The Internet for Criminal Prosecutors

The Asia-Pacific Economic
Telecommunications Working Group
(APECTEL)

First Meeting of The Security and Prosperity Steering Group
Experts' Group on Cybercrime

Kuala Lumpur, Malaysia
September 24, 2011

1

What you need to know

What evidence is available

Investigative techniques

2

Topics we'll cover

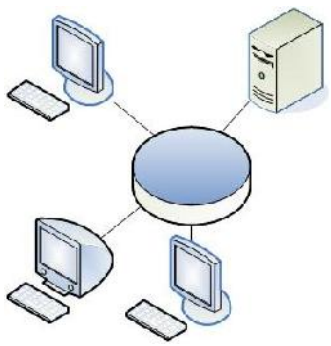
Do you know all of this already?

- Networks
- ISPs
- Packet switching
- IP addresses
- IP tracebacks
- WHOIS
- Wireless Internet (Wi-Fi)
- NATs
- Proxies
- Client/server model
- Peer-to-peer file sharing
- Hacking
- Social engineering
- Botnets

3

Network

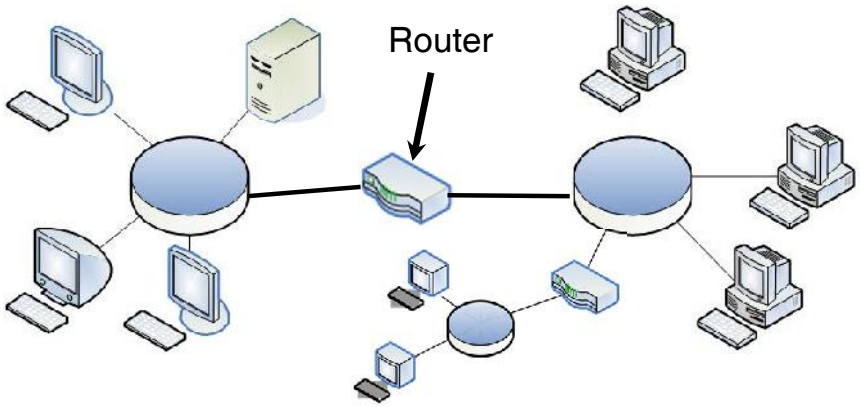
Computers connected together



4

Internetwork

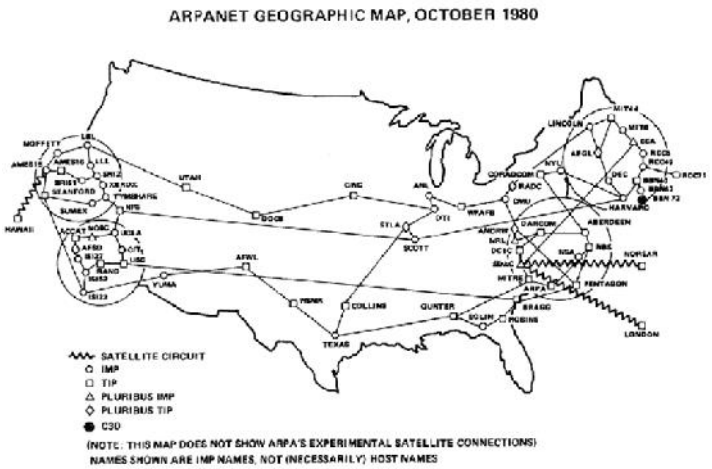
Networks connected together



5

Internet

The biggest internetwork on the planet



6

Server

A networked computer offering a service

7

The client/server model

Why the Internet is useful

Send me
“www.tasteyoulove.com”

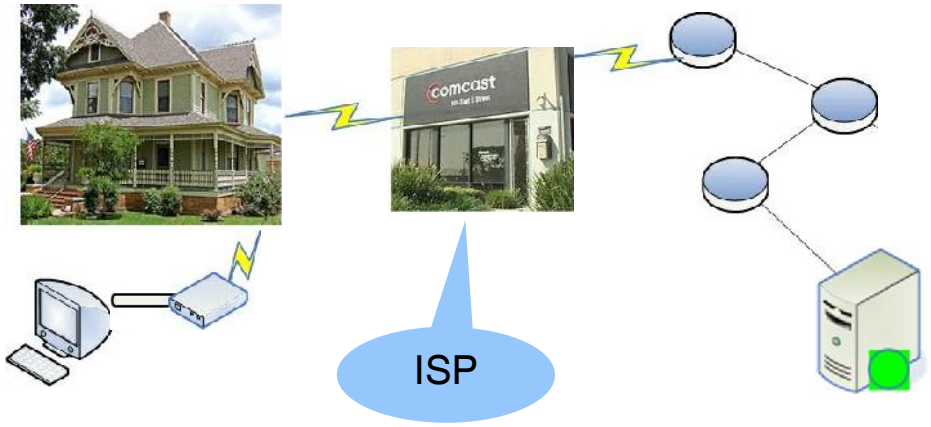
Client request

Server response

8

Internet Service Provider (ISP)

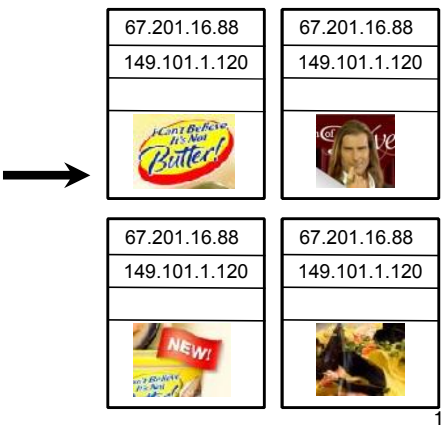
A company that connects you to the Internet



9

How computers send data

Everything is broken up into “packets”



10

How computers send data

Computers send the packets

11

Internet Protocol (IP) Addresses

Tell the Internet where to send packets

67.201.16.88
149.101.1.120
0111001010101011 1011011000100101 0100... 

Source ("from")

Destination ("to")

Part of data Being sent

12

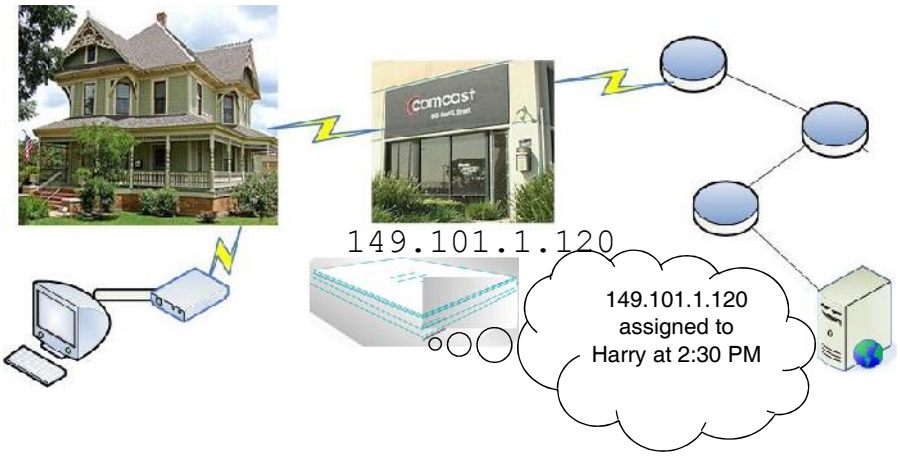
Internet Protocol (IP) Addresses

Everyone on the Internet has one

13

Assigning IP addresses

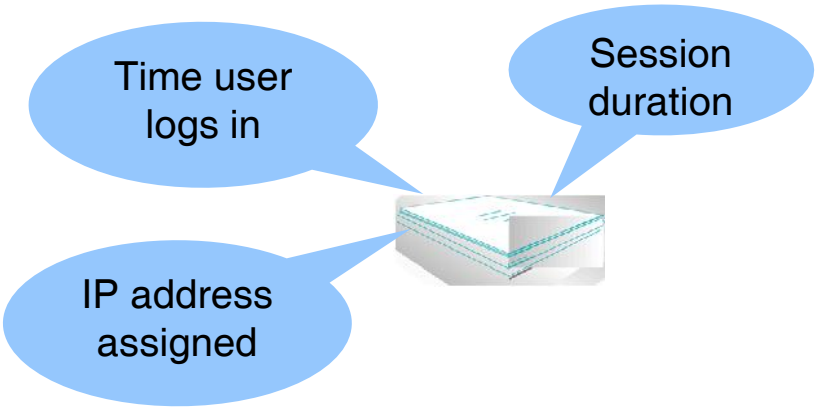
Assigned to home users by their ISP



14

ISP logs

ISPs keep track



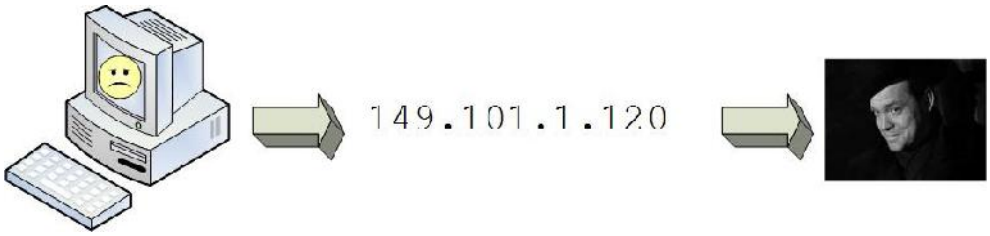
15

Investigative Techniques

16

IP address as clue

Investigations focus on getting the IP address



Computer crime scene

IP address

Suspect

17

Traceback

Learning who was using an IP address

149.101.1.120

?

18

Traceback, Step 1

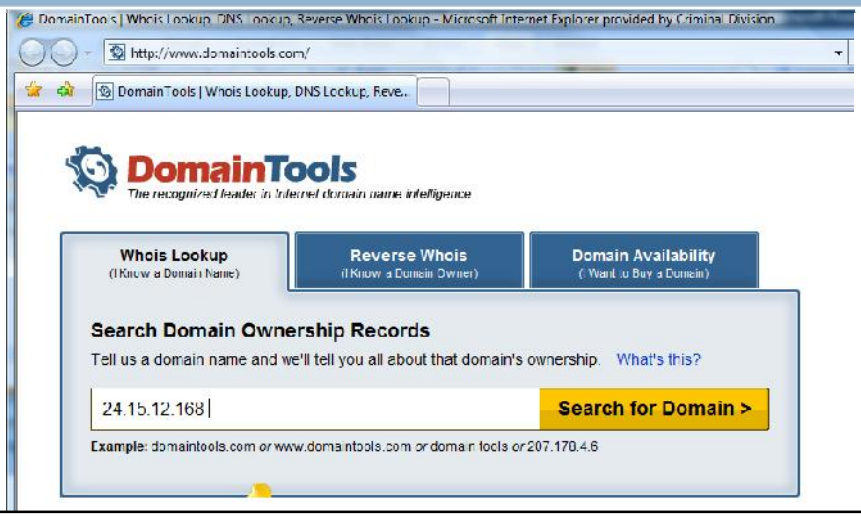
Use IP whois to learn the ISP for that address

149.101.1.120 → comcast

19

Using WHOIS to look up an IP

Easy way: www.domaintools.com



20

Using WHOIS to look up an IP

Easy way: www.domaintools.com

IP Information for 24.15.12.168

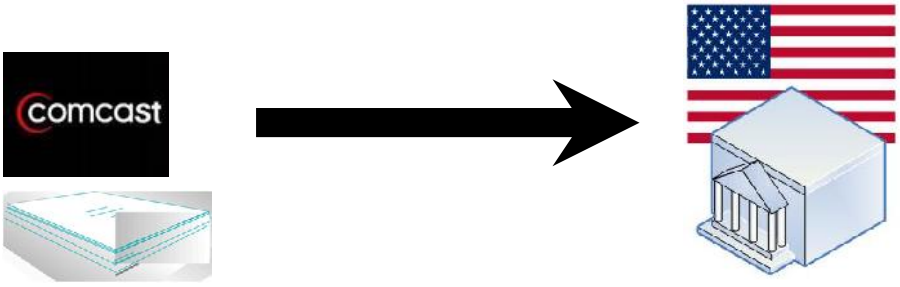
IP Location:	United States Chicago Comcast Cable Communications
Resolve Host:	c-24-15-12-168.hsd1.il.comcast.net
IP Address:	24.15.12.168 W R P D T
Blacklist Status:	Clear

```
OrgName:    Comcast Cable Communications, Inc.
OrgID:      CMCS
Address:    1800 Bishops Gate Blvd
City:       Mt Laurel
StateProv:  NJ
PostalCode: 08054
Country:    US
```

21

Get the logs from Comcast

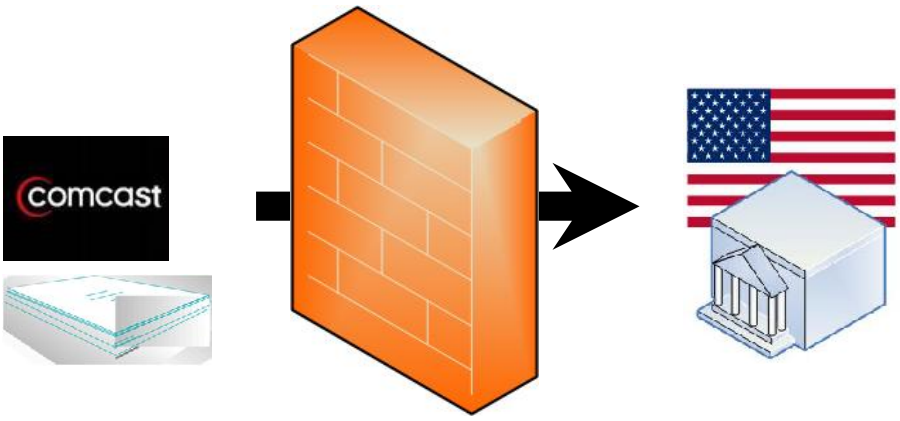
Ask them who had that IP address



22

Introducing ECPA

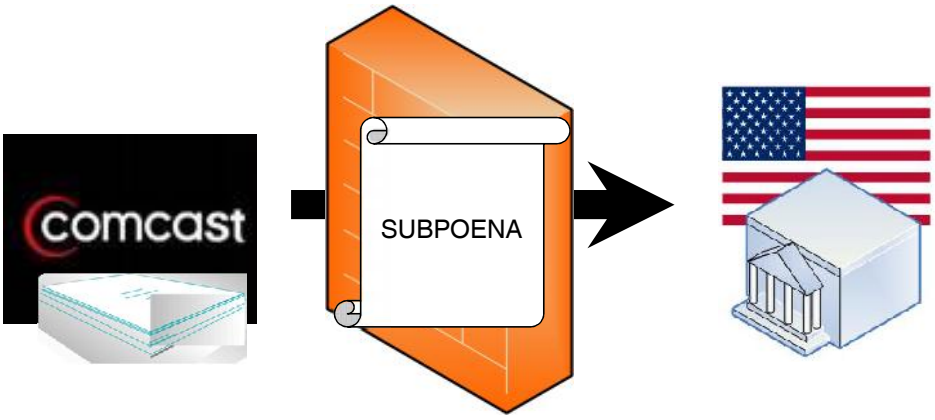
Electronic Communications Privacy Act
(18 U.S.C. § 2701-11)



23

ECPA and the Traceback

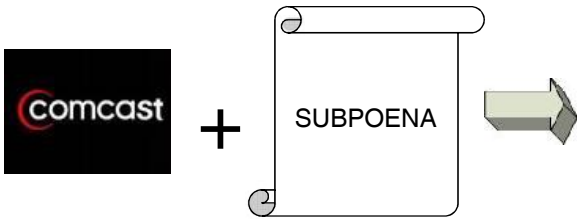
Use a subpoena to get subscriber info



24

Traceback, ideally

Now, the ISP can tell you who it was

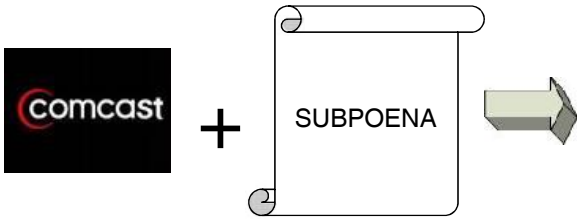


Harry Lime
225 W. 57th Street
New York, NY

25

Complications

What if it isn't this easy?

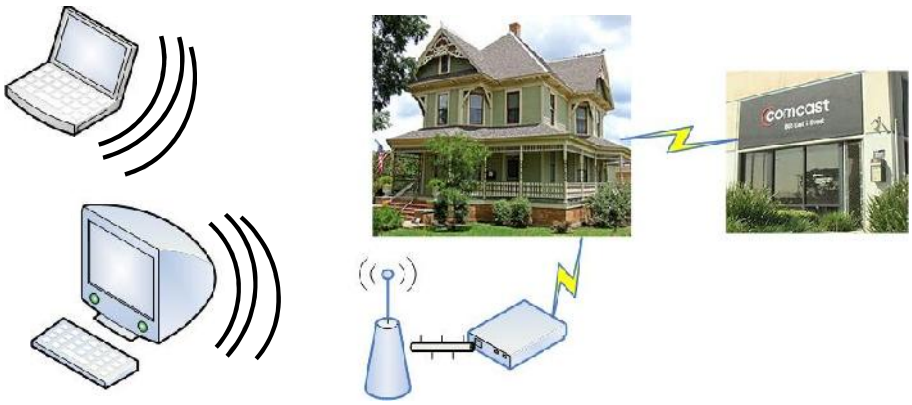


Foreign country, questionable ISP

26

Wireless (Wi-Fi) Internet

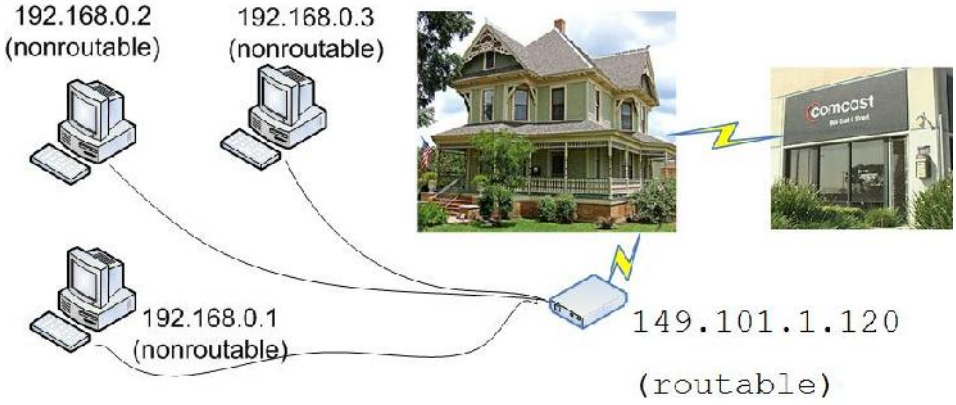
Using radio instead of cables



27

Network Address Translation

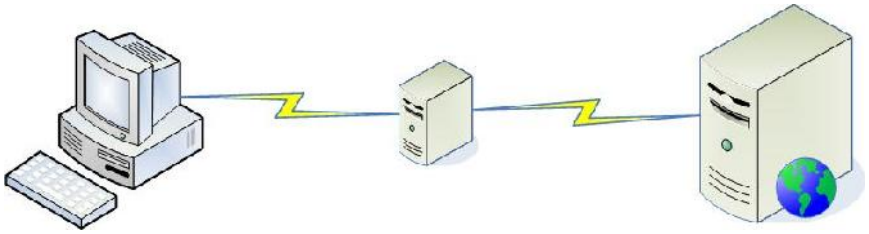
The NAT: Sharing IP addresses



28

Proxy

Hiding IP addresses by using intermediaries



29

Scenario

Scam e-mail sent. Who sent it?

Date: Thu, 22 Oct 2009 11:59:02 +0100
To: nospam@mailinator.com
From: admin@lottery.co.uk
Subject: WINNER OF UK LOTTERY USD$4.6M.

If you are the correct owner of this email address then be glad this day as the result of the UK lotto online e-mail address free-ticket winning draws of 29th August 2009 has just been released and we are glad to announce to you that your email address won

30

Analyzing e-mail headers

Closer to the top = closer to the truth

Received: from qsmtp1.tiresrflat.info (unknown [174.127.82.151]) … ; Mon, 23 May 2011 15:05:22 -0400 (EDT)
Reply-To: <philmat58@yahoo.com.hk>
Date: Mon, 23 May 2011 14:05:23 -0500
To: nospam@mailinator.com
From: admin@lottery.co.uk
Subject: WINNER OF UK LOTTERY USD$4.6M.

If you are the correct owner of this email address …

31

Look up that IP

Using our friend Domaintools

32

Look up that IP

Using our friend Domaintools

IP Information for 174.127.82.151

IP Location:	United States Providence Hosting Services Inc
ASN:	AS36351
Resolve Host:	174.127.82.151.static.midphase.com
IP Address:	174.127.82.151 W R P D T

```
NetRange:       174.127.64.0 - 174.127.127.255
CIDR:           174.127.64.0/18
OriginAS:       AS32780
```

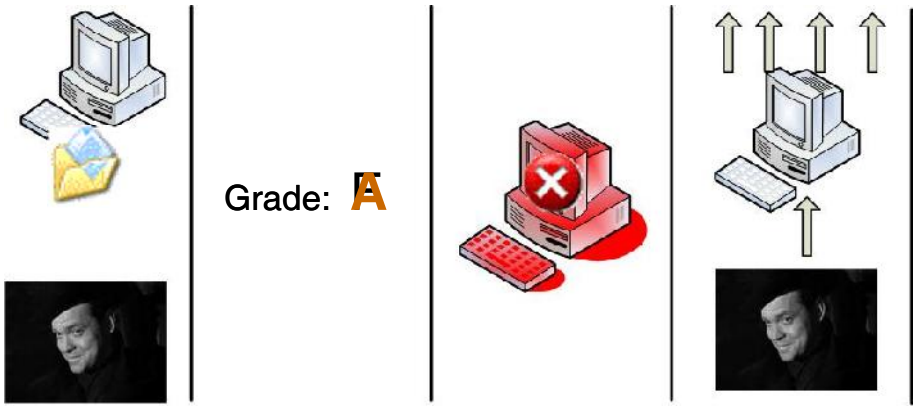
33

Variety of Internet Crime

34

Hacking: The goals

Confidentiality, Integrity, Availability, and Use



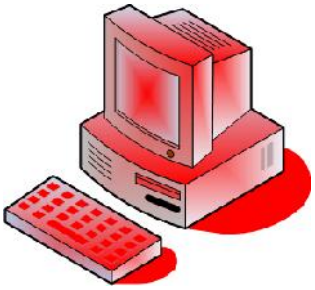
35

Vulnerabilities and exploits

Errors in code, and ways to take advantage

Xyq5%zZ[{/

abc
d



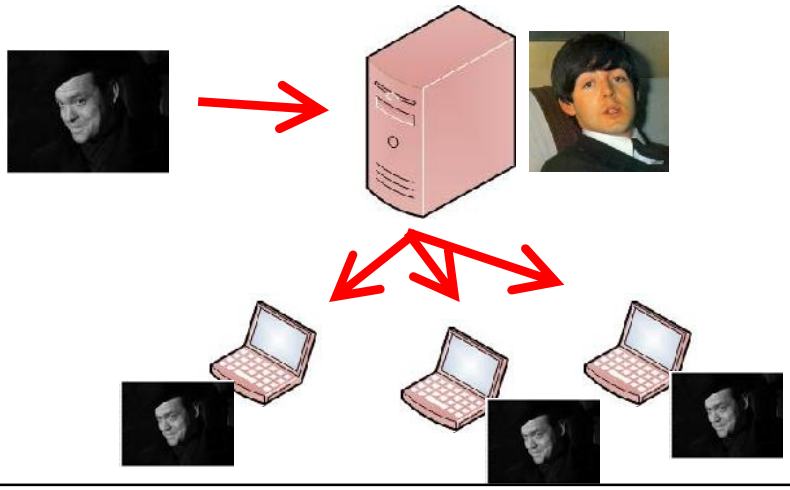
36

Common vulnerabilities

Server software, applications

37

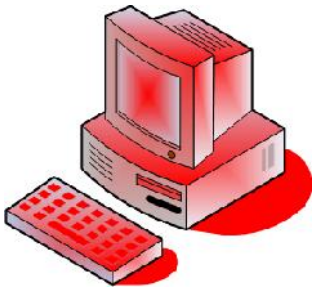
One hack leads to another



38

Bots

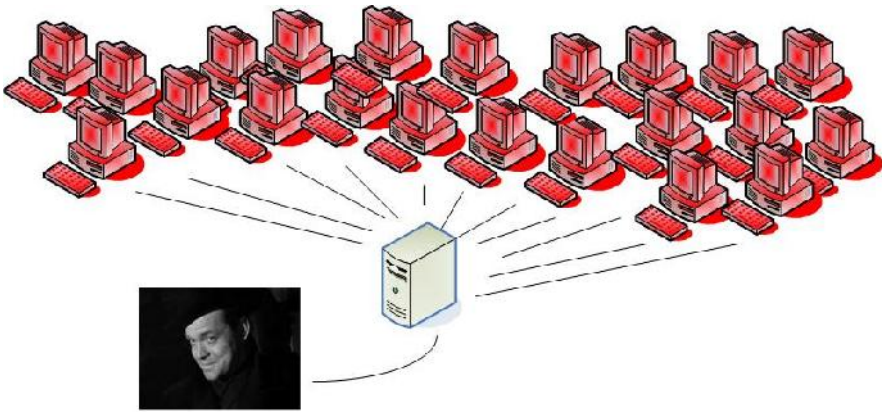
Personal computers



39

Botnets

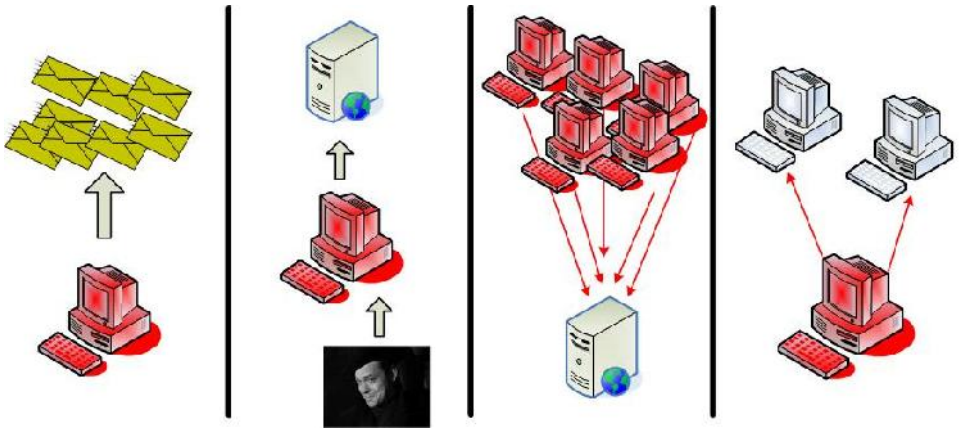
Huge collections of bots



40

Uses for botnets

Spam; proxies; attacks; making more bots



41

Peer-to-Peer file sharing (P2P)

42

Review: the client/server model

The opposite of peer-to-peer

Send me
"www.tasteyoulove.com"

Client request

Server response

43

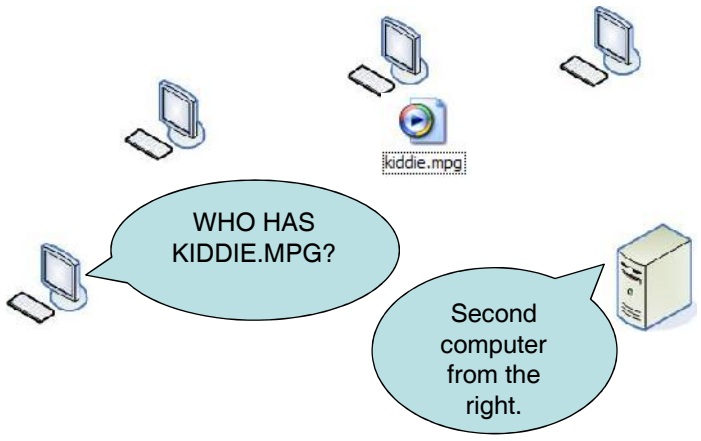
What is Peer-to-Peer?

Sharing files, using servers as little as possible

44

Old style P2P

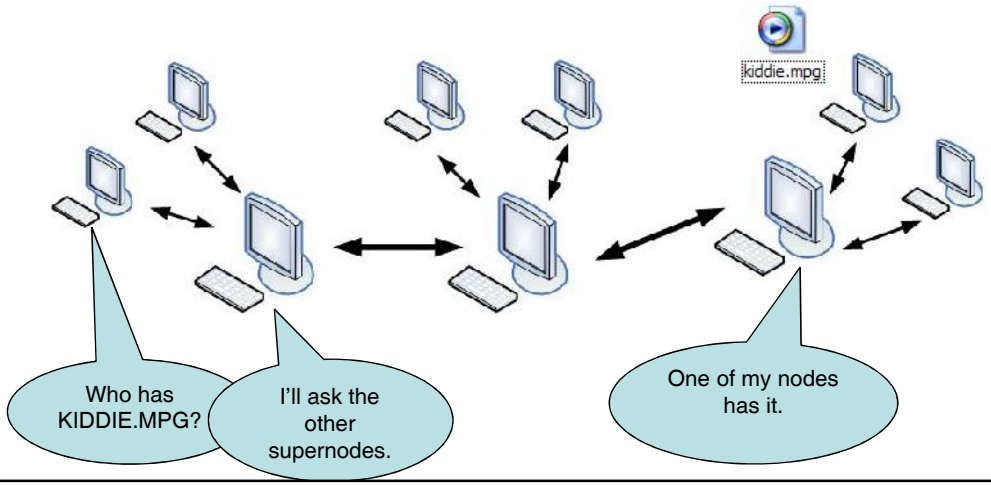
Relied on a server to keep track of the peers



45

Newer style P2P

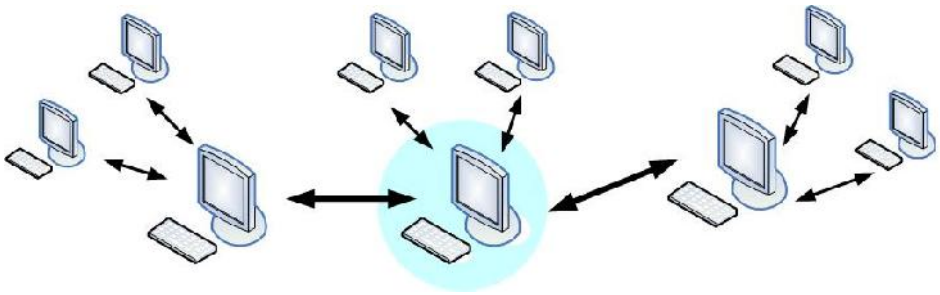
Uses “supernodes” instead of central servers



46

Investigating P2P

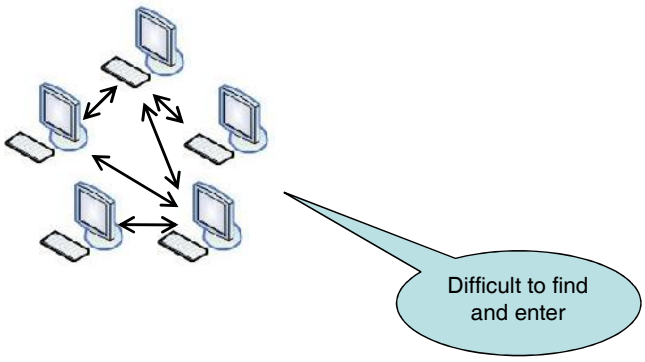
Done through undercover work



47

Today: Gigatribe and Darknets

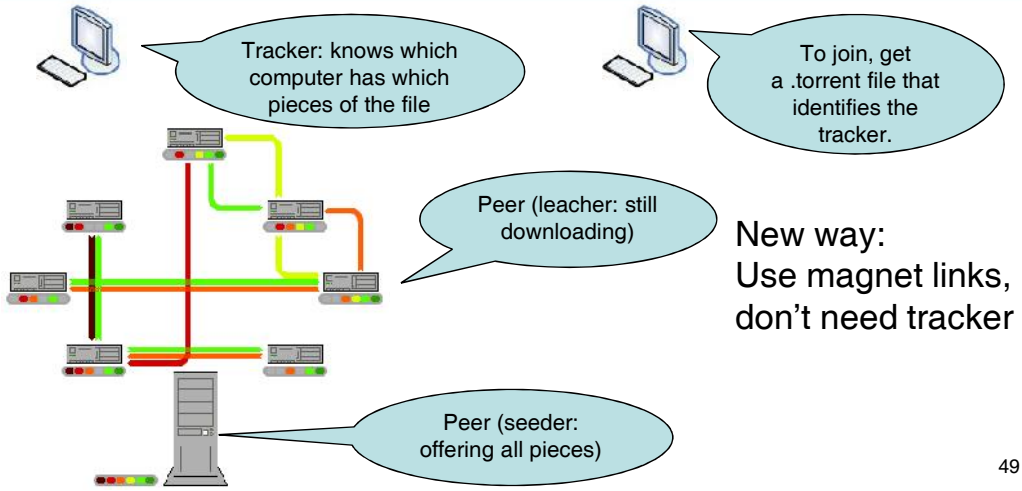
Small, private communities sharing files



48

Today: BitTorrent

Efficient technology for a huge number of people to share huge files



New way:
Use magnet links, don't need tracker

49

www.cybercrime.gov
Computer Crime and Intellectual Property Section
U.S. Department of Justice

50