POLICÍA DE INVESTIGACIONES DE CHILE
Inspectoría General

3 JUN 2014
DIA
1547

REF.: APRUEBA INSTRUCTIVOS QUE SE INDICAN. /

SANTIAGO, 13 JUN 2014

ORDEN GENERAL Nº 2390 / VISTOS:

a) Lo dispuesto en el artículo 4° de la Ley Orgánica de la Policía de Investigaciones de Chile, aprobada por Decreto Ley Nº 2.460, de 24.ENE.979, que consagra la misión fundamental de la Policía de Investigaciones de Chile.

b) Lo señalado en el artículo 79 del Código Procesal Penal, el cual establece que la Policía de Investigaciones de Chile será el auxiliar del Ministerio Público en las tareas de investigación y deberá llevar a cabo las diligencias necesarias para cumplir los fines previstos en el mencionado cuerpo legal, en especial en los artículos 180, 181 y 187, de conformidad a las instrucciones que le dirigen los fiscales.

c) La Ley Nº 19.223, de 07.JUN.993, que tipifica figuras penales relativas a la Informática.

d) La Orden General Nº 2.322, de 15.SEP.011, que aprueba los Protocolos de Actuación Policial para la Investigación Criminal.

e) El Oficio (R) Nº 1.547, de 25.OCT.013, de la Subdirección Operativa, que solicita a la Inspectoría General, estudiar propuesta de actualización del Protocolo de Actuación Policial para la Investigación de los Delitos Informáticos, versión 002.

f) El Radiograma Nº 52, de 12.FEB.013, de la Brigada Investigadora del Ciber Crimen Metropolitana, que imparte instrucciones al personal institucional sobre las solicitudes remitidas a esa Unidad para obtener información de fuentes externas.

g) La necesidad de dar continuidad al trabajo de estandarización de la función policial, en conformidad con las directrices establecidas para la documentación de los sistemas de gestión de calidad, propendiendo hacia el mejoramiento continuo y la satisfacción de los usuarios.

h) La facultad que me confieren la Ley Orgánica y el Reglamento Orgánico de la Policía de Investigaciones de Chile.

ORDENO:

1º.- APRUÉBANSE los instructivos que a continuación se indican:

- Instructivo para solicitar a la BRICIBMET que requiera información a fuentes externas.

- Instructivo para identificar el proveedor de una IP.

- Instructivo para extraer cabeceras de correo electrónico.

2º.- Los señalados instructivos, que se adjuntan a la presente Orden General deberán utilizarse en la forma y oportunidad que corresponda.

3º.- DÉJASE sin efecto el Radiograma Nº 52, de 12.FEB.013, de la Brigada Investigadora del Ciber Crimen Metropolitana.

REGÍSTRESE, COMUNÍQUESE Y PUBLÍQUESE EN LA ORDEN DEL DÍA Y BOLETÍN OFICIAL.

MARCOS VÁSQUEZ MEZA
Director General
Policía de Investigaciones de Chile

EVC/PMA/fjn
Distribución:
- Subdirecciones
- Insgral
- Jefaturas
- Repoles/UU.DD.
- B.O/O.D.
- Archivo/

INSTRUCTIVO PARA SOLICITAR A LA BRICIBMET QUE REQUIERA INFORMACIÓN A FUENTES EXTERNAS

ELABORADO POR:	FIRMA:	REVISADO POR: JENADEC	FECHA VIGENCIA:
Brigada Investigadora del Ciber Crimen Metropolitana		FIRMA:	
		APROBADO POR:	VERSIÓN: 001
		FIRMA:	

1. PROPÓSITO:

El propósito de este instructivo es entregar las directrices para la confección de la documentación requerida por la Brigada Investigadora del Ciber Crimen Metropolitana (BRICIBMET) para solicitar información a fuentes externas.

2. ALCANCE Y RESPONSABLE:

Este instructivo tiene alcance a las investigaciones por delitos informáticos que requieran información de fuentes externas, con excepción de las investigaciones desarrolladas por personal de la BRICIBMET.

Los responsables de la correcta aplicación y cumplimiento de este instructivo son el Jefe de Unidad y los Oficiales Investigadores respectivos.

3. DEFINICIONES Y/O ABREVIATURAS:

Conforme al Protocolo de Actuación Policial para la Investigación de los Delitos Informáticos (JNE-BCM-001).

4. DESARROLLO

Descripción del Instructivo:

4.1 Se deberá confeccionar un Oficio dirigido a la BRICIBMET conforme a los requisitos del Reglamento de Documentación y Archivo, señalando el nombre de la fuente externa que se desea consultar y adjuntará la Orden de Investigar y/o Instrucción Particular vigente correspondiente.

4.2 Respecto al contenido del Oficio es importante señalar que dependiendo de la fuente externa a quien se realizará la consulta, se debe adjuntar y proporcionar los siguientes antecedentes según corresponda:

4.2.1 Proveedores de Correo electrónico:

- **Servicios de Microsoft (Hotmail)**

Señalar el nombre de la dirección de correo asociada a la investigación y el rango de fechas y horas a consultar, según corresponda.

- **Servicios de Google (gmail) y Proveedores Nacionales**

Es necesario indicar el nombre de la dirección de correo asociada a la investigación y el rango de fechas y horas a consultar, según corresponda. Así también, adjuntar un Oficio de la Fiscalía dirigido directamente a la empresa, es importante que este documento contenga logo de la fiscalía correspondiente, timbre, nombre y firma del fiscal a cargo de la investigación y nombre de la dirección de correo que se desea consultar.

4.2.2 Proveedores de Conectividad ISP

- **Direcciones IP:**

  Es necesario indicar la IP y fechas y horas de utilización de la dirección IP, señalando zona horaria, en caso de no ser horario nacional.

Dirección IP	Fecha de conexión	Horario de conexión
190.162.99.70	17.JUN.2009	Entre 14:30:00 y 15:00:00.
190.161.176.248	28.JUN.2009	Entre 19:00:00 y 19:30:00

- **Rastreo de Equipos Computacionales (Computadores, Tablets y Smartphones)**

  Deberá señalar la fecha de ocurrencia del hecho y la MAC ADDRESS o IMEI del equipo computacional.

4.2.3 Titulares de Sitios Web

- **Redes Sociales:**

  Para consultar cuentas en redes sociales, es imprescindible indicar la URL del sitio web, el nombre de usuario que se puede obtener desde la URL, dirección de correo electrónico asociado al usuario, screenshot (captura de pantalla) y la Orden de la fiscalía debe especificar algún delito en particular y nunca por "otros hechos", de lo contrario las empresas extranjeras tienden a no informar.

- **Otros Sitios Web:**

  Debe indicar la URL del sitio web, la URL asociada a la investigación, el nombre de usuario o cualquier otro antecedente que sirva para la identificación de la persona.

4.3 Para el caso del **Servicio de Yahoo y Twitter**, las solicitudes deben hacerse a través de los mecanismos descritos en los tratados de asistencia legal mutua, por medio de la Fiscalía Nacional, por cuanto no hay contacto directo con estas empresas.

4.4 La información señalada anteriormente, deberá ser enviada al correo electrónico asistencia@cibercrimen.cl, según corresponda. Sin embargo, posteriormente remitirá por canal regular la documentación respectiva.

4.5 Una vez que obtenga la información, corresponderá continuar con las diligencias señaladas en el Protocolo de Actuación Policial para la Investigación de los Delitos Informáticos (JNE-BCM-001).

5. REGISTROS:

- Oficio a la BRICIBMET solicitando información.

INSTRUCTIVO PARA IDENTIFICAR EL PROVEEDOR DE UNA IP

ELABORADO POR:	FIRMA:	REVISADO POR: JENADEC	FECHA VIGENCIA:
Brigada Investigadora del Ciber Crimen Metropolitana		FIRMA:	
		APROBADO POR:	VERSIÓN: 001
		FIRMA:	

1. PROPÓSITO:

El propósito de este instructivo es entregar las directrices para identificar el proveedor de conectividad (ISP) asociado a una IP determinada.

2. ALCANCE Y RESPONSABLE:

Este instructivo tiene alcance a las investigaciones por delitos informáticos que requieran identificar el proveedor de una IP determinada.

Los responsables de la correcta aplicación y cumplimiento de este instructivo son el Jefe de Unidad y el Oficial Investigador correspondiente.

3. DEFINICIONES Y/O ABREVIATURAS:

Conforme al Protocolo de Actuación Policial para la Investigación de los Delitos Informáticos (JNE-BCM-001).

4. DESARROLLO

Generalidades:

Es importante tener en cuenta que los ISP mantienen un registro histórico de conexiones de 6 meses de antigüedad, por lo que si la dirección IP a consultar es de una fecha anterior es muy factible que la empresa informe no poseer registros.

Descripción del Instructivo:

4.1 Para consultar una dirección IP lo primero es establecer el país de origen y la empresa proveedora. Para esto existen numerosos sitios de consultas donde se lista la información asociada a la dirección IP, los más utilizados son los siguientes.

www.lacnic.org
www.nic.com
www.ip-adress.com

4.2 Una vez consultada la dirección IP en el sitio Web este nos entregara la información del país de origen y del ISP asociado a esa dirección IP.

Ejemplo

200.55.215.90 IP:
200.55.215.90
200.55.215.90 server location:
Santiago in Chile
200.55.215.90 ISP:
Gtd Internet S.A.

En este caso el ISP corresponde a GTD Internet S.A.

4.3 Con el nombre del proveedor que obtenga, debe continuar con las diligencias establecidas en el Protocolo de Actuación Policial para la Investigación de los Delitos Informáticos (JNE-BCM-001).

5. REGISTROS:

No hay

INSTRUCTIVO PARA EXTRAER CABECERAS DE CORREO ELECTRÓNICO

ELABORADO POR:	FIRMA:	REVISADO POR: JENADEC	FECHA VIGENCIA:
Brigada Investigadora del Ciber Crimen Metropolitana		FIRMA:	
		APROBADO POR:	VERSIÓN: 001
		FIRMA:	

1. PROPÓSITO:

El propósito de este instructivo es entregar las directrices necesarias para extraer una IP desde un mensaje de correo electrónico.

2. ALCANCE Y RESPONSABLE:

Este instructivo tiene alcance a las investigaciones por delitos informáticos, donde sea posible visualizar un mensaje de correo electrónico desde un computador o dispositivo digital.

Los responsables de la correcta aplicación y cumplimiento de este instructivo son el Jefe de Unidad y el Oficial Investigador respectivo.

3. DEFINICIONES Y/O ABREVIATURAS:

Conforme al Protocolo de Actuación Policial para la Investigación de los Delitos Informáticos (JNE-BCM-001).

4. DESARROLLO

Generalidades

Todo mensaje de correo trae una cabecera y un cuerpo. La cabecera contiene información de fechas, el origen y destino del mensaje, la ruta específica que sigue el mensaje a medida que atraviesa cada servidor de correo, direcciones IP y otros datos técnicos. El cuerpo contiene el contenido del mensaje es decir el texto, imágenes, documentos adjuntos, etc.

Las cabeceras poseen líneas de código insertadas automáticamente por el programa que envía el correo y por cada uno de los servidores de correo por los que va pasando hasta llegar al destinatario, esto produce que cada cabecera varíe de acuerdo al cliente de correo que se utilice.

No obstante existen parámetros comunes para todas las cabeceras, a continuación un ejemplo de una cabecera y de los parámetros más comunes:

```
Delivered-To: j.jara@cibercrimen.cl
Received: by 10.220.189.204 with SMTP id df12cs22787vcb;
        Fri, 23 Jul 2010 10:25:22 -0700 (PDT)
Received: by 10.114.109.19 with SMTP id
h19mr5917977wac.141.1279905921647;
        Fri, 23 Jul 2010 10:25:21 -0700 (PDT)
Return-Path: <sircacha@portalnet.cl>
Received: from usa.portalnet.cl ([216.18.194.162])
        by mx.google.com with ESMTP id
d30si924562waa.71.2010.07.23.10.25.21;
        Fri, 23 Jul 2010 10:25:21 -0700 (PDT)
Received-SPF: neutral (google.com: 216.18.194.162 is neither permitted
nor denied by best guess record for domain of sircacha@portalnet.cl)
client-ip=216.18.194.162;
Authentication-Results: mx.google.com; spf=neutral (google.com:
216.18.194.162 is neither permitted nor denied by best guess record
for domain of sircacha@portalnet.cl) smtp.mail=sircacha@portalnet.cl
Received: from localhost ([127.0.0.1])
        by usa.portalnet.cl with esmtpa (Exim 4.69)
        (envelope-from <sircacha@portalnet.cl>)
        id 1OcLzv-0007Vr-D0
        for e.jimeno@cibercrimen.cl; Fri, 23 Jul 2010 14:25:23 -0300
Received: from 190.44.96.36 ([190.44.96.36]) by portalnet.cl (Horde
MIME
        library) with HTTP; Fri, 23 Jul 2010 14:25:23 -0300
Message-ID: <20100723142523.v1xwzt449wsoo4ko@portalnet.cl>
Date: Fri, 23 Jul 2010 14:25:23 -0300
From: sircacha@portalnet.cl
To: Jaime Jara < j.jara@cibercrimen.cl >
```

Campos de la Cabecera

- **Date:** Fecha y hora de envío del mensaje. Es importante saber el huso horario del sitio, considerando que para obtener la hora local a partir de la hora universal hay que utilizar el huso horario correspondiente al sitio de observación para hacer la transformación.
- **Subject:** Asunto del mensaje
- **To:** Destinatario del mensaje
- **Message-ID:** Es una etiqueta que identifica el mensaje con un ID que garantiza que sea único en toda la Internet.
- **From :** Indica quien envía el mensaje.
- **Return-Path:** Indica por donde debe ser rutado el mensaje en caso de devolución.
- **Received:** Indica todas y cada una de las maquinas (servidores de correo) por donde ha ido pasando el mensaje. Cada Servidor de correo inserta un "Received", de manera que estudiando detenidamente la cabecera es posible hacer el seguimiento de un mensaje.

Descripción del Instructivo:

4.1 La IP del mensaje enviado se encuentra en el campo received, pero como se señaló anteriormente este campo aparecerá cada vez que el mensaje pase por un servidor de correo, es por esto que debemos buscar la IP en la primera etiqueta de envío, por lo general se ubica leyendo la cabecera de abajo hacia arriba, tomando el ejemplo anterior la IP de origen del mensaje y la fecha y hora de envío estaría ubicada en esta línea de código

```
Received: from 190.44.96.36 ([190.44.96.36]) by portalnet.cl (Horde
MIME library) with HTTP; Fri, 23 Jul 2010 14:25:23 -0300
Message-ID: <20100723142523.v1xwzt449wsoo4ko@portalnet.cl>
Date: Fri, 23 Jul 2010 14:25:23 -0300
From: sircacha@portalnet.cl
To: Jaime Jara < j.jara@cibercrimen.cl >
Subject: RE: Solicitud de Antecedentes
```

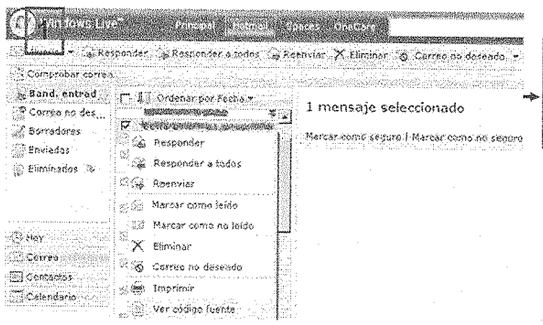
4.2 Desglosando la información contenida en el bloque de código:
Received: from 190.44.96.36 ([190.44.96.36]) by portalnet.cl (Horde MIME library) with HTTP; Fri, 23 Jul 2010 14:25:23 -0300

Por tanto, tenemos que:
- Dirección IP desde donde se envío el mail : 190.44.96.36
- Fecha de envío del mensaje: viernes 23.JUL.2010
- Hora del envío : 14:25:23 -0300 (huso horario Chile)

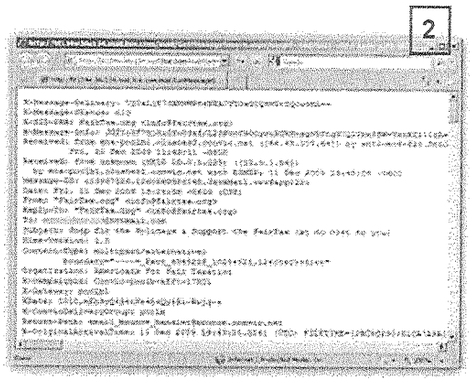
4.3 Las cabeceras de mail no son mostradas por los gestores de correo de forma automática, y por ello para verlas es necesario mirar en su código. El como hacerlo depende del programa o gestor de correo que se utilice.

4.4 En este sentido, la forma de extraer la información, según el programa o gestor de correo utilizado, se realizará como se indica a continuación:

HOTMAIL

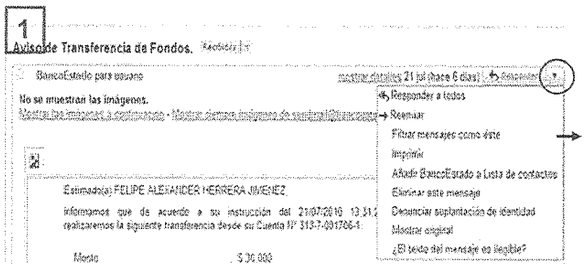


Una vez abierto el programa posesionarse Sobre el mensaje que se desea visualizar hacer click con el botón derecho del mouse Y seleccionar la opción, Ver código Fuente



Se desplegara un ventana en el navegador con El código del correo electrónico

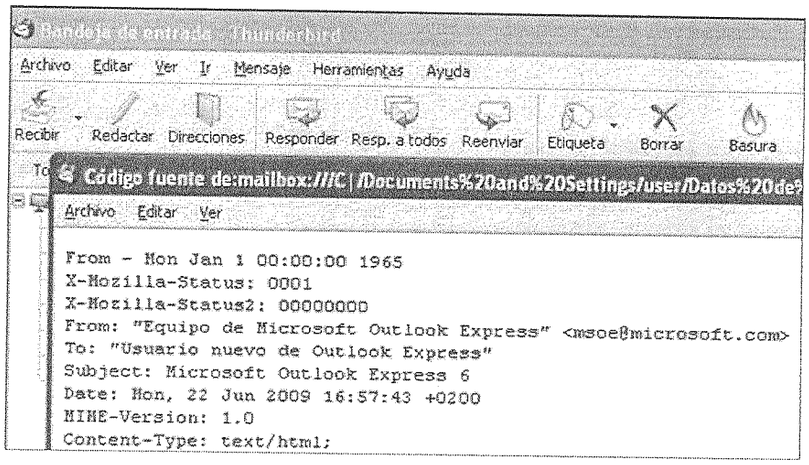
GMAIL



Una vez abierto el correo hacer click en el icono De forma de triangulo inverso ubicado en la parte Superior derecha, posteriormente seleccionar la opción, Mostrar Original

Se desplegara un ventana en el navegador con El código del correo electrónico

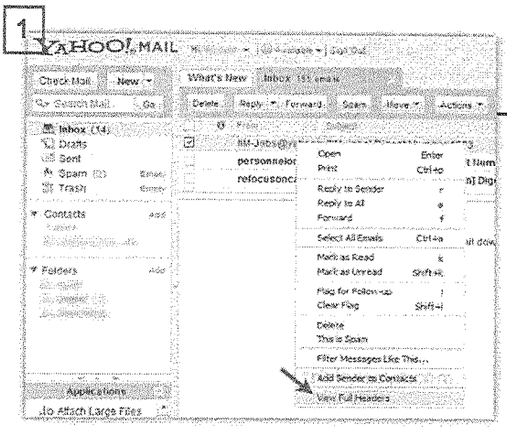
MOZILLA FIREFOX



Se debe seleccionar el mensaje y pulsar las teclas *Control+U*. La otra vía es hacer clic en la opción *Formato original del mensaje* del menú Ver. El código se abrirá como texto puro en una ventana aparte.

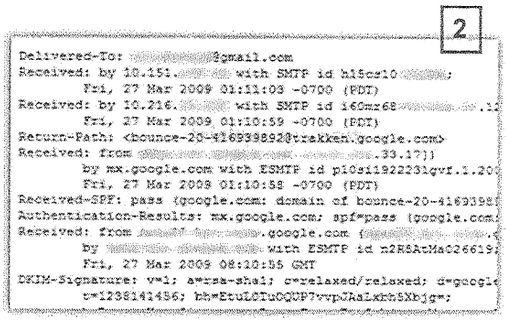
YAHOO

1



Una vez abierto el programa posesionarse Sobre el mensaje que se desea visualizar hacer click con el botón derecho del mouse Y seleccionar la opción, Ver encabezado completo

2



Se desplegara un ventana en el navegador con El código del correo electrónico

4.5 Como resultado obtendrá la IP desde donde se envió el mensaje, debiendo continuar conforme al Protocolo de Actuación Policial para la Investigación de los Delitos Informáticos (JNE-BCM-001)

5. REGISTROS:

No hay.