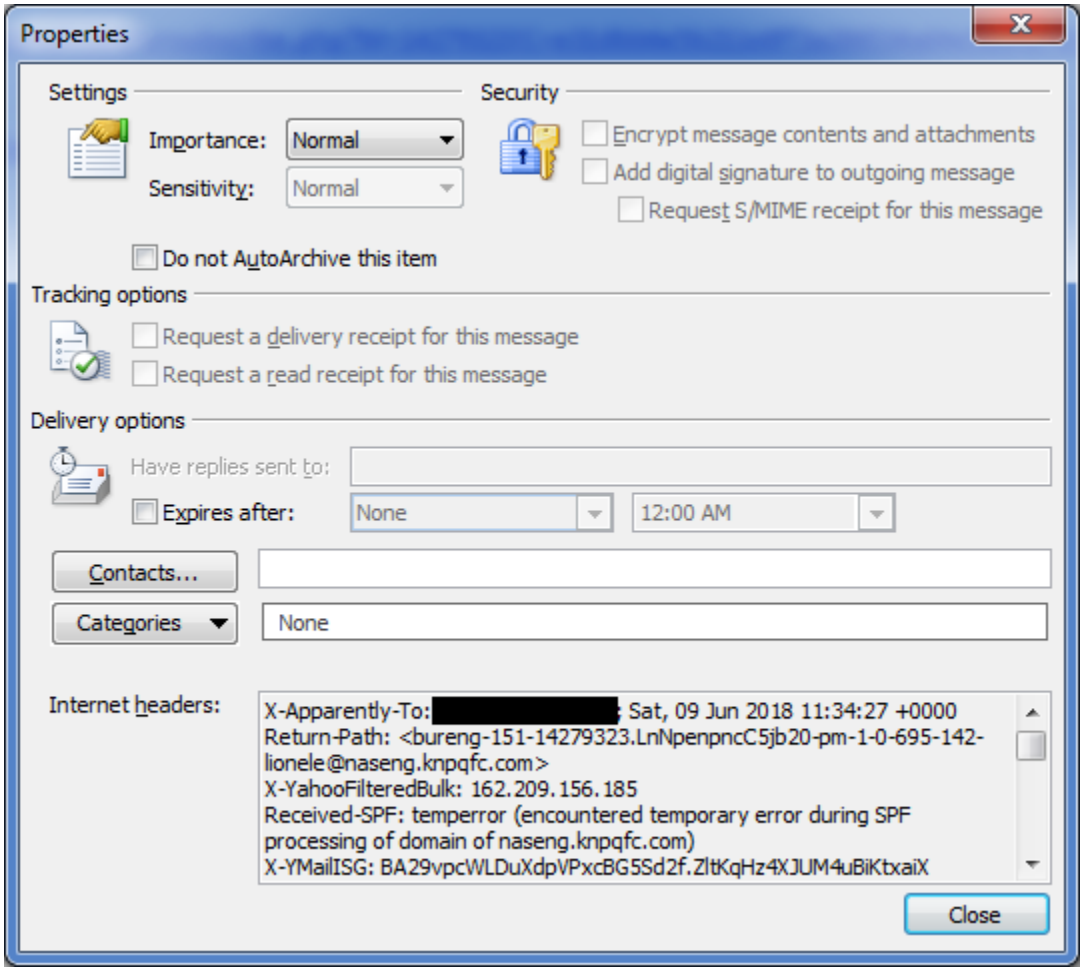
Message

The **Message** group of the Info tab contains information about the original message.

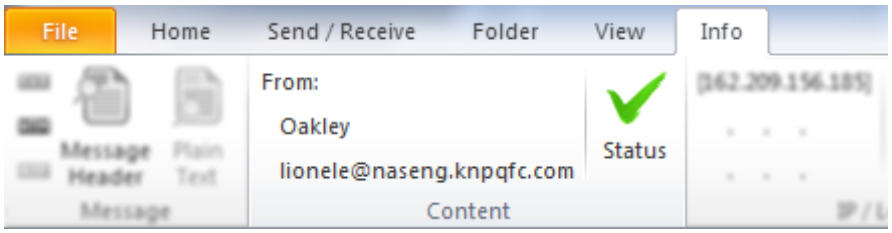
- **TXT/HTM/RTF** icons show the type of the original message - it does not depend if Outlook was set to read the message in a different format (say it was set to read all messages in Plain Text)

- **Message Header** button provides an easy way to get the header information of the currently selected e-mail. It provides the same information Outlook provides under "Internet headers:" but before having to open the e-mail message:



- **Plain Text** button will allow you to read an e-mail message in plain text to prevent any HTML/RTF code execution, but will only work if the e-mail was not already sent in plain text format or Outlook was not set to read all messages in Plain Text.

Content



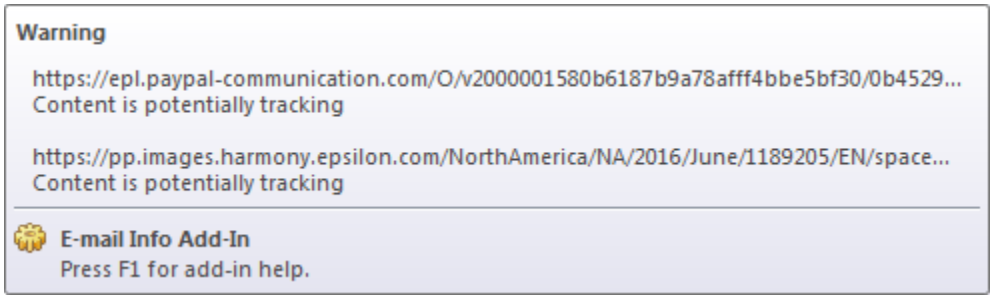
The **Content** group of the Info tab contains the sender information and validation information in regards to the currently selected e-mail.

- E-mail name displayed by Outlook
- The actual e-mail address from which the message was sent
- The **Status** icon can have three possible states. It represents a number of checks that are being performed on the current e-mail. Initially, every e-mail has an OK status but as various items like attachments and links are processed, the status might change.

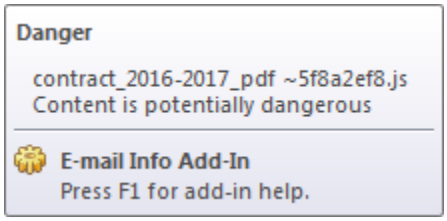
  Hovering over the **Status** icon will show the issues encountered which caused the icon to change from the OK status.

indicates that no known error was encountered

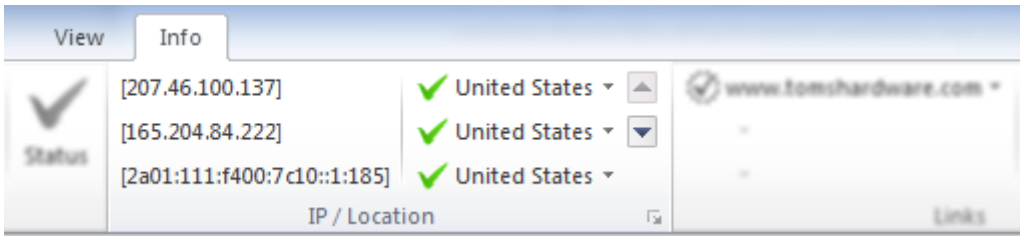
implies some warnings have occurred, for example if the e-mail contains a tracking image (1x1 GIF images that companies use to track if the e-mail was opened or not)



implies some more serious content in the e-mail (for example some executable attachments or files that Microsoft considers dangerous)

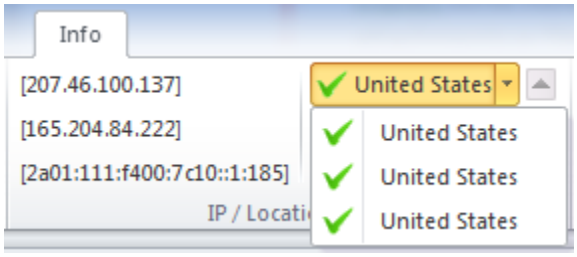


IP / Location

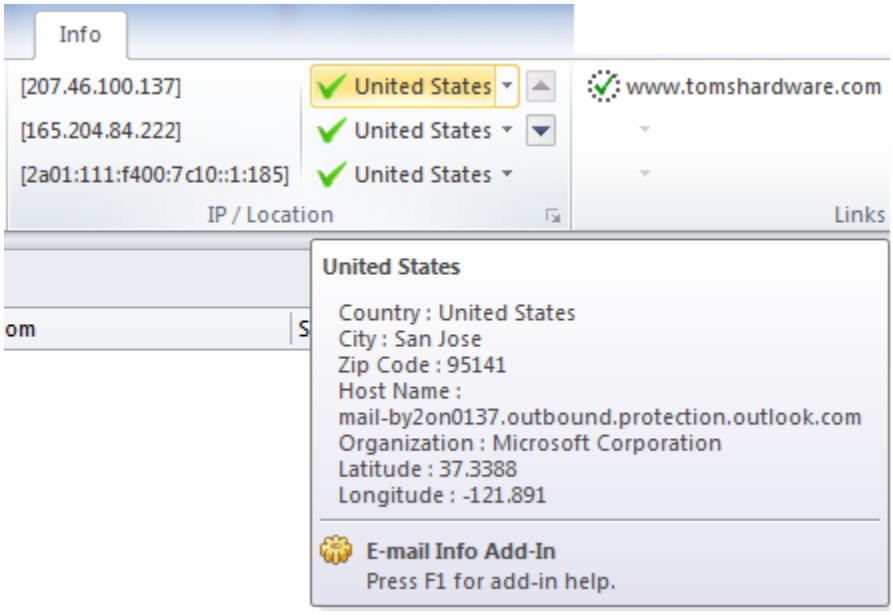


The **IP / Location** group of the Info tab contains information about the servers that processed this e-mail message. This information and more is found in the message header. The IP of the servers that processed this e-mail is shown. The IP information is ran against GeoIP providers to get detailed location information. Both IPv4 and IPv6 formats are handled though only some of the GeoIP providers handle both formats. By checking the IPs embedded in the message header, it can be determined where the e-mail is coming from.

The information provided by GeoIP providers is not always 100% accurate, though most providers try to stay within a 99% accuracy. To increase the accuracy of the information, up to 4 GeoIP providers can be used to get data for each IP address.

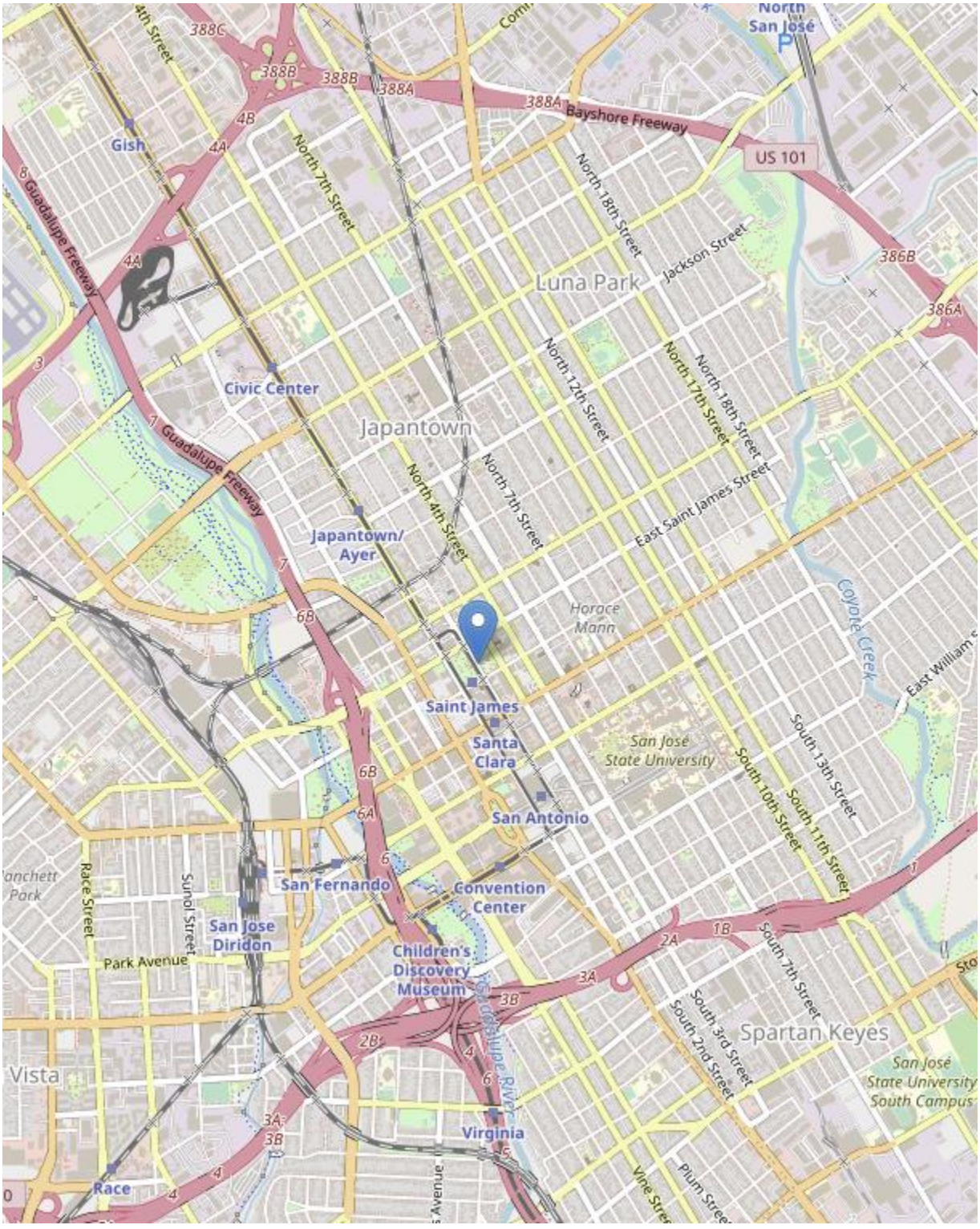


The location information obtained from the GeoIP providers can be viewed by hovering over the buttons showing the country.

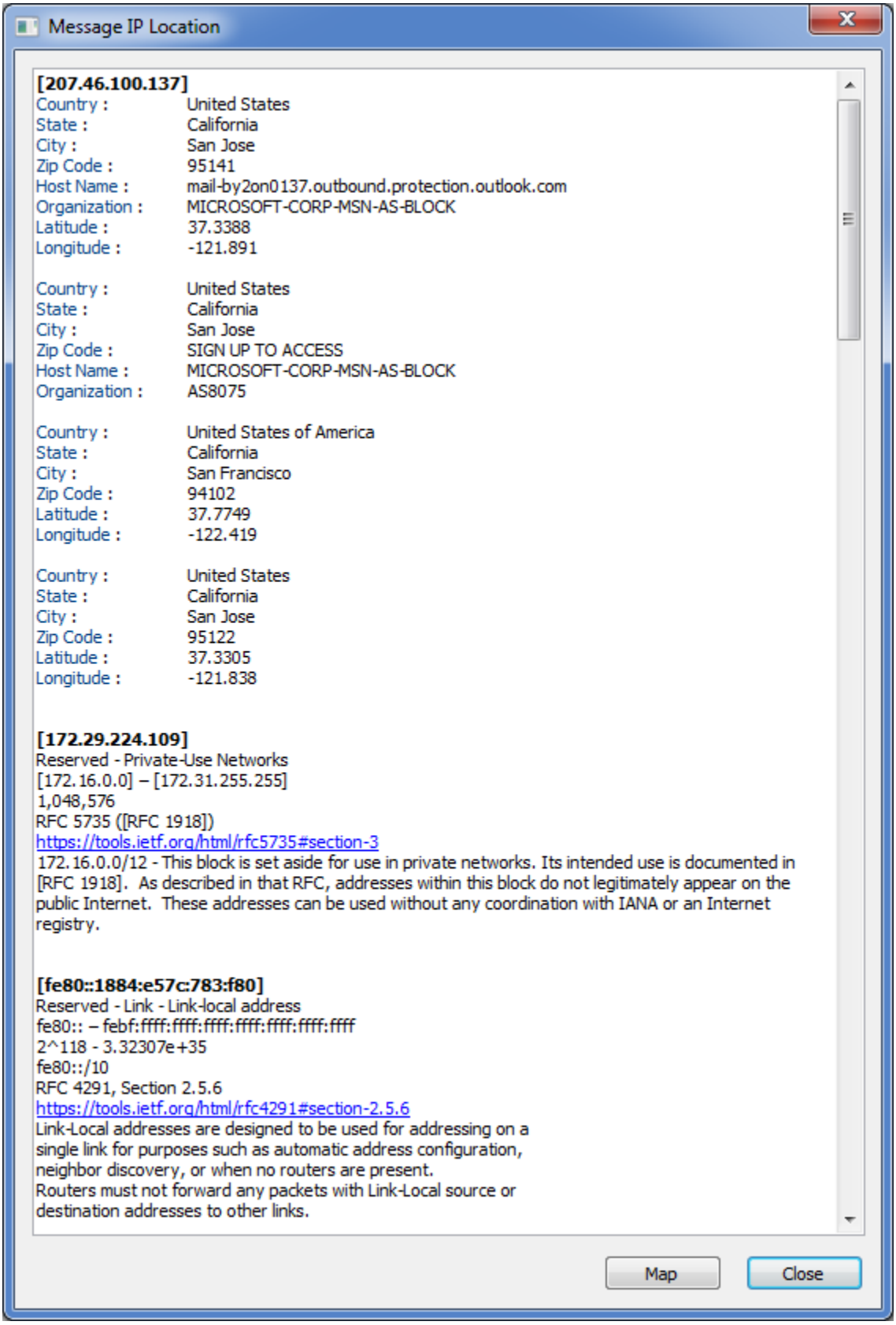


Clicking on the country button will bring up a web-browser that will use the latitude and longitude returned by the GeoIP provider to point to a map location around the world to get a better idea on where the e-mail was sent from.

Note: the mapping location information is just an approximation!

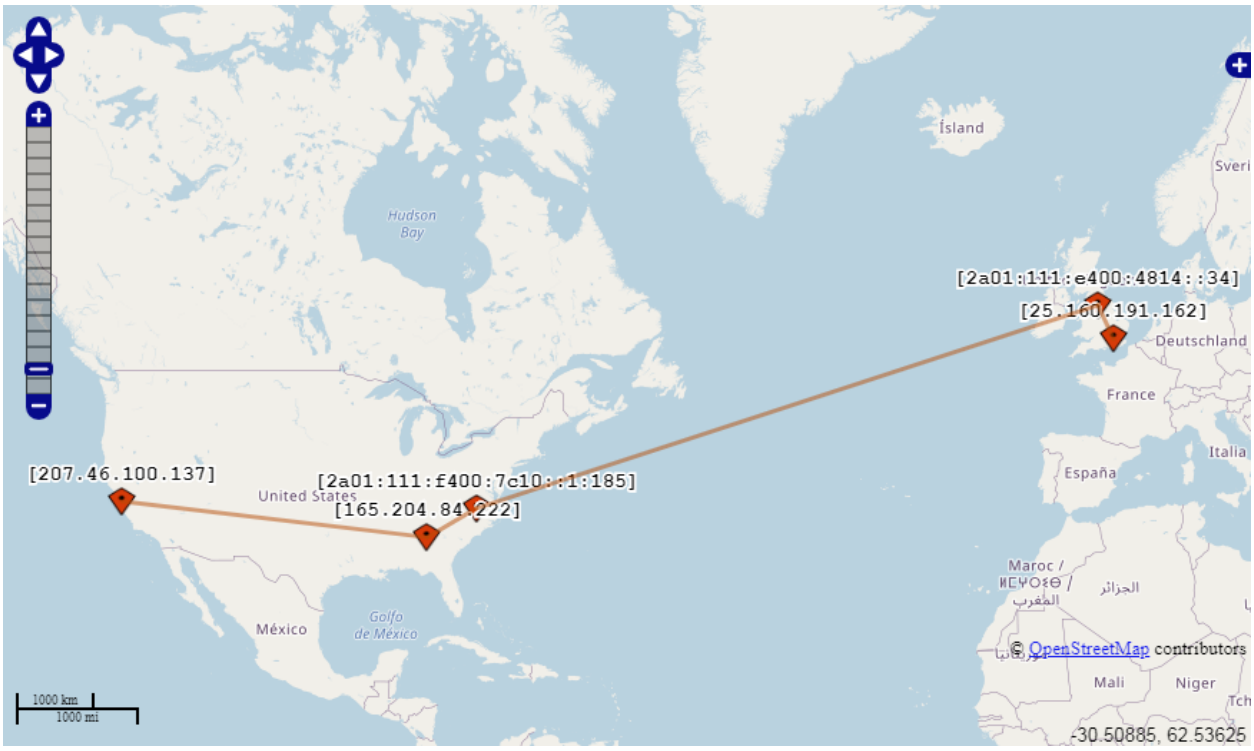


In addition to the IP location displayed, the e-mail can pass through internal servers and other reserved IP addresses. This additional information can be viewed by clicking the dialog box launcher.

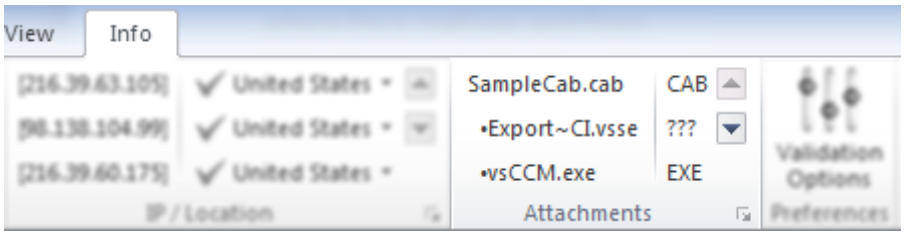


It is also possible to map all the server locations on the world map (by clicking the Map button), to easily see through which locations the e-mail has passed through.

Note: as some corporations have servers located in multiple countries, the information obtained from different GeoIP providers might point to different world locations.



Attachments



The **Attachments** group of the Info tab contains information about the attachments contained in the current e-mail. If there are no attachments, this group will not be displayed.

The attachments are checked against a list of common file signatures to validate if the files are indeed of the type the extension suggests. Some compound file types like zip/cab/etc… are also inspected internally to check their contents. Due to the large number of files types, it is really not possible to check against all existing file types. Unrecognized file types will be marked as **???**.

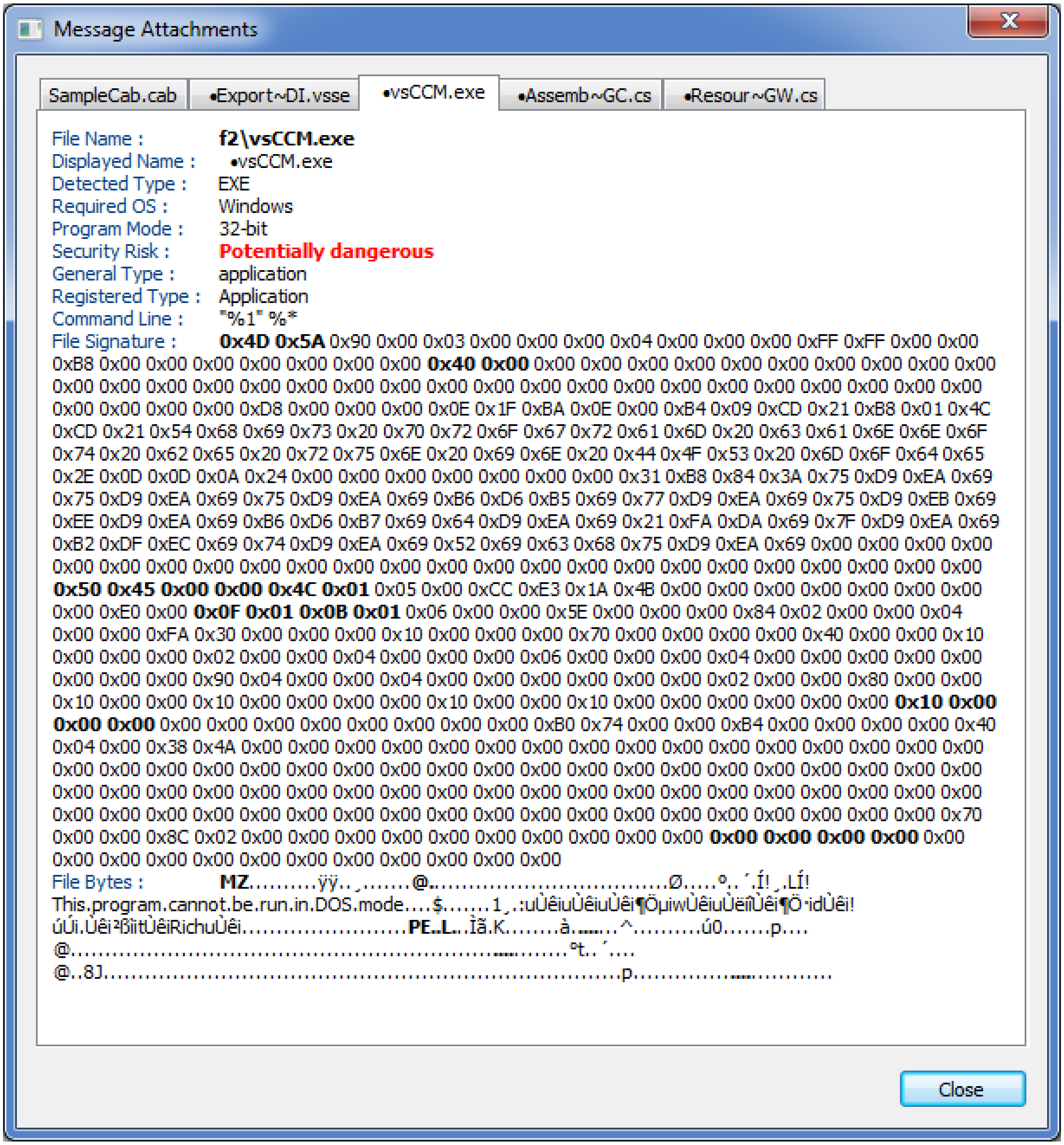
Clicking on the file name will allow the user to save the file to disk. This will also allow to save files that Outlook blocks for security measures. As such, **use this feature at your own risk** and only when you're certain the attachment comes from a trusted source.

Note: contents of compound files are not saved to disk.

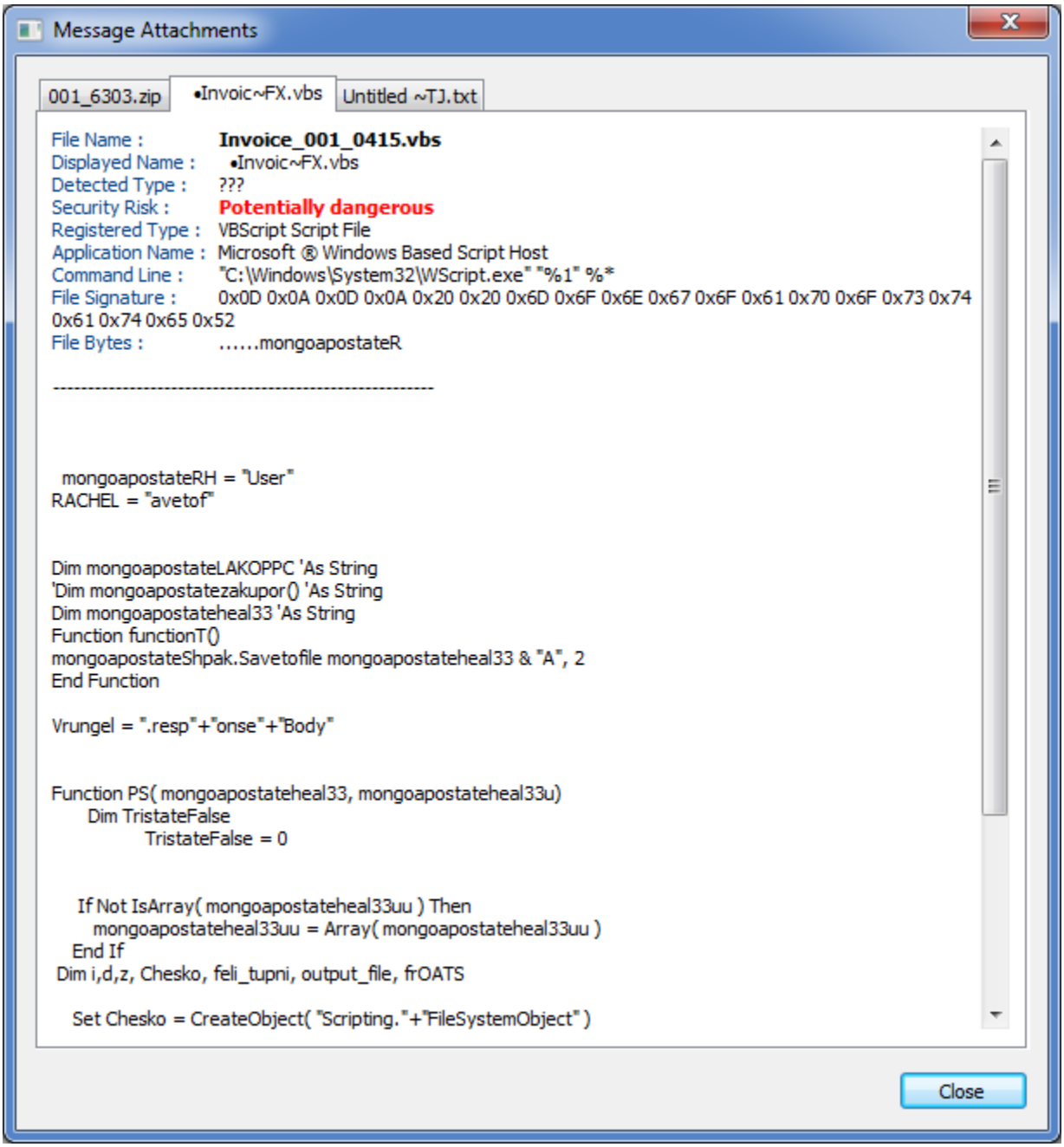
To get detailed information in regards to the file content, click on the dialog box launcher. The detailed information will show:

- the binary file content
- the default application that will be run when double clicking on the specific file if downloaded on disk
- the specific file bytes that were used in the file recognition
  - as such, the file bytes can be spread across multiple areas of the file
  - to make it easier to read, the bytes in question are highlighted in bold
- unrecognized files are also displayed, allowing for the ability to inspect potential scripts and viruses, without being executed to cause damage

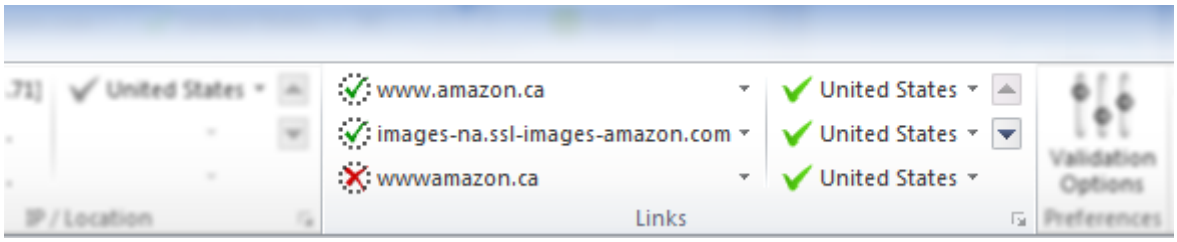
Note: below is the more complex recognition of executable files which have identifier signatures across multiple file offsets!



Note: below is a script/potential virus, that was sent as part of a zip file



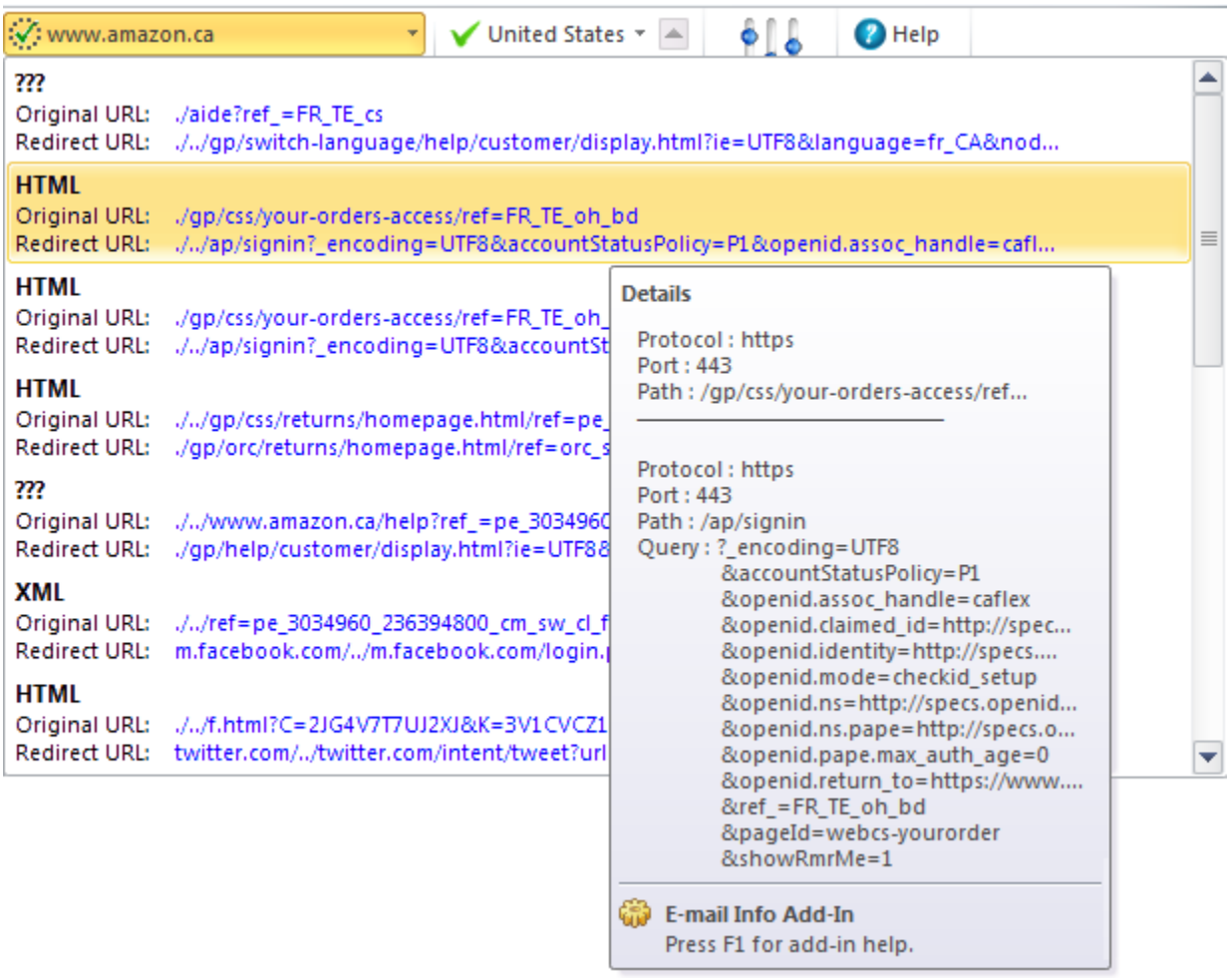
Links



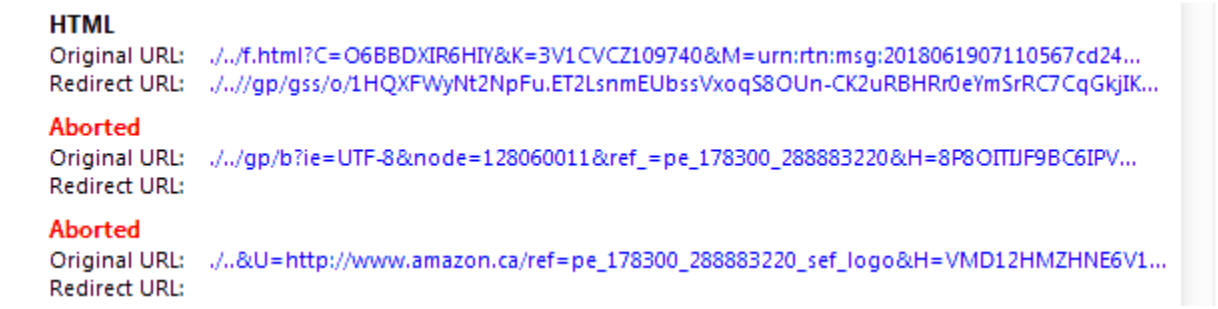
The **Links** group of the Info tab contains information about the links contained in the current e-mail. If there are no links, this group will not be displayed.

The links in the current e-mail are queried individually to check for any possible redirects and the data that will be retrieved if the link is clicked. The data is queried in binary form so there is no possible execution of the data obtained. The data retrieved is checked similarly to the file attachments to try and determine the type of data retrieved.

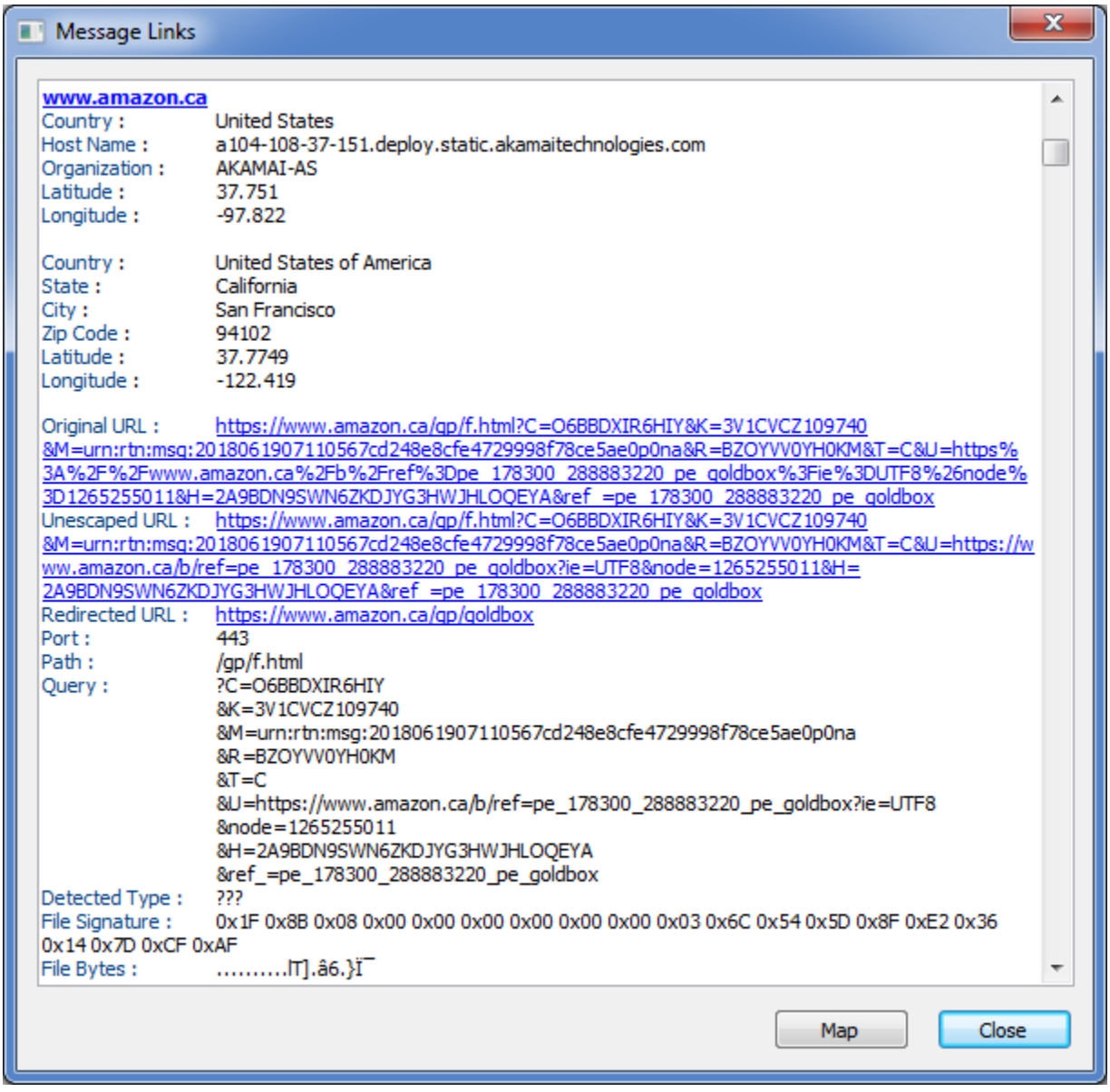
Links that contain redirects are also followed to make sure that the correct data is obtained. The original and redirect URLs are displayed. Hovering over the information displays detailed information about both the original and the redirected URLs.



Note: this application is not as complex as a full browser (like Google Chrome for example) so in some cases, it is possible that some link queries will fail (the server request fails to respond within a specified time, or the link might be incorrect, or the number of retries (specified in the Options dialog) is exceeded).



Detailed information about all the links can be obtained by clicking the dialog box launcher of the **Links** group.

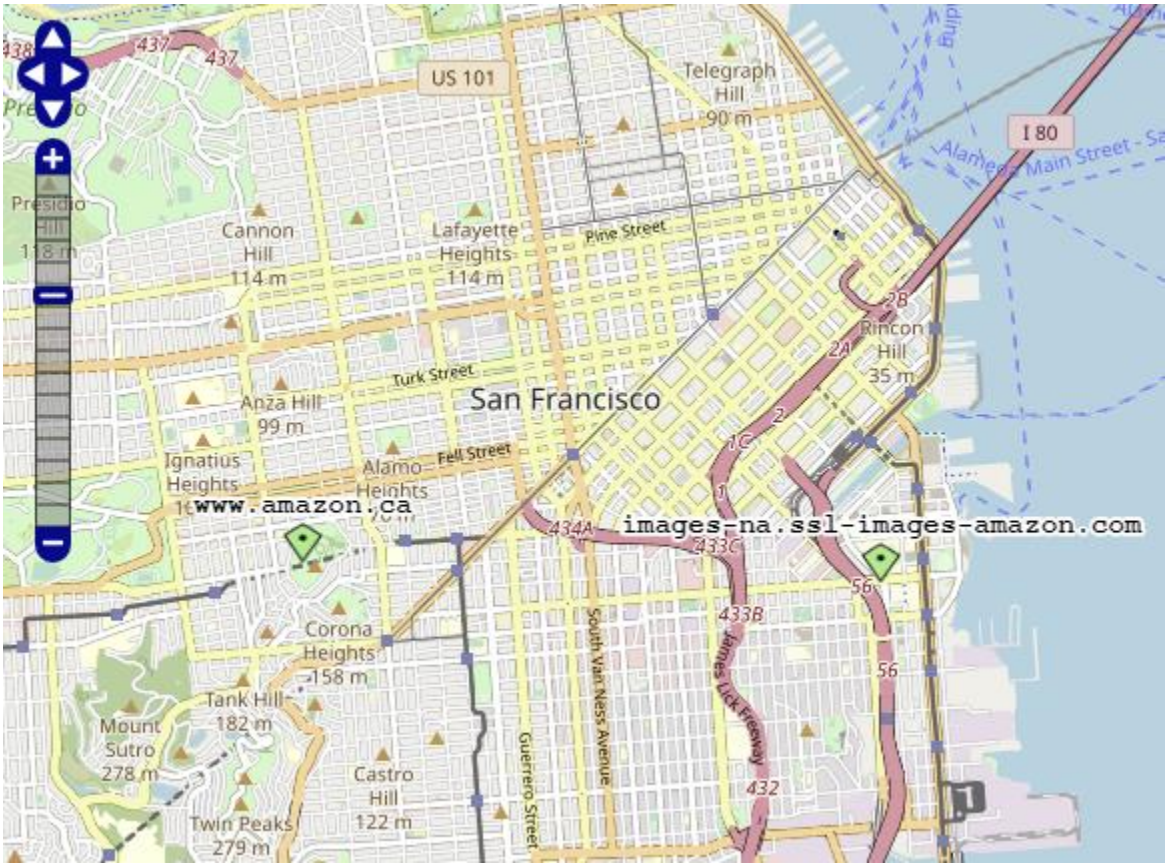


Note: sometimes links point to tracking data to check if e-mails were opened/read (like 1x1 pixel GIF images) – opening these links for validating the content will cause the e-mail sender to assume the e-mail was opened/read.

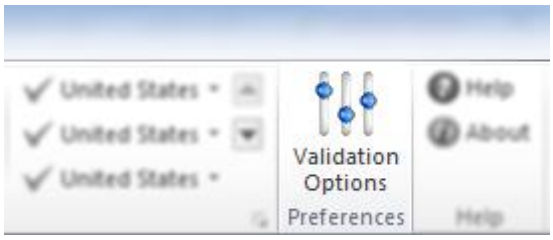
Note: the number of Geo IP providers that can take a server name is smaller than the ones that process IPv4 or IPv6 information.

It is possible to map the server locations for the links. This is especially useful when trying to figure out if some of the links are suspicious in nature, where they originated.

Note: the mapping location information is just an approximation!



Preferences

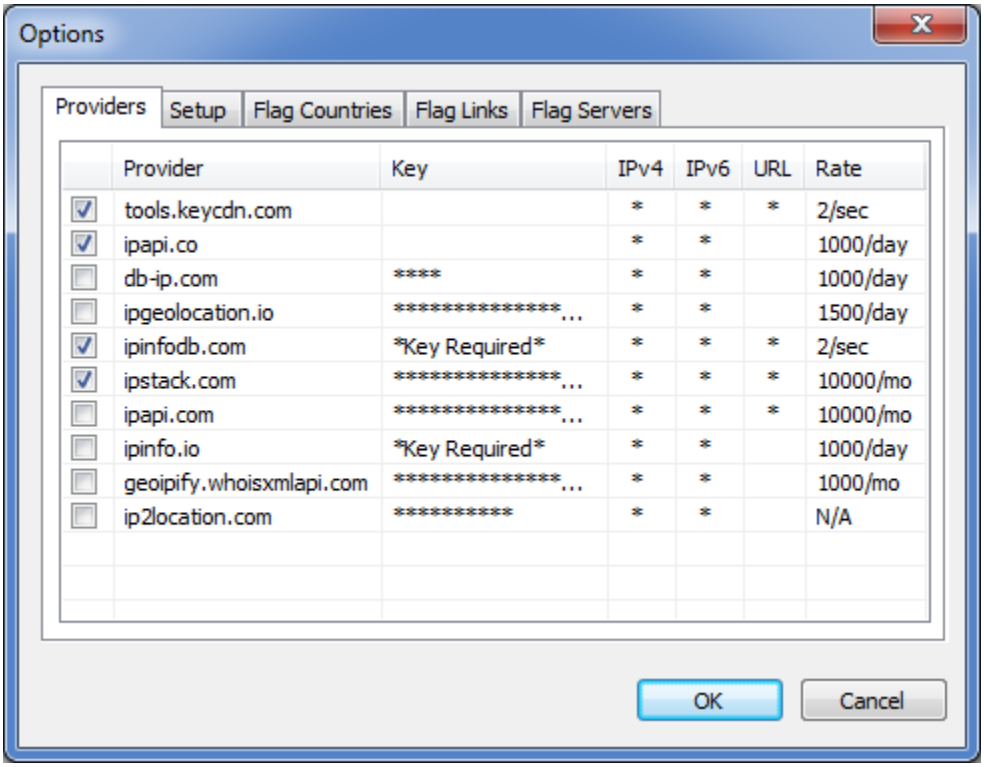


The **Preferences** group of the Info tab contains a number of options that affect how the plug-in will behave.

The **Providers** tab shows all Geo IP providers that the plug-in can make use of.

- There is a minimum of one provider selected to be able to show IP location information.
- There can be a maximum of 4 providers selected.
- For each provider, there is information if they handle IPv4, IPv6 or URL server data. To get links information, at least one provider that handles URL data needs to be selected.
- Some providers require a key to return information – the key can be obtained from the provider's website – it is a free registration.
    - Double-clicking on the provider column will bring up a web-browser pointing to the specific provider clicked on.
    - Double-clicking on the key field will allow a new key to be entered
- Most providers have limits on the number of requests that are provided for free (the limit at the time of publishing are shown in the last column). If a larger number of requests is required, most providers offer paid plans

  Note: the limits may change without notice at the provider's discretion
- The list of providers can be reordered in this list and it will be reflected in the results displayed in the **Info** ribbon

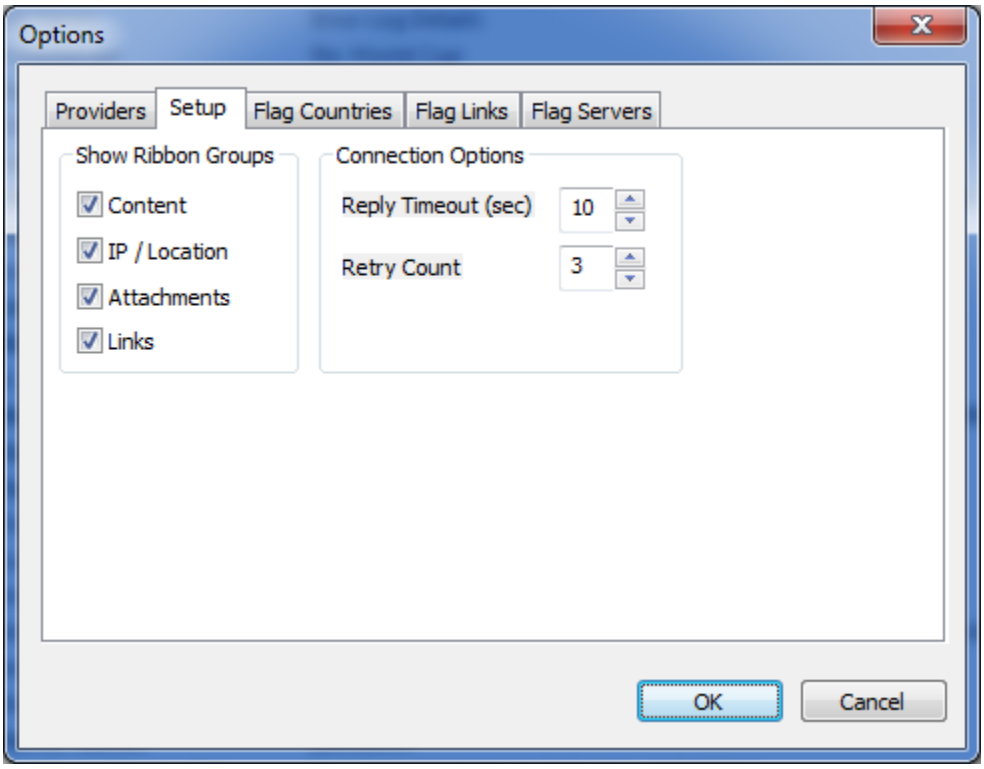


The **Setup** tab allows the user to select which groups should be visible in the Info tab. It also contains some server request parameters.

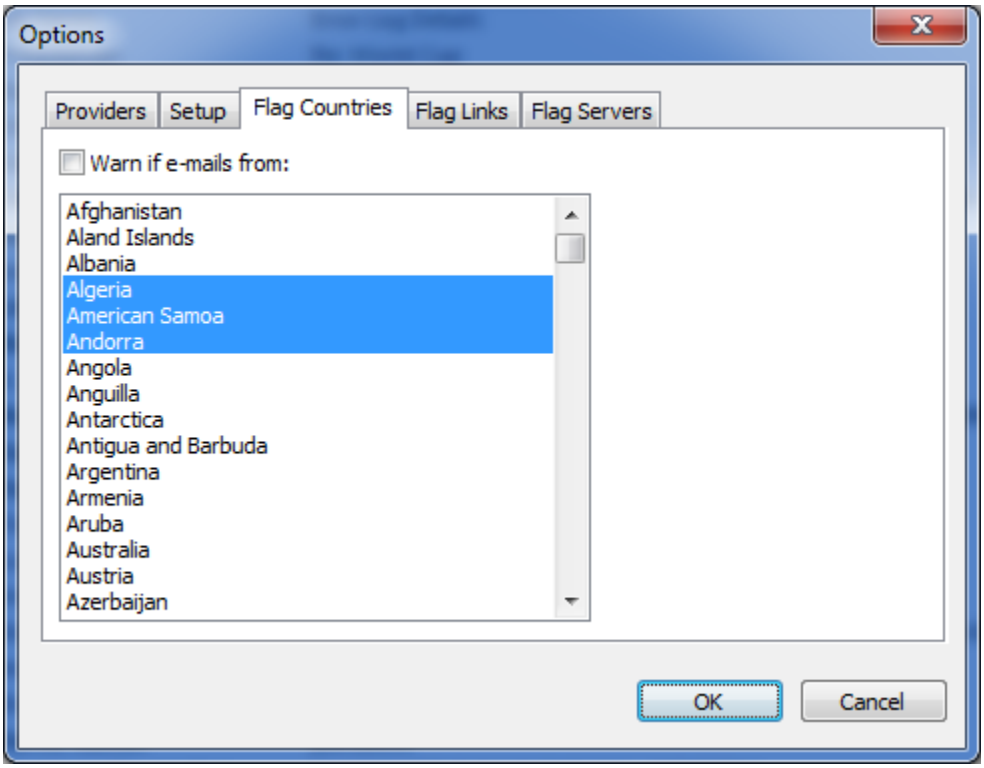
- The **Content**, **IP / Location**, **Attachments** and **Links** groups can be hidden from view (they're all visible by default), though some of the groups are automatically hidden if they don't contain any data.

- **Reply timeout (sec)** – if a request for IP or link information fails to complete within the time mentioned here, it is aborted. There are many reasons why the request can fail and there's no point in waiting forever for a request to finish.

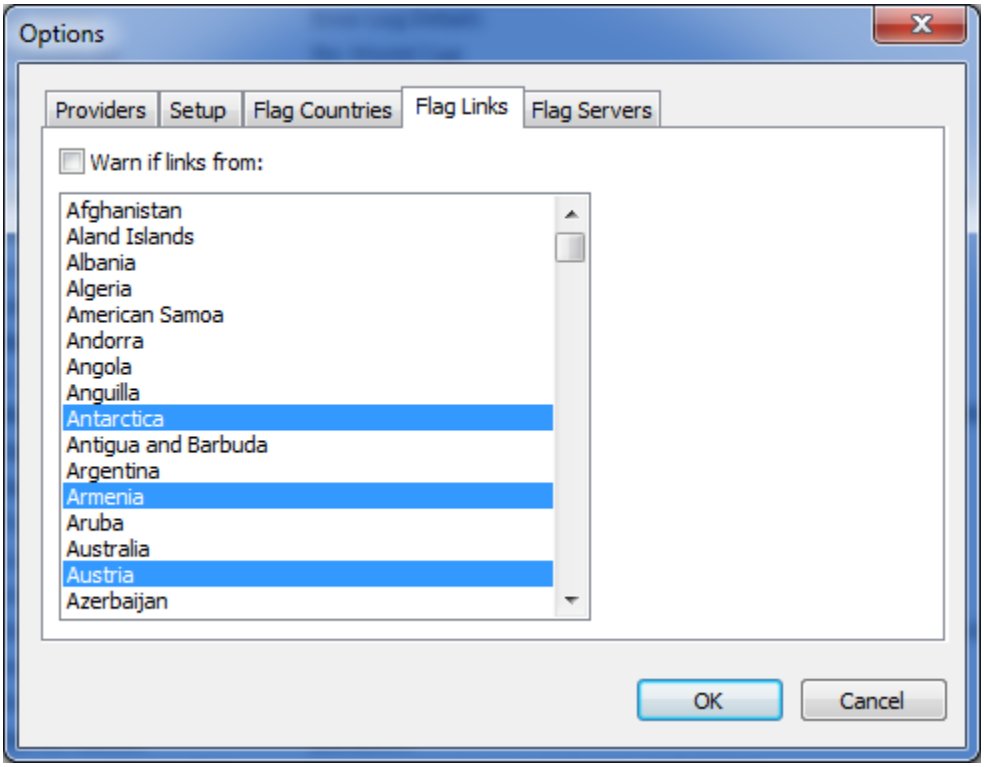
- **Retry count** – number of times a failed request will be retried. For example, if the server is down, no number of retries will retrieve the requested data, hence the limit on the number of retries – no point in retrying forever.



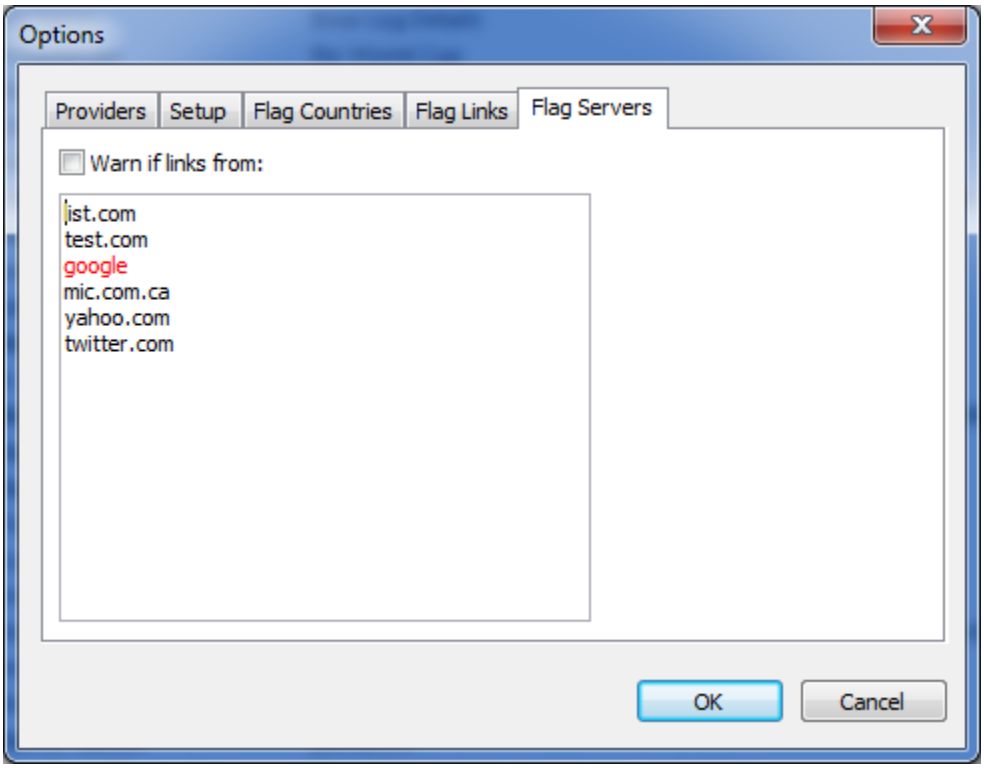
The **Flag Countries** tab allows the user to select a number of countries that can be used against the incoming e-mail IP information. If the e-mail passes through a server from that country, a warning will appear in the Status button of the Content group.



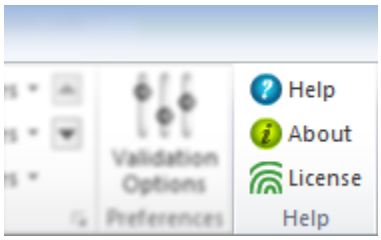
The **Flag Links** will do the same thing as Flag Countries, but for Links.



The **Flag Servers** allows the user to set up a list of servers that will be checked against the links in the e-mail and if any of them is found, a warning will appear in the Status button of the Content group.
Note: improperly formatted servers will be highlighted.



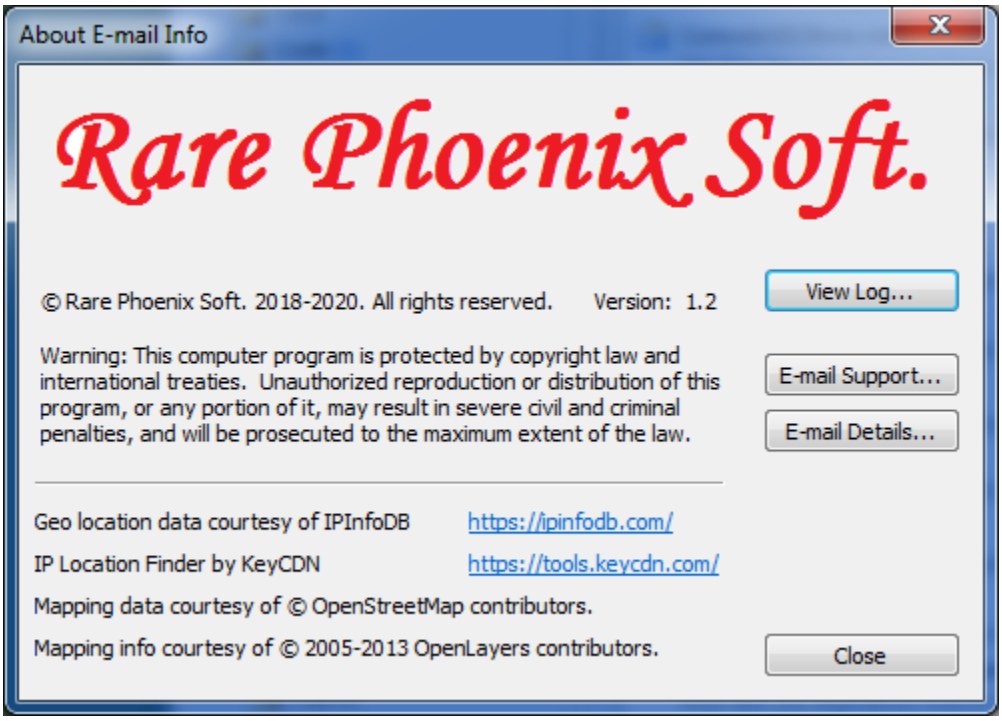
Help



The **Help** group of the Info tab contains three options.

- The **Help** button brings up this document.
- The **About** button brings up the dialog below.
- The **License** button has three states and also brings up a dialog to allow the user to enter a full license.
  - Trial period expired
  - Trial license
  - Full license

About Dialog



- The **View Log** button will bring up an error log that will show errors that have occurred for this Outlook add-in. This log helps out the development team fix some of those errors.

- The **E-mail Support** button will bring up an e-mail message containing the current error log information. This log could be e-mailed to the development team to fix the errors encountered.

- The **E-mail Details** button will create an e-mail with all the details about the current e-mail message. This information could be sent to a friend with detailed computer knowledge in case there are doubts about the contents of the e-mail.

License Dialog