# Investigation & Prosecution of Cybercrime: Introduction

## CJ341 – Cyberlaw & Cybercrime
## Lecture #16

**M. E. Kabay, PhD, CISSP-ISSMP**
**mailto:mkabay@norwich.edu**
**V: 802.479.7937**
**Prof Information Assurance & Statistics**
**School of Business & Management**

*Copyright © 2011 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.*

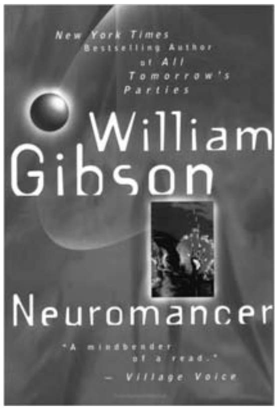
## Topics

- **Overview of Cyberspace**
- **Moore**
  - ❑**Tracing a Suspect on the Internet**
  - ❑**Locating Information from E-Mails**
  - ❑**Proactive vs Reactive Strategies**
- **Clifford**
  - ❑**Three Cybercrime Scenarios**

*Copyright © 2011 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.*

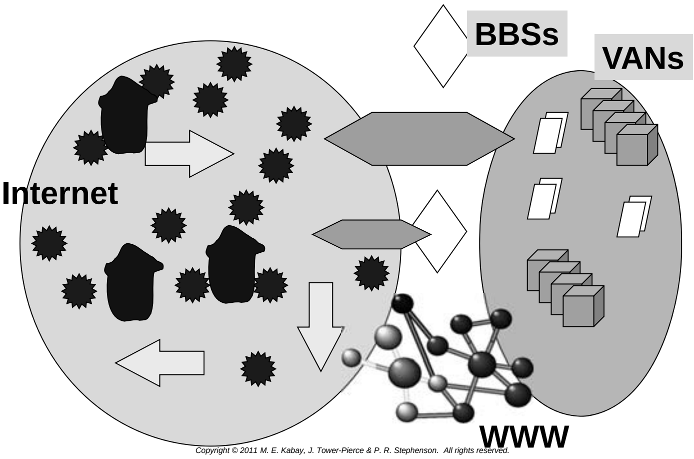
## Overview of Cyberspace

- **The Evolution of Cyberspace**
- **News**
- **The Internet**
- **The World Wide Web**


New York Times Bestselling Author of All Tomorrow's Parties
William Gibson
Neuromancer
"A mindbender of a read."
– Village Voice

*Copyright © 2011 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.*

## Evolution of Cyberspace



BBSs

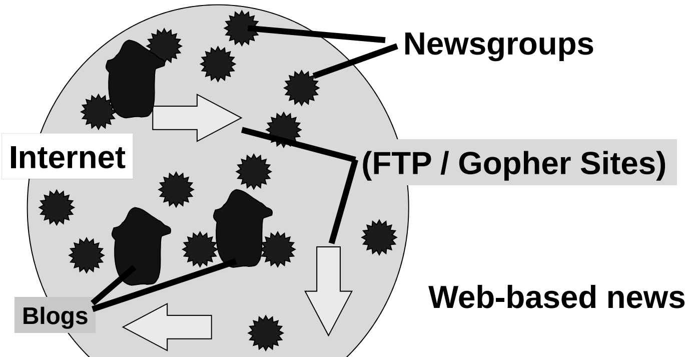
VANs

Internet

WWW

*Copyright © 2011 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.*

## Disintermediated News



Newsgroups

Internet

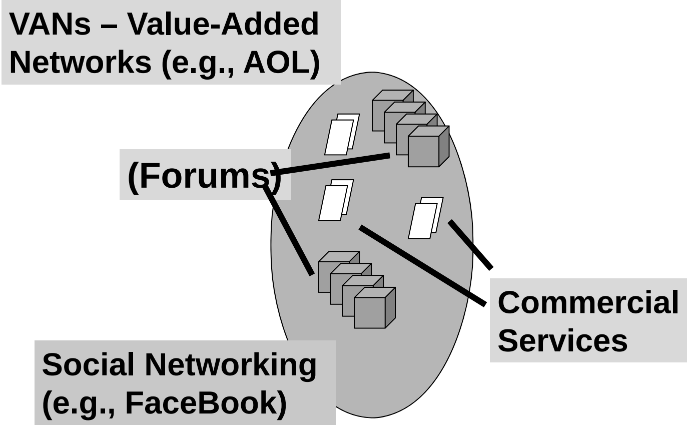
(FTP / Gopher Sites)

Web-based news

Blogs

*Copyright © 2011 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.*

## Discussions



VANs – Value-Added Networks (e.g., AOL)

(Forums)

Commercial Services

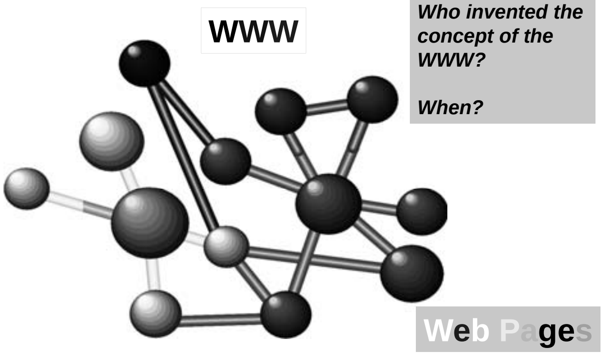
Social Networking (e.g., FaceBook)

*Copyright © 2011 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.*

## The Web

*Who invented the concept of the WWW?*

*When?*



*Copyright © 2011 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.*

## Online Forums

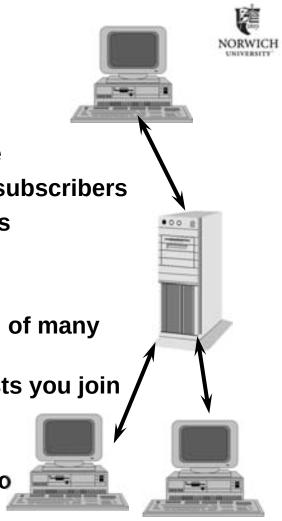
*These communications channels may be critically important in forensic investigations; e.g., CISO at NU regularly uses these channels when Investigating alleged security or honor-code violations.*

- ➢ Types
  - ❑Usenet
  - ❑IRC
  - ❑ICQ
  - ❑Mailing lists
  - ❑Private or public discussion groups
    - ✓Yahoo Groups
    - ✓GOOGLE Groups
- ➢ Chat Clients often include multi-user capabilities
  - ❑AIM, Trillian, Digsby….

*Copyright © 2011 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.*

## Online Forums & Mailing Lists

- ➢ Mailing-list software
  - ❑Users subscribe & unsubscribe
  - ❑Sends out e-mail messages to subscribers
  - ❑Copies replies to all participants
  - ❑e.g., Majordomo
- ➢ Some mailing lists have Digests
  - ❑Single large file per day instead of many messages
  - ❑Check the options in mailing lists you join
- ➢ Online special-interest portals include discussions
  - ❑E.g., commentary in response to postings

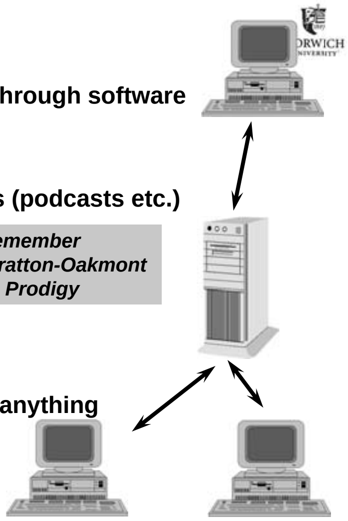


*Copyright © 2011 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.*

## Online News

- ➢ Users access news groups through software
  - ❑E.g., USENET (NEWS://)
  - ❑Other groups, blogs
  - ❑RSS feeds from Web sites (podcasts etc.)
- ➢ Moderated newsgroups
  - ❑Editor/moderator
  - ❑Controls what appears
  - ❑High signal-to-noise ratio
- ➢ Unmoderated
  - ❑Automatic distribution of anything
  - ❑Low signal-to-noise ratio
  - ❑Subject to *spamming*

*Remember Stratton-Oakmont vs Prodigy*



*Copyright © 2011 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.*

## Online Forums: BBSs (OLD)

Historical interest (e.g., *War Games*, 1983)

- ➢ Access via phone calls & modems
- ➢ Professional and amateur
- ➢ May require long-distance calls
- ➢ Unregulated: hatred, obscenity
- ➢ Some moderated, others unmoderated
- ➢ Unreliable: virus-infected software
- ➢ A few run by and for criminals
  - ❑Stolen software
  - ❑Ads for stolen goods

*Copyright © 2011 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.*

## The Internet

- ➢ *An internet* is network of networks
  - ❑*The Internet* grew out of ARPANET
  - ❑Based on TCP/IP linkage of networks (see next slide)
- ➢ Includes > 1B users
  - ❑Has 200-300 million nodes
  - ❑Growing by 2,000,000 users/month
- ➢ Users often have free (uncharged) access
  - ❑Some cities have “Freenet” service

*Copyright © 2011 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.*

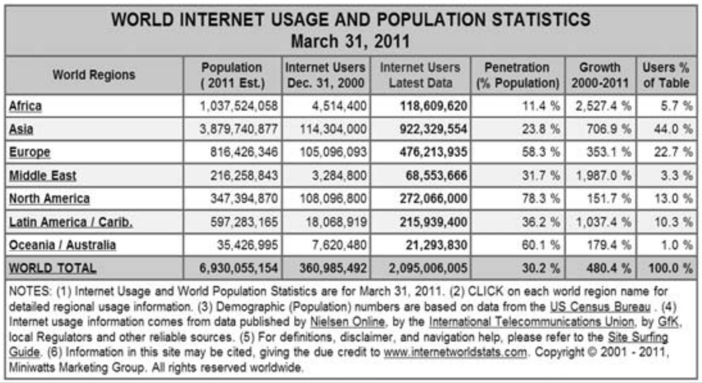
# The Internet

- ➢ TCP/IP based internetworking
  - ❑Transmission Control Protocol = TCP
  - ❑Internet Protocol = IP
  - ❑Packet-switched protocols
  - ❑Dynamic routing of packets for high efficiency
- ➢ Began as DARPA project in late 1960s
  - ❑Defense Advanced Research Projects Agency
  - ❑Steady expansion during 1970s & 1980s
  - ❑Explosive growth late 1980s and in 1990s
  - ❑.com domain opened for general use in 1993

Copyright © 2011 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

# INTERNET USAGE STATISTICS
## The Internet Big Picture
### World Internet Users and Population Stats

http://www.internetworldstats.com/stats.htm

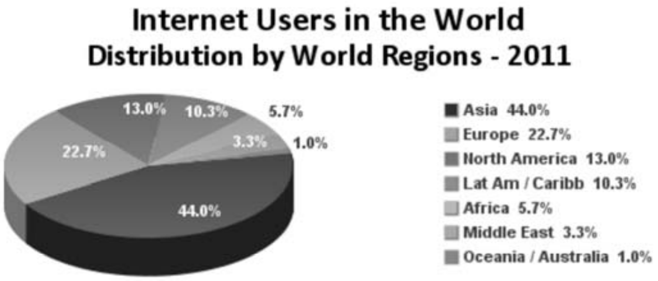


WORLD INTERNET USAGE AND POPULATION STATISTICS
March 31, 2011

| World Regions | Population ( 2011 Est.) | Internet Users Dec. 31, 2000 | Internet Users Latest Data | Penetration (% Population) | Growth 2000-2011 | Users % of Table |
|---|---|---|---|---|---|---|
| Africa | 1,037,524,058 | 4,514,400 | **118,609,620** | 11.4 % | 2,527.4 % | 5.7 % |
| Asia | 3,879,740,877 | 114,304,000 | **922,329,554** | 23.8 % | 706.9 % | 44.0 % |
| Europe | 816,426,346 | 105,096,093 | **476,213,935** | 58.3 % | 353.1 % | 22.7 % |
| Middle East | 216,258,843 | 3,284,800 | **68,553,666** | 31.7 % | 1,987.0 % | 3.3 % |
| North America | 347,394,870 | 108,096,800 | **272,066,000** | 78.3 % | 151.7 % | 13.0 % |
| Latin America / Carib. | 597,283,165 | 18,068,919 | **215,939,400** | 36.2 % | 1,037.4 % | 10.3 % |
| Oceania / Australia | 35,426,995 | 7,620,480 | **21,293,830** | 60.1 % | 179.4 % | 1.0 % |
| **WORLD TOTAL** | **6,930,055,154** | **360,985,492** | **2,095,006,005** | **30.2 %** | **480.4 %** | **100.0 %** |

NOTES: (1) Internet Usage and World Population Statistics are for March 31, 2011. (2) CLICK on each world region name for detailed regional usage information. (3) Demographic (Population) numbers are based on data from the US Census Bureau . (4) Internet usage information comes from data published by Nielsen Online, by the International Telecommunications Union, by GfK, local Regulators and other reliable sources. (5) For definitions, disclaimer, and navigation help, please refer to the Site Surfing Guide. (6) Information in this site may be cited, giving the due credit to www.internetworldstats.com. Copyright © 2001 - 2011, Miniwatts Marketing Group. All rights reserved worldwide.

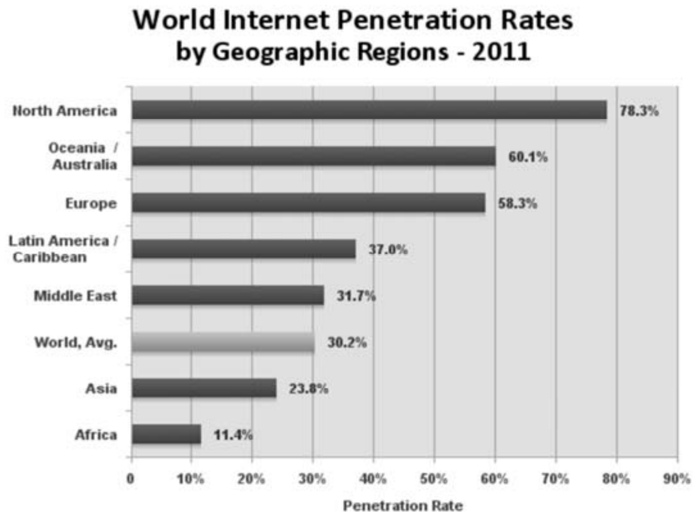
# Internet Users by Region (1)



Internet Users in the World
Distribution by World Regions - 2011

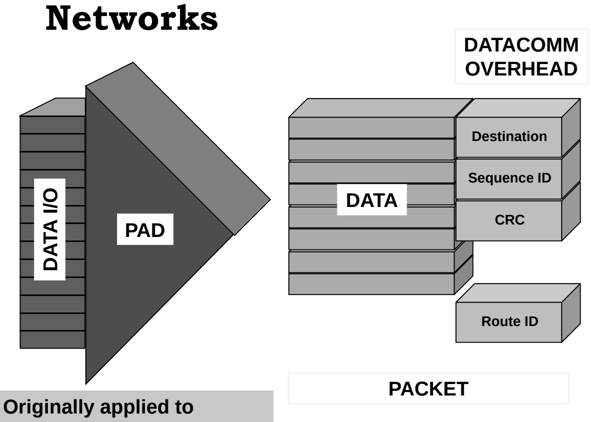
Source: Internet World Stats - www.internetworldstats.com/stats.htm
Basis: 2,095,006,005 Internet users on March 31, 2011
Copyright © 2011, Miniwatts Marketing Group

Copyright © 2011 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.



World Internet Penetration Rates
by Geographic Regions - 2011

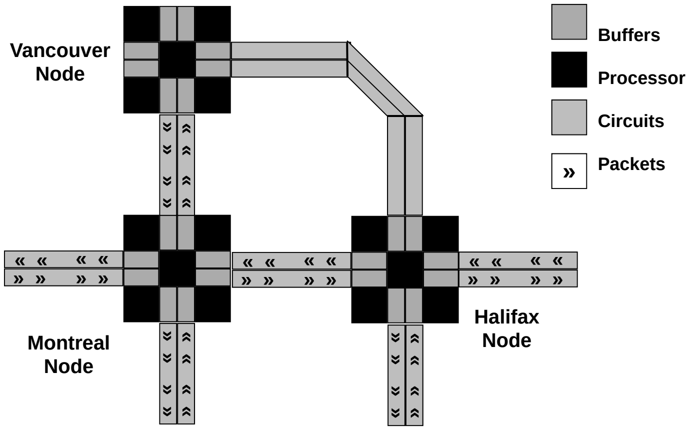
# Basics: Packet-Switching Networks



Originally applied to Telephony in X.25 networks

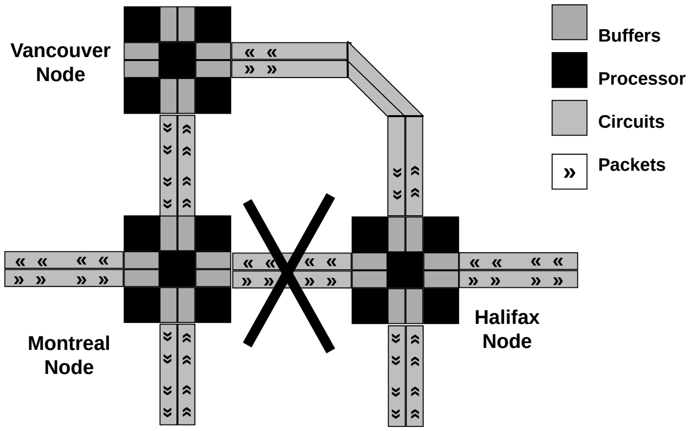
Copyright © 2011 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

# Basics: Datagram Routing



Copyright © 2011 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

# Basics: Datagram Routing



Copyright © 2011 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

# Basics of TCP/IP -- Video

- *Warriors of the Net:* 12 minutes – used by permission of the authors.

http://www.mekabay.com/overview/warriors_of_the_internet.mpg

Copyright © 2011 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

# Tracing a Suspect on the Internet

- The Dynamic IP Address
- Locating the Host
- DNS Lookup
- betterwhois.com
- SamSpade Program
- Locating Information from E-Mails
- E-Mail Headers

Copyright © 2011 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

# The Dynamic IP Address

- Suspect may have own connection to 'Net
  - ❑ Has permanent IP address
  - ❑ E.g., gmail.com has IP address 64.233.171.83
  - ❑ Norwich.edu is 192.149.109.197
- Or suspect connects to Internet via ISP
  - ❑ DHCP (Dynamic Host Configuration Protocol)
  - ❑ User is assigned temporary "dynamic" address
  - ❑ Re-used and not unique
  - ❑ Logged by ISP for some time (days to forever)
  - ❑ Must absolutely get cooperation of ISP and obtain records (if they still exist) under subpoena
  - ❑ The records will show match of dynamic address to user's modem's MAC (media access control) address and from there to the *assigned* modem location, authorized user, address and so on

What would an unsecured WAP do to this linkage?

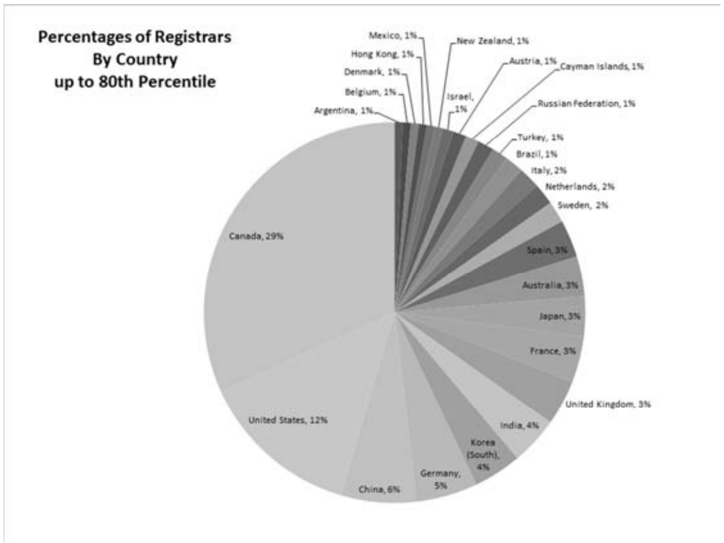
Copyright © 2011 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

# Locating the Host

- ICANN (Internet Corporation for Assigned Names and Numbers) http://www.icann.org/
  - ❑ Global coordination of IP address assignments
  - ❑ Defines rules for domain names
- InterNIC < http://www.icann.org/ > points to registrars around world
  - ❑ See lists e.g., http://www.internic.net/origin.html

ICANN

Copyright © 2011 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.



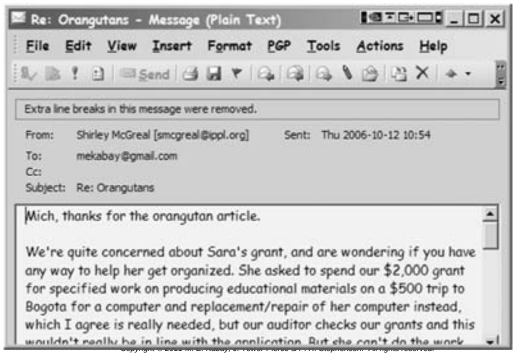
## DNS Lookup

- WHOIS functions available online from each registrar
  - ❑But http://www.betterwhois.com/ works with all registrars (see next page)
- Many other tools available online for DNS lookup
- SamSpade tool and service from **http://www.samspade.org** can find many records as well as providing additional functions (see page after next)
- Info in registry may be false or out of date
  - ❑Often see dummy phone numbers in DNS

Copyright © 2011 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

## Locating Information from E-Mails

- Headers are crucially important
  - ❑Often stripped from display



Re: Orangutans - Message (Plain Text)

Extra line breaks in this message were removed.

From: Shirley McGreal [smcgreal@ippl.org] Sent: Thu 2006-10-12 10:54
To: mekabay@gmail.com
Cc:
Subject: Re: Orangutans

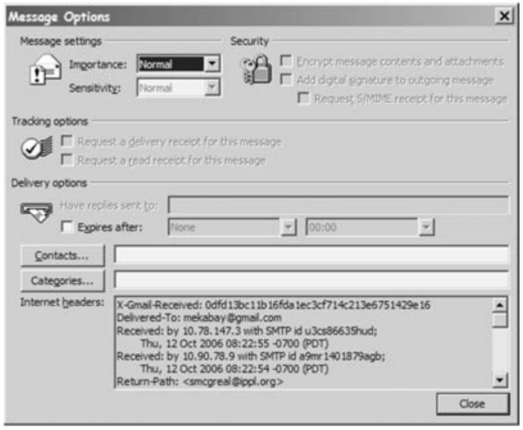
Mich, thanks for the orangutan article.

We're quite concerned about Sara's grant, and are wondering if you have any way to help her get organized. She asked to spend our $2,000 grant for specified work on producing educational materials on a $500 trip to Bogota for a computer and replacement/repair of her computer instead, which I agree is really needed, but our auditor checks our grants and this wouldn't really be in line with the application. But she can't do the work

## E-Mail Headers

- Can be displayed through e-mail options

*This example is from MS-Outlook*



Message Options

Message settings
Importance: Normal
Sensitivity: Normal

Security
☐ Encrypt message contents and attachments
☐ Add digital signature to outgoing message
☐ Request S/MIME receipt for this message

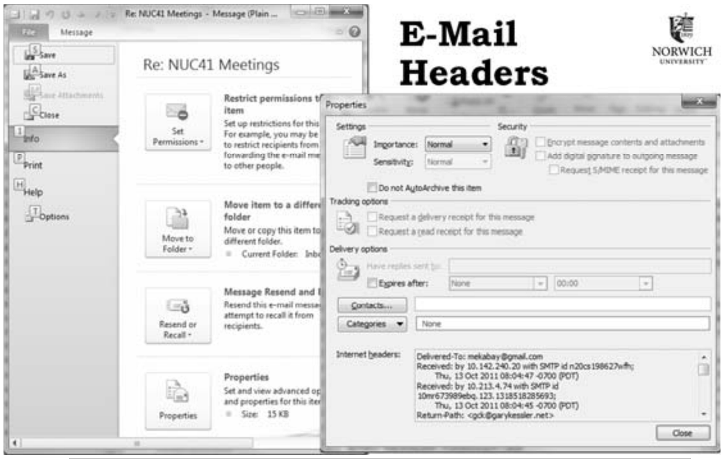
Tracking options
☐ Request a delivery receipt for this message
☐ Request a read receipt for this message

Delivery options
Have replies sent to:
☐ Expires after: None 00:00

Internet headers:

```
X-Gmail-Received: 0dfd13bc11b16fda1ec3cf714c213e6751429e16
Delivered-To: mekabay@gmail.com
Received: by 10.78.147.3 with SMTP id u3cs86635hud;
        Thu, 12 Oct 2006 08:22:55 -0700 (PDT)
Received: by 10.90.78.9 with SMTP id a9mr1401879agb;
        Thu, 12 Oct 2006 08:22:54 -0700 (PDT)
Return-Path: <smcgreal@ippl.org>
```

## E-Mail Headers



Re: NUC41 Meetings - Message (Plain ...

Re: NUC41 Meetings

Restrict permissions t[o this] item
Set up restrictions for this ... For example, you may be ... to restrict recipients from forwarding the e-mail me[ssage] to other people.

Move item to a differe[nt] folder
Move or copy this item to ... different folder.
Current Folder: Inb[ox]

Message Resend and ...
Resend this e-mail messa[ge] ... attempt to recall it from recipients.

Properties
Set and view advanced op[tions] and properties for this ite[m]
Size: 15 KB

Properties

Settings
Importance: Normal
Sensitivity: Normal
☐ Do not AutoArchive this item

Security
☐ Encrypt message contents and attachments
☐ Add digital signature to outgoing message
☐ Request S/MIME receipt for this message

Tracking options
☐ Request a delivery receipt for this message
☐ Request a read receipt for this message

Delivery options
Have replies sent to:
☐ Expires after: None 00:00

None

Internet headers:

```
Delivered-To: mekabay@gmail.com
Received: by 10.142.240.20 with SMTP id n20cs198627wfh;
        Thu, 13 Oct 2011 08:04:47 -0700 (PDT)
Received: by 10.213.4.74 with SMTP id
10mr673989ebq.123.1318518285693;
        Thu, 13 Oct 2011 08:04:45 -0700 (PDT)
Return-Path: <gck@garykessler.net>
```

**NEVER simply forward an e-mail of interest to an investigator; always copy and paste the headers into your message to avoid corrupting the header.**

## Proactive vs Reactive Strategies

- Some crimes are difficult to locate before they happen – need victim complaint to find out
  - ❑Identity theft
  - ❑Cyberstalking
- Others benefit from dragnets
  - ❑Child pornography
  - ❑Child abuse
- Officers need familiarity with argot (slang), culture

Copyright © 2011 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

## Online Stings: Entrapment?

- Must not give any basis for claim that officer *initiated, suggested, prompted,* or *encouraged*
  - ❑Illegal activity or
  - ❑Investigative actions that violate privacy or
  - ❑Convert a civilian into an agent of law enforcement to violate legal restrictions
- ENTRAPMENT can destroy case
  - ❑Why? 4th Amendment safeguards
- Sorrells v. United States (1932)
  - ❑SCOTUS ruled that entrapment defense must show proof that LEO *encouraged* crime
  - ❑Defendant *would not have been predisposed* to commit crime

Copyright © 2011 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

## United States v. Poehlman (2000)

- Poehlman alleged to have met undercover LEO to have sex with minor
- But defendant said he started online discussions with LEO to form *adult* relationship
- LEO wrote she was looking for someone “to train her daughters in the ways of the world”
- Poehlman explicitly said he wasn’t interested and LEO responded that she would terminate relationship
- Poehlman offered to “train” daughters as way of continuing relation but claimed he had no intention of having sex with them – was ploy
- SCOTUS ruled in favor of defendant: evidence that pedophilia was not his original intent & LEO was significantly responsible for his actions

Copyright © 2011 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

## Three Cybercrime Scenarios

*YOU ARE RESPONSIBLE FOR STUDYING THESE CASES IN DETAIL*

- Cases presented by Ivan Orton in Ch 3 of Prof Clifford’s text:
  - ❑Janet Davis – intrusion and data theft
  - ❑Mel Howard – intrusion and data destruction
  - ❑Allen Worley – harassment and stalking via e-mail
- Study closely – will be discussed throughout remainder of course AND IN EXAMS
  - ❑Events
  - ❑Investigation
  - ❑Prosecution

Copyright © 2011 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

# DISCUSSION

Copyright © 2011 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.