CORREO ELECTRÓNICO

Dr. Santiago Acurio Del Pino

Agenda

- Conceptos Básicos
- Explicar como funciona E-mail
- Interpretar la cabecera de un E-mail
- Mail anónimos
- Preguntas

Conceptos Básicos

Concepto, funcionamiento, composición, protocolos de comunicaciones

Correo Electrónico

- El correo electrónico es, junto con la telefonía móvil, el sistema que más ha cambiado la manera de comunicarse entre las personas. Es un sistema que permite intercambiar información escrita y archivos con cualquier otro usuario que tenga conexión a Internet
- El correo electrónico es un servicio del Internet, en el principio solo se podía enviar texto, ahora se puede enviar un mensaje en formato HTML.

Dirección de Correo Electrónico

- E-mail es un servicio para enviar mensajes o archivos adjuntos .
  - Una dirección E-mail tiene dos partes:
  - La parte de usuario (sacurio)
  - La parte de dominio unido con el símbolo de arroba(@hotmail.com)

    sacurio@hotmail.com
- El usuario normalmente no está registrado y los Dominios si.

Estructura de un correo electrónico

- SINTAXIS: Nombre
- usuario@subdominio.dominio.dominio inicial
- Ejemplo: acurios@minpec.gov.ec
- SUBDOMINIO: Nombre de rango inferior
- DOMINIO: Nombre de rango superior que lo administra

Nombres de Dominio: Conceptos

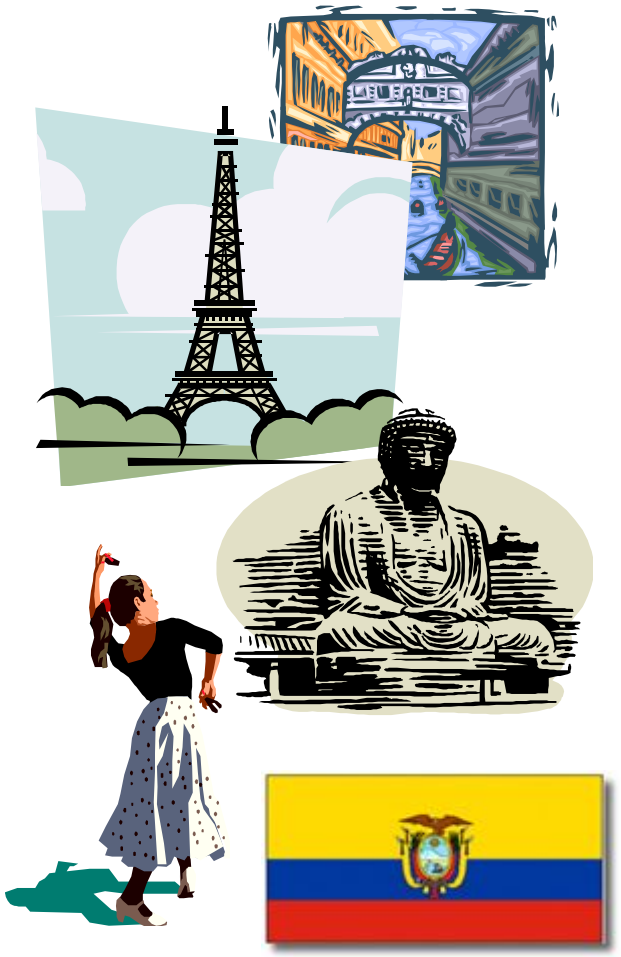
- NOMBRE DE DOMINIO: Nombre mediante el cual nos damos a conocer en Internet. Es la dirección electrónica (dirección IP) expresada en palabras de fácil relación.
- DNS: DOMAIN NAMES SERVICE: Es el método de conversión de los dominios en Internet a direcciones IP que pueden ser identificadas por los ordenadores

Nombres Genéricos

- a. gTLD
- *Empresas (Compañías)*: COM
- *Instituciones de carácter Educativo, Universidades*: EDU
- *Organizaciones no Gubernamentales:* ORG
- *Entidades del Gobierno:* GOV
- *Instalaciones Militares*: MIL
- *Escuelas o Colegios*: .K12
- *Proveedoras de servicios de red:* .NET
- *Organismos Internacionales:* .INT

Nombres con código de país

- b. ccTLD
  - *España = es*
  - *Francia = fr*
  - *Reino Unido (United Kingdom) = uk*
  - *Italia = it*
  - *Japón = jp*
  - *Australia = au*
  - *Suiza = ch*
  - *Irlanda = ir*
- Ecuador = ec



Nombres de Dominio

- Los tanto los gTLD como los ccTLD, están formados por al menos dos niveles, tomaremos como ejemplo el nombre del dominio derecho.com.ec.

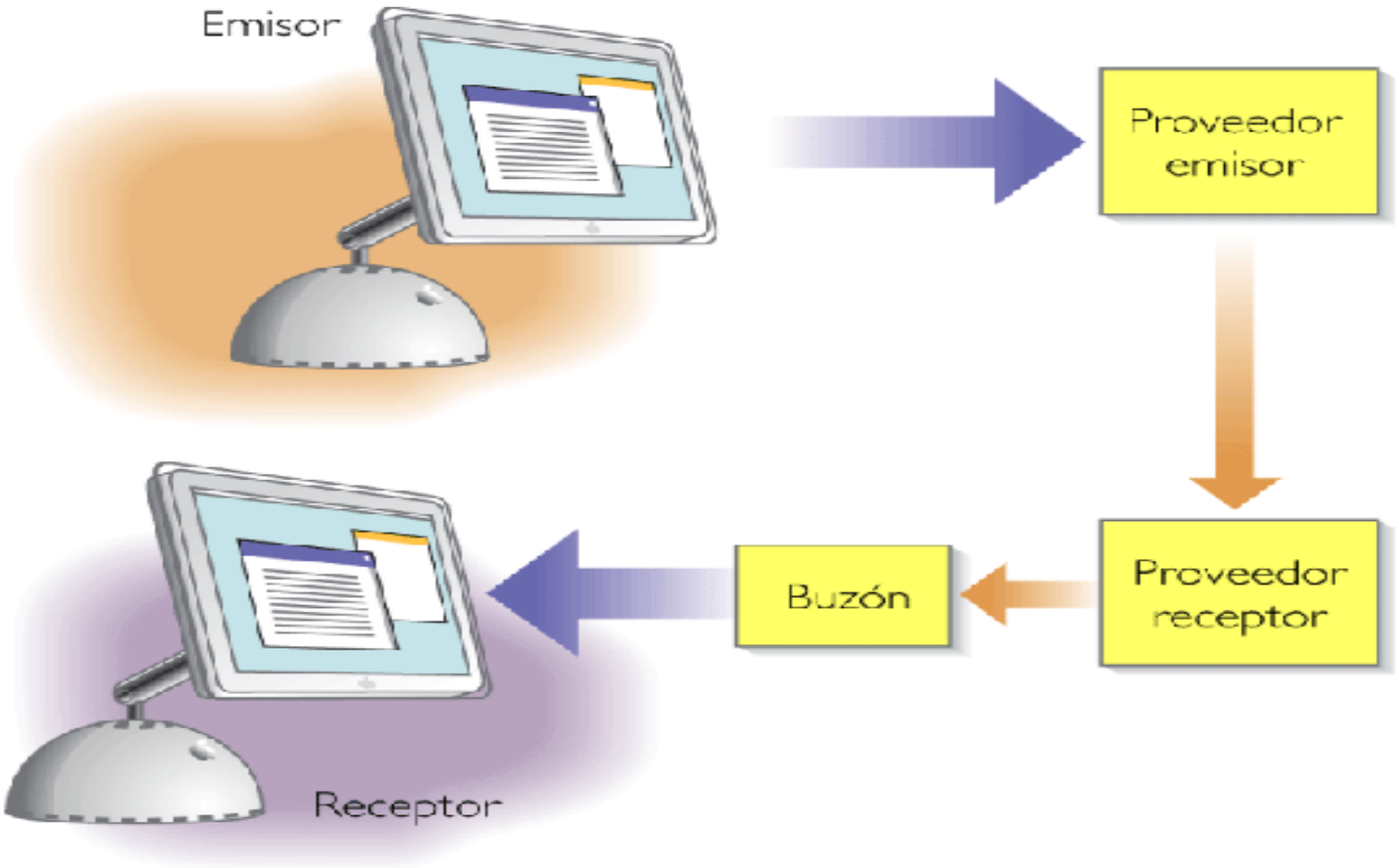
forense.com.ec

- Las forma de identificar los niveles es contar de derecha a izquierda respetando los puntos que permiten una diferenciación entre los mismos. El primer nivel corresponderá al elemento denominativo que se encuentra en primer lugar comenzando desde la derecha y su limite u extensión alcanza hasta el primer punto ubicado a su izquierda.

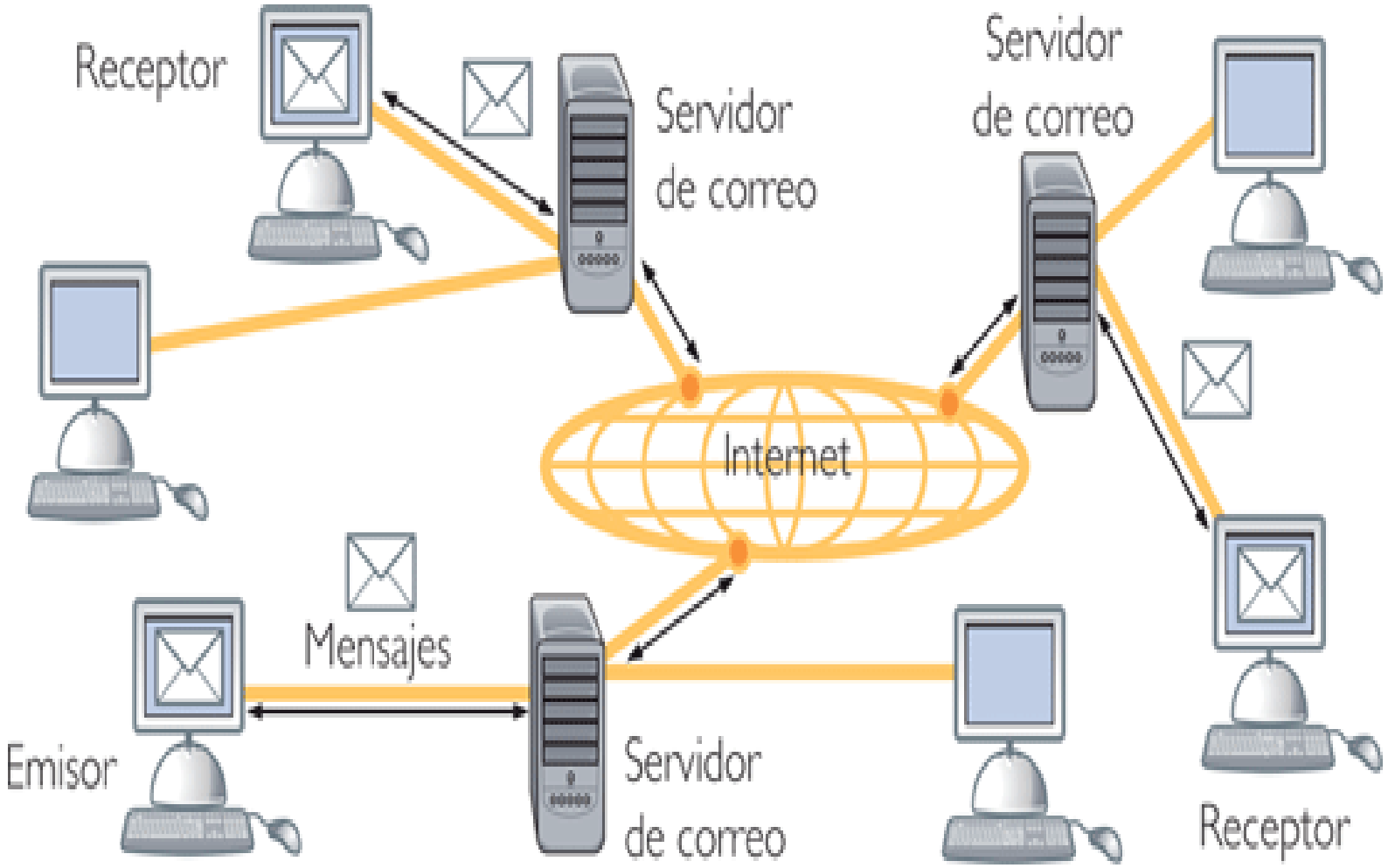
Nombres de dominio

- Es así que en el nombre de dominio utilizado como ejemplo corresponde al prefijo EC el primer nivel.
- Este nivel tiene connotaciones geográficas, que en el presente caso nos remiten al Ecuador y permiten organizar a los niveles inferiores.
- El segundo nivel está conformado por el sufijo genérico COM que hace referencia al tipo de organización, en este caso una institución comercial.
- El tercer nivel está conformado por la denominación FORENSE que corresponde a nuestra cátedra.

Correo Electrónico



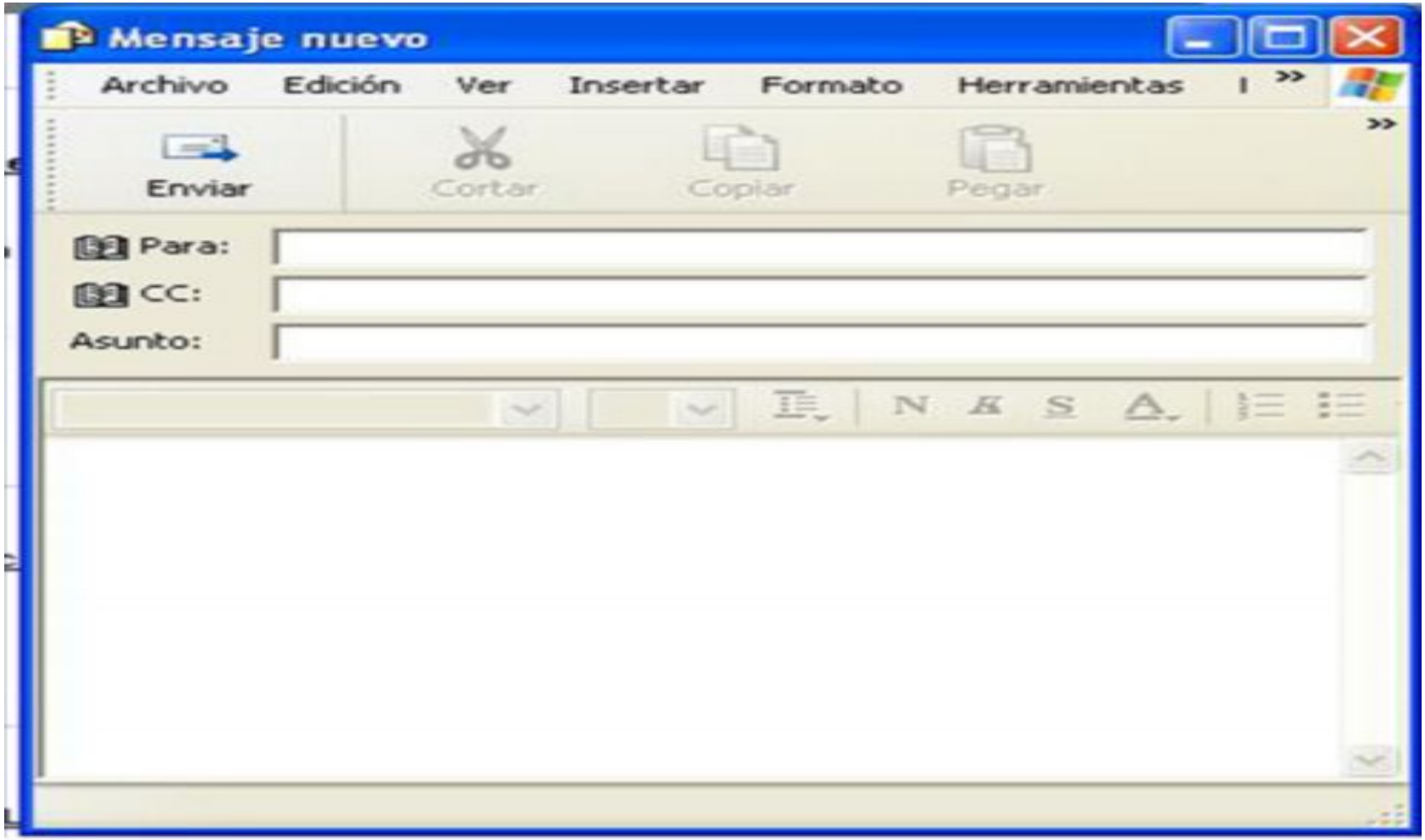
Correo Electrónico



Correo Electrónico

- Las operaciones básicas que podemos realizar con el correo electrónico son:
- Enviar mensajes. Para enviar un mensaje basta con incluir en la ventana *Destinatario* el nombre de este o su identificación, llamada dirección de correo electrónico.
- Recibir mensajes. Cuando nos conectamos a Internet, la aplicación nos avisa (por ejemplo, emitiendo un sonido) cada vez que llega un nuevo mensaje.
- Responder mensajes. Es una opción muy sencilla para contestar un mensaje recibido. Normalmente, el programa que gestiona el correo permite incluir el mensaje recibido en la respuesta.
- Remitir mensajes. Se emplea para reenviar un mensaje recibido a otras personas de nuestra agenda.
- Adjuntar archivos. Junto al texto del mensaje podemos incluir archivos con imágenes, sonidos, etc. Pero no conviene mandar archivos muy grandes, pues el tiempo necesario para enviar o recibir el mensaje es proporcional al tamaño de los archivos.

Correo Electrónico



Protocolos de Correo Electrónico

- El protocolo SMTP (Simple Mail Transfer Protocol) permite el envió de mensajes (correo saliente) desde el cliente hacia el buzón del servidor de correo.
- El protocolo POP (Post Office Protocol) permite recibir mensajes (correo entrante) desde el servidor de correo hacia el cliente (se almacena en el disco duro del destinatario).
- El protocolo IMAP (Internet Message Access Protocol). Sirve para buscar solo los mensajes que incluyan determinada palabra en el apartado “Asunto”.

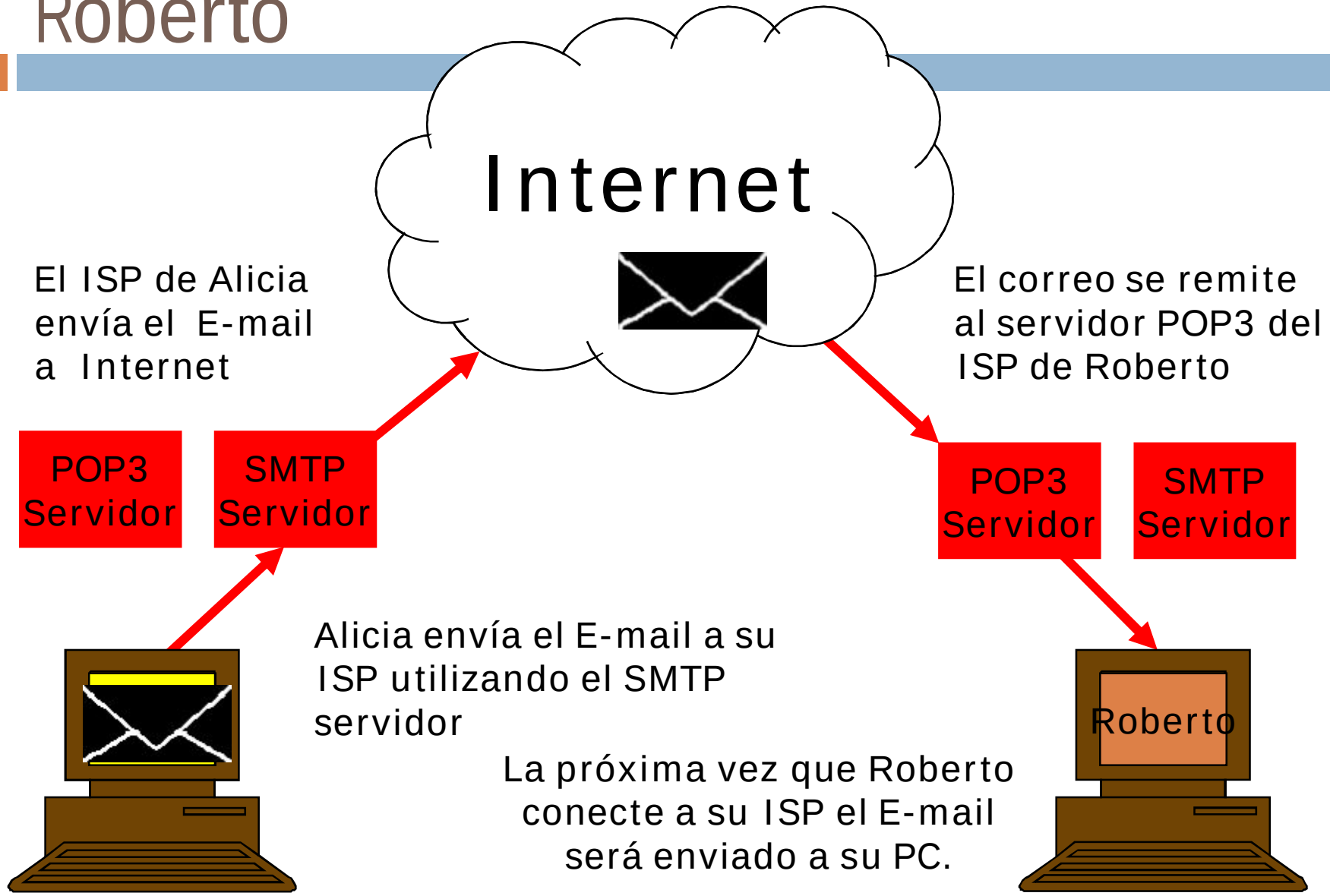
Análisis del Correo Electrónico

Cabecera Técnica, Números IP, Time Stamp

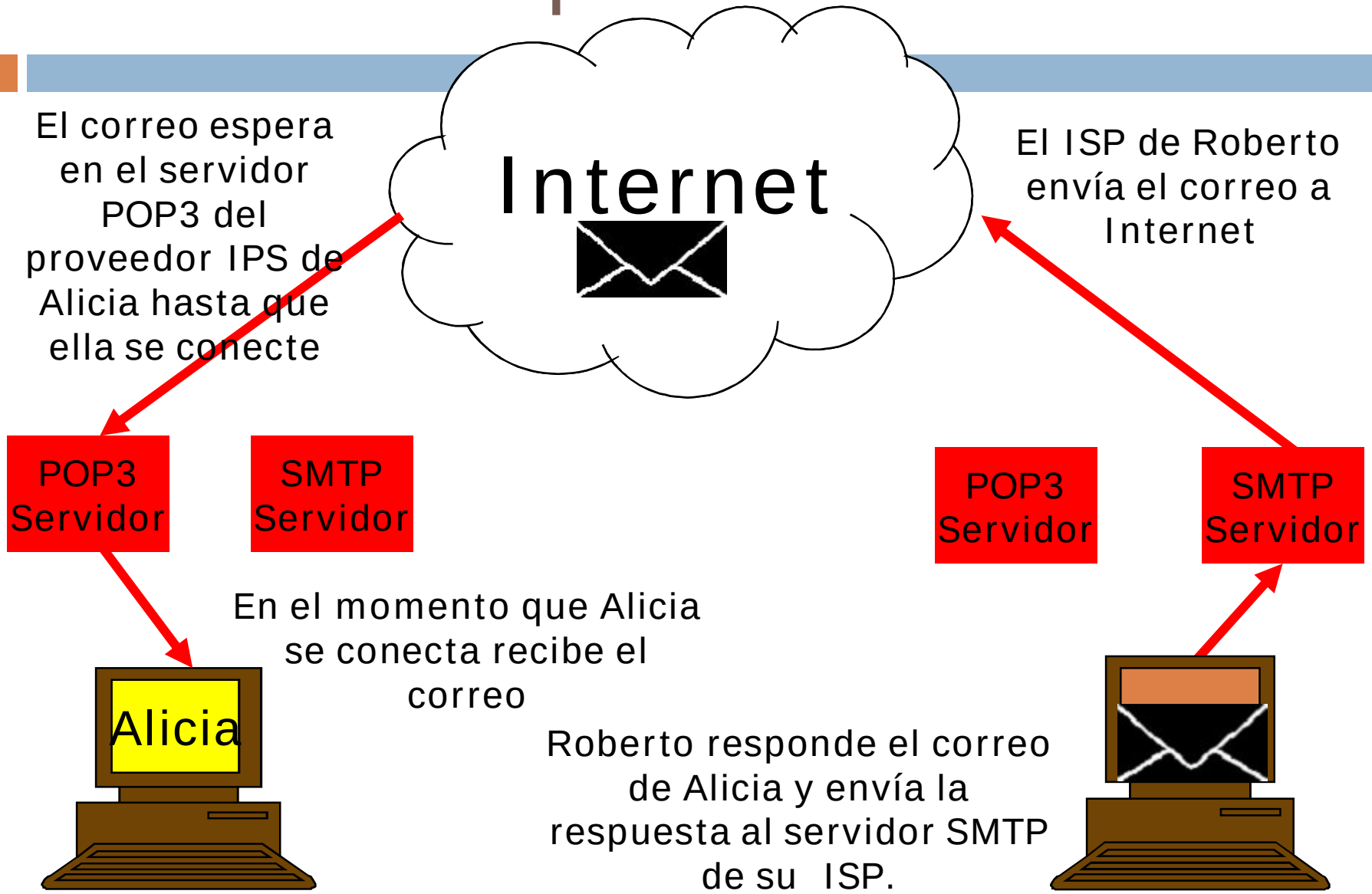
Como funciona el mail

- Un mensaje de correo pasa al menos por cuatro máquinas durante su vida (Estadios):
  - Computador del emisor : donde se compone el mensaje.
  - Servidor de Correo del emisor (Simple Mail Transfer Protocol-SMTP).
  - Servidor de Correo del receptor (Post Office Protocol- POP3)
  - Computador del receptor : donde se recibe el mensaje.
  - Cuando el receptor accede al mensaje, generalmente, se borra del servidor de correo. Baja a su ordenador.

Ejemplo: Alicia le manda un correo a Roberto



Roberto le responde Alicia



Información en el Correo Electrónico

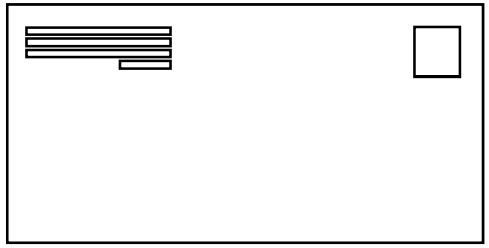
- Mailboxes:
  - INBOX : CARPETA DE ENTRADA
  - SEPARATE FOLDERS : CARPETAS
  - OUTBOX : CARPETA DE SALIDA
  - TRASH : BASURA
  - ENVIADOS
  - BORRADOR
- Libreta de direcciones.

Web Mail

- La mayoría de los ISP proporcionan acceso a su mail box mediante un interface WEB.
- Servicios de correo electrónico gratuito (hotmail, yahoo, Gmail) y muchos más…..
- Logfiles sólo pueden ser proporcionados por los ISP.

Partes componentes de un mensaje de Correo Electrónico

- Un mensaje tiene :
- Header/Cabecera (El sobre)
- Body/Cuerpo(la carta)



Partes componentes de un mensaje de Correo Electrónico

- Cabecera :
  - Contiene información sobre el emisor , receptor, fecha y hora
- Cabecera Técnica :
  - Contiene información sobre el emisor , receptor, fecha y hora direcciones IP, servidores de correo, received, message-id, etc.
- Cuerpo :
  - Contenido del E-mail y archivos adjuntos.

Encabezado General

Español	Ingles	Contenido
DE:	FROM:	Abelardo López <abelardolopez98@prodigy.net.mx>
ENVIADO :	SENT:	Miércoles, 11 de febrero, 2004 7:16 PM
PARA :	TO:	< kylegrimes@msn.com>
COPIA:	CC:	Gabriel Grimes <grimesgk@hotmail.com>
TITULO:	SUBJECT:	Hace mucho tiempo

El encabezamiento General se lee desde arriba hacia abajo.

Componentes del Encabezado General

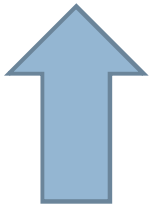
- *From o De*, Emisor de la correspondencia, contiene el nombre del autor, Abelardo López, su identificación en el Internet, abelardolopez98, su nombre de dominio primario es un proveedor de servicios de Internet, prodigy, que tiene un dominio de red, .net, y un dominio territorial, .mx, que pertenece a México.
- *Sent o Enviado*, es la fecha y hora de su envió, designado por la computadora de origen, Miércoles, 11 de Febrero, 2004, 7:16 PM.
- *To o Para,* destinatario de la correspondencia, contiene su identificación en el Internet, kylegrimes, su nombre de dominio primario es un proveedor de servicios de Internet, msn (Microsoft Network), que tiene un dominio de comercio, com.

Componentes del Encabezado General

- *CC,* copia enviada a, contiene el nombre de otro destinatario secundario, Gabriel Grimes, su identificación en el Internet, grimesgk, su nombre de dominio primario es un proveedor de servicios de correspondencia electrónica, hotmail, que tiene un dominio de comercio, com.
- *Subjec o Título,* es el tema de la correspondencia escrita por el emisor, Hace mucho tiempo.
- Los signos de puntuación, como los puntos, < >, y la @ son indicaciones para el protocolo de manejo en el Internet.

Encabezado Técnico

MIME-Version: 1.0
Received: from [216.136.226.197] by hotmail.com (3.2) with ESMTP id MHotMailBD737B61008E4D888E2C506160; Thu, 20 Sep 2001 11:07:30-0700
Received: from [12.26.159.122] by web20808.mail.yahoo.com via HTTP; Thu, 20 Sep 2001 11:07:29 PDT
From: Polaris99992001@yahoo.com Thu, 20 Sep 2001 11:07:58 -0700
Message-id: <20010920180729.36281.qmail@web20808.mail.yahoo.com>



El encabezamiento completo se lee desde abajo hacia arriba.

Componentes del encabezado técnico

- *Message-id*, 20010920180729.36281.qmail@web20808.mail.yahoo.com, indica una identificación asignada al correo electrónico por el servidor que inicialmente procesó la correspondencia original. La identificación es única, y sirve para verificar la originalidad del mensaje.
- *From,* el emisor del mensaje y la fecha y hora de su envío (según la computadora que lo envió). Siempre se debe verificar el uso horario a fin de tener la hora correcta.
- *Received from*, muestra el número IP de la computadora del origen, 12.26.159.122, que puede ser un compuesto del numero local y la red que procesa el mensaje, *by*, o por, el servidor que inicialmente procesó el mensaje, web20808.mail.yahoo.com, *via,* o por cual protocolo, http (protocolo de transferencia de hipertexto), fecha y hora del Internet, Thu, 20 Sep 2001 11:07:29 PDT (hora normal de la Zona del Pacífico).

Componentes del encabezado técnico

- *Received from*, el número IP mencionado del destinatario, 216.136.226.197, *by*, o por, el servidor de HOTMAIL, hotmail.com, *with ESMTP id,* una nueva identificación del mensaje asignado por el nuevo servidor, MHotMailBD737B61008E2C506160, la fecha y hora de su recepción, Thu, 20 Sep 2001 11:07:30-0700.
- *MIME-Version: 1.0*, Es la versión de encabezado

Otros encabezados técnicos

Return-Path: <mark_cameron1962@hotmail.com>

Received: from hotmail.com ([64.4.37.61]) by mta05-svc.ntlworld.com (InterMail vM.4.01.03.27 201-229-121-127-20010626) with ESMTP id <2002102914083 9.HPQJ27595.mta05-svc.ntlworld.com@hotmail.com> for <ruthdixon@ntlworld.com>; Tue, 29 Oct 2002 14:08:39 +0000

Received: from mail pickup service by hotmail.com with Microsoft SMTPSVC; Tue, 29 Oct 2002 06:08:38 -0800

Received: from 217.40.21.116 by pv2fd.pav2.hotmail.msn.com with HTTP; Tue, 29 Oct 2002 14:08:38 GMT

X-Originating-IP: [217.40.21.116]

Otros encabezados técnicos

X-Apparently-To:nhtctc42@yahoo.co.uk via 216.136.226.29; 22 Nov 2002 23:57:28 -0800 (PST)

Return-Path:paul.b@hotpop.com

Received:from 204.57.55.14 (EHLO babyruth.hotpop.com) (204.57.55.14) by mta125.mail.scd.yahoo.com with SMTP; 22 Nov 2002 14:57:27 -0800 (PST)

Received:from hotpop.com (kubrick.hotpop.com [204.57.55.16]) by babyruth.hotpop.com (Postfix) with SMTP id 9E1B2214F5D; Fri, 22 Nov 2002 22:47:20 +0000 (UTC)

Received:from LT02BAYER (host217-42-213-53.range217-42.btcentralplus.com [217.42.213.53]) by smtp-2.hotpop.com (Postfix) with ESMTP id 651F31BA4F0; Fri, 22 Nov 2002 22:47:00 +0000 (UTC)

Message-ID:00b501c291af$e0cada10$0a01020a@NH2TC.ORG

Reply-to:"Paul Bayer" paul@otleyinternet.co.uk

From:"Paul Bayer" <paul.b@HotPOP.com>

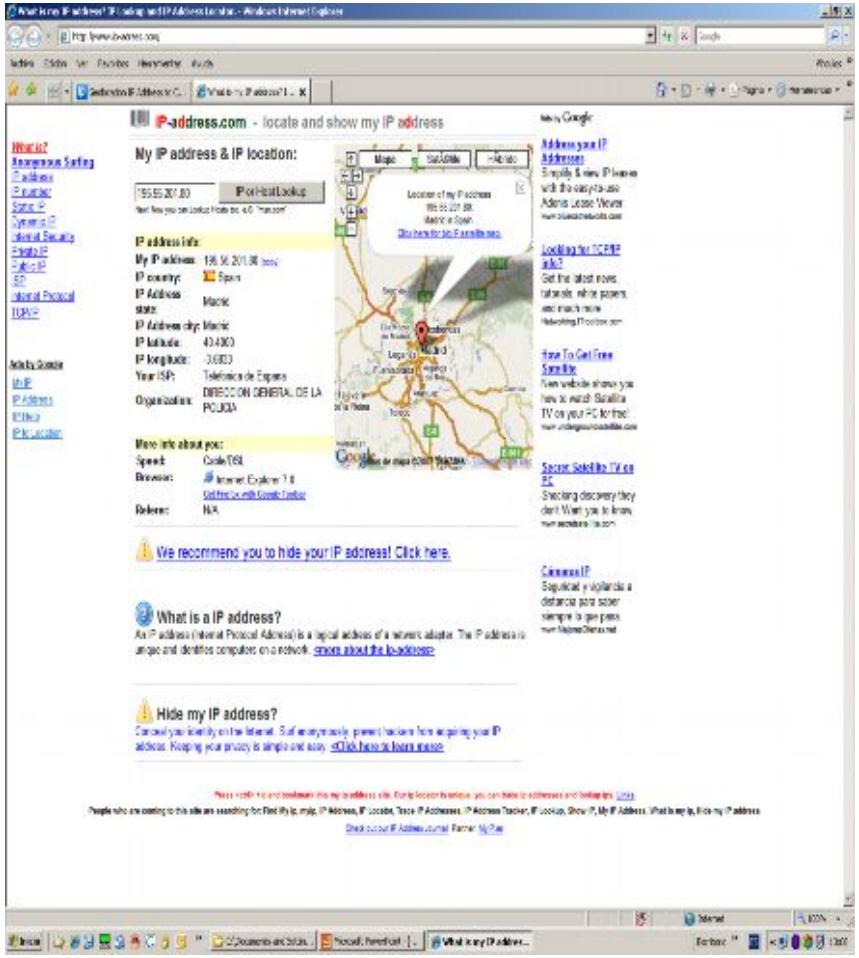
Que hacemos con la información de la Cabecera técnica

- Con la información del encabezado técnico podemos verificar el origen del mensaje enviado, buscando con el número IP registrado el dominio de donde se origino el mensaje. Para eso se utiliza una interfaz, "WHOIS?" que significa "¿Quién es?", para determinar el servicio utilizado, ubicar la dirección geográfica de los servidores y los puntos de contacto, y localizar (a veces) la instalación donde se encuentra un computador.
- Se puede poner la dirección IP en la página Web: http://samspade.org para averiguar los datos antes señalados, también se puede acudir a la página de INTERNIC.
- Podemos usar también meta buscadores como GOOGLE, ALTAVISTA, YAHOO, etc.

Samspade.org

Localizadores Geográficos

(IP-adress.com, IP2-location...etc.)



Mails Anónimos

Un problema para los operadores de justicia

Web Mails Anónimos

- Ofrecen la posibilidad de enviar E-mail de forma totalmente anónima:
- El servicio no realiza ningún tipo de comprobación previa y no almacena normalmente ningún dato de sus usuarios.
  - No son almacenadas copias de los mensajes y archivos adjuntos enviados.
  - El servicio es completamente gratuito.
- Ejemplos:
  - cotse.com
  - anonymiser.com
  - hushmail.com y muchos más.....

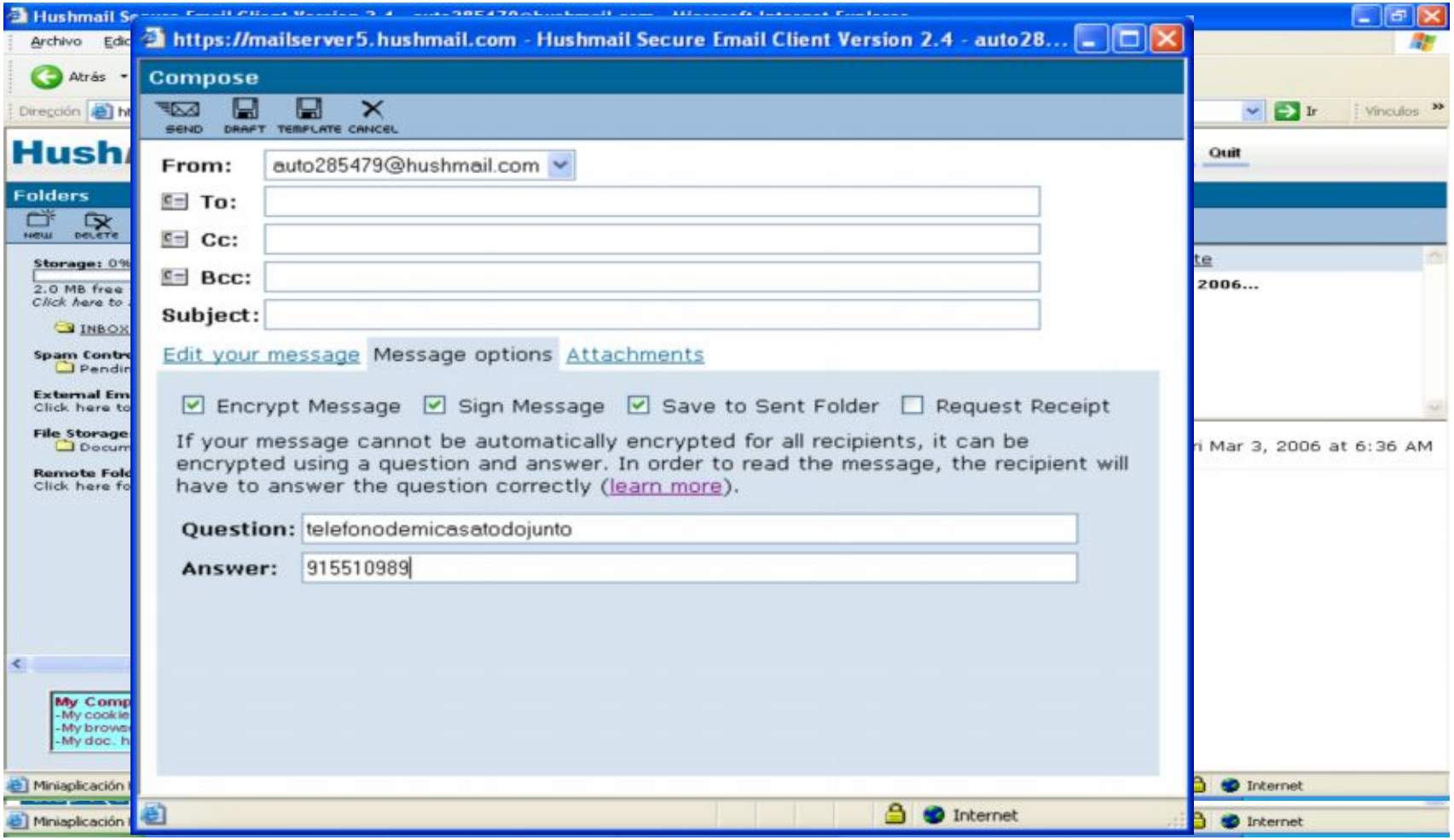
Ejemplo


Read email
Write email
DMZ | HOUSE
WRITE EMAIL:
Date : 26. januar 2004
To : engly@stofanet.dk
From : cyberpanser@hotmail.com
Subject : test
"Click here to launch attachment window"
Attachments :
This is a test - study the header....
SEND MAIL
Back

Contenido del Mail anónimo

- La cabecera no contiene la IP origen del mensaje.
- Será el proveedor del servicio de correo el único que puede disponer de los datos reales del emisor.

Otro ejemplo



Para que puede ser usado el correo electrónico

Como instrumento:

- Amenazas
- Chantajes y extorsiones
- Calumnias e injurias
- Fraudes
- Falsedad documental
- Distribución de pornografía infantil
- Propiedad intelectual
- Virus
- Comunicaciones entre miembros de organizaciones delictivas

Como objeto del delito

- Descubrimiento y revelación de secretos
- Secreto de las comunicaciones

Como medio de prueba:

- Documental
- Indicios por los trazos de la transmisión
- Interceptación del correo electrónico

Siempre hay que recordar

- El envío de un e-mail se puede realizar usando un cliente de correo y mediante servicios de correo web.
- Ser muy precisos en momento de leer las cabeceras de los correos.
- Las datos sobre horas y fechas deben ser precisos cuando consultamos a un proveedor de servicios de Internet.
- Para más información RFC 821: Simple Mail Transfer Protocol http://www.rfc-editor.org/

Preguntas

Muchas Gracias por su atención

Dr. Santiago Acurio Del Pino
Fiscalía General del Estado
sacurio@hotmail.com
acurios@minpec.gov.ec