Networks and the Internet

A Primer for Prosecutors and Investigators

Al Rees
Trial Attorney
Computer Crime and Intellectual Property Section (CCIPS)
Criminal Division, U.S. Department of Justice

Getting There...

- From networks to the Internet
- Locating a place on the Internet
- Applications that let people use the Internet

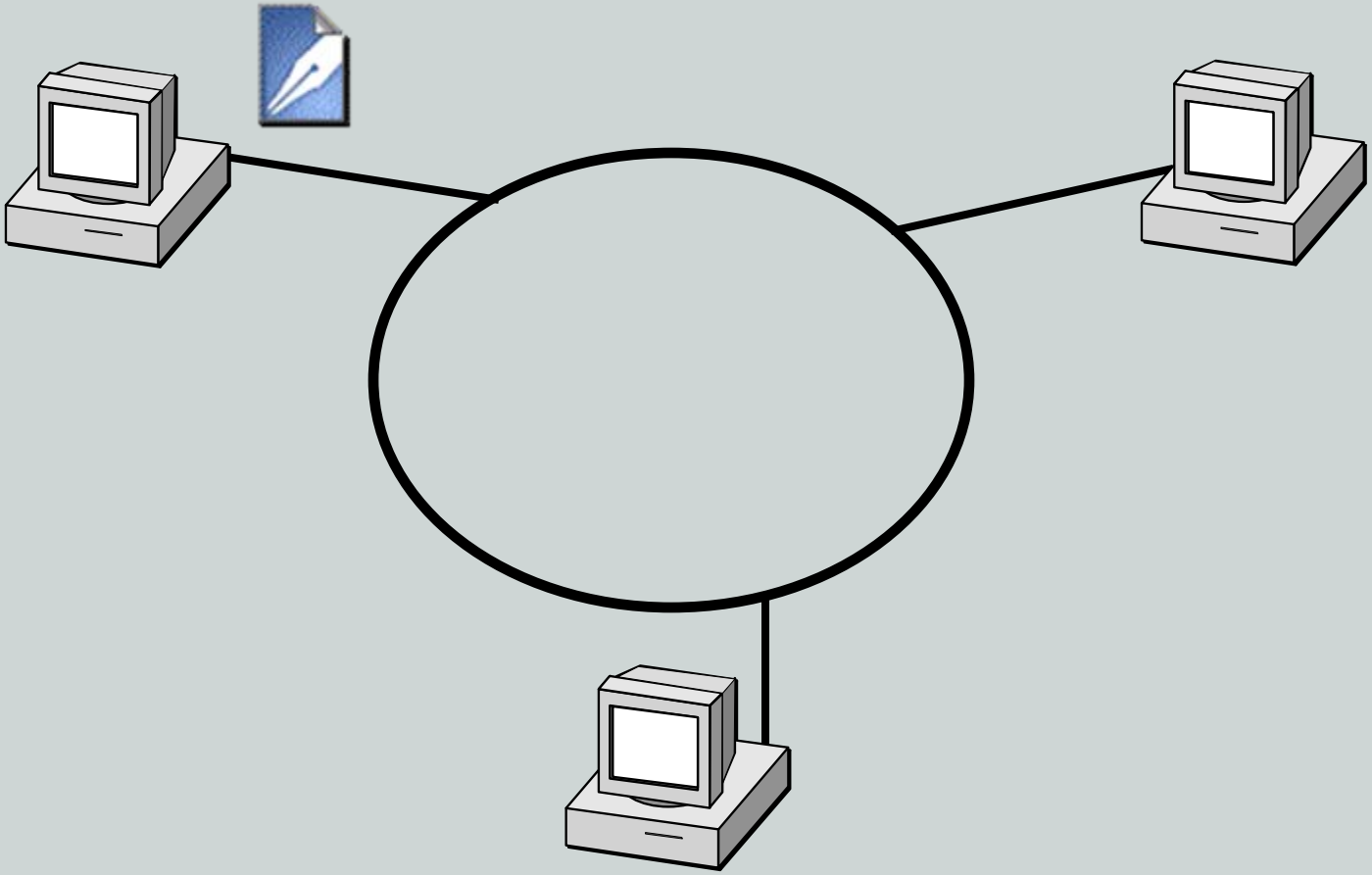
...to Get the Evidence

- What evidence does Internet use create?
- Where is this evidence located?
- How do we gather this evidence?

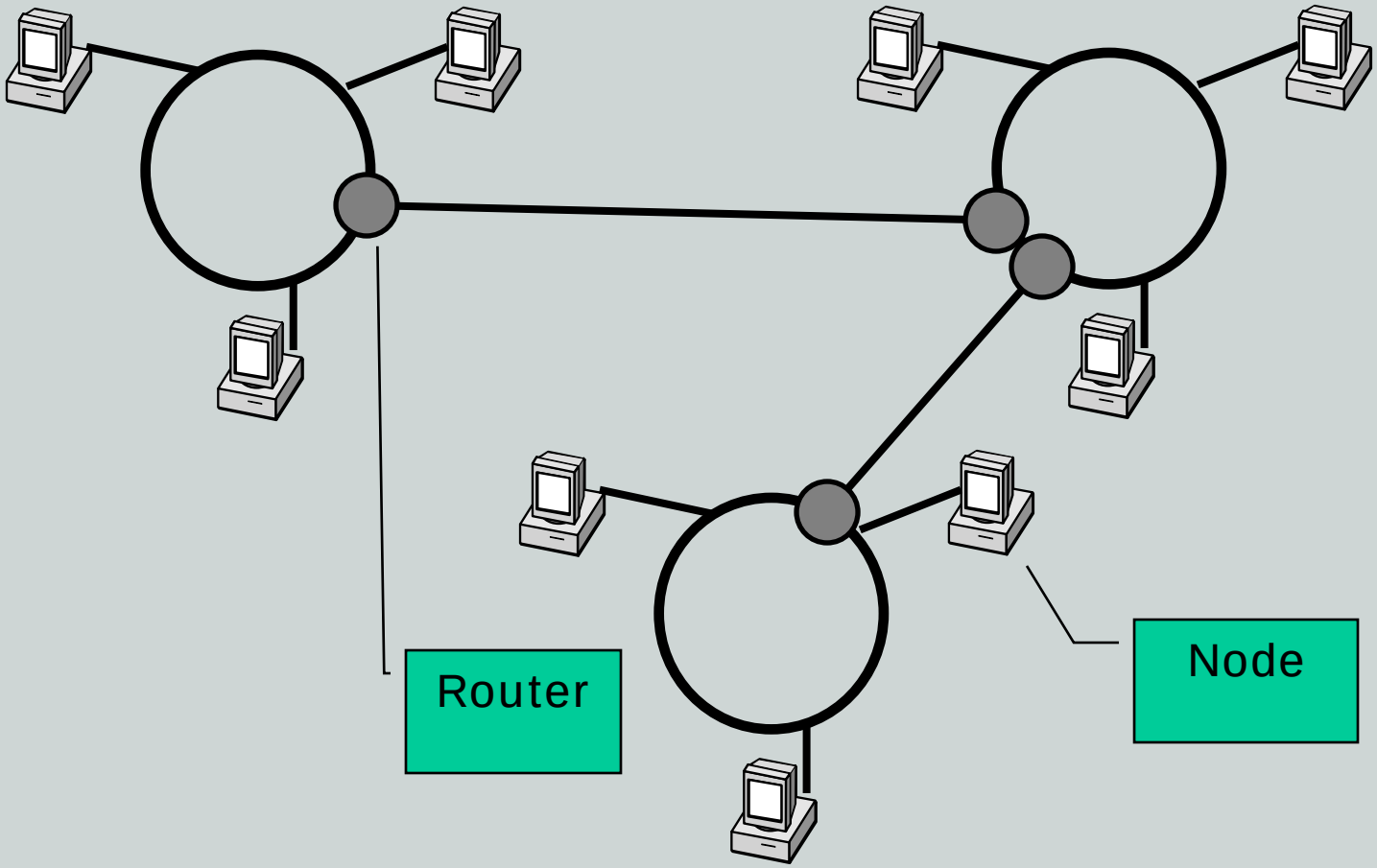
Getting There...

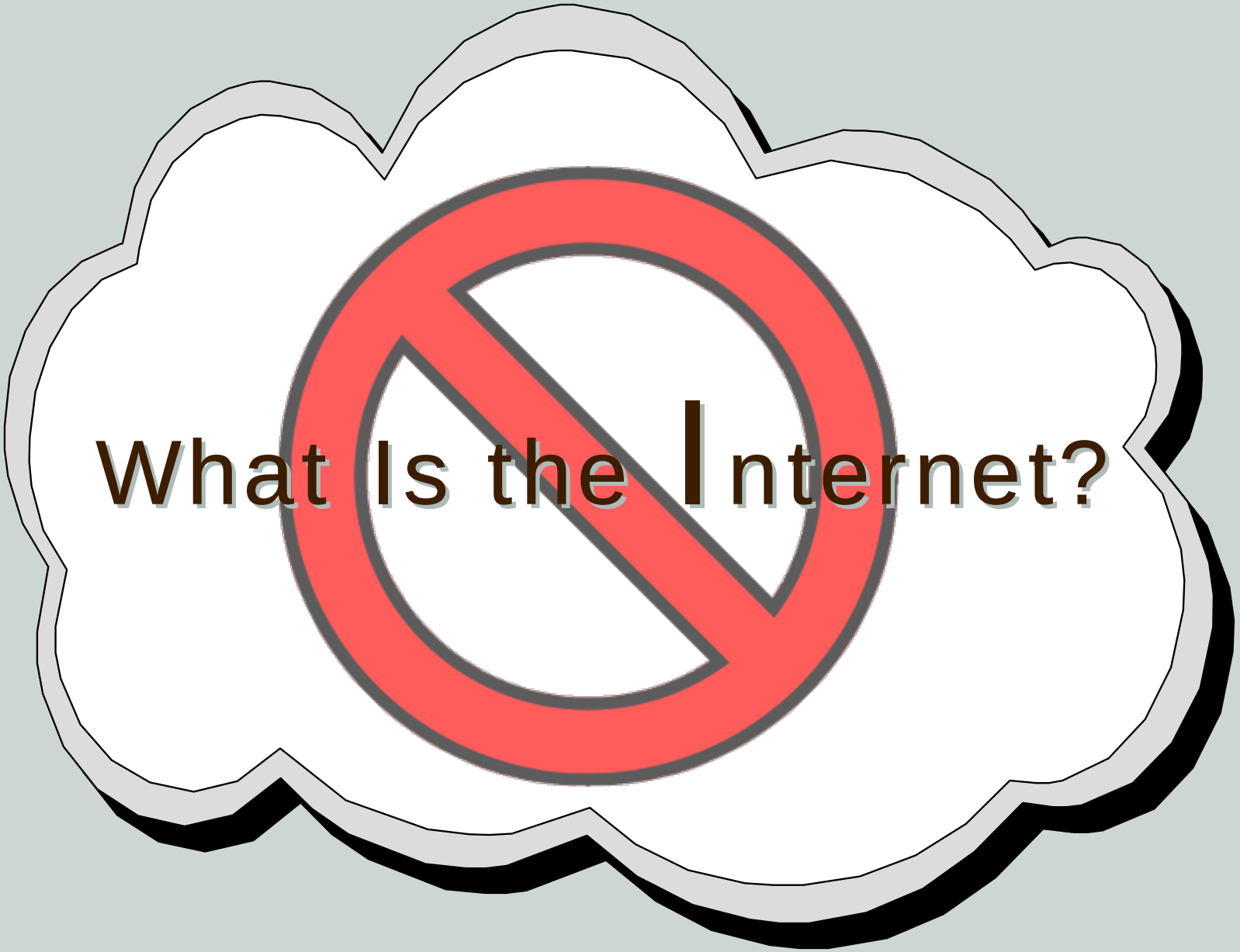
- From networks to the Internet
- Locating a place on the Internet
- Applications that let people use the Internet

What is a network?



What is an inter-network?




What Is the Internet?

A Decentralized Network

- No “center”
- No one is in charge
- No one knows exactly where all the components are located

How do Internet hosts exchange data?

WEB PAGE

MOVIE

E-MAIL MESSAGE

VOICE

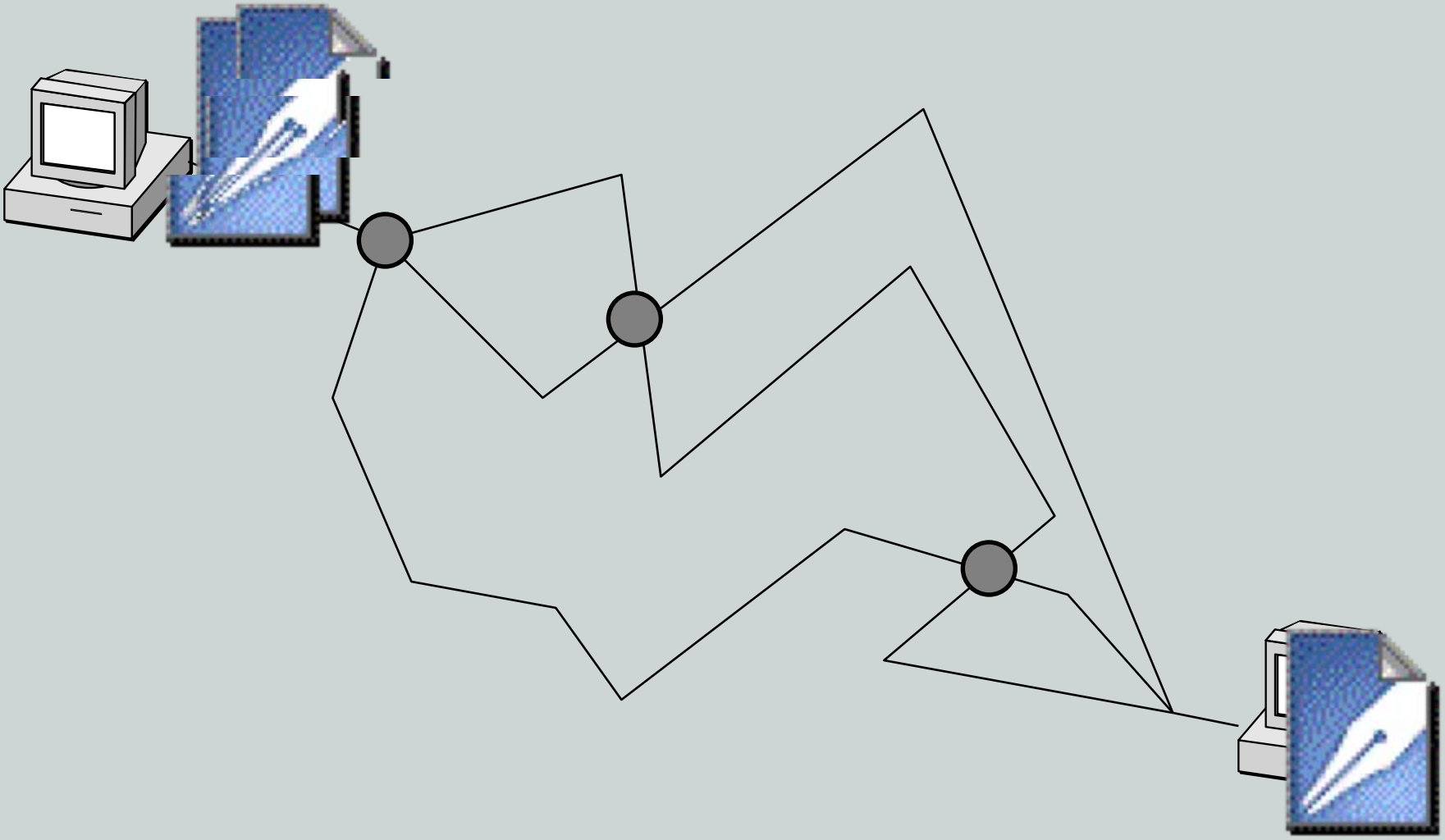
SOFTWARE

DATA

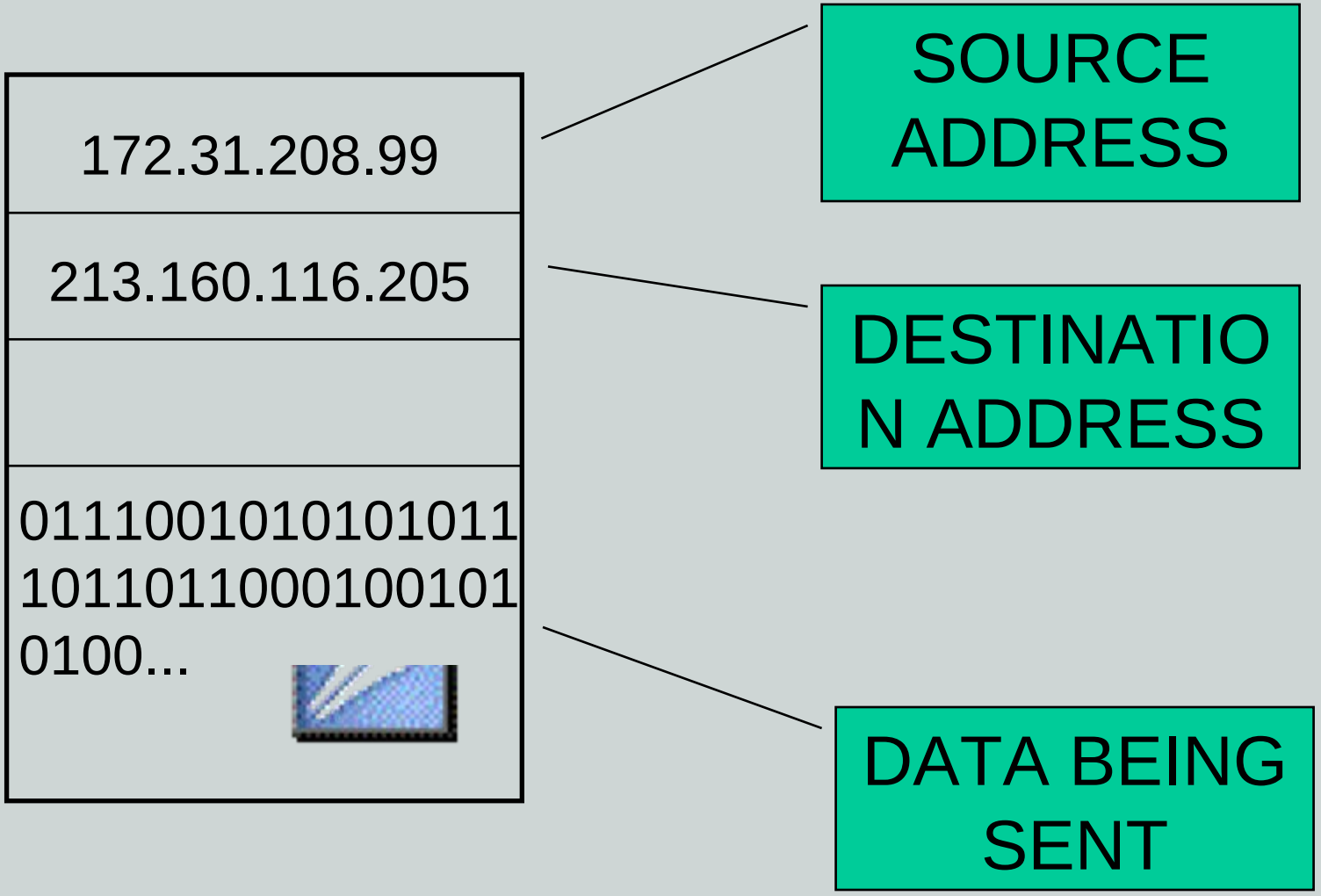
Exchanging Data

- Information to be sent to another Internet host is divided into small **DATA PACKETS**
- The data packets are sent over the network to the receiving host
- The receiving host assembles the data packets into the complete communication

Exchanging Data



Internet Protocol (IP) Packets



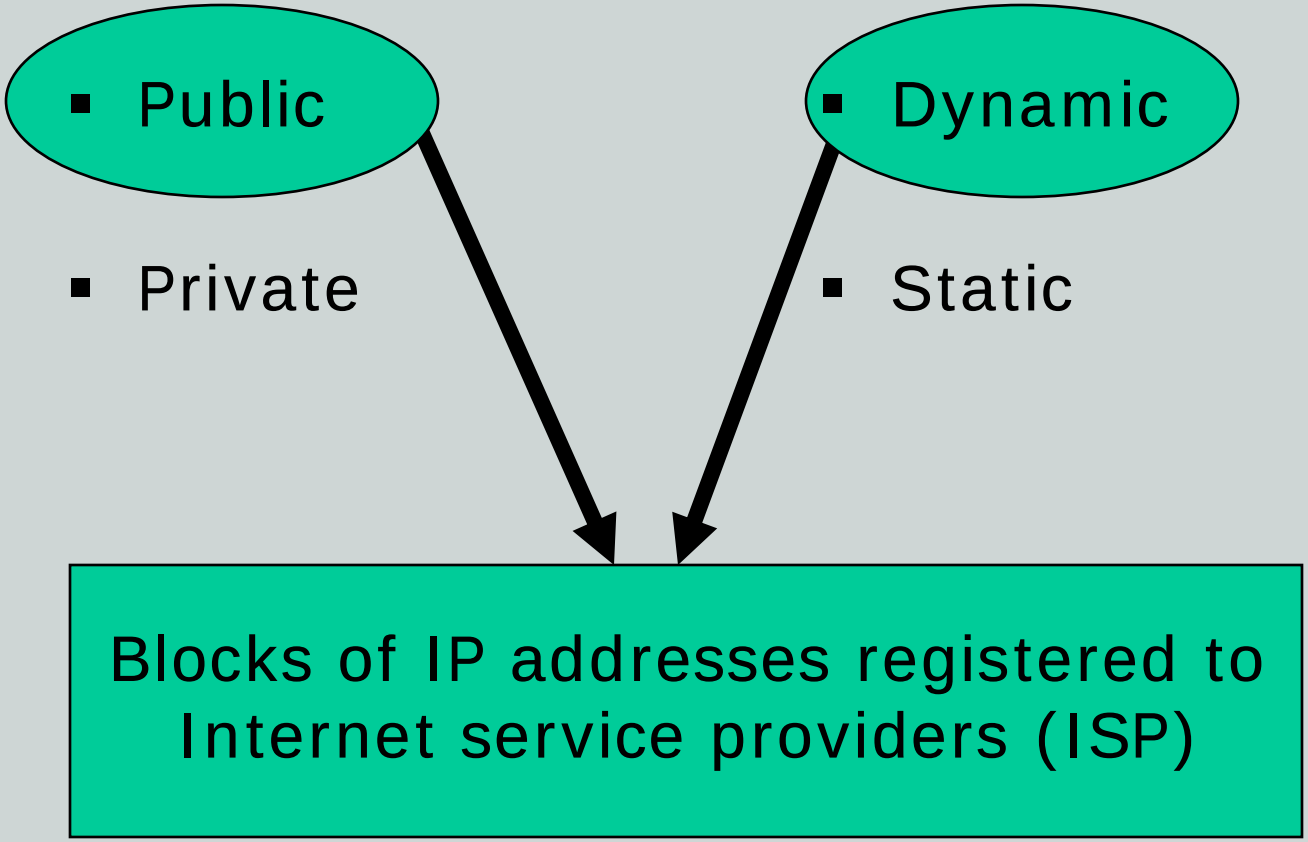
Getting There...

- From networks to the Internet
- Locating a place on the Internet
- Applications that let people use the Internet

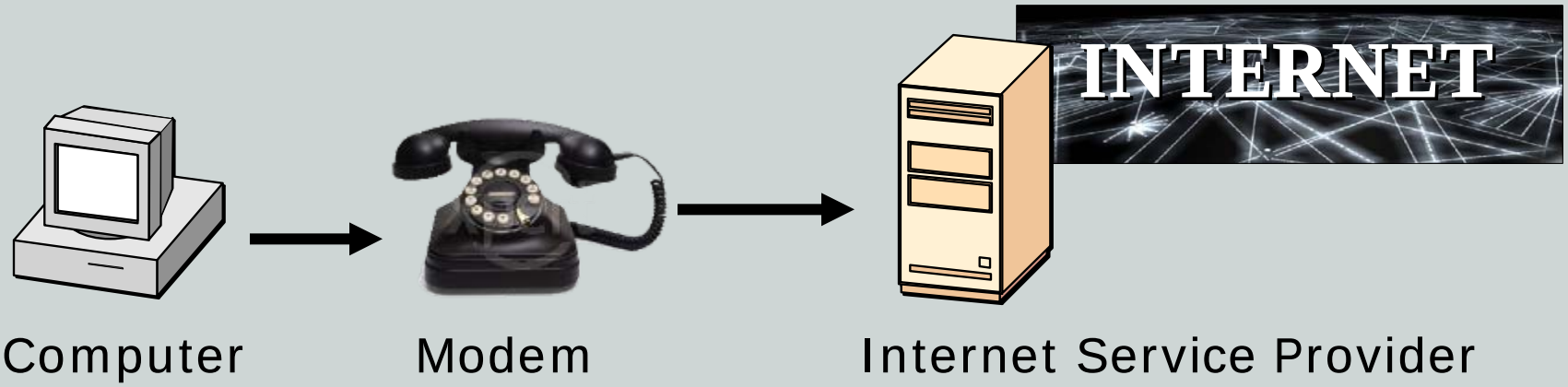
IP Addresses

213.160.116.205

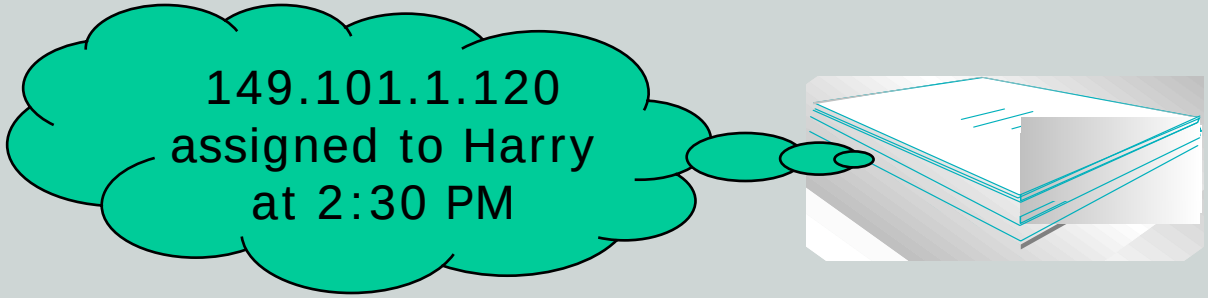
Assigning IP Addresses



Assigning IP Addresses

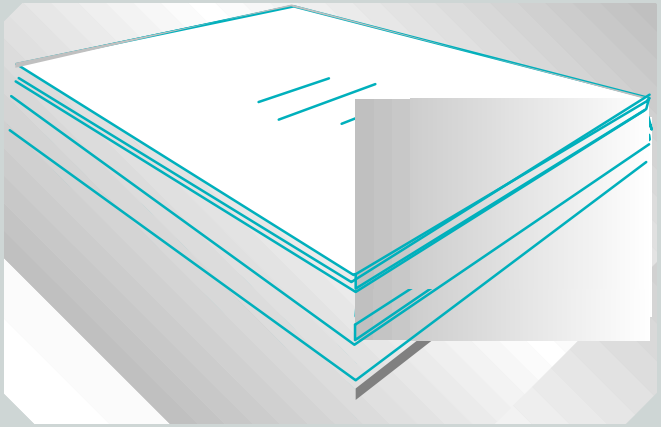


149.101.1.120



ISP Login Records

- The ISP-equivalent of telephone company records
- Records each time a user logs in (or tries and fails)
- Logs show
  - Start time
  - Session duration
  - Account identifier
  - Assigned IP address



The Traceback

- We know the IP address used by the suspect
- How do we find out who this person is?

149.101.1.120 →

Step 1: What ISP has that address?

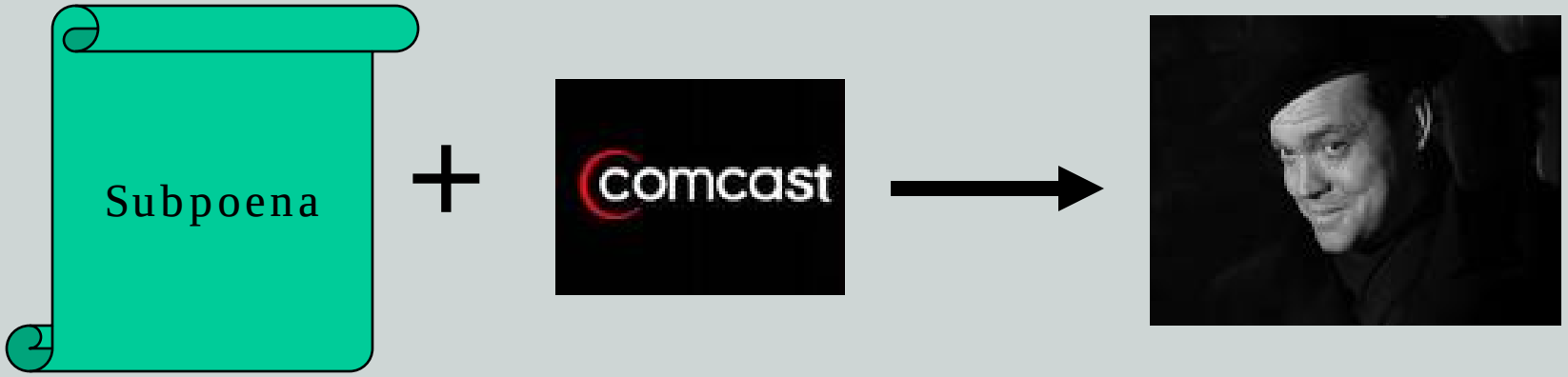
- Use the "**IP whois**" service to find out what ISP owned that IP address.

149.101.1.120 → 

Step 2: What user had that address at that time?

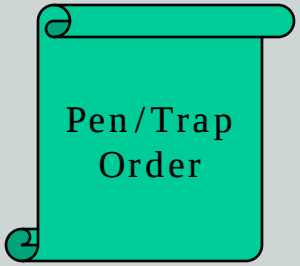
- Subpoena the ISP to find out who had that address

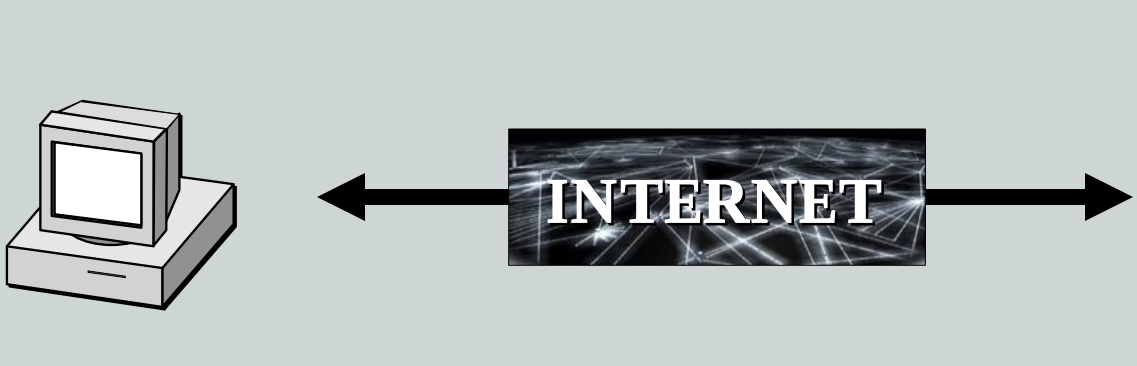
- Specify at least the address and the time and date with time zone.



Another Location Method: Prospective Evidence Gathering

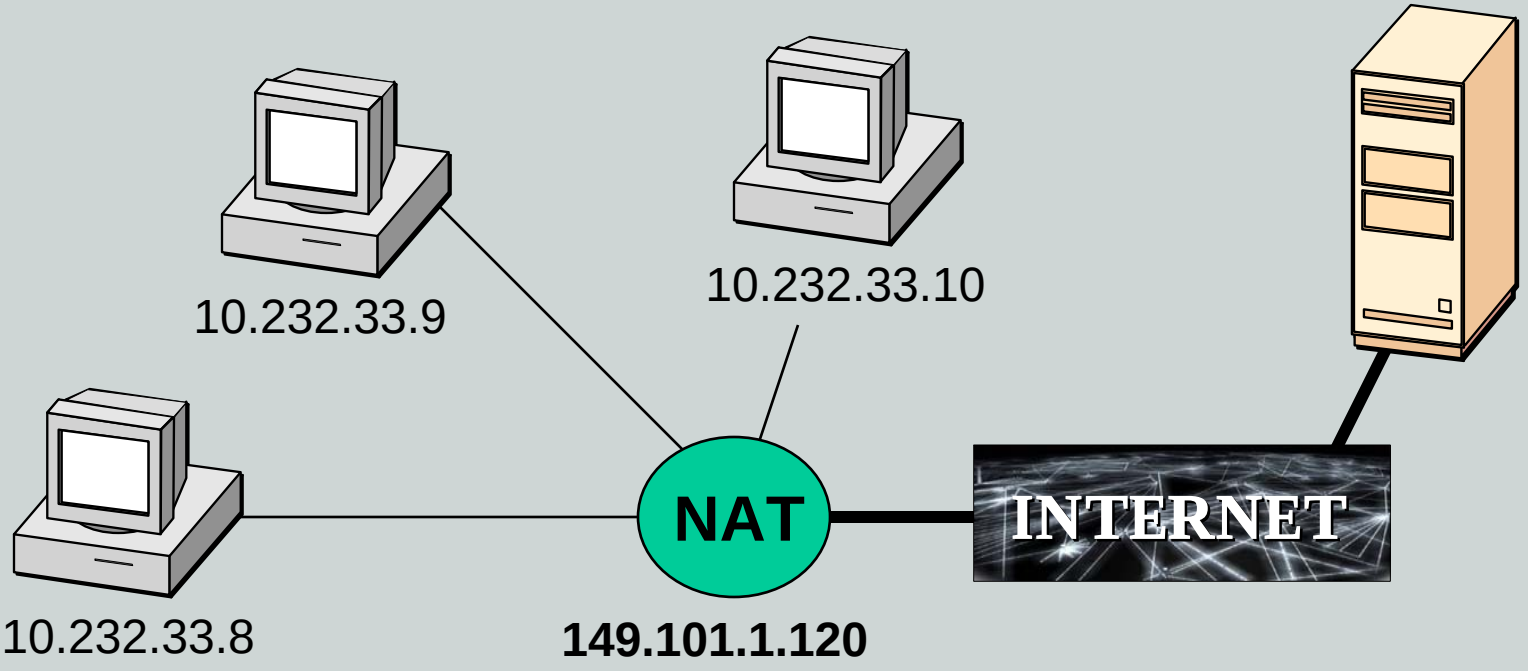
- We know that our suspect was at a site and believe he'll return
- A pen/trap device installed at the site's server provides the suspect's IP address when he returns





A Twist: The NAT

- Several computers share one IP address
- Outside world sees the same address regardless of which computer communicates



Another Twist: The Proxy

- "Laundering" communications through someone else's IP address
- Outside world sees only the proxy's IP address

Infamous Proxies

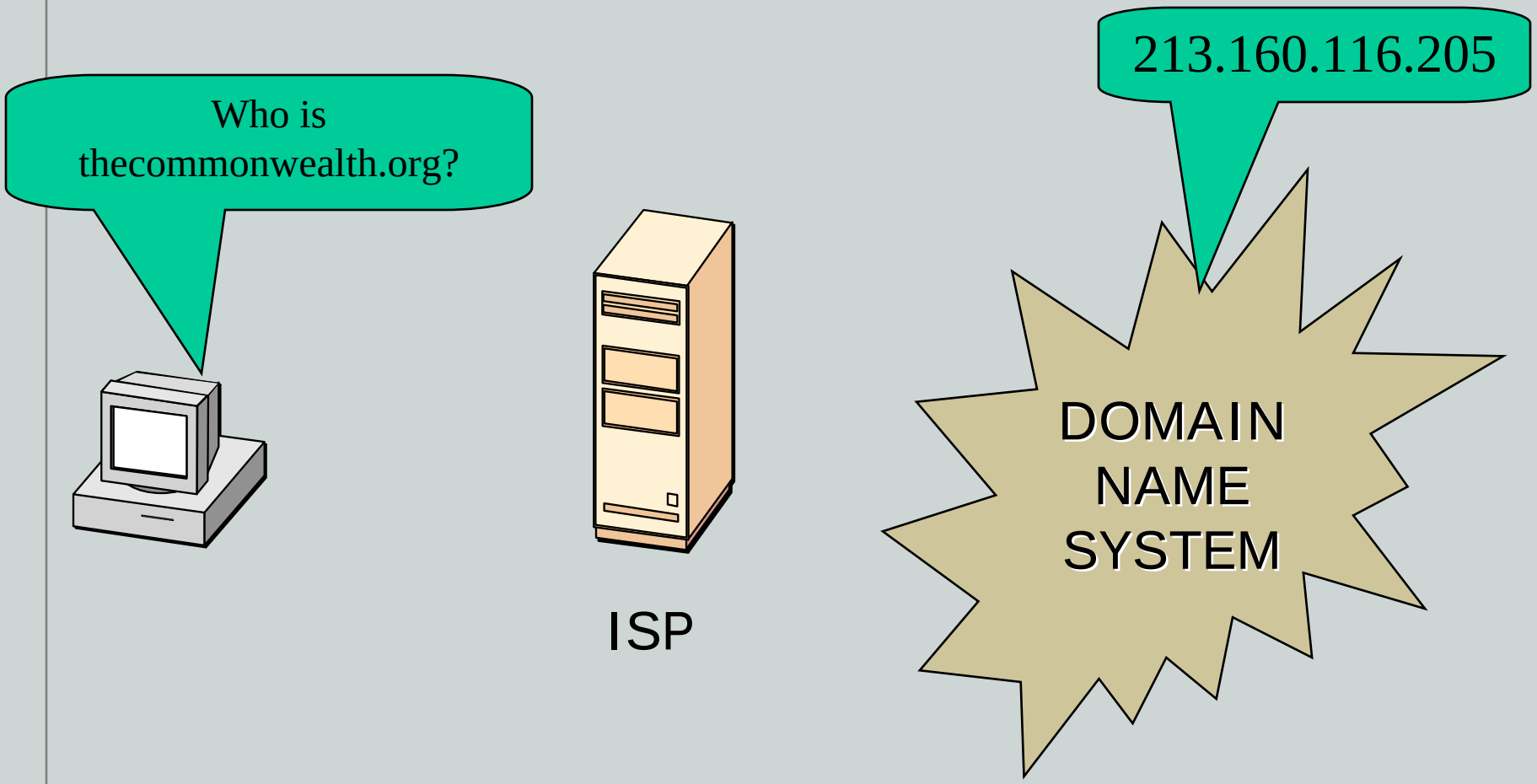
- America Online's proxy cache
- Proxy caches used by private companies
- Bots
- Anonymizers

Domain Names

- How humans handle IP addresses
- Every domain name has “whois” information
  - Owner, physical address, contact information
  - Almost always wrong if the domain name is registered by a criminal
- Assume nothing about geography

thecommonwealth.org = 213.160.116.205

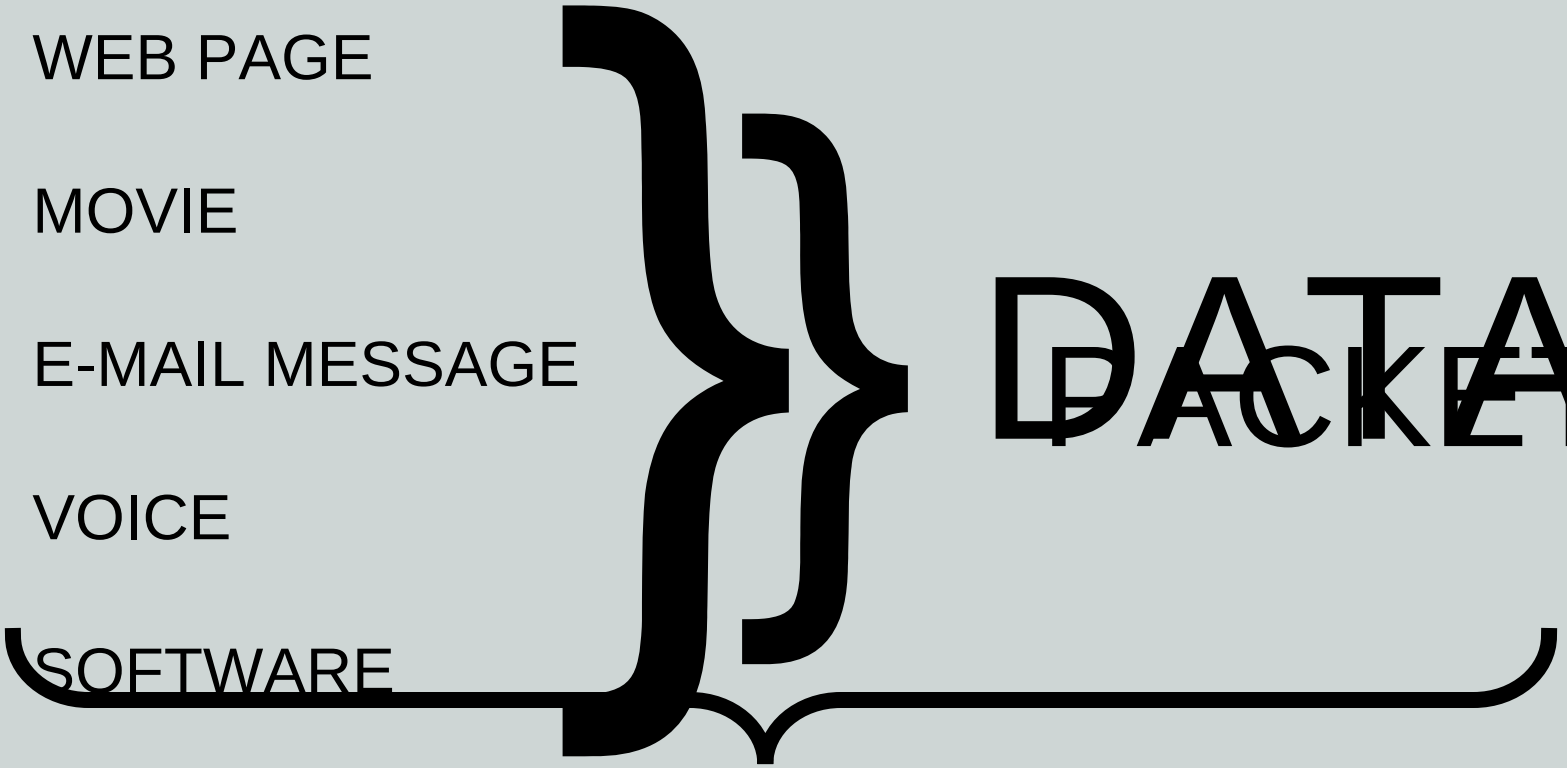
Domain Name Queries



Getting There...

- From networks to the Internet
- Locating a place on the Internet
- Applications that let people use the Internet

How People Use the Internet



Internet Use Applications

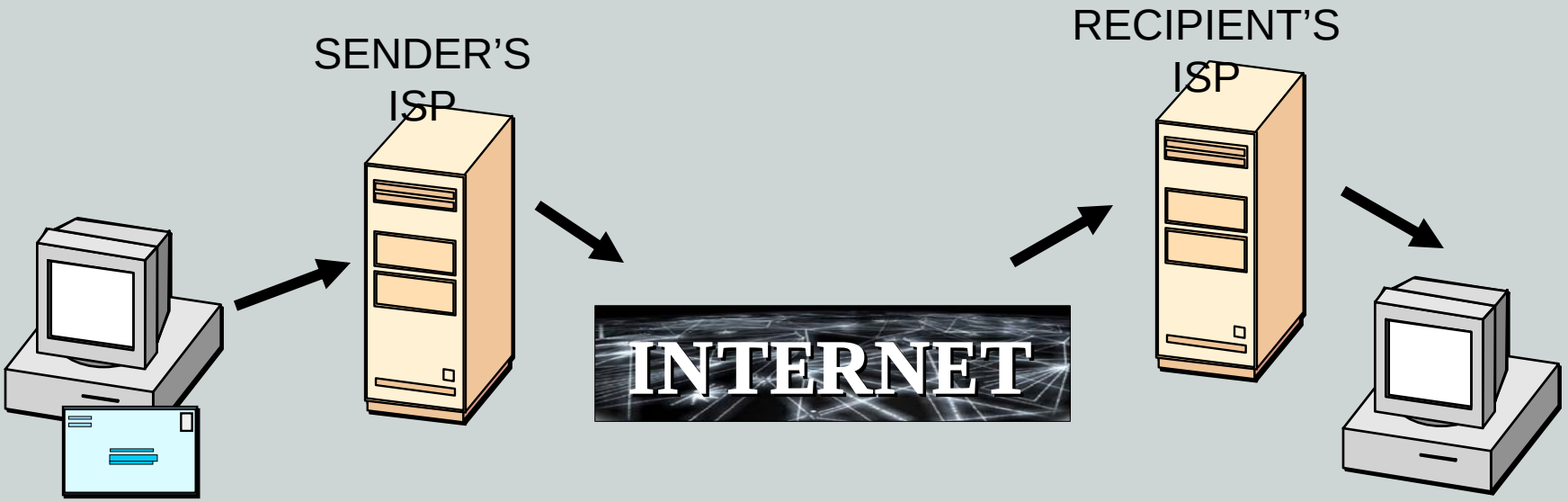
- E-mail
- Web browser
- Peer-to-peer (P2P)
- Instant messaging (IM)
- Internet relay chat (IRC)
- File transfer protocol (FTP)

Internet Use Applications

- E-mail
- Web browser
- Peer-to-peer (P2P)
- Instant messaging (IM)
- Internet relay chat (IRC)
- File transfer protocol (FTP)

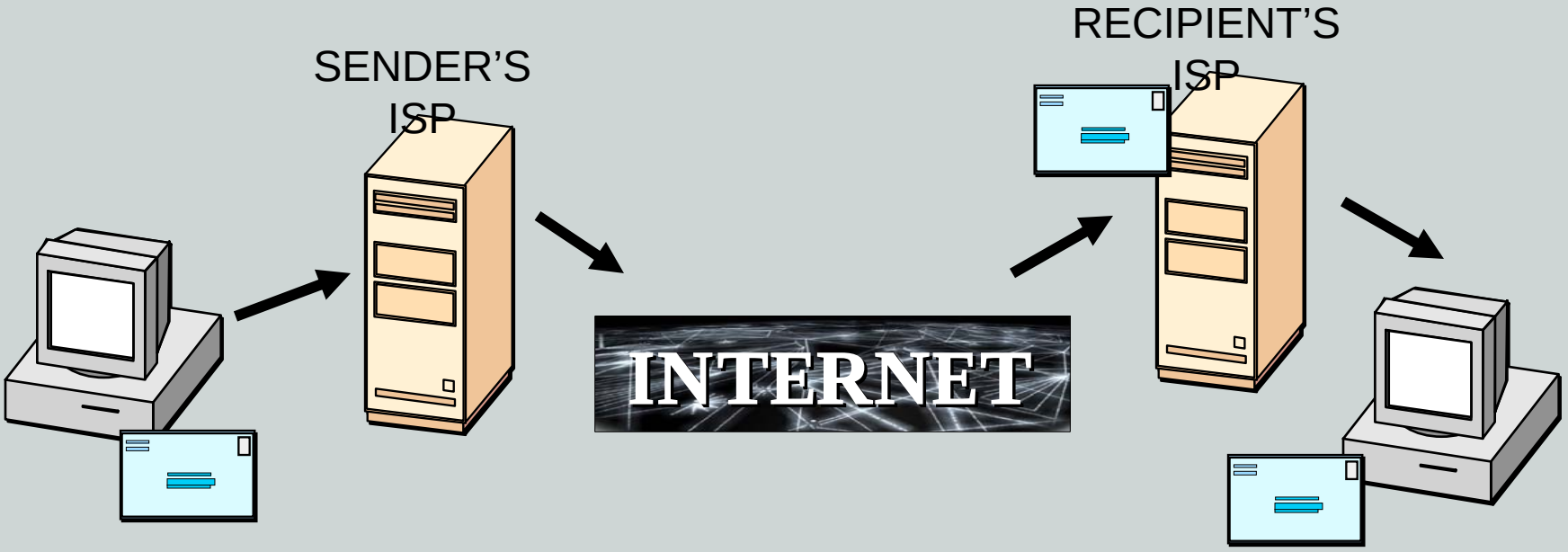
E-Mail Basics

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



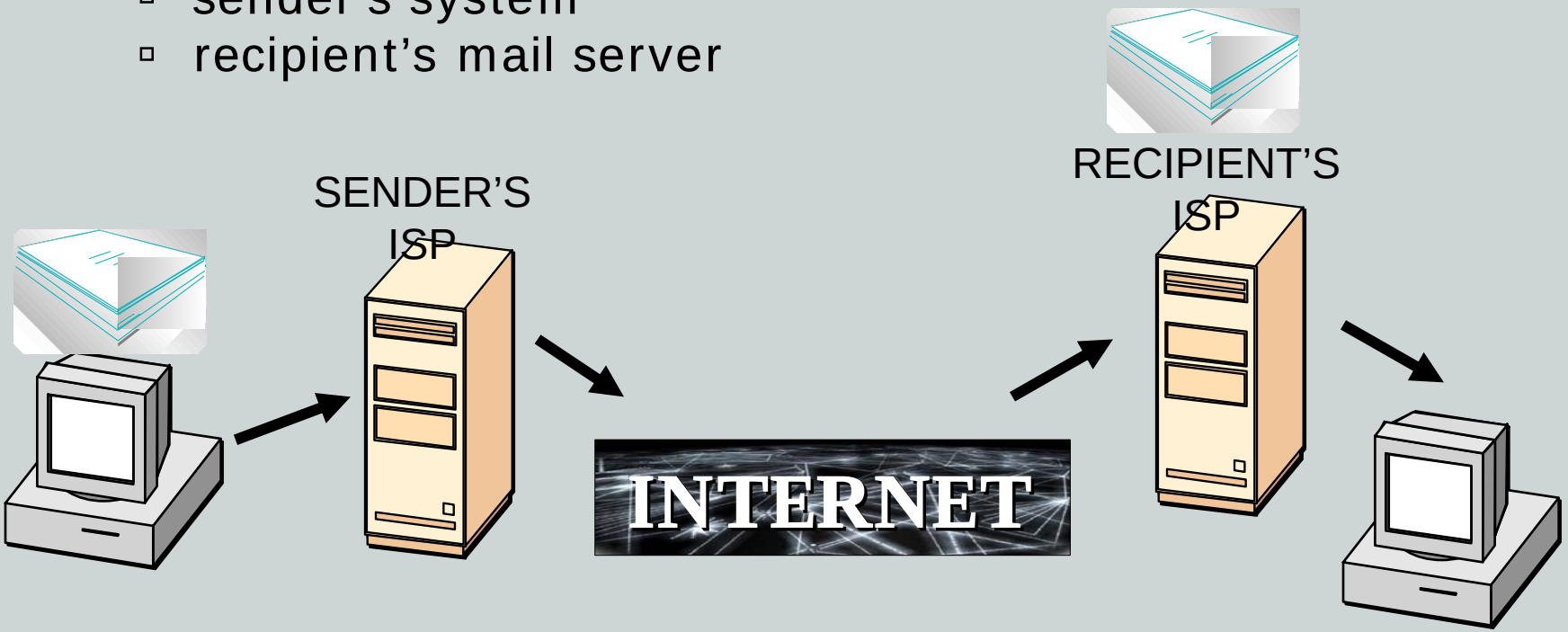
Evidence of Past Activity – Content

- 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



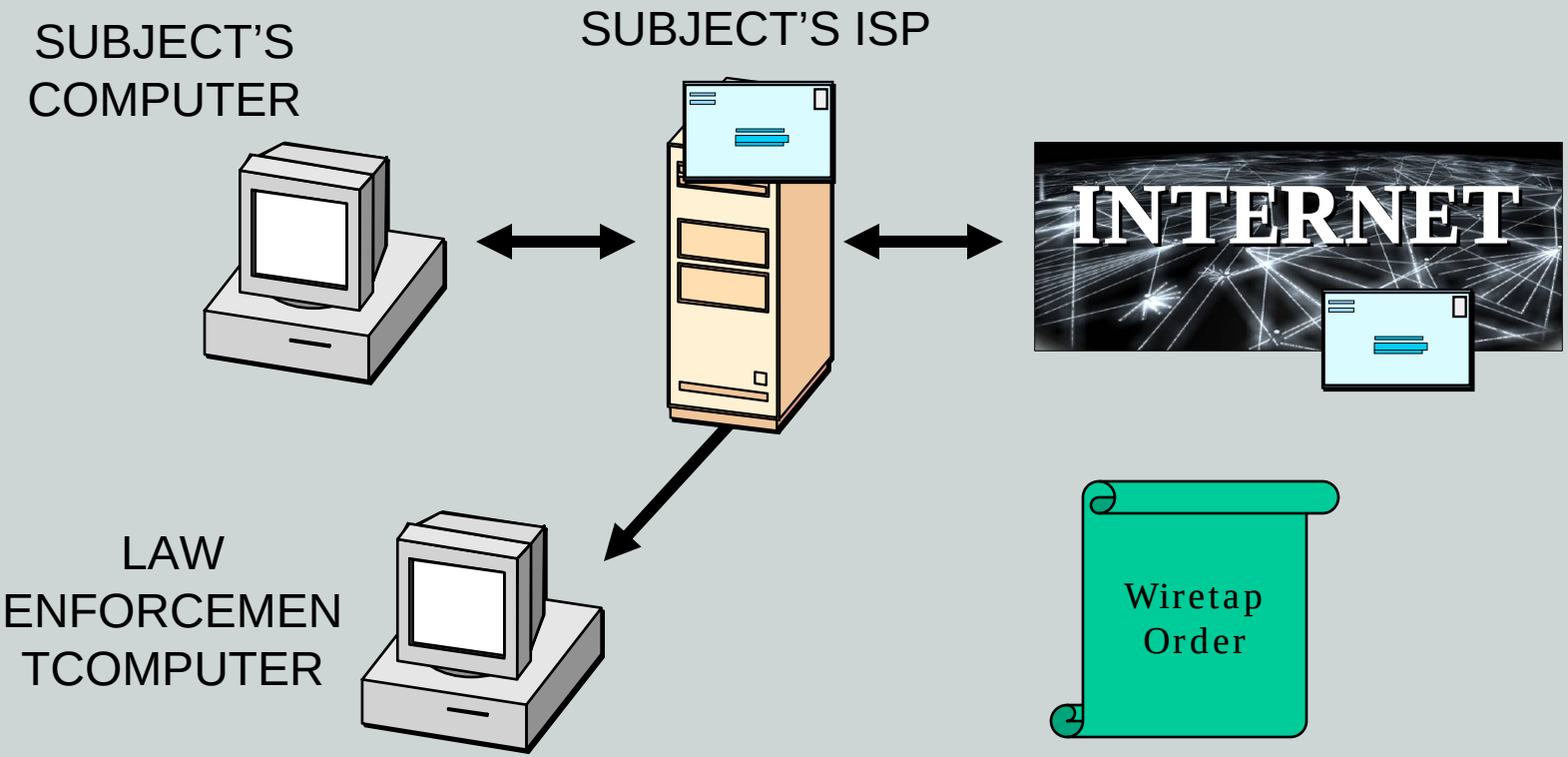
Evidence of Past Activity – Traffic Data

- 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



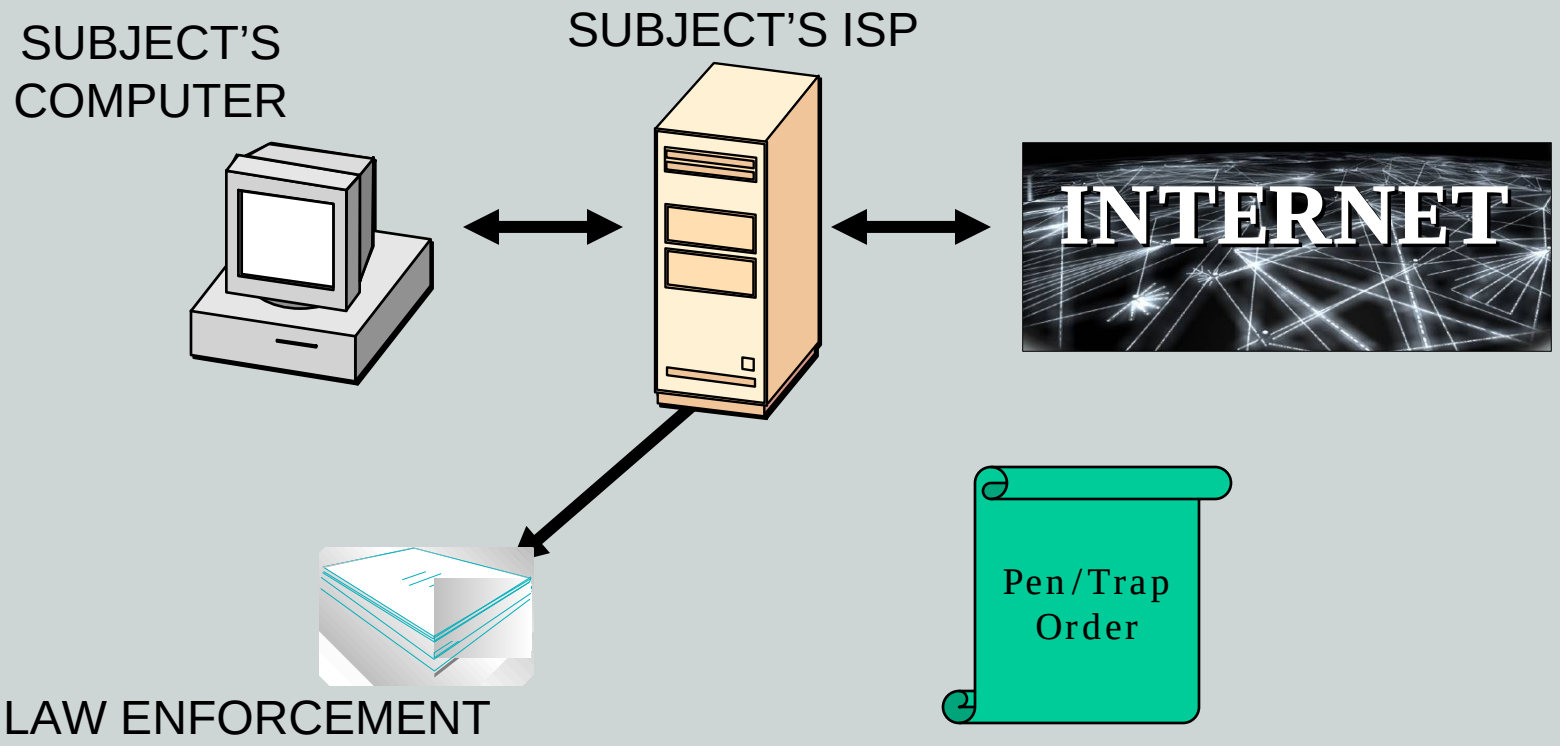
Prospective Evidence – Content

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



Prospective Evidence – Traffic Data

- Install a pen/trap at user's ISP to find out the e-mail addresses the user corresponds with



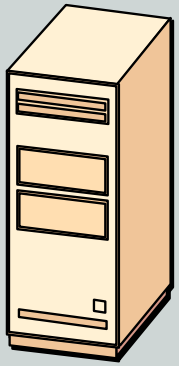
Internet Use Applications

- E-mail
- Web browser
- Peer-to-peer (P2P)
- Instant messaging (IM)
- Internet relay chat (IRC)
- File transfer protocol (FTP)

What is a web site?

- Three components
  - Domain name (or other address)
  - A web hosting server
  - Files sitting on the web hosting server

eac.int



A Twist: Virtual Hosting

- One server hosts hundreds of web sites
- All web sites share a single IP address
- Think carefully before you seize or search an entire server

Web Addresses

- Uniform Resource Locators (URL)

http://www.thecommonwealth.org/Internal/163207/151537/148540/podcast/

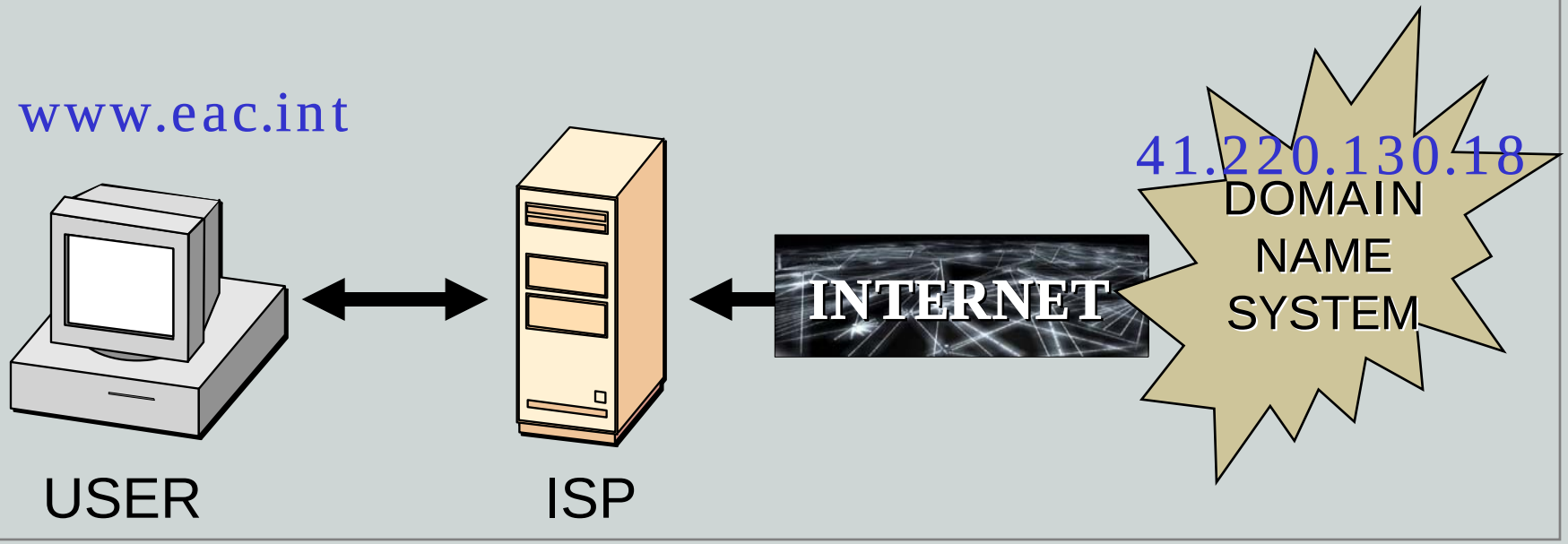
Computer **File**

http://www.eac.int/index.php/secretariat.html

Computer **File**

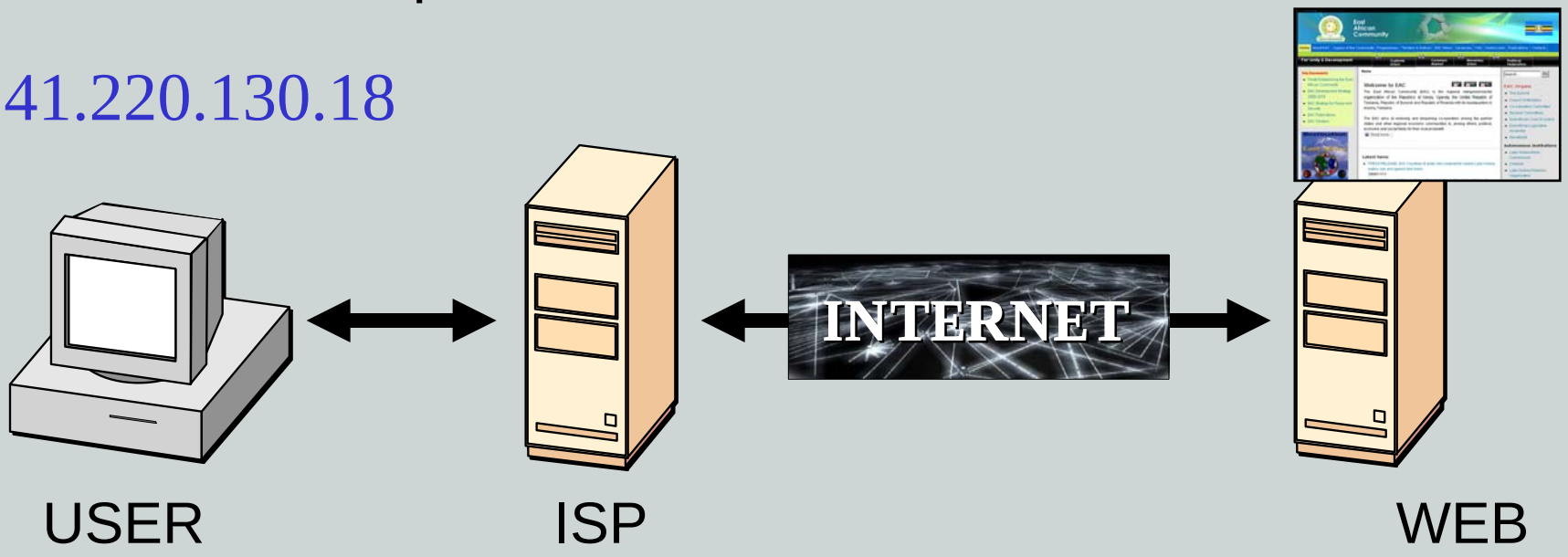
Browsing the Web: Client-Server Interaction

- User types a URL or clicks on link
- User's computer looks up IP address



Browsing the Web: Client-Server Interaction

- User's **CLIENT PROGRAM** sends a request to the **WEB SERVER** at the specified IP address
- The web server transmits a copy of the requested document (the web page) to the user's computer

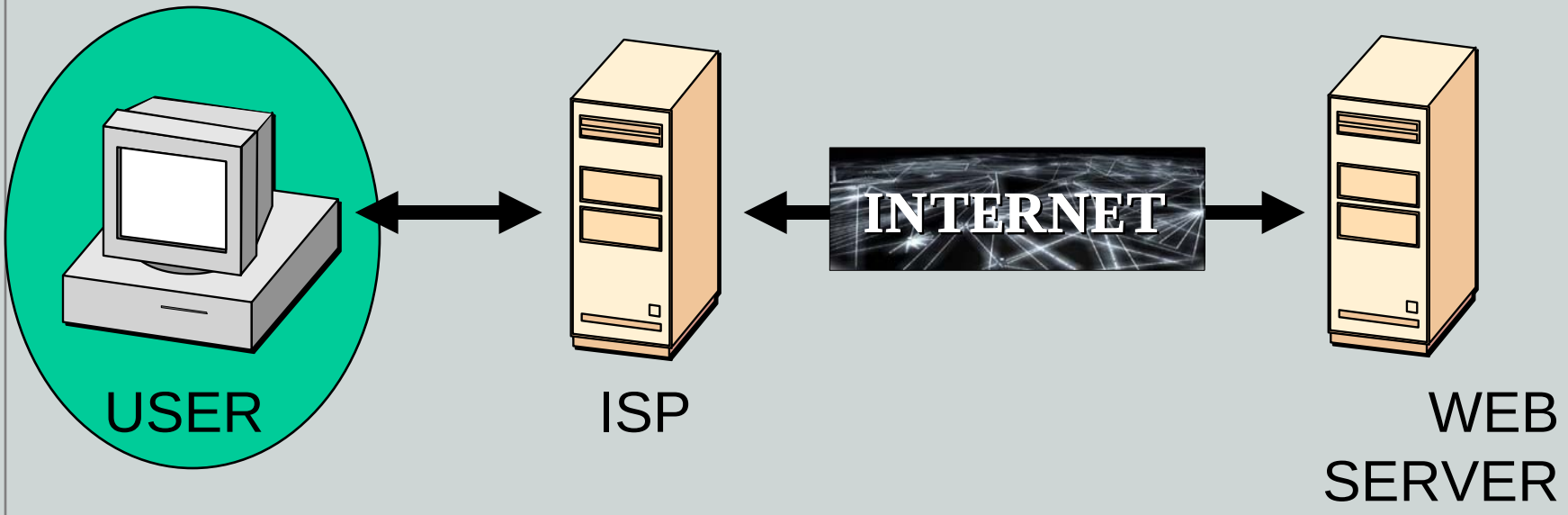


Browsing the Web: Client-Server Interaction

- The client program displays the transmitted document on the user's screen

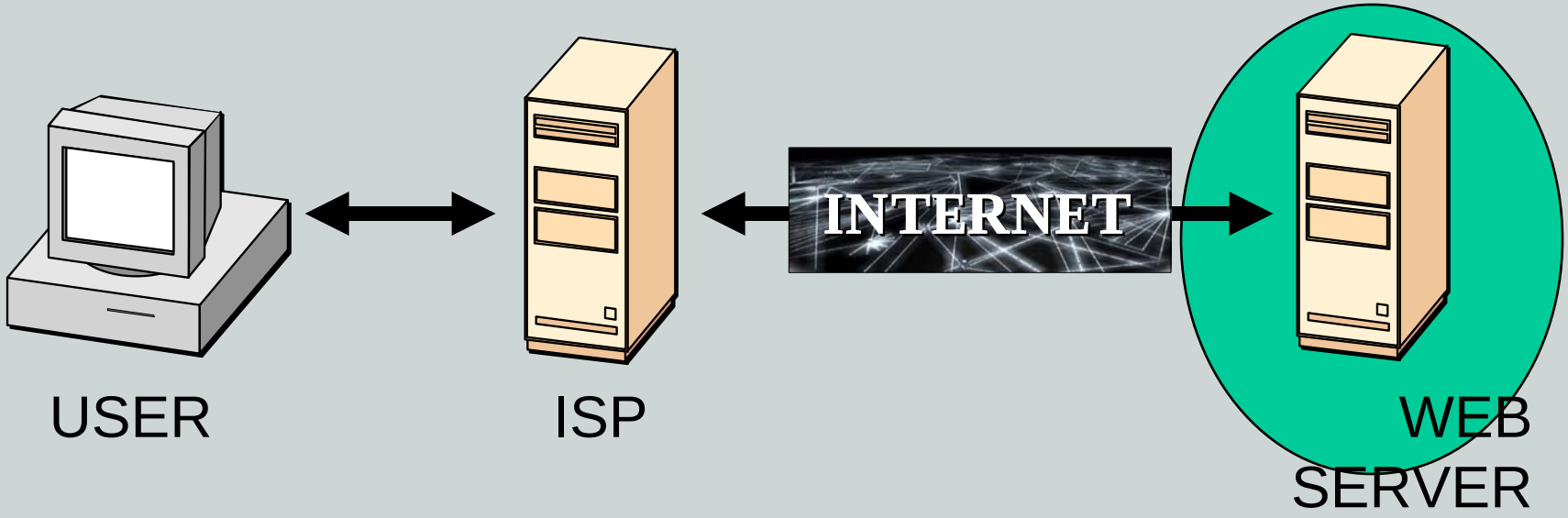
Evidence of Web Query: On User's Computer

- Cache directory
  - Copies of recently viewed web pages
- History file
  - List of recently visited pages



Evidence of Web Query: On Web Server

- Detailed logs of each request for any page
  - Date, time
  - Number of bytes
  - IP address of the system that requested the data



Example Web Server Log

10.143.28.198 - - [11/Feb/2007:22:45:17 -0500] "GET /tank.htm HTTP/1.1" 401 - "-" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.1) Gecko/20061204 Firefox/2.0.0.1“

10.143.28.198 - visitor [11/Feb/2007:22:45:23 -0500] "GET /images/lolita.png" 200 3788 "http://www.eruditorium.org/" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.1) Gecko/20061204 Firefox/2.0.0.1“

10.143.28.198 - visitor [11/Feb/2007:22:46:11 -0500] "POST /dynamic/ HTTP/1.1" 200 413 "http://www.eruditorium.org/" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.1) Gecko/20061204 Firefox/2.0.0.1"

See a theme?

- To do anything on the Internet, a computer communicates with another computer using an **IP address**
- Hopefully, that other computer will log what the suspect has done
- With that in mind…

Other Internet Use Applications

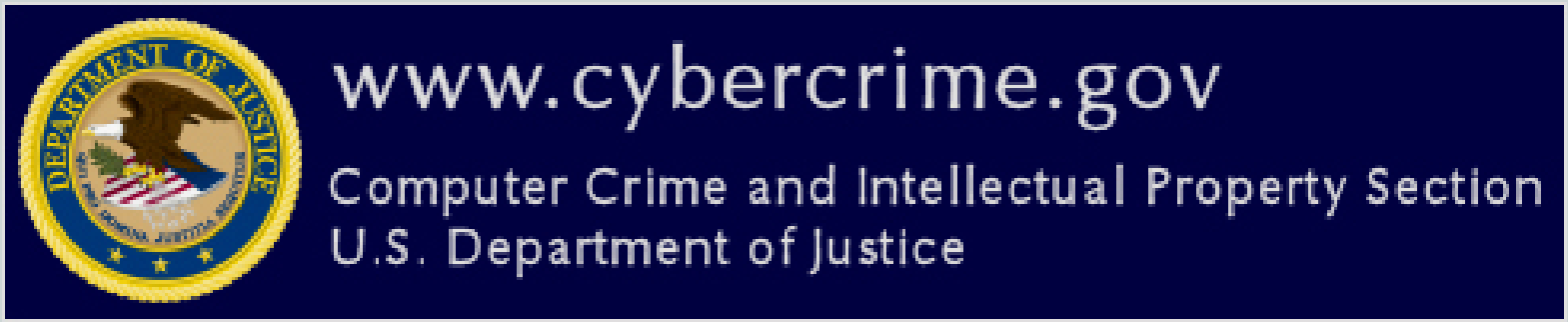
- Peer-to-peer (P2P)
- Instant messaging (IM)
- Internet relay chat (IRC)
- File transfer protocol (FTP)

In Closing...

- The Internet is a packet-switched network
- Systems keep many records about their interactions with the rest of the network
- Those records often help us locate and identify criminal actors, or at least to bolster the other evidence against them

Al Rees

Trial Attorney, CCIPS



albert.rees@usdoj.gov

(202) 514-1026