



# Email Investigations

## An Introduction

Al Rees

Trial Attorney

Computer Crime and Intellectual Property Section (CCIPS)

Criminal Division, U.S. Department of Justice

- Understanding email basics
- Collecting email and associated data
- Finding information in email messages

- Understanding email basics
- Collecting email and associated data
- Finding information in email messages

# Requirements for Email

- Email application
  - Computer-based application
  - Web-based email (webmail)
  - Generates an **email address**
- Internet connection
  - Relies on an **Internet Protocol (IP) address**
- Service provider
  - Internet service provider (ISP)
  - Webmail service provider

# Email Address

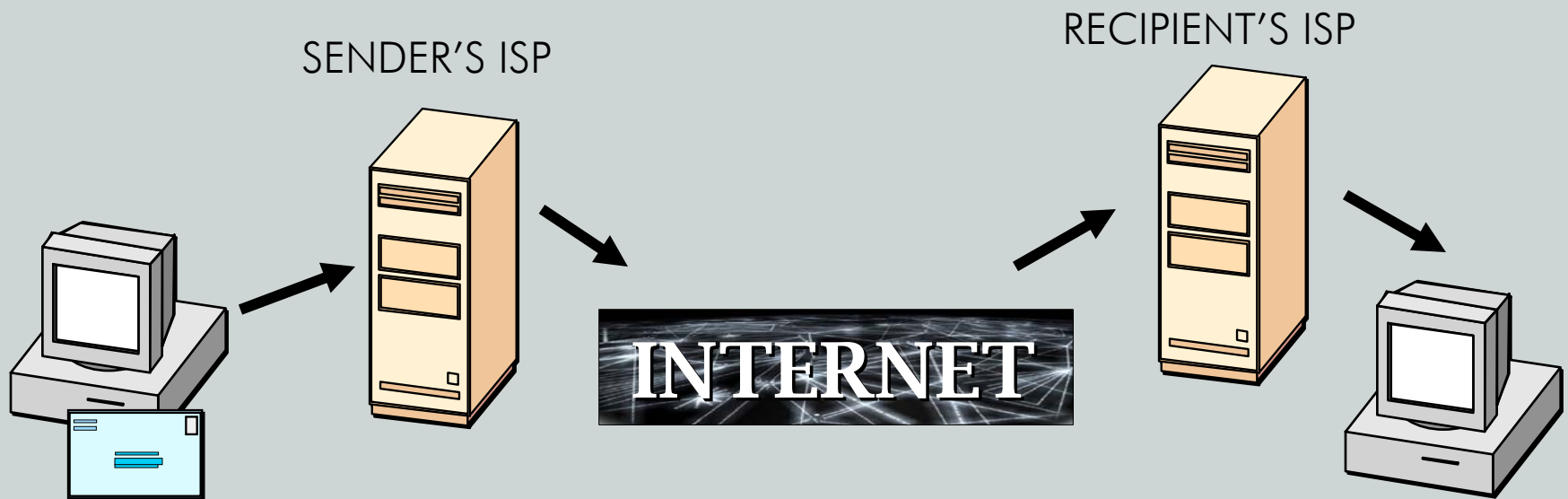
albert.rees@usdoj.gov

# IP Address

149.101.1.120

# E-Mail Basics

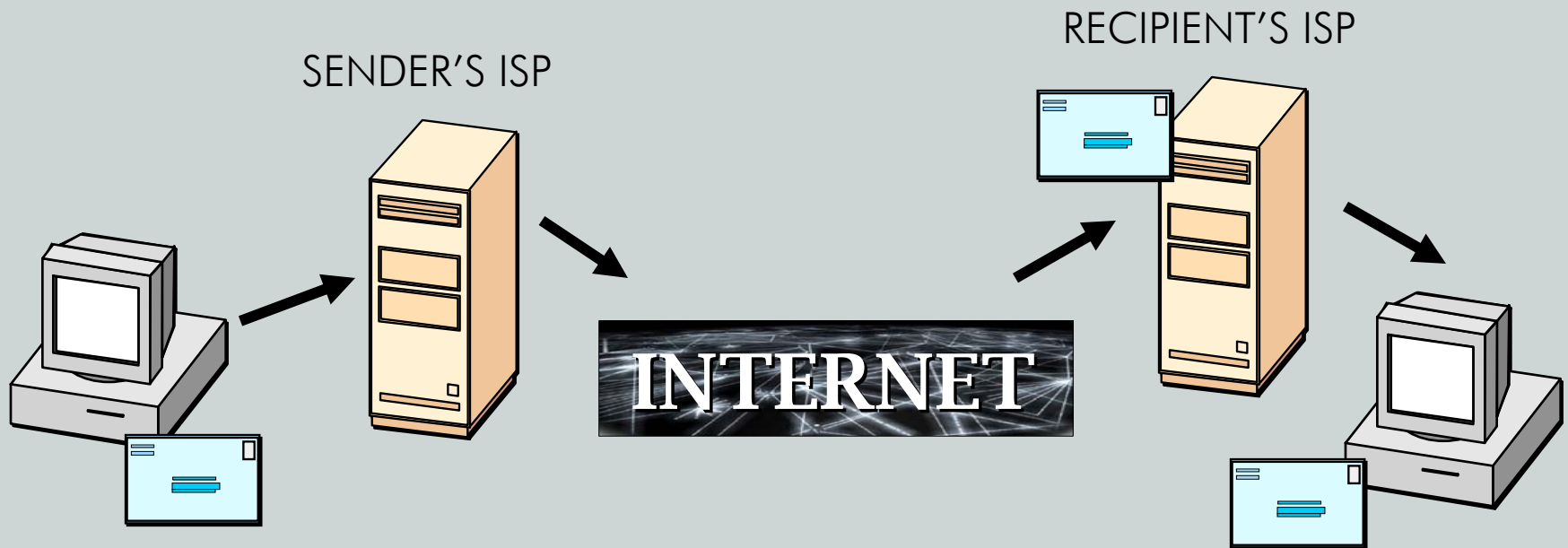
- E-mail travels from sender to recipient's host, where it resides on a **MAIL SERVER** until the recipient retrieves it



- Understanding email basics
- Collecting email and associated data
- Finding information in email messages

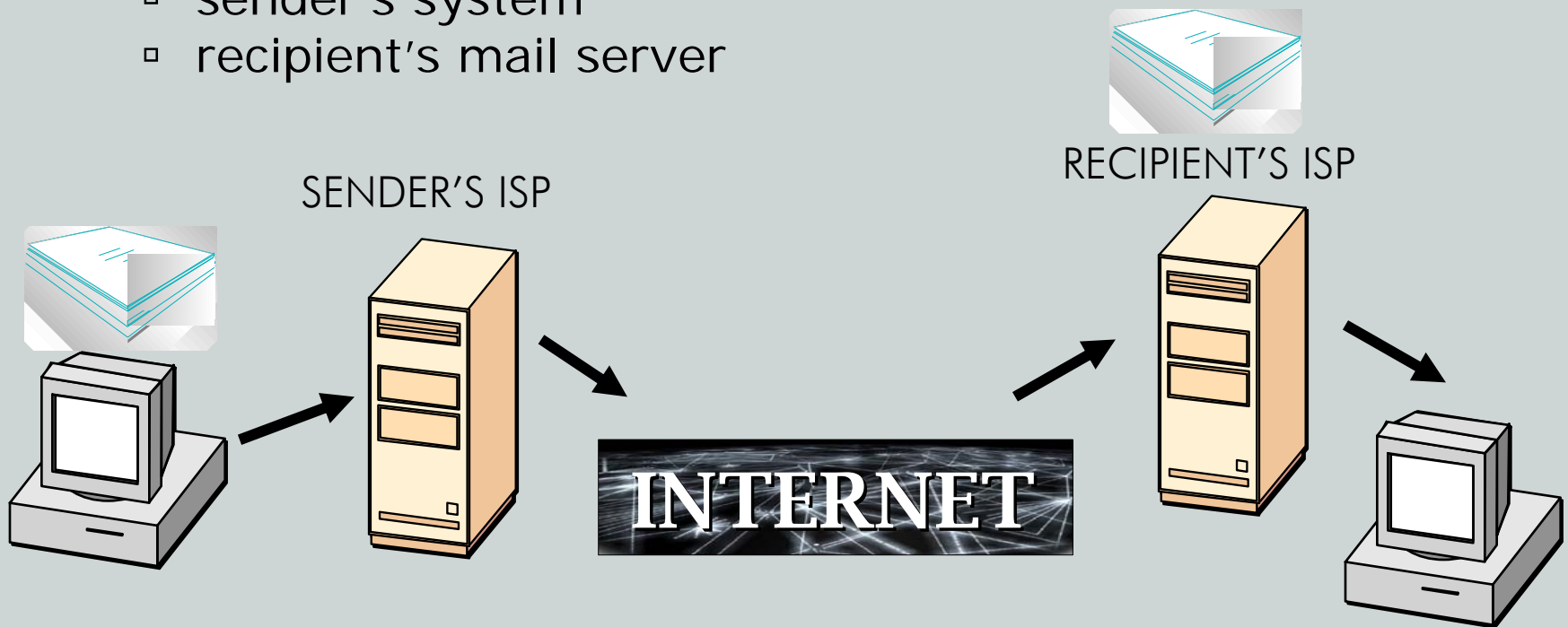
# Evidence of Past Activity – Content

- Copies of a previously sent e-mail message may be stored on the
  - sender's system
  - recipient's mail server (even after addressee has read it)
  - recipient's own machine



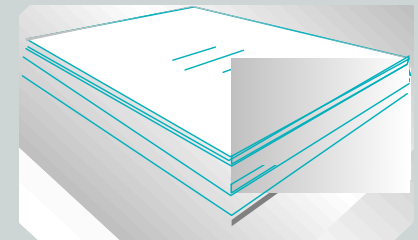
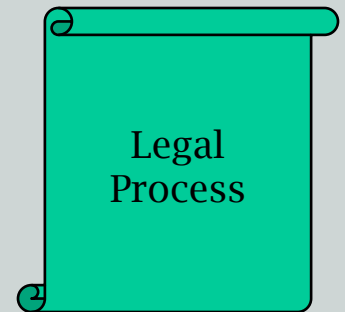
# Evidence of Past Activity – Traffic Data

- A record of the e-mail transmission (date, time, source, destination) usually resides in the **MAIL LOGS** of the
  - sender's system
  - recipient's mail server



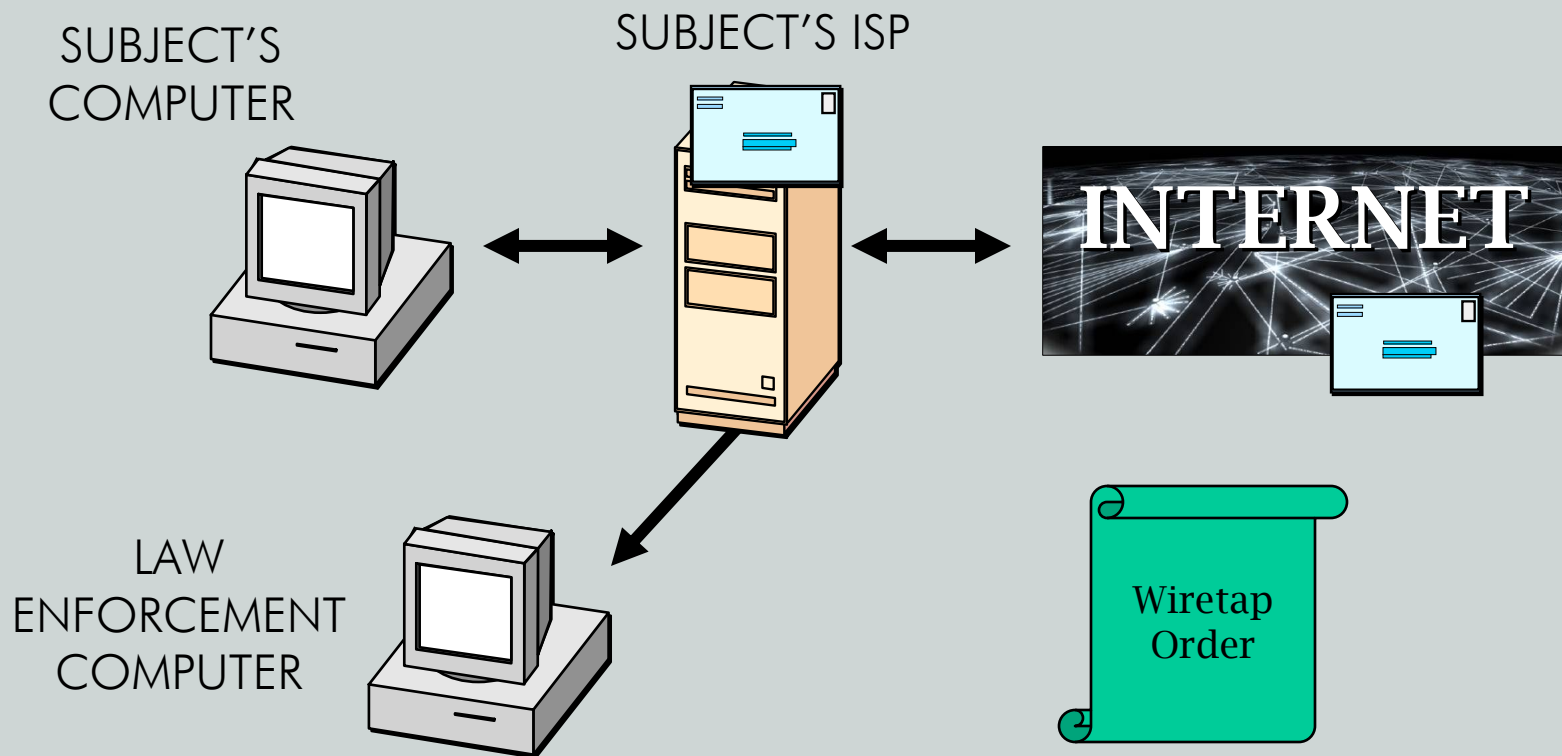
# Gathering Evidence of Past Activity

- Evidence on a computer or network
  - Search and seizure
  - Imaging and analyzing
  
- Evidence with a service provider
  - Data preservation or retention
  - Ability to provide evidence
  - Legal procedures
  - International considerations



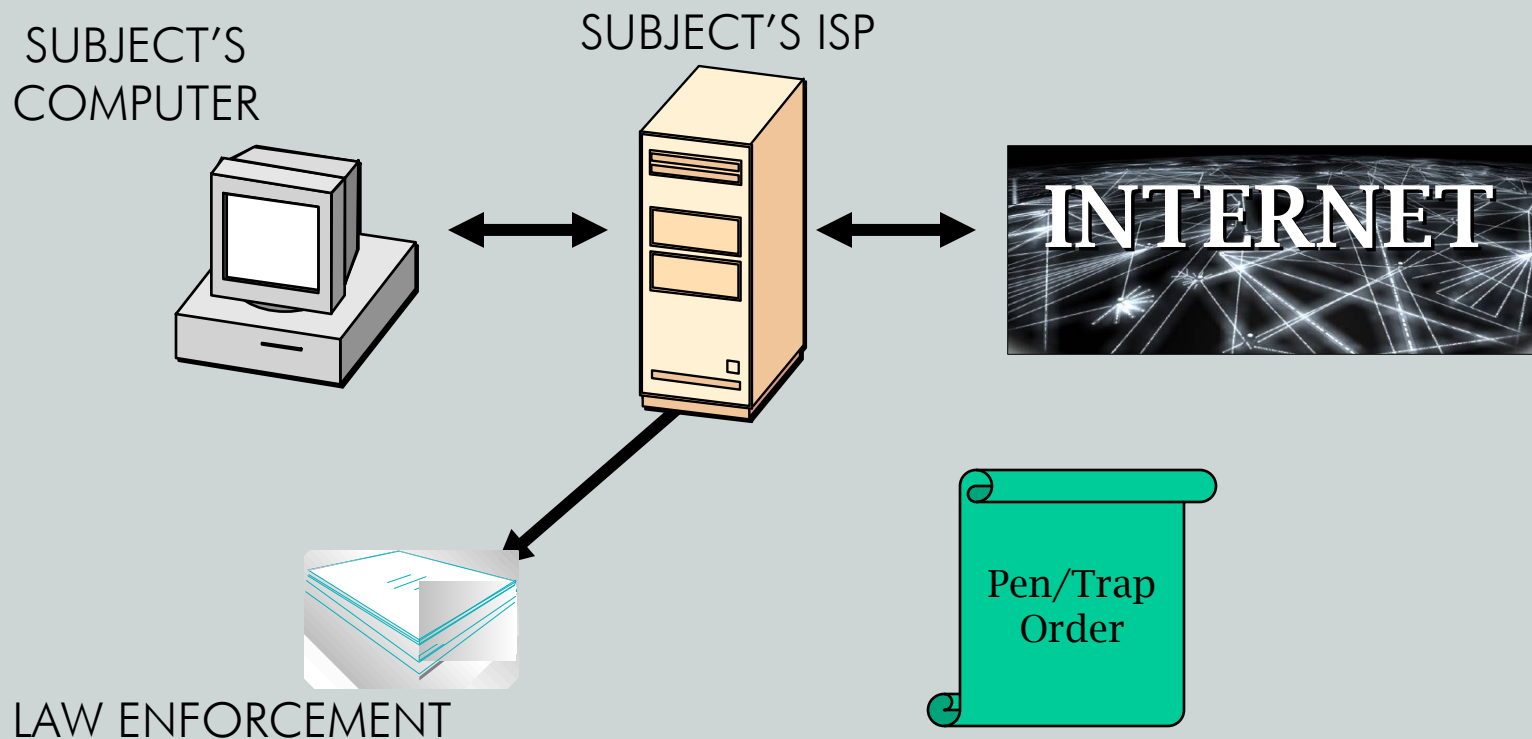
# Prospective Evidence – Content

- Interception, “wiretap”
- Creates a “cloned” account



# Prospective Evidence – Traffic Data

- Install a pen/trap at user's ISP to discover who corresponds with the user



- Understanding email basics
- Collecting email and associated data
- Finding information in email messages

# Finding Information in Email

- Content
  - Subject
  - Body
  - Attachments
  - Links
  
- Traffic data
  - Sender and recipient
  - Routing information
  - Date and time

# Content

## Message0005

**Subject:** pics from last weekend

**From:** Maryland Dirtbag

**Date:** 2/20/2007 1:22:41 PM

**To:** pswift2007@gmail.com

## Message Body

Buddy, here is the pics from last weekend. I flet like a king on presidents holiday.

>From: "Peter Swift" <pswift2007@gmail.com>

>To: <mdhosebag@hotmail.com>

>Subject: last one

>Date: Thu, 15 Feb 2007 14:53:26 -0500

>

>this is the last one for a bit, you should be able to get you jollies from

# Content

- Subject line
- Body
- Attachments
- Hyperlinks

# Email Headers

## Standard Header Information

Delivered-To: pswift2007@gmail.com  
 Received: by 10.64.153.3 with SMTP id a3cs152336qbe;  
 Tue, 20 Feb 2007 10:22:41 -0800 (PST)  
 Received: by 10.114.126.1 with SMTP id y1mr3442785wac.1171995758192;  
 Tue, 20 Feb 2007 10:22:38 -0800 (PST)  
 Return-Path: <mdhosebag@hotmail.com>

Tue, 20 Feb 2007 10:21:38 -0800

Message-ID: <BAY115-F286B576945D5DB4E9F0288B3890@phx.gbl>

Received: from 65.54.250.200 by by115fd.bay115.hotmail.msn.com with HTTP;

Tue, 20 Feb 2007 18:21:36 GMT

X-Originating-IP: [66.166.254.82]

X-Originating-Email: [mdhosebag@hotmail.com]

X-Sender: mdhosebag@hotmail.com

From: "Maryland Dirtbag" <mdhosebag@hotmail.com>

To: pswift2007@gmail.com

Bcc:

Subject: pics from last weekend

Date: Tue, 20 Feb 2007 13:21:36 -0500

Mime-Version: 1.0

Content-Type: multipart/mixed; boundary="----=\_NextPart\_000\_1290\_1f21\_3b10"

X-OriginalArrivalTime: 20 Feb 2007 18:21:38.0744 (UTC) FILETIME=[F6436B80:01C7551B]

Return-Path: mdhosebag@hotmail.com

X-OriginalArrivalTime: 20 Feb 2007 18:21:38.0744 (UTC)

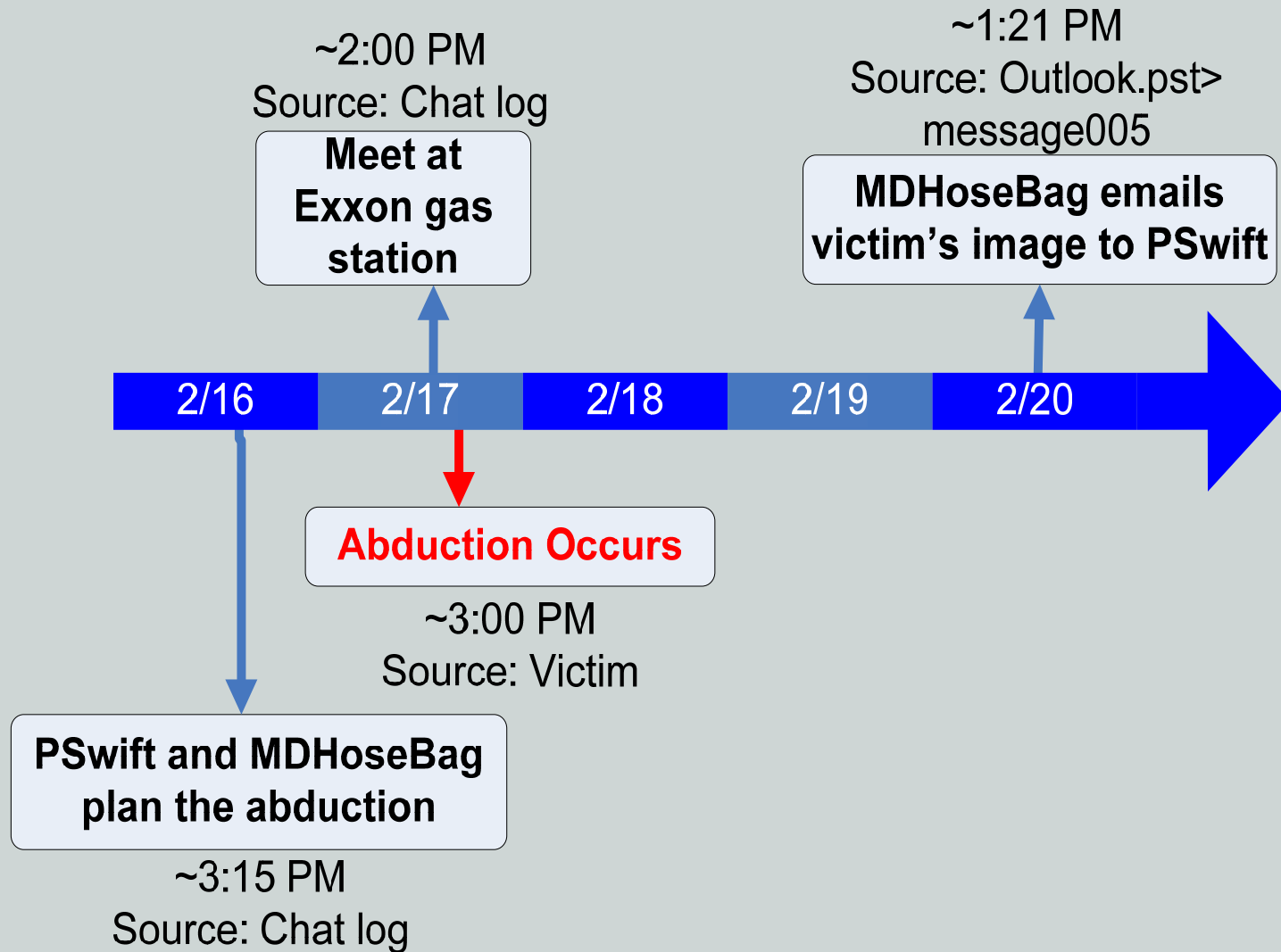
# Traffic Data

- When created
- How created
- When sent
- When received
- Who sent and received
- Routing

# Email Analysis: A Starting Point

- Iterative process
- Generates leads
- Direct evidence
- Timeline analysis

# Timeline of Events



# Issues

- Spoofing
- Phishing
- Spamming

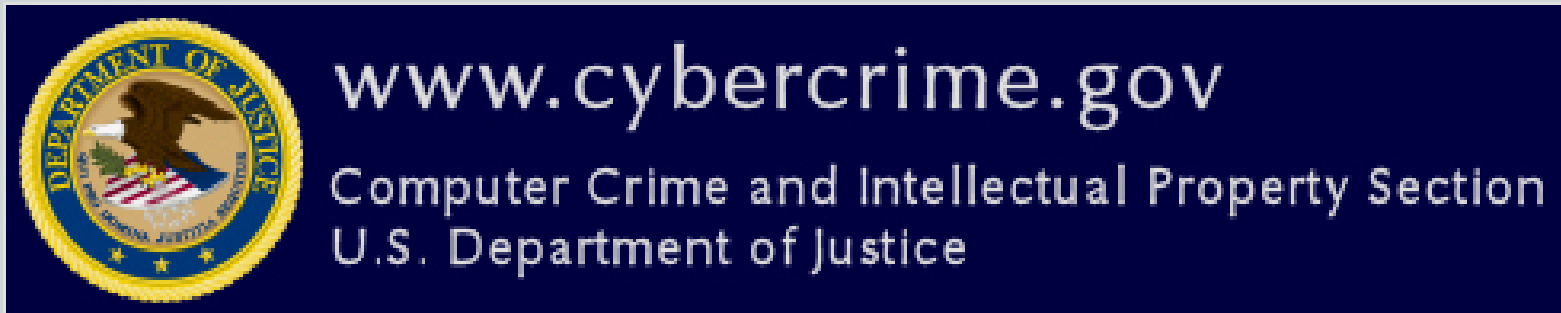
## In Closing...

- Understanding email basics
- Collecting email and associated data
- Finding information in email messages

...any questions?

**Al Rees**

Trial Attorney, CCIPS



albert.rees@usdoj.gov  
(202) 514-1026