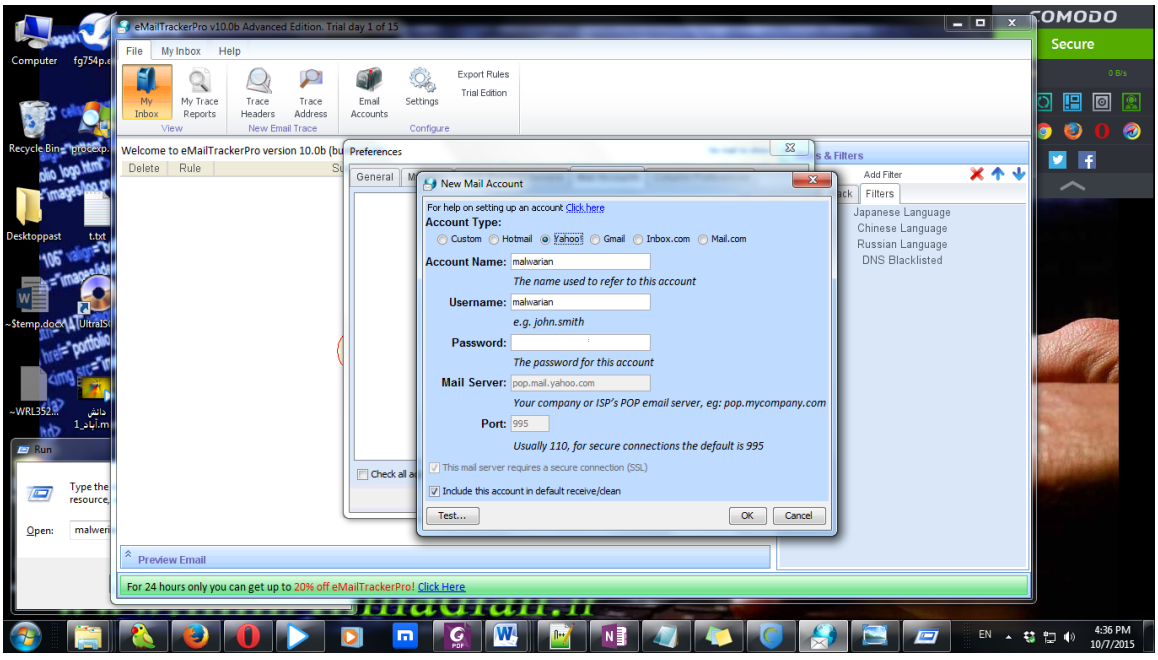
به طور کلی ردیابی ایمیل رویکردی است که از آن برای نظارت بر ایمیل‌های دریافتی استفاده می شود تا:
ایمیل‌های مخرب شناسایی شوند.

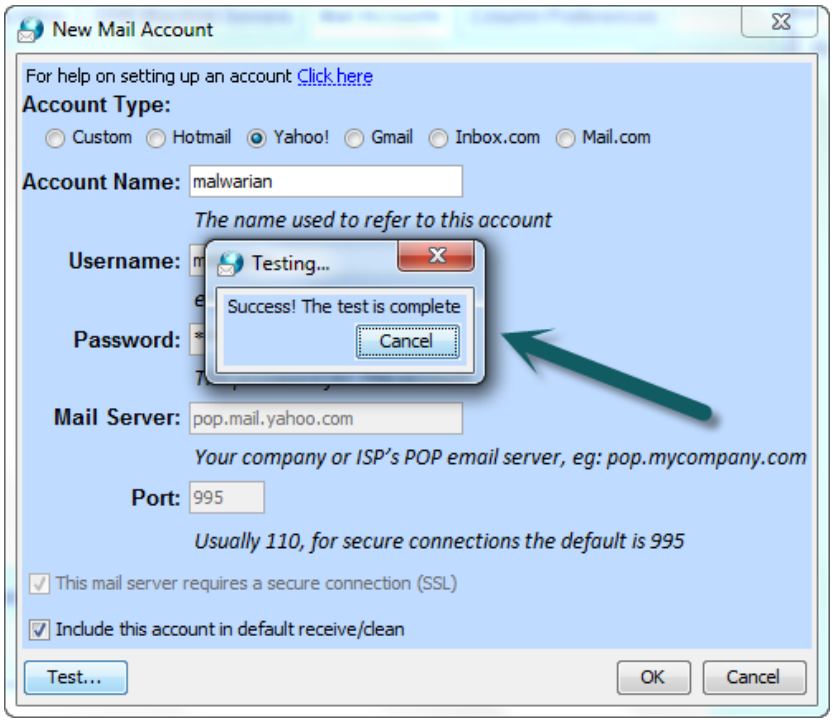
- موقعیت ارسال و نقشه مسیر ارسالی به گیرنده مشخص گردد.
- مدت زمان خواندن ایمیل مشخص گردد.
- مشخص گردد که گیرنده نامه به لینک‌های درون نامه دسترسی پیدا کرده است یا نه.
- ضمیمه‌های ارسالی نامه مشخص گردد.
- اگر بازه زمانی برای انقضای اعتبار نامه تنظیم شده است مشخص گردد.

eMailTrackPro، برنامه است به منظور ردیابی نامه‌های دریافتی که سعی می‌کند موقعیت ردیابی گام های طی شده را در قالب یک نقشه GUI نمایش دهد.اطلاعات این نقشه بر اساس گام‌های طی شده بسته توسط پروتکل IP در مسیریاب های مسیر صورت می‌گیرد و در نهایت اطلاعات عمومی نامه مورد تحلیل شامل فرستنده و دریافت کننده نامه، تاریخ و موضوع نامه و موقعیت ارسالی نامه مشخص می‌گردد.

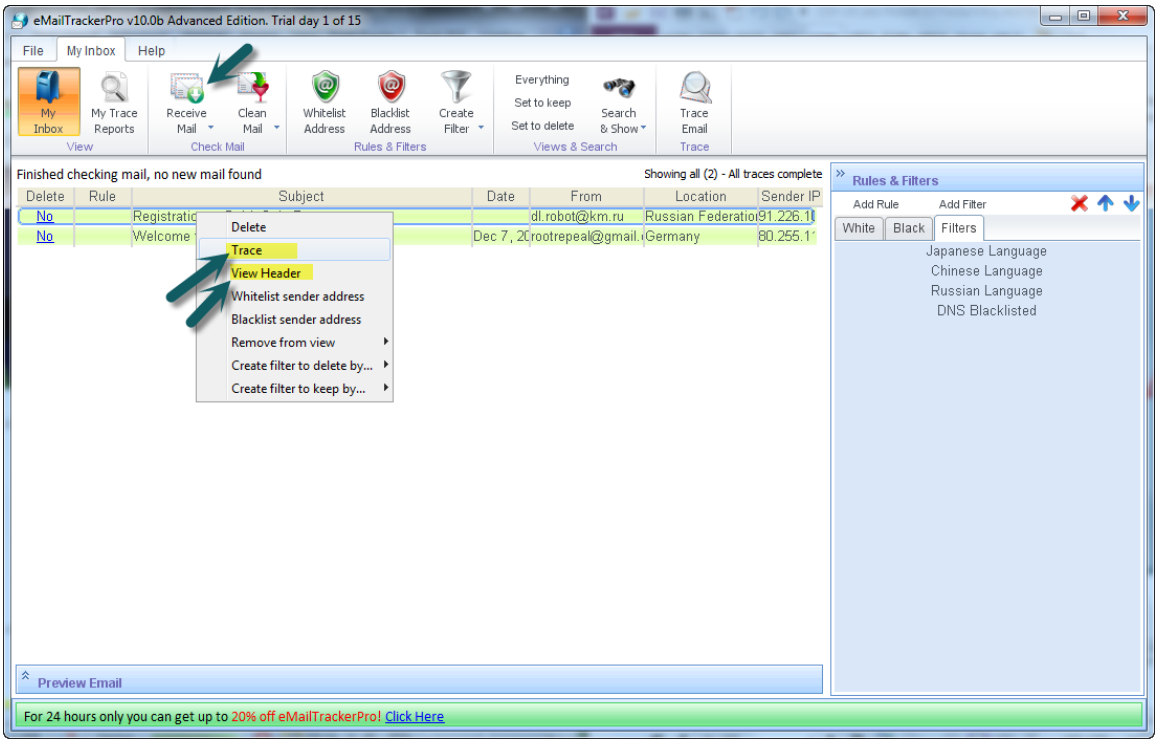
برای انجام این آزمایش ابتدا نیاز به نصب این برنامه داریم .البته لازم به ذکر است که به علت تحریم در حال حاضر تنها با فیلترشکن یا VPN امکان نصب این برنامه وجود دارد.

بعد از نصب این برنامه در ابتدا می‌توان اطلاعات حساب ایمیل مورد نظر را در برنامه وارد کرده و تست انجام اتصال به سرور POP آن را مطابق تصاویر ذیل انجام داد.

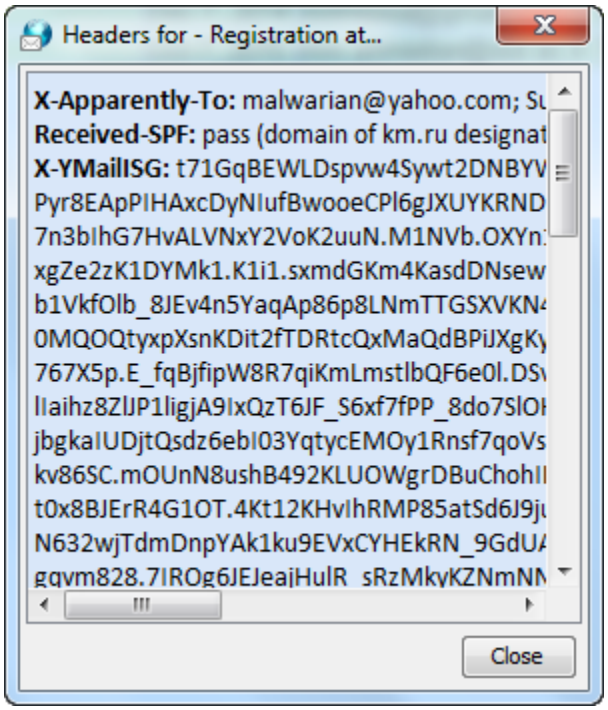




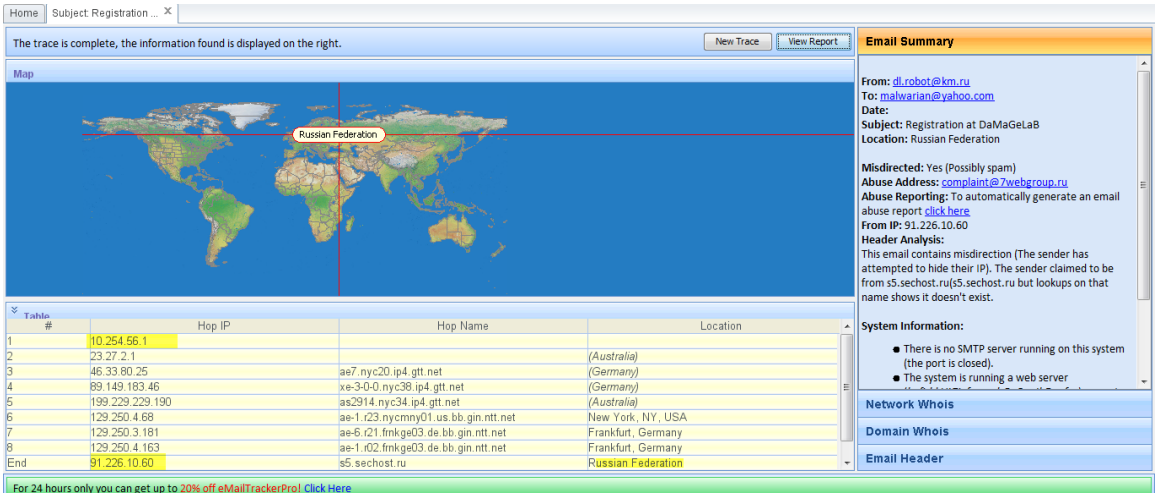
بعد از تنظیم اطلاعات حساب و اتصال برنامه به سرور میل می‌توانیم با کلیک بر روی دکمه ReciveMail مطابق تصویر ذیل ایمیل‌های درون صندوق ایمیل خود را در این برنامه بارگذاری نماییم.



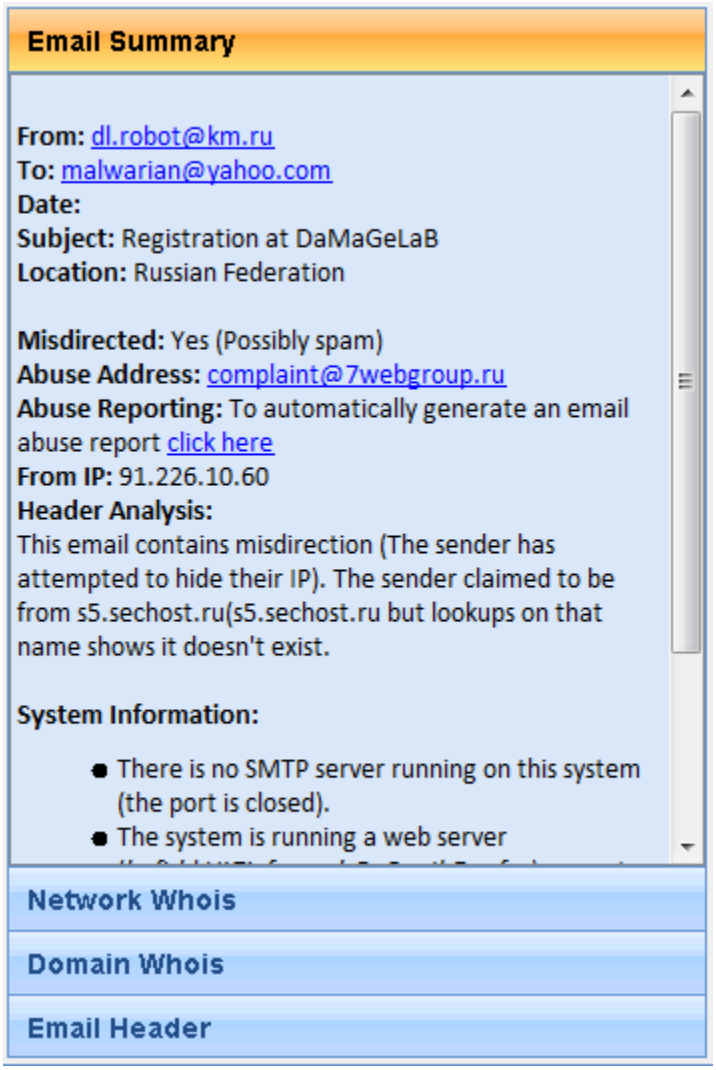
با کلیک راست نمودن روی هر نامه دریافتی می توان ایمیل مورد نظر را ردگیری نمود یا سرآیند آن را مشاهده نمود. به طور کلی سرایند یک ایمیل در لایه کاربرد تعریف میگردد و شامل فیلدهای متعددی است که به کمک آن میل سرور قادر به مدیریت نامه ها و نمایش بدنه ایمیل به کاربران می باشد.



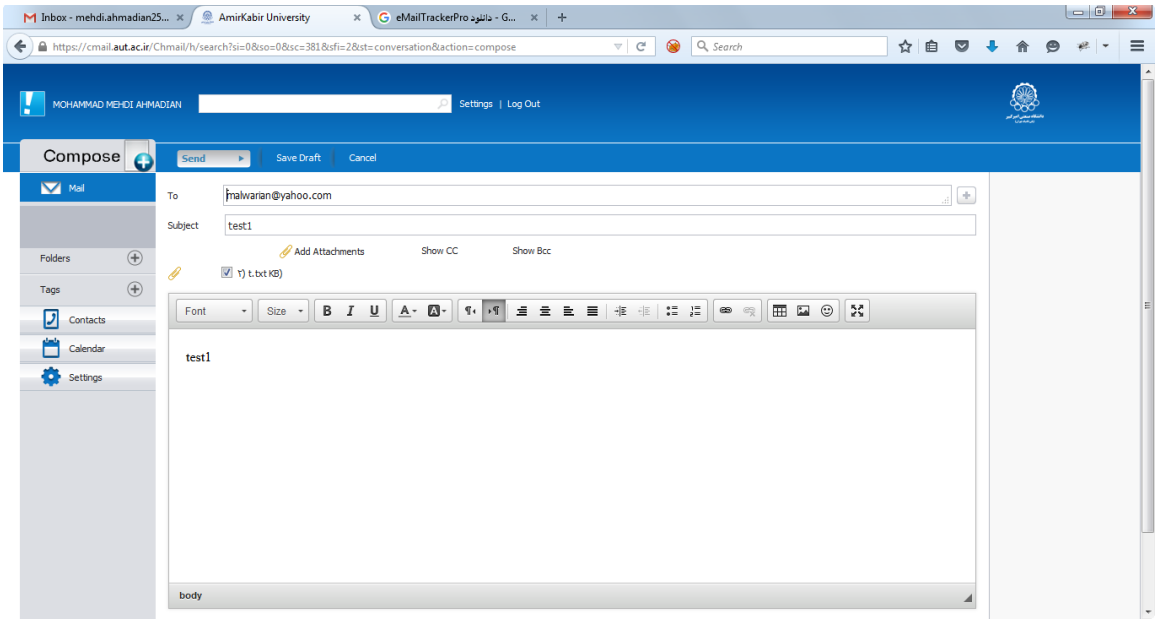
همانطور که در تصویر ذیل مشاهده می‌کنید برای یک نمونه نامه فرایند ردیابی صورت گرفته است.



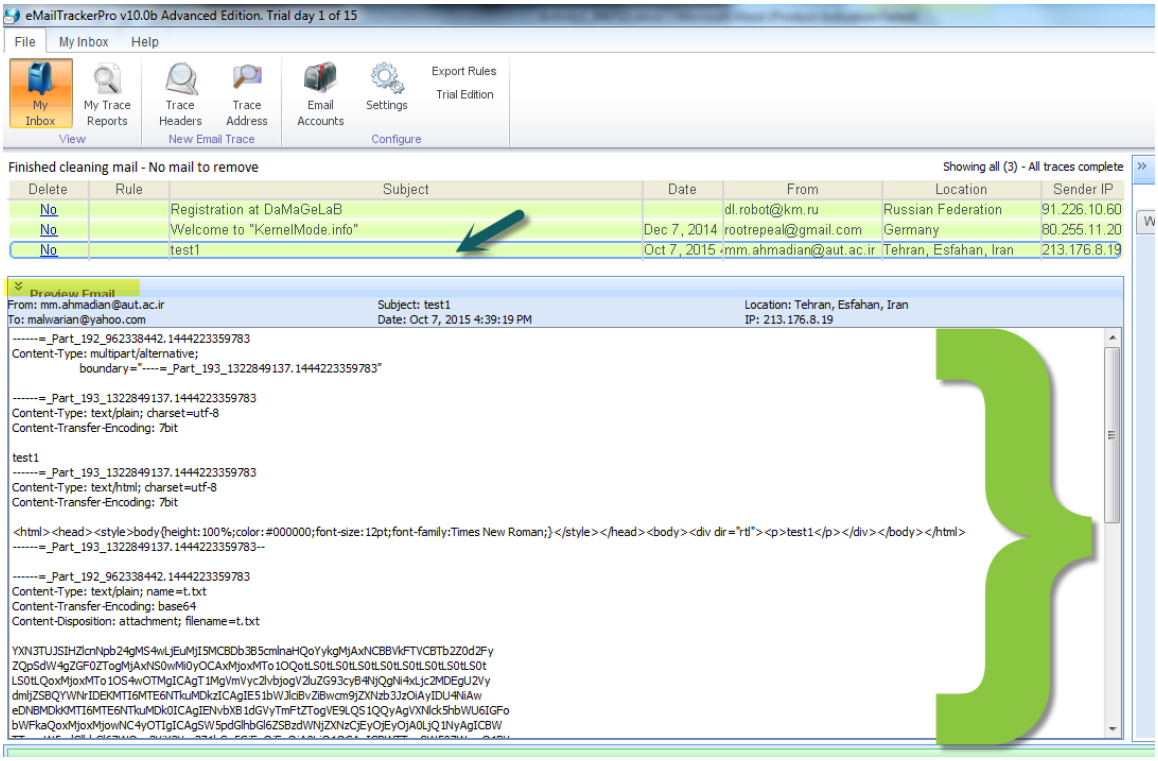
در سمت راست این تصویر اطلاعات جزئی تر این ردیابی به شکل ذیل مشهود است.



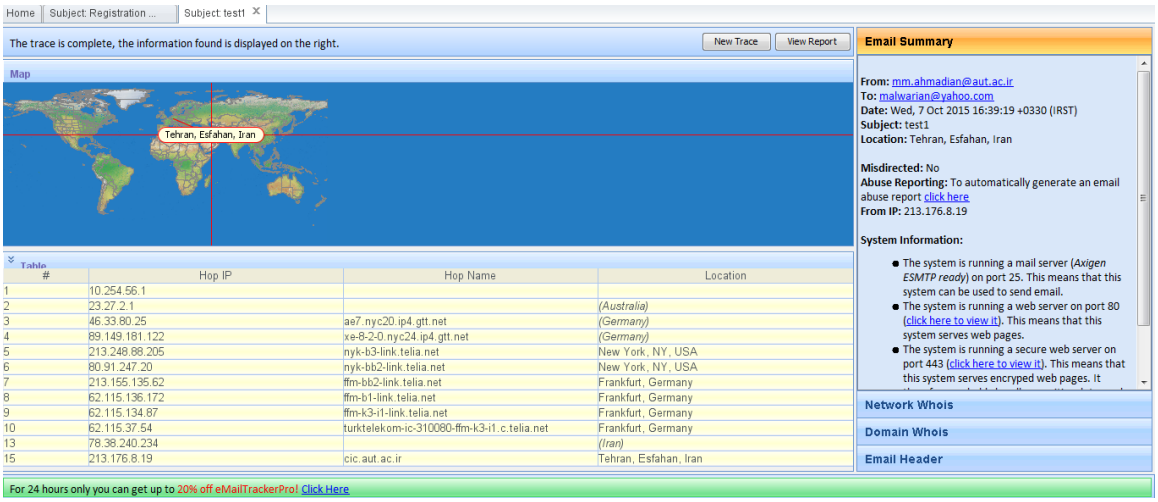
جهت بررسی دقیق فرایند ردیابی نامه های دریافتی توسط برنامه eMailTrackPro ابتدا از میل سرور داخلی دانشگاه صنعتی امیرکبیر نامه‌ای را به حساب تنظیم کرده در eMailTrackPro به شکل ذیل ارسال می‌کنیم.



حال بعد از دریافت و بارگذاری نامه دریافتی اقدام به بررسی و ردیابی نامه دریافتی به شکل ذیل می نماییم.



در تصویر ذیل مبدا ارسال پیام به شکل ذیل مشخص گردیده است.



با کلیک بر روی دکمه ViewReport می‌توان گزارش خروجی توصیفی این ردیابی را به شکل ذیل مشاهده نمود.

Computer **213.176.8.19** has been found. It is almost certainly located in **Tehran, Esfahan, Iran** as it has an exact match in the eMailTrackerPro database.

This system is a mail, web and secure web server (click here for details).

Network Contact Information: The following details refer to the network that the system is on.

+98 21 6469961
Computer and Information Center Amir Kabir University of Technology Hafez Ave. No 424 Tehran Iran

Click here to hide the in-depth information on this email *(more info)*

- The sender's IP in this case is taken from a 'Received' header stamp from a different server to the one the sender first communicated with because the IP in that line was not usable.
  The closest tracable IP to the sender was - 213.176.8.19

- The sender of this email appeared to have the address mm.ahmadian@aut.ac.ir. This information is easily faked so should not be treated as conclusive.

Click here to hide the route map *(more info)*

The following map shows the route between you and the entity to which you traced. A solid line represents a hop to a known location, and a dotted line represents a hop to a guessed location.

Click here to hide information on each hop along the route *(more info)*

The table below identifies the Internet route taken to reach the destination requested.

This is valuable data when tracking the end location because it helps qualify the actual final position. In some instances the final location has been derived from the network registration details, which is often the head office location for the Internet Service Provider (ISP). The ISP location is often local to the destination traced, but sometimes also located elsewhere, particularly in the case of large national ISPs. The physical (authoritative) locations of systems in last 2 or 3 hops of the route provide helpful location information as they are often in the vicinity of the destination being traced. Authoritative locations are shown in **bold**, locations derived from registration details appear in *italic*.

Address of Hop	Name of Hop	Location
10.254.56.1		(Private)
23.27.2.1		*Australia*
46.33.80.25	ae7.nyc20.ip4.gtt.net	*Germany*
89.149.181.122	xe-8-2-0.nyc24.ip4.gtt.net	*Germany*
213.248.88.205	nyk-b3-link.telia.net	**New York, NY, USA**
80.91.247.20	nyk-bb2-link.telia.net	**New York, NY, USA**
213.155.135.62	ffm-bb2-link.telia.net	**Frankfurt, Germany**
62.115.136.172	ffm-b1-link.telia.net	**Frankfurt, Germany**
62.115.134.87	ffm-k3-i1-link.telia.net	**Frankfurt, Germany**
62.115.37.54	turktelekom-ic-310080-ffm-k3-i1.c.telia.net	**Frankfurt, Germany**
78.38.240.234		*Iran*
213.176.8.19	cic.aut.ac.ir	**Tehran, Esfahan, Iran**

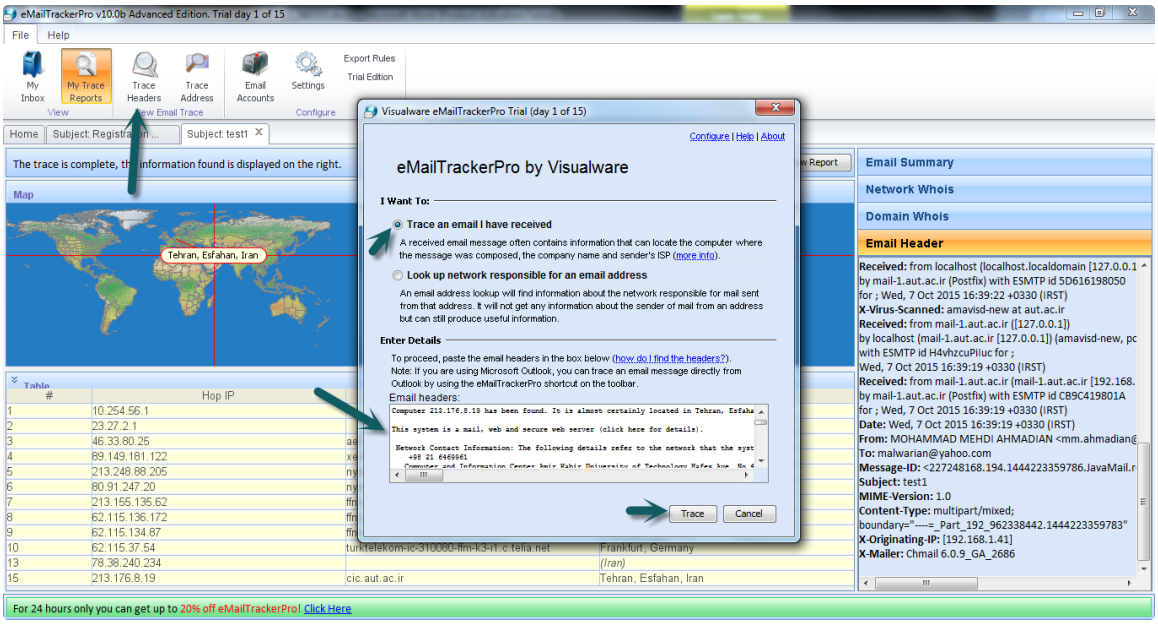
ردیابی گام های عبوری ایمیل ارسالی مشخص می‌کند این ایمیل از مسیر ایران،آلمان،امریکا،استرالیا عبور کرده است تا به یک آی پی اختصاصی برسد.در جدول ذیل جزئیات ردیابی انجام شده شامل بررسی اجمالی نامه ارسالی،استعلام شبکه ارسالی،استعلام دامنه ارسال کننده نامه و سرایند نامه مشخص شده است. در جدول ذیل توجه به بخش های Hilight شده خالی از لطف نیست.

#	عنوان اطلاعات	جزئیات
۱	Email Summary	**From:** mm.ahmadian@aut.ac.ir **To:** malwarian@yahoo.com **Date:** Wed, 7 Oct 2015 16:39:19 +0330 (IRST) **Subject:** test1 **Location:** Tehran, Esfahan, Iran **Misdirected:** No

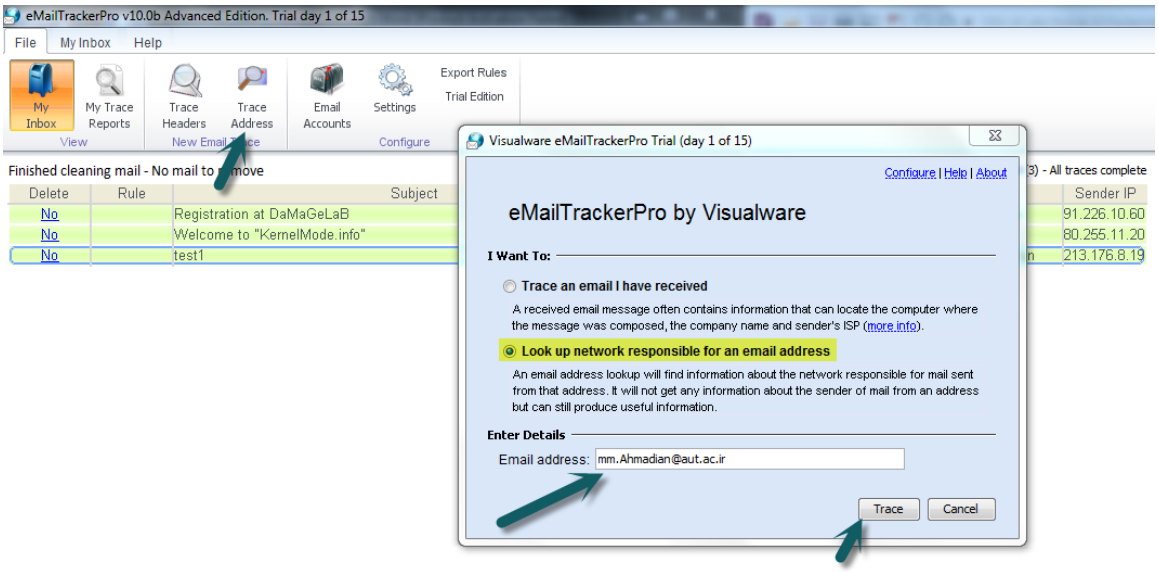
Abuse Reporting: To automatically generate an email abuse report click here **From IP:** 213.176.8.19 **System Information:** • The system is running a mail server (*Axigen ESMTP ready*) on port 25. This means that this system can be used to send email. • The system is running a web server on port 80 (click here to view it). This means that this system serves web pages. • The system is running a secure web server on port 443 (click here to view it). This means that this system serves encryped web pages. It therefore probably handles sensitive data, such as credit card information. • There is no FTP server running on this system (the port is closed).		
This is the RIPE Database query service. % The objects are in RPSL format. % % The RIPE Database is subject to Terms and Conditions. % See http://www.ripe.net/db/support/db-terms-conditions.pdf % Note: this output has been filtered. % To receive output for a database update, use the "-B" flag. % Information related to '213.176.8.0 - 213.176.8.255' % Abuse contact for '213.176.8.0 - 213.176.8.255' is 'ipdomain@irost.com' **inetnum:** 213.176.8.0 - 213.176.8.255 **netname:** AKU **descr:** Amir Kabir University of Technology **descr:** Tehran **country:** IR **admin-c:** SL13-RIPE **tech-c:** MR26-RIPE **status:** ASSIGNED PA **mnt-by:** IROST-MNT **created:** 2002-03-13T11:11:14Z **last-modified:** 2002-03-13T11:11:14Z **source:** RIPE # Filtered **person:** Mitra Rezazadeh **address:** Computer and Information Center **address:** Amir Kabir University of Technology **address:** Hafez Ave. No 424 **address:** Tehran **address:** Iran **phone:** +98 21 6469960 **fax-no:** +98 21 6469961 **nic-hdl:** MR26-RIPE **mnt-by:** IROST-MNT **created:** 1970-01-01T00:00:00Z **last-modified:** 2001-09-22T03:24:03Z **source:** RIPE # Filtered **person:** Saied Mohammad Taghi Lavasani **address:** Computer and Information Center **address:** Amir Kabir University of Technology **address:** Hafez Ave. No 424 **address:** Tehran **address:** Iran **phone:** +98 21 640 6689 **fax-no:** +98 21 646 9961 **nic-hdl:** SL13-RIPE **mnt-by:** IROST-MNT **created:** 1970-01-01T00:00:00Z **last-modified:** 2001-09-22T03:24:03Z	Network Whois	۲

source: RIPE # Filtered % This query was served by the RIPE Database Query Service version 1.80.1 (DB-4)		
Domain information could not be found for 213.176.8.19.	Domain Whois	۳
Received: from localhost (localhost.localdomain [127.0.0.1]) by mail-1.aut.ac.ir (Postfix) with ESMTP id 5D616198050 for ; Wed, 7 Oct 2015 16:39:22 +0330 (IRST) **X-Virus-Scanned:** amavisd-new at aut.ac.ir **Received:** from mail-1.aut.ac.ir ([127.0.0.1]) by localhost (mail-1.aut.ac.ir [127.0.0.1]) (amavisd-new, port 10024) with ESMTP id H4vhzcuPiluc for ; Wed, 7 Oct 2015 16:39:19 +0330 (IRST) **Received:** from mail-1.aut.ac.ir (mail-1.aut.ac.ir [192.168.1.40]) by mail-1.aut.ac.ir (Postfix) with ESMTP id CB9C419801A for ; Wed, 7 Oct 2015 16:39:19 +0330 (IRST) **Date:** Wed, 7 Oct 2015 16:39:19 +0330 (IRST) **From:** MOHAMMAD MEHDI AHMADIAN <mm.ahmadian@aut.ac.ir> **To:** malwarian@yahoo.com **Message-ID:** <227248168.194.1444223359786.JavaMail.root@mail-1.aut.ac.ir> **Subject:** test1 **MIME-Version:** 1.0 **Content-Type:** multipart/mixed; boundary="----=_Part_192_962338442.1444223359783" **X-Originating-IP:** [192.168.1.41] **X-Mailer:** Chmail 6.0.9_GA_2686	Email Header	۴

البته در برنامه eMailTrackPro می‌توان تصویر ذیل با کلیک بر روی دکمه Traceheader و وارد نمود سرآیند نامه(بدون حتی تعریف حساب کاربری) در حد عمومی تر سرآیند مورد نظر را بررسی کرد.



یکی دیگر از امکانات این برنامه امکان ردیابی یک آدرس ایمیل به شکل ذیل است که تنها اطلاعاتی در مورد میل سرور آدرس مورد نظر و محل و آی پی آن می‌دهد و اما برخلاف روش ردیابی متن ایمیل‌ها دراین شیوه بر اساس صرفا آدرس ایمیل مقصد هیچ اطلاعات دیگری در مورد صاحب حساب ایمیل نمی‌توان گرداوری نمود.



پاسخ سوالات باقی مانده:

این نکته قابل توجه است که این برنامه در ردیابی نامه های Forward شده ارسال کننده نامه را همان شخصی تصور میکند که نامه را Forward کرده است. البته اگر نامه Forward شده در قالب ضمیمه Forward شده باشد با باز کردن سرآیند آن می توان فرستند اصلی آن را دریابی نمود(پاسخ سوال ۴).

در صورتی که این برنامه نتواند در ردیابی گام های بسته آی پی اطلاعاتی را جمع آوری کند این امر حاکی از وجود فایروال‌هایی در این گام ها می باشد که اجازه دسترسی به پورت ۴۳ را مسدود کرده اند(از این پورت جهت IP location lookups استفاده می گردد(پاسخ سوال ۳).

اطلاعات ردیابی بر اساس اطلاعات آی پی های موجود در بسته ایمیل دریافتی میباشند و چناچه ای پی ها ردیابی شده تغییر نمایند این اطلاعات بر اساس بسته قدیمی به دست آمده اند(پاسخ سوال ۵).