



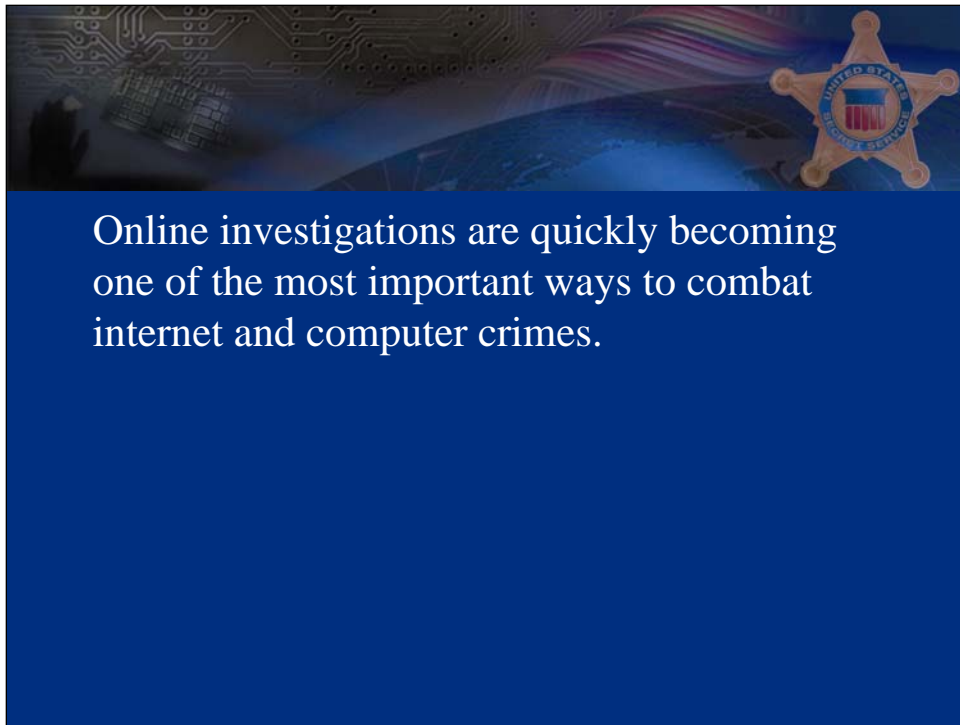
Collecting Digital Evidence:
Online Investigations



SA Matt Ralls
United States Secret Service, Oklahoma City Field Office

Recopilar la Evidencia Digital
Investigaciones de Internet

Agente Especial Matt Ralls
Servicio Secreto de Estados Unidos, Oficina de Campo de Oklahoma City



Las investigaciones de Internet están creciendo rápidamente convirtiéndose en una de las formas más importantes de combatir los delitos relacionados al Internet y a las computadoras

Objectives

- Learn about common applications such as P2P, IRC, VOIP
- How to perform online reconnaissance
- How to protect the investigators online identity
- What information do Internet Service Providers have, and how can we obtain it?
- International Issues

Objetivos

Aprender acerca de las aplicaciones comunes como IRC, P2P, VOIP

Como llevar a cabo una acción de reconocimiento usando el Internet

Como proteger la identidad del investigador en línea

¿Qué información tienen los proveedores de servicios de Internet, y

cómo la podemos obtener?

Asuntos internacionales

Common Applications



- P2P: Peer to Peer
 - Utilized primarily in child exploitation and intellectual property rights violations
- IRC: Internet Relay Chat
- Messenger Programs
 - Yahoo, AIM, ICQ
- VoIP
 - refers to communications services—voice, facsimile, and/or voice-messaging applications—that are transported via the Internet

Aplicaciones comunes

P2P: Programas “de colega a colega”

Utilizados principalmente en delitos que involucran la explotación de niños y violaciones de derechos sobre la propiedad intelectual.

IRC: Chat por Internet

Programas de Mensajes electrónicos

Yahoo, AIM, ICQ

VOIP (Protocolo de Voz por el Internet)

se refiere a servicios de comunicaciones — voz, facsímile, y/o aplicaciones de mensajería de voz — transportadas a través del Internet

Peer to Peer Simplified



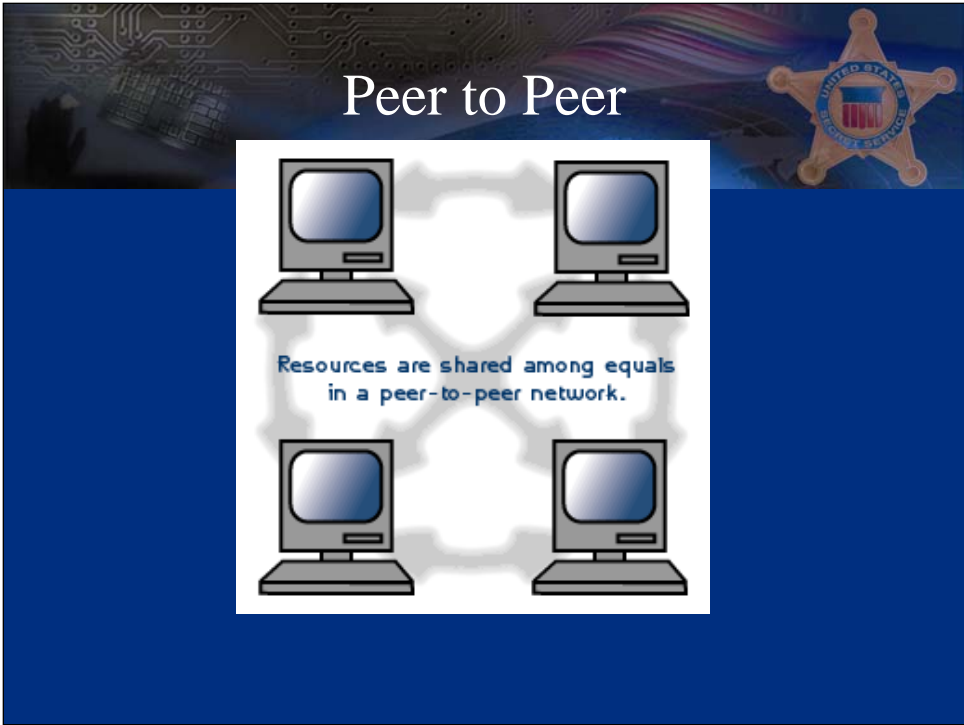
- Peer to Peer is different from traditional file downloading in that a software program is utilized to locate other computers which have a file you want.
- There is no centralized server
- Popular P2P applications: Limewire, BitTorrent

“De colega a colega” Simplificado

El P2P es diferente a las descargas tradicionales de archivos en que un software es utilizado para ubicar otras computadoras que tienen un archivo que usted desea.

No hay un servidor centralizado

Aplicaciones populares de P2P: Limewire, BittTorrent



Colega a Colega

Se comparten los recursos entre iguales en una red de colega a colega

Investigative Tools



- SnagIt and other screen capture programs are invaluable at taking a screenshot or a video of what it is you are seeing on screen.

Give example of ICE's Operation Fairplay (?????? IF POSSIBLE)

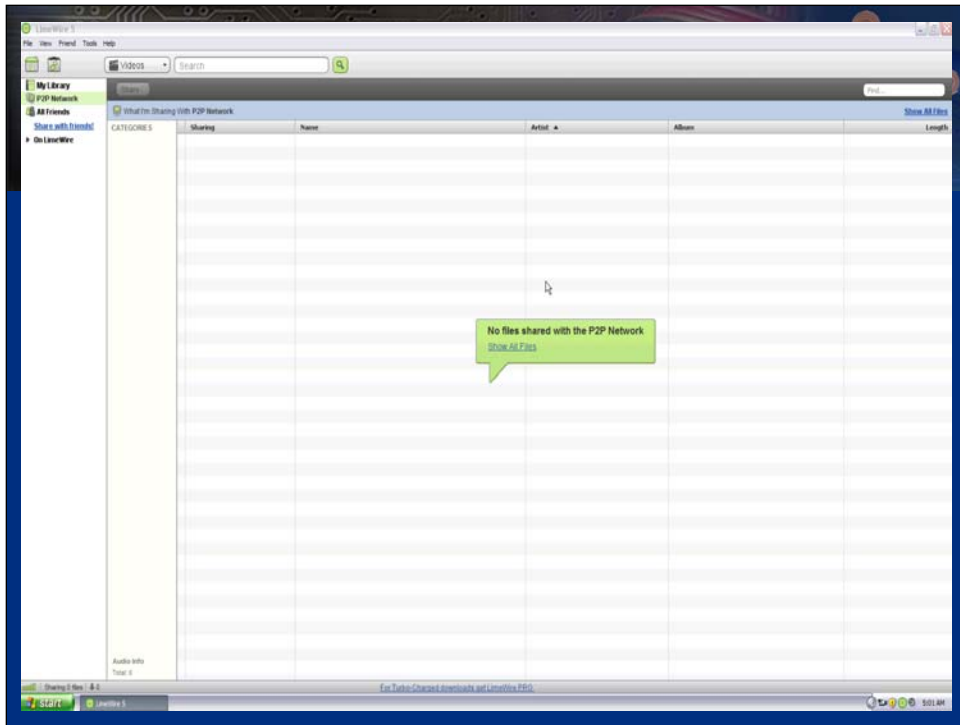
Dar un ejemplo de la Operación Juego Limpio (?????? SI ES POSIBLE)

Emphasize how a screen capture program can be setup to display the exact time and date that an investigator is conducting online activity such as obtaining information from a P2P network.

Destacar como puede configurarse un programa de captura de pantalla para mostrar la fecha y hora exacta en que un investigador está realizando una actividad en línea, como por ejemplo, obtener información de una red P2P.

Herramientas de investigación

SnagIt y otros programas de captura de pantalla son invaluable para capturar una vista instantánea de la pantalla o un video de lo que se ve en la pantalla



Cover Operation Fairplay
Cubrir la Operación Juego Limpio

Online Reconnaissance



- Google
- Bing
- Wiki
- Pipl.com
- Google Maps
- Whois.net
- ADD MORE***

Reconocimiento del Internet

Google

Bing

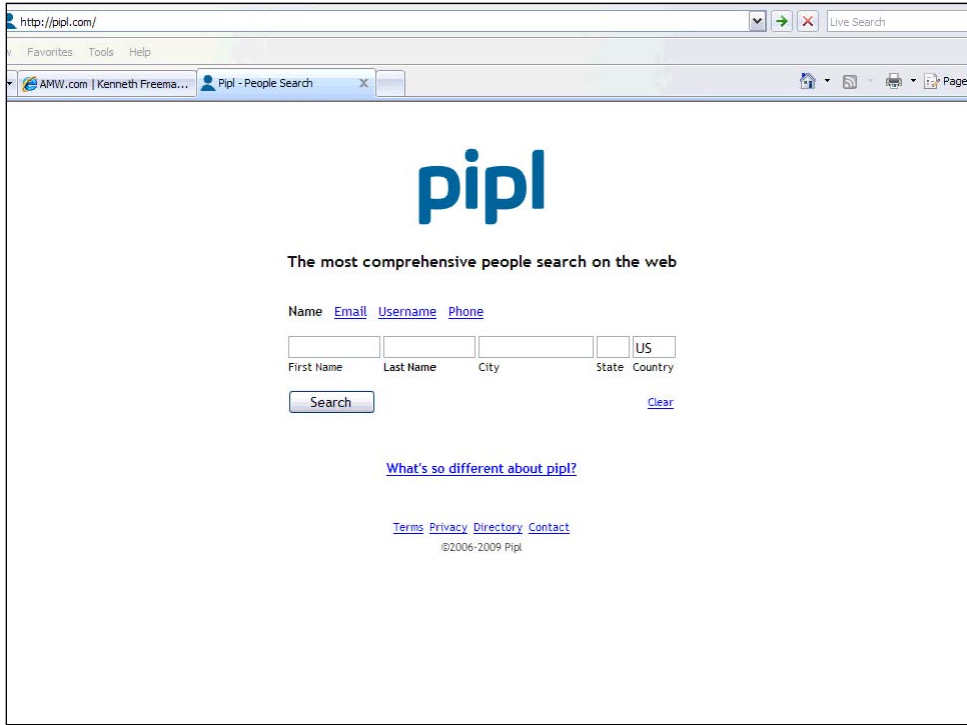
Wiki

Pipl.com

Mapas Google

Whois.net

AGREGAR MÁS***



Protecting the Investigator's Online Identity

- Backstop all internet accounts to a “non-government” name, account, address.
- Never utilize a government computer for any reconnaissance activity.

Describe how a simple IP lookup for an IP found in an email header or a server log can be traced back.

Describir la manera en que puede rastrearse una búsqueda simple por un IP ubicado en un encabezamiento de un correo electrónico o en un registro del servidor.

Proteger la identidad del investigador en línea

Asegúrese que todas las cuentas de Internet, incluyendo el nombre, la cuenta, la dirección, etc. no deben de estar afiliadas al gobierno.

Jamás usar una computadora del gobierno para cualquier actividad de reconocimiento del Internet.

Working with Internet Service Providers (ISP's)

- For the most part, in the United States working with an ISP is much the same as working with any other consumer communications provider:
- Send them the appropriate legal process, they will send you what you want.
- One major difference is that, unlike a cell phone, Internet Protocol (IP) Addresses change very often (need specific date and time)

Trabajar con los proveedores de servicios del Internet

Por lo general, trabajar en los Estados Unidos con un proveedor de servicios de Internet es lo mismo que trabajar con cualquier otro proveedor de comunicaciones al consumidor.

Enviarles el proceso legal apropiado, ellos le enviarán lo que usted desee.

(DISCUSS SUBSCRIBER NOTIFICATION)

(HABLAR DE NOTIFICACIONES AL SUBSCRIPTOR)

Una distinción importante es que, a diferencia de un teléfono celular, las direcciones de Protocolo de Internet (IP) cambian muy seguido (es necesario tener la fecha y hora específica).

International Issues



- www.babelwith.me
- www.google.com (translate)
- www.Forwardedge2.com (international resources)

Asuntos Internacionales

www.babelwith.me

www.google.com (traducir)

www.Forwardedge2.com (recursos internacionales)