CERTConf2005 Forensics: Overview

What this class is…

- A dense, relatively fast-paced excursion into the world of cyber forensics.
- ‘Technical’ means the class will require a certain amount of technical expertise.
- ‘Practical’ means that the information we cover will provide you with the technical capacity for conducting basic forensic investigations, practically, not legally.
- I’m a firm believer in ‘hands on’ however this venue doesn’t lend itself well, to this – so go straight home afterward and do this stuff! ;-)

What this class is…

- The courses today (1-4) will touch on many areas of Cyber Forensics but will not go to any exceeding depth in any one area
- This is designed to broaden your skill set and introduce you to many areas of Cyber Forensics in a short period of time, not to make you an expert in any one facet

What is Cyberforensics?

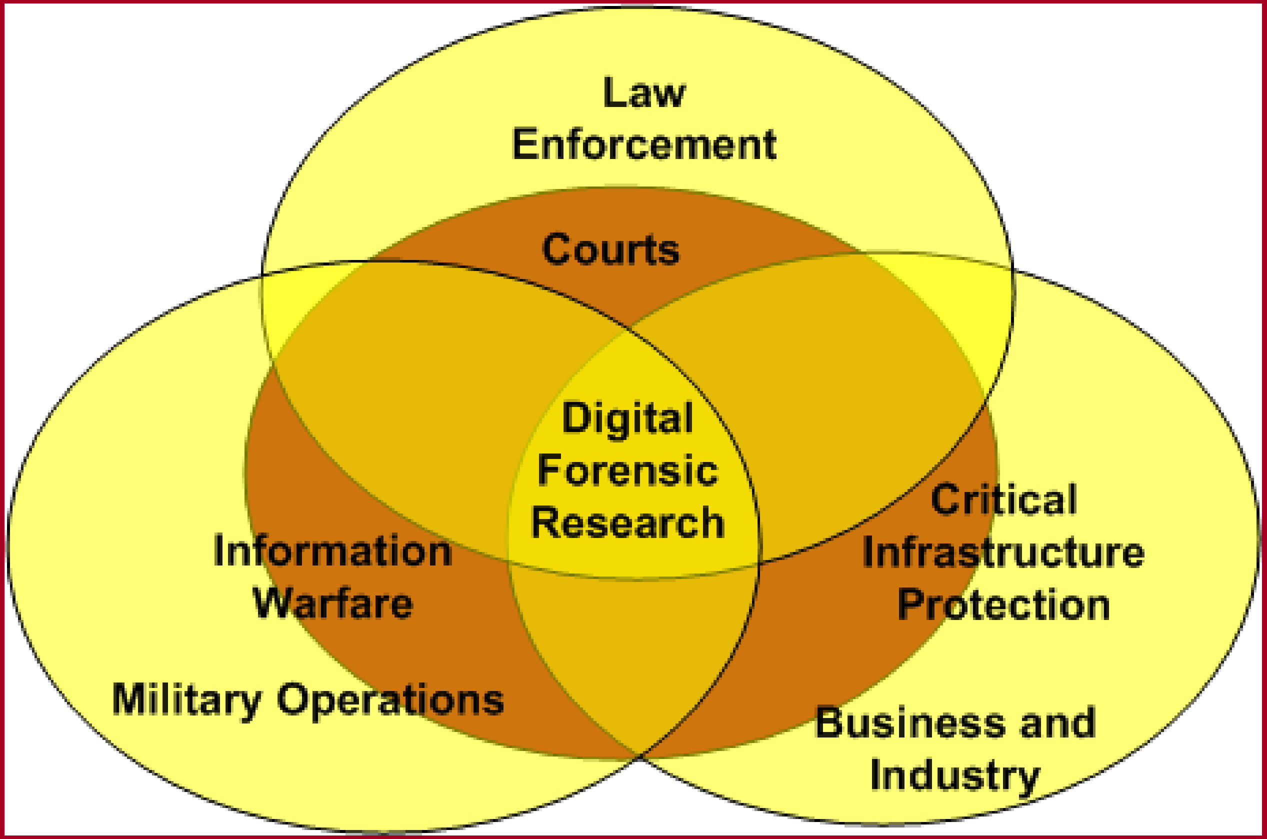
- This really depends on the point of view…
- Traditionally Cyber forensics involves the
  - preservation,
  - collection,
  - validation,
  - identification,
  - analysis,
  - interpretation,
  - documentation and
  - presentation
- …of computer evidence stored on a computer.

- "Forensics is the application of science to the legal process."
  - Jim Christy, DCCI

Viewpoint

- According to the CFEWG curriculum group there are three perspectives of cyberforensics
  - Law enforcement
    - FBI/IRS/private party
  - Business/Industry
    - Cisco/L3
  - Military/counterintelligence
    - AF OSI/NSA
- Although not mutually exclusive, each can have its own thrust.

Viewpoint


Law Enforcement
Courts
Digital Forensic Research
Information Warfare
Critical Infrastructure Protection
Military Operations
Business and Industry

Viewpoint

- Each perspective has difference objectives, even though there is overlap, the approaches of each remain ah-hoc and uncoordinated
- Technology is vendor-driven
- No industry certification
- No standards
- Interesting situations with the court system

Coverage from OS perspective

- Windows
  - 95% of cases FBI sees involve Windows
  - Topics
    - File systems: FAT & NTFS
    - Multiple tools:
      - Commercial
      - Freeware
        - » Windows & Linux!
    - Live response
    - Network forensics

Coverage from OS Perspective

- UNIX/Linux
  - Topics
    - File systems: EXT2/3
    - Multiple tools:
      - Freeware
      - Not much industry drive for commercial tools
    - Live response
    - Network forensics

Topics we will cover…

- Topics include:
  - the incident response process;
  - forensic duplication and data recovery;
  - Windows and UNIX file systems;
  - binary analysis;
  - network attacks and their signatures;
  - data hiding techniques;
  - malicious code detection;
  - network forensics and surveillance; and
  - tools and techniques for investigating computer intrusions for both UNIX/Linux and Windows systems.

Cybercrime & Cyberwarfare

- "Information warfare specialists at the Pentagon estimate that a properly prepared and well-coordinated attack by fewer than 30 computer virtuosos strategically located around the world, with a budget of less than $10 million, could bring the United States to its knees."

Center for Strategic & International Studies (CSIS)
http://www.csis.org/pubs/cyberfor.html

Cybercrime & Cyberwarfare

- "Such a strategic attack, mounted by a cyberterrorist group, either substate or nonstate actors, would shut down everything from electric power grids to air traffic control centers."

Center for Strategic & International Studies (CSIS)
http://www.csis.org/pubs/cyberfor.html

Scope of the Problem

- In1990 a computer hard drive seized in a criminal investigation would contain approximately 50,000 pages of text
- The same situation with hard drives now, contain **5 million to 50 million pages** of data.
  - But the ability of these agencies to retain computer talent is seriously jeopardized by the compensation packages offered by the private sector.

Center for Strategic & International Studies (CSIS)
http://www.csis.org/pubs/cyberfor.html

Computer Crime

- Sample of computer crimes from 2001
  - Demoted employee installs a logic bomb, which later deactivates hand-held computers used by the sales force.
  - eBay
    - User advertises goods, but on receiving payment never ships the goods.
    - Advertised collectibles turn out to be fakes
  - Disgruntled student sends threatening emails, leading to school closing down.
  - Ring of software pirates use web site to distribute pirated software

Stephenson, 2001.

Computer Crimes

- Software company employee is indicted for altering a copyright program to overcome file reading limitations
- Hacker accesses 65 U.S. Court computers and downloads large quantities of private information.
- Hacker accesses bank records, steals banking and personal details.
- 15 year old boy runs scripts that invoke DOS against eBay, Yahoo!, AOL, etc.

• Moral: NO SUCH THING AS TYPICAL COMPUTER CRIME.

• Must be flexible in your response

Stephenson, 2001.

References

- Stephenson, P. (2001). *Investigating Computer-Related Crime*. CRC Press.
- Center for Strategic & International Studies (CSIS) http://www.csis.org/pubs/cyberfor.html
- **Dcii.gov**

CERTConf2005 Threat Vectors

Hacker Types

- Script Kiddy
- Disgruntled employee
- Professional Hacker
- Innovator
- Political
- State Sponsored
- Terrorist Organization

Hacker Motivations

- Disgruntled employee
- Further Terrorist goals
- Financial gain
- Political
- Industrial Espionage

Disgruntled employee

- Number of personal reasons including;
  - Revenge
  - Emotional
  - Financial

Terrorist goals

- Disrupt social stability
- Cause chaos
- Economic destabilization
- Cause great loss of life
- Political gain i.e., change of government.

Cyber Infrastructure Protection

- Hiring professional hackers to disrupt the Critical Cyber Infrastructure.
- 85% - 90% of this Critical Infrastructure is operated and owned by the private sector.

Financial gain

- Organized crime groups
- Russian professional hacker organizations, banks and credit card company clearing houses.
- Individuals
- Inside employees
- Competitors

Industrial Espionage

- Competitors
- Ascertain competitor’s long range strategic goals
- Obtain customer data base
- Obtain competitor’s infrastructure information. IT and physical.

Threat Vector

- Motive
- Means
- Opportunity
- Agent

Motive

- Why makes someone what to gain unauthorized access into a network?
- What is the typical profile?
  - Script kiddy – Twinkies and the Dew – 2:00 AM momas' basement.
  - Want-a-be hacker in his own basement

Professional Hacker

- Motives
  - Financial gain
  - Political

Protection mechanisms

- Minimize the target
- Stay current on knowledge base
- Deterrence
- Protection
- Detection
- Reaction
- Protecting IT assets, Alan Hood Scientist for Britain's DERA 1997

Cyberterrorism

- There is a convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.
- Georgetown University May 23, 2000 Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services
  U.S. House of Representatives.

Examples of Cyberterrorism

- In 1996, a computer hacker allegedly associated with the White Supremacist movement temporarily disabled a Massachusetts ISP and damaged part of the ISP's record keeping system.

Continued

- In 1998, Spanish protestors bombarded the Institute for Global Communications (IGC) with thousands of bogus e-mail messages. E-mail was tied up and undeliverable to the ISP's users, and support lines were tied up with people who couldn't get their mail.

Continued

- In 1998, ethnic Tamil guerrillas swamped Sri Lankan embassies with 800 e-mails a day over a two-week period. The messages read "We are the Internet Black Tigers and we're doing this to disrupt your communications." Intelligence authorities characterized it as the first known attack by terrorists against a country's computer systems.

Continued

- During the Kosovo conflict in 1999, NATO computers were blasted with e-mail bombs and hit with denial-of-service attacks by hacktivists protesting the NATO bombings. In addition, businesses, public organizations, and academic institutes received highly politicized virus-laden e-mails from a range of Eastern European countries, according to reports. Web defacements were also common. After the Chinese Embassy was accidentally bombed in Belgrade, Chinese hacktivists posted messages such as "We won't stop attacking until the war stops!" on U.S. government Web sites.

Thwarting cyberterrorism

- National cyber security adviser Richard Clarke has warned that the U.S. is "vulnerable to sophisticated attacks. Not to 14-year-olds, but to a sophisticated group or nation-state. . . . It could lead to catastrophic damage to the economy, and, if done at a time of national security crisis, it could lead to catastrophic damage to our national defense."
-

CERTConf2005
Hex

Why HEX?

- While hex is less readable than ascii text, it is more readable than binary…
  - The number 65535 would be written down as 16 ones, or 1111111111111111_2
  - Prone to error…was that 16 or 17 1's?
  - To condense the same information we use a base 16 system, called **hexadecimal**.

What is HEX?

- Hex uses decimals first,followed by alphabetic characters.
- It is fairly straightforward to convert back and forth from binary to hex

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F

BIN %	OCT	DEC	HEX 0x
1	1	1	1
10	2	2	2
11	3	3	3
100	4	4	4
101	5	5	5
110	6	6	6
111	7	7	7
1000	10	8	8
1001	11	9	9
1010	12	10	A
1011	13	11	B
1100	14	12	C
1101	15	13	D
1110	16	14	E
1111	17	15	F
10000	20	10	10
10001	21	11	11

NUCIA

Your Key to Security

Converting

- If you write down 1234, (base 10) you are talking about the number one thousand, two hundred and thirty four.
- This can be rewritten as:

```
1 *  1000 =  1000
2 *   100 =   200
3 *    10 =    30
4 *     1 =     4
```

```
1 * 10^3
2 * 10^2
3 * 10^1
4 * 10^0
```

Converting

- It is the same in all other bases, each place represents a power of the base:

```
%1010 would be

  1 * 2^3
  0 * 2^2
  1 * 2^1
  0 * 2^0
```

```
0x1234 will be

  1 * 16^3
  2 * 16^2
  3 * 16^1
  4 * 16^0
```

Converting

- What is 0xCB in Decimal?

- C = 12 and B = 11 so
  12 * 16^1 + 11 * 16^0 = 203

What about binary?

C = 12 = 1100   B = 11 = 1011

CB = 1100 . 1011

so 0xCB = %11001011

Converting

- What is 0xAF1 in Decimal?

- A = 10, F = 15 so

  10 * 16^2 + 15 * 16^1 + 1 * 16^0 = 2801

What about binary?

A = 1010 F = 1111 1 = 0001

AF1= 1010 . 1111 . 0001

so 0xAF1 = %101011110001

Practical bits

- Netmask:
  - So most people just type in:

    255.255.255.0
  - What does this mean?

Practical bits

- Netmask:

IP address are ‘dotted quad’, basically the dots just break up bits to make them easier to read.

How many bits does it take to represent 256 (base 10)?

Practical bits

- Netmask:

11111111 = 255, so 8 bits for 256 unique values

Therefore, 255.255.255.0 is ‘decimal dotted quad” for the base 2 number:

11111111.11111111.11111111.00000000

This is also sometimes referred to as as /24 network because there are 24 1’s

Netmasks *almost* always start with sequential 1’s and end with sequential 0’s

…slight diversion now…

- Netmask:

11111111 . 11111111 . 11111111 . 00000000

network (subnet) host

So this particular netmask (/24) allows for 256 different hosts…(well actually a bit less – but lets just say 256) on one subnet. Every time you add a bit to the netmask, you get more subnets and less hosts per subnet.

Example:

192.168.100.0 – 192.168.100.255

…slight diversion now…

- Netmask:

<u>11111111.11111111.11111111.1</u>   <u>0000000</u>

network (subnet)   host

So this particular netmask (/25) has 2 subnets...

Example:

192.168.100.0 – 192.168.100.127   subnet1

192.168.100.0 – 192.168.100.255   subnet2

So /26 has 4 subnets, /27 has 8 subnets, all the way through /30 which has 64 subnets (4 hosts per)

…slight diversion now…

- Netmask:

Looking at Netmasks that ‘lower’ than /24 get into Class A,B,C type discussions and are definitely out of scope here…

Basically each fourth of the dotted quad controls a class, so using letters to represent the class a bit belongs to:

AAAAAAAA.BBBBBBBB.CCCCCCCC.xxxxxxxx

Class D is used for broadcasting

Class E is “Experimental” is basically a leftover from bureaucratic / political “design by committee” fallout

Practical Bits

- Netmask:
  - What's the mask actually do?
  - Used for Bitwise AND with a host's address
  - If my computer is 137.48.112.123

  and my netmask is 255.255.255.0

```
    10001001.00110000.01110000.01111011
    11111111.11111111.11111111.00000000
AND 10001001.00110000.01110000.00000000
```

so for the very common /24 netmask the result may be familiar then the last number (123) is the host id, and the others 137.48.112 is the network.

Why does all this matter?

- So as a forensic examiner you might not be overly concerned with netmasks, or the class of a particular network
- And you may not be able to decode machine language when you see it
- But you should understand what it is and realize that decoding it correctly could change data into information…

Why does all this matter?

- In the physical world if an investigator found a letter at a crime scene he would not throw it away just because the crime was committed in Nebraska and the letter was written in Chinese.

Why does all this matter?

- A set of 1's and 0's that translates into an peculiar set of Hex characters may appear to be gibberish, but upon proper decoding, it may reveal an MIME encoded message (for example)
- Just because the data isn't in a particularly useful form, doesn't mean that it's not valuable.

Encoding is not Encrypting

- It is also important to note the different between Encoding and Encrypting
- Encoding is done primarily to make information EASY to interpret
- Encrypting is done primarily to make information HARD to interpret

Encoding is not Encrypting

- The very fact that data has been encrypted is sometimes enough to raise ‘red flags’
- Depending on circumstances the existence of encrypted files may create, or be a contributing factor for Probable Cause
- This is not the case with encoded files

The Hex Editor

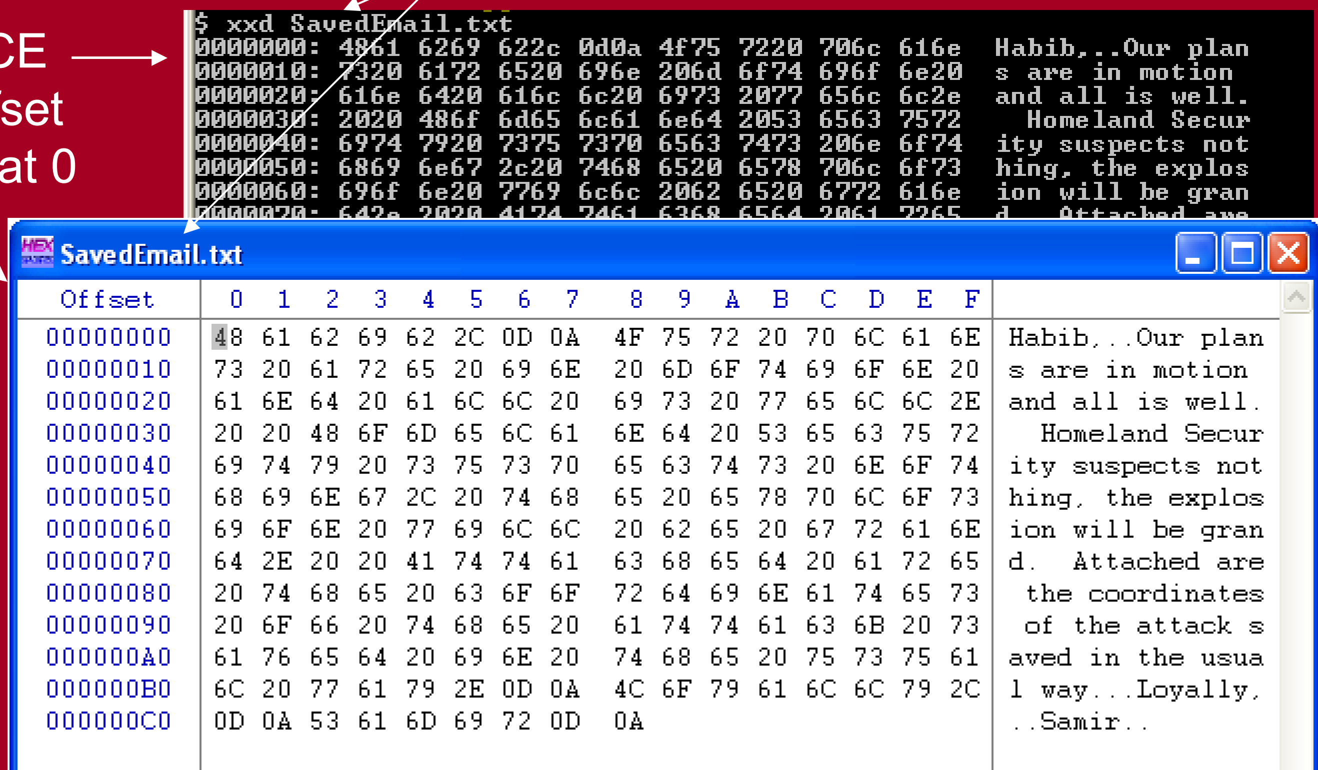
- In windows you may find a tool such as winhex, frHed, or Hackman valuable:
- In Linux maybe something like xxd, Heme, SHED, gHex, KHexEdit or some other abstraction (Autopsy for example has a hex view option).

Hex Editor

You can use these hex tools at varying granularity…by file:

Viewing a FILE

NOTICE the offset starts at 0



Hex Editor

- How is this different?

Viewing a DISK

Contents do not start at 0

Removable Medium 2

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Access
0011B1A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0011B1B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0011B1C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0011B1D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0011B1E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0011B1F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0011B200	48	61	62	69	62	2C	0D	0A	4F	75	72	20	70	6C	61	6E	Habib,..Our plan
0011B210	73	20	61	72	65	20	69	6E	20	6D	6F	74	69	6F	6E	20	s are in motion
0011B220	61	6E	64	20	61	6C	6C	20	69	73	20	77	65	6C	6C	2E	and all is well.
0011B230	20	20	48	6F	6D	65	6C	61	6E	64	20	53	65	63	75	72	Homeland Secur
0011B240	69	74	79	20	73	75	73	70	65	63	74	73	20	6E	6F	74	ity suspects not
0011B250	68	69	6E	67	2C	20	74	68	65	20	65	78	70	6C	6F	73	hing, the explos
0011B260	69	6F	6E	20	77	69	6C	6C	20	62	65	20	67	72	61	6E	ion will be gran
0011B270	64	2E	20	20	41	74	74	61	63	68	65	64	20	61	72	65	d. Attached are
0011B280	20	74	68	65	20	63	6F	6F	72	64	69	6E	61	74	65	73	the coordinates
0011B290	20	6F	66	20	74	68	65	20	61	74	74	61	63	6B	20	73	of the attack s
0011B2A0	61	76	65	64	20	69	6E	20	74	68	65	20	75	73	75	61	aved in the usua
0011B2B0	6C	20	77	61	79	2E	0D	0A	4C	6F	79	61	6C	6C	79	2C	l way...Loyally,
0011B2C0	0D	0A	53	61	6D	69	72	0D	0A	00	00	00	00	00	00	00	..Samir.........
0011B2D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0011B2E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....

Files

- Many “low level” things can be determined at the Hex level
- Files always have particular header information (this is different then file-extensions like .doc or .jpeg)

Files

When considering “graphics files”

; Windows Bitmap graphics BMP=0x00:"BM" ; Compressed BM? File BM_=0x00:"SZDD"

; Graphics Interchange Format bitmap graphics GIF=0x00:"GIF8"

; Graphics Interchange Format bitmap graphics (GIF 87a) GIF87A=0x00:"GIF87a"

; Graphics Interchange Format bitmap graphics (GIF 89a) GIF89A=0x00:"GIF89a"

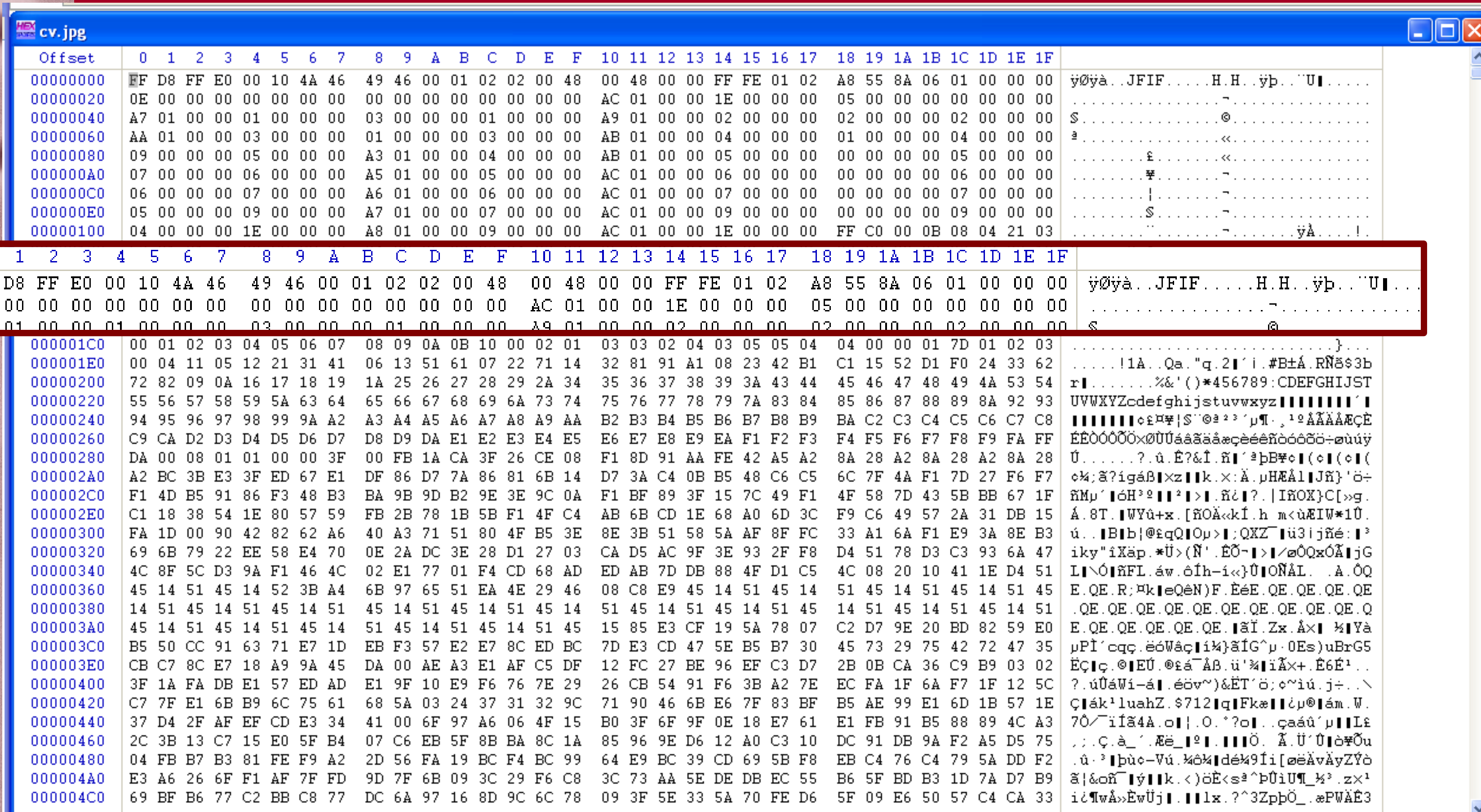
; JPEG Bitmap graphics JPE=0x00:0xFF,0xD8,0xFF,0xE0,0x00,0x10,"JFIF"

; JPEG Bitmap graphics JPG=0x00:0xFF,0xD8,0xFF,0xE0,0x00,0x10,"JFIF" JS=0x00:"/"

These are standard types, the information is widely available, these particular lines came from drivespy.ini

Files

- This is the hex representation of a jpg:



Files

- If files are simply stored in ‘hidden’ areas, like unallocated, slack, or interpartition space, they will still have header information
- If files are enciphered some way (like stereography) then there is no header information
- If files are encrypted / compressed, there may not be header information about the file, but there will typically be header information about the encryption / compress for decryption / decompression purposes

Files

- In some cases you may find portions or fragments of a file. If you suspect that the fragment may be part of what used to be JPEG for example (because near where the header should be you found “FIF” and you know that jpeg headers contain “JFIF”) you can attempt to recover the file by editing the correct header information back to the disk.

Cyberforensics
Hard Disk Duplication

Duplication is Science

Why?

- Why even create a copy? Why not perform analysis on the actual hard disk?
  - Evidence
    - Bagged n sealed
    - Chain of custody
    - Basically
      - what if you accidentally made a mistake?
      - To show that no evidence was “planted”
    - Preserving the Integrity of the Evidence

Why?

- No matter what tool you are using, a “write blocking” adapter will prevent costly mistakes

Evidence

- Federal Rules of Evidence (FRE)
- To prove the content of a writing, recording, or photograph, the original writing, recording or photograph is required, except as otherwise provided in these rules or by Act of Congress
- FRE #1002—item or information presented in court must be original
- FRE 1001(3) outlines one of these exceptions:
- Definitions and Duplicates: If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect accurately, is an original

Evidence

- Admissibility of Duplicates FRE #1003, A duplicate is admissible to the same extent as an original unless 1) a genuine question is raised as to the authenticity of the original ,or 2) in the circumstances it would be unfair to admit the duplicate in lieu of the original

Chain o Custody

- Evidence tag for each hard drive or media
  - Time and date of action
  - Number we assigned to that case
  - Number of this particular tag
  - Consent required? Signature of person owning information
  - Whom evidence belonged? Who provided information
  - Complete description of evidence including quantity
  - Who rec'd evidence and signature of recipient

Chain o Custody

- Back of evidence tag
  - Who the evidence was rec’d from and location it was in
  - Date of receipt
  - Reason the evidence was given to another person
  - Who rec’d evidence and where was evidence was rec’d or located

Initial Response: Live Sys

- Volatile data before forensic image
  - Volatile data
  - Registers, cache contents
  - Memory contents
  - State of networks
  - State of running processes
  - Contents of storage media
  - Contents of removable and backup media

Initial Response: Live Sys

- Create a step-by-step plan, document it:
  - Establish a new shell: cmd.exe (W), bash (U)
  - Record the system date and time: date, time (W), w (U)
  - Who is logged on: loggedon (W), w (U)
  - Record open sockets: netstat (W), netstat –anp (U)
  - Processes that open sockets: fport (W), lsof (U)
  - Currently running processes: pslist (W), ps (U)
  - System that recently connected: nbtstat (W), netstat (U)
  - Record system time: date, time (W), w (U)
  - Record step taken: doskey (W), script, vi, history (U)
- This stuff can be scripted!

Terminology

- *Forensic Duplication:* bit for bit copy (dd, dcfldd, odd)
- *Qualified Forensic Duplicate:* file that contains every bit, but is stored in an altered form (encase)
- *Restored Image:* a Forensic Dup or Qualified Forensic Dup that has been restored to a drive (dd, encase, etc)
- *Mirror Image:* a duplicate created with hardware (SF-5000, Solo-2)

Offline duplication

- Assuming the computer is ‘offline’
  - There are a couple avenues to take
    - Logical copy
      - Windows drag n drop / cut n paste
      - Here we are talking about things like files and directories
    - Physical copy
      - Bit for bit copy
      - Here we are obviously talking about bits
    - Advantages / Disadvantages to the two methods?

Offline Duplication

- Physical copies of the hard drive contain more information that a logical copy. Things like:
  - Information left in virtual memory / page files, swap space, etc
  - Files and directories marked as deleted then partially written over, slack space, etc
  - "unallocated" space that is actually in use

Integrity

- When writing an image to a new hard disk for analysis it’s a good idea to ‘clean’ the disk first
- This is where the ‘writing zeros’ or ‘zero-filling’ comes into play

Proving Integrity

- As a professional, your word is often not enough to establish that the copy is an exact copy of evidence obtained earlier.
- This can be mitigated using a HASH like MD5 or SHA-1 – some forensic packages may even use things like CRC.

Hashing

- One of the best ways to describe hashing is to describe a hash as a fingerprint [of an image].
- Fingerprints uniquely identify a much larger object (human) from a much smaller object (the fingerprint)

Hashing

- …similarly, a digital hash is a unique representation of a larger object – like an image
- This hash is a file that is completely separate for the image that it is fingerprinting and has a set length – like 128 or 160 bits.
- A 1 MB file and a 1 GB files will both produce hashes of the same length

Hashing

- There are many automated tools that provide hashing components.
- Most *nix distributions provide hashing tools by default, for windows you'll have to download software

Hashing

```
$ md5sum.exe SavedEmail.txt
b13e0863a5ab9f329b59a0d15519f9ea *SavedEmail.txt
```

```
$ sha1sum.exe SavedEmail.txt
017f2def39d04cb5f42cb0562b5bc4b41b2eebc8 *SavedEmail.txt
```

```
[root@localhost root]# md5sum SavedEmail.txt ; sha1sum SavedEmail.txt
04851fe8301dde9086e1838e9d564b72  SavedEmail.txt
7fac072552ac7368eb42e54eae90f35987bcaf08  SavedEmail.txt
[root@localhost root]#
```

Hashing

- The same software typically provides the means to check to see if the hash of a given file has changed

```
[root@localhost root]# md5sum SavedEmail.txt > SavedEmail.md5
[root@localhost root]# md5sum -c SavedEmail.md5
SavedEmail.txt: OK
[root@localhost root]# sha1sum SavedEmail.txt > SavedEmail.sha1
[root@localhost root]# sha1sum -c SavedEmail.sha1
SavedEmail.txt: OK
[root@localhost root]#
```

- Add a space to the email…

```
[root@localhost root]# md5sum -c SavedEmail.md5
SavedEmail.txt: FAILED
md5sum: WARNING: 1 of 1 computed checksum did NOT match
[root@localhost root]# sha1sum -c SavedEmail.sha1
SavedEmail.txt: FAILED
sha1sum: WARNING: 1 of 1 computed checksum did NOT match
[root@localhost root]#
```

Hashing

Use something like md5deep or sha1deep for recursion:

```
C:\tools\md5deep>md5deep -r * > c:\file.dat

C:\tools\md5deep>md5deep -rX c:\file.dat *

C:\tools\md5deep>md5deep -rX c:\file.dat *
b31540d38eb675b77c2b417b374bada5  C:\tools\md5deep\README.txt

C:\tools\md5deep>
```

Side Rant: Hashing DLs

- When downloading software a hash is often provided along with the download.
  - What purpose does this hash serve?

Duplication gotchas

- Some file systems have limits to maximum file size…like the 2.1 GB barrier Hard/Soft or the 8.4 Hardware barriers
  - In such cases, the image would have to segmented into multiple images that can later be restored into one
  - Or you could use a filesystem that supports larger files :-)

dd

- dd has *many* flags (options)
- You must first understand:

    dd if=/*source* of=/*destination*

    if = infile, or evidence you are
        copying (a hard disk, tape, etc.)
    source = source of evidence
    of = outfile, or copy of evidence
        destination = where you want to
        put the copy

dd

- dd if=/dev/hda of=/dev/ImageCopy1
- In addition to hard drives, dd works well restoring block-oriented devices, such as tapes.
- Some useful optoins are:

  ibs = input block size
  obs = output block size
  bs = block size

  count = number of blocks to copy
  skip = # of blocks to skip at start of input
  seek = # of blocks to skip at start of output

dcfldd

- An enhanced version of dd – DOD Computer Forensics Lab dd
- Able to generate hashes as the image is created – otherwise works just like dd

dcfldd if=/dev/hdd of=/mnt/disk.dd bs=2k hashwindow=2M hashlog=/mnt/disk.md5

odd

- Odessa – Open Digital Evidence Search and Seizure Architecture
- ODD – open data duplicator
  - – Client / server
    - Both can be on one machine
  - – Plugin based
    - Auto extract images
    - Auto hashing
    - Auto string search

Others…

- Safeback
- Forensic ToolKit Imager
  - Can convert between dd,en,safeback etc
- Encase
  - Supports ‘interesting methods’
    - Crossover cable
    - ‘live’ acquisition

‘Hard’ to recover

- *Deletion* and *replacement*
  Deleting the file and replacing it immediately with another file of the same name and exactly the same size may completely overwrite the original file.
- *Low level formatting*
  LLFing of the computer hard disk will destroy all data. LLF is usually only carried out once by the manufacturer - the Format command in DOS/Windows does NOT perform a low level format – in fact an ‘actual’ LLF can not be performed by a PC on a ‘new’ hard disk.

‘Hard’ to recover

- *"Anti-Forensic Software“*
  Specialist software is available which claims to completely remove all trace of deleted files from a hard disk, including residual traces of old deleted files in slack space (unused space left over at the end of a cluster), by overwriting those areas multiple times with random data.
- *Encryption*
  Encryption is an effective way to conceal incriminating evidence. An encrypted file can usually only be opened if the decryption key is obtained.

“Easy” to Recover

- *Deletion*
  One of the easiest situations for an investigator is when a suspect has simply deleted all incriminating files just before the PC is obtained.
- When a file is deleted, the operating system simply marks the cluster(s) the file is occupying as now being available for use again in the File Allocation Table. It does not in any way destroy or damage the data in the cluster(s) itself, apart from (typically) replacing the first letter of the filename with the greek letter sigma. The file has effectively been removed from the index. The forensic investigator is easily able to recover the file by simply extracting it straight from the cluster.

‘Easy’ to recover

- The situation becomes more difficult as time passes. Since deletion the operating system now sees the cluster(s) as being available for use (un-re-allocated). The next time a new file is saved onto the disk there is a danger that the file, or part of it, will be stored in the cluster containing the old deleted file.
- However, under certain circumstances it is still possible to recover some of the old file, even if a new file has been saved to the same cluster, because of the slack space.
- Consider the simplified situation where a cluster contained an important document, 30k in length. The file is removed from the index in the FAT but the document remains in the cluster. A new document is then saved to the same cluster, however the new document is only 20k in length. The last 10k of the original document will still be present in the slack space at the end of the cluster and can be retrieved.

“Easy” to Recover

- *Formatting*
  The process of formatting using the Format command in Windows or DOS performs a **high level format.** This is non-destructive to data on the disk. The process simply resets the index in the File Allocation Table so that operating system sees the disk as empty. The information is still there, only the operating system does not know how to get to it. Data on a disk which has been high level formatted can usually be recovered.
- *Defragmentation*
  When the operating system stores files on the hard disk, it splits them up into clusters. If the file is larger than the cluster size, several clusters will be used. These clusters are not necessarily adjacent to each other, but may be spread across the surface of the hard disk, depending on space available.
  - The process of defragging simply identifies clusters that contain parts of the same file, and moves them together so that they make, as far as possible, a contiguous block. In this process the system will use space allocated as free in the File Allocation Table, it is therefore possible that data being moved will overwrite space occupied by a deleted file, however this is by no means guaranteed.

Slack Space

- Assuming a file was stored contiguously (not fragmented)…

Habib,

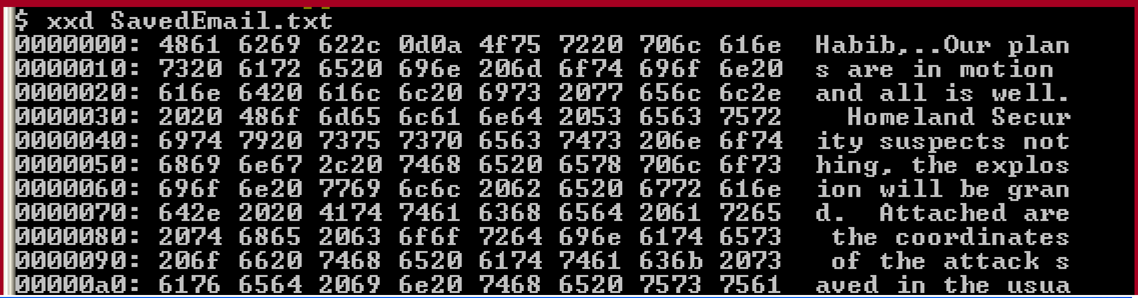
Our plans are in motion and all is well. Homeland Security suspects nothing, the explosion will be grand. Attached are the coordinates of the attack saved in the usual way.

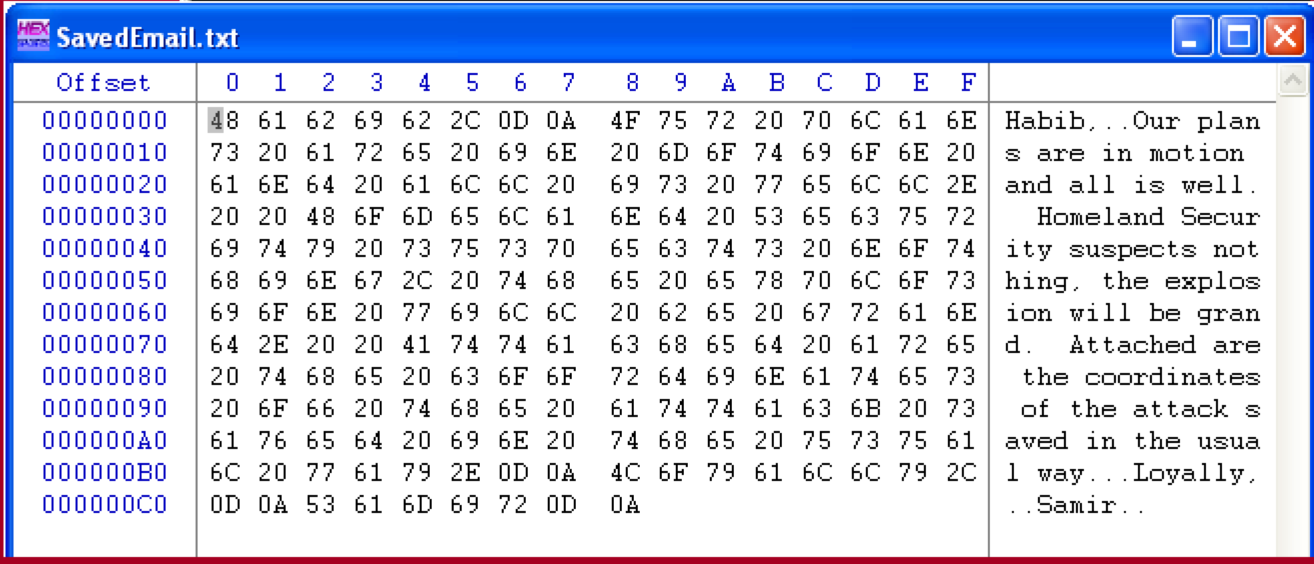
Loyally,

Samir

Slack Space

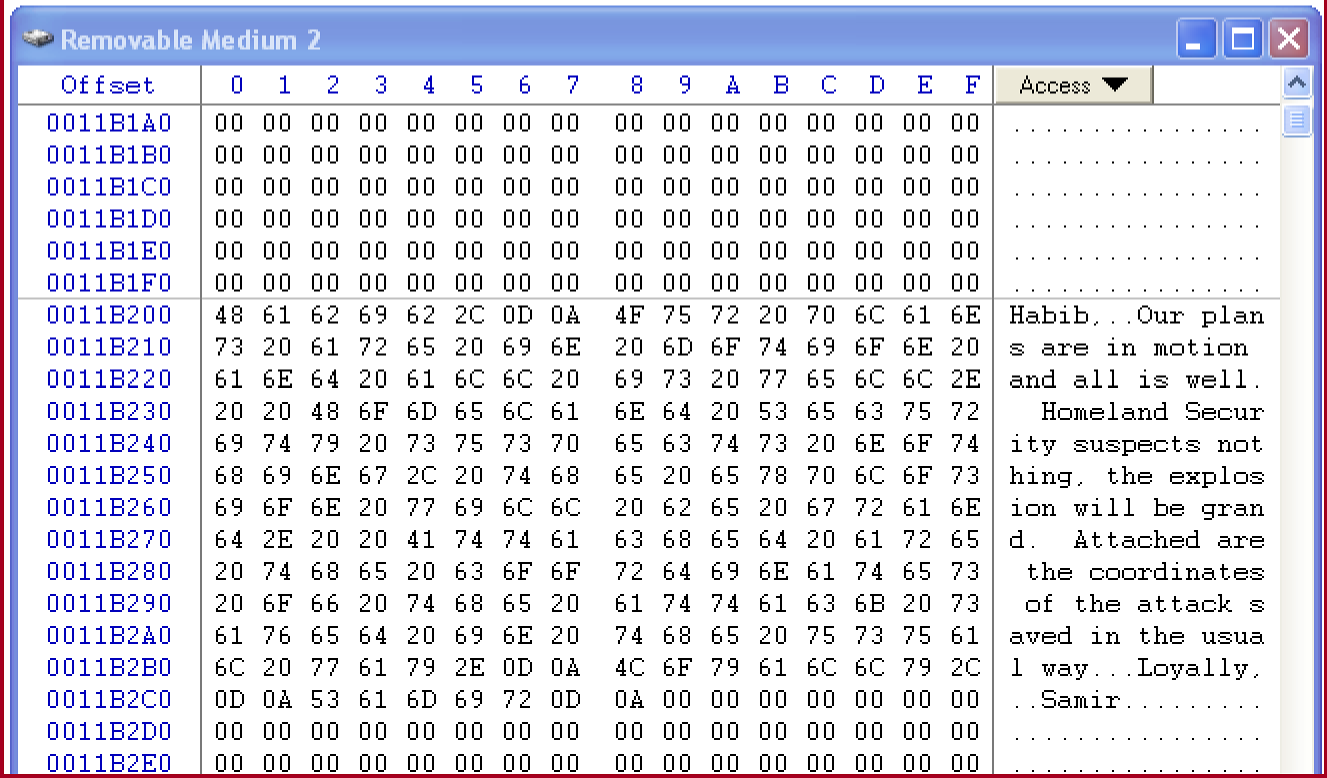
- Using tools like xxd or winhex we can see how the file is stored in hex:





Slack Space

- How is this different?


Removable Medium 2

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Access
0011B1A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0011B1B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0011B1C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0011B1D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0011B1E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0011B1F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0011B200	48	61	62	69	62	2C	0D	0A	4F	75	72	20	70	6C	61	6E	Habib,..Our plan
0011B210	73	20	61	72	65	20	69	6E	20	6D	6F	74	69	6F	6E	20	s are in motion
0011B220	61	6E	64	20	61	6C	6C	20	69	73	20	77	65	6C	6C	2E	and all is well.
0011B230	20	20	48	6F	6D	65	6C	61	6E	64	20	53	65	63	75	72	Homeland Secur
0011B240	69	74	79	20	73	75	73	70	65	63	74	73	20	6E	6F	74	ity suspects not
0011B250	68	69	6E	67	2C	20	74	68	65	20	65	78	70	6C	6F	73	hing, the explos
0011B260	69	6F	6E	20	77	69	6C	6C	20	62	65	20	67	72	61	6E	ion will be gran
0011B270	64	2E	20	20	41	74	74	61	63	68	65	64	20	61	72	65	d. Attached are
0011B280	20	74	68	65	20	63	6F	6F	72	64	69	6E	61	74	65	73	the coordinates
0011B290	20	6F	66	20	74	68	65	20	61	74	74	61	63	6B	20	73	of the attack s
0011B2A0	61	76	65	64	20	69	6E	20	74	68	65	20	75	73	75	61	aved in the usua
0011B2B0	6C	20	77	61	79	2E	0D	0A	4C	6F	79	61	6C	6C	79	2C	l way...Loyally,
0011B2C0	0D	0A	53	61	6D	69	72	0D	0A	00	00	00	00	00	00	00	..Samir.........
0011B2D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0011B2E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....

Resources

- http://www.wiebetech.com/
- http://odessa.sourceforge.net/
- http://sourceforge.net/projects/dcfld
- http://www.sf-soft.de/winhex/index-
- http://www.law.cornell.edu/rules/fre/

CERTConf2005
File Systems

Interface

- IDE / ATA
- SCSI (scuzzy)
- Serial ATA

Various limitations (usually addressing) create limits on hard drive sizes. Commonly 2.1, 8.4, 32 and 137 GB.

The $#%* cable

- ATA 33 and lower can use a 40 pin ribbon cable
- _Anything_ higher requires an 80 pin to reduce crosstalk between the wires
- The ribbon cables are sometimes color coded.
- Typically the “Master Drive” is on one end, and the “Slave Drive” is in the middle.

Bridging

- Similar to a networking bridge, you can circumvent interface standards using ATA bridges. Something like a Firewire – ATA bridge.
- This has a couple benefits from a forensic point of view:
  - External, swappable
  - Write blocking in hardware
  - Ability to use the same interface every time

SCSI

- Still mainly found in servers as opposed to desktops
- Physically the hardware is very similar – usually the controller is the difference
- Raid is almost always used

SCSI

- SCSI's main advantage is on the bus:
  - Each ATA device controls the entire bus for actions (write / read / etc)
  - SCSI devices can share, queue, etc
- SCSI devices are IDed 0-7 or 0-14 and can all be chained together on a single controller (but must be terminated on the ends)

SCSI

- While ATA took a sequential approach to versions (1,2,3,4,5) scsi created many variations: LVD, LVD/SE, DIFF, Ultra, Ultrawide, Ultra4 (also Ultra320), etc.
- You must have matching controllers and devices as well as the correct cable for each.

The OSI of File Systems

Application Storage
Classification
Space Management
Allocation Units
Data Classification
Physical

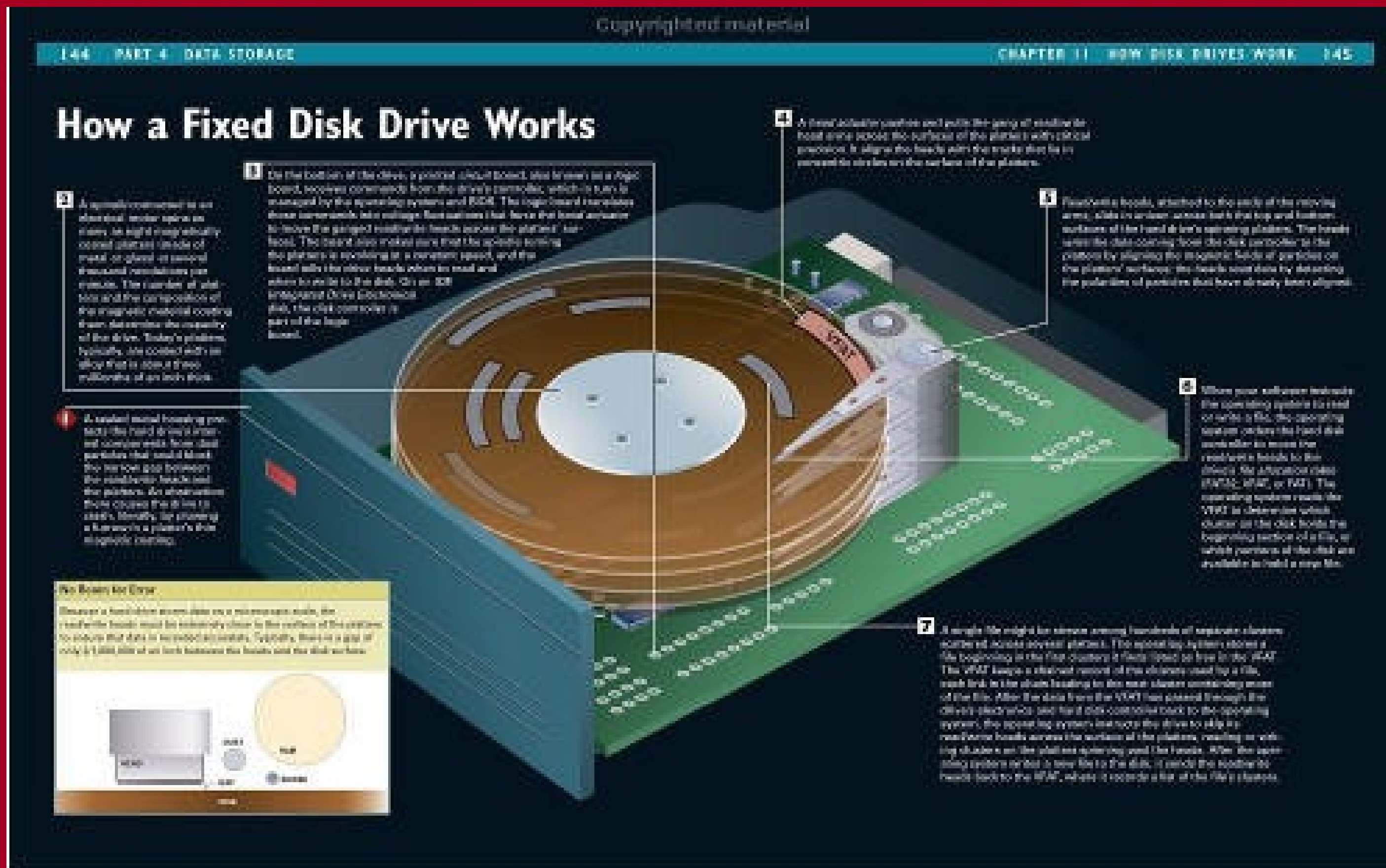
The OSI of File Systems

FAT / NTFS	EXT2
Files	Files
Folders	Directories
FAT (MFT)	Inodes
Clusters	Blocks
Partitions	Partitions
Sectors	Sectors

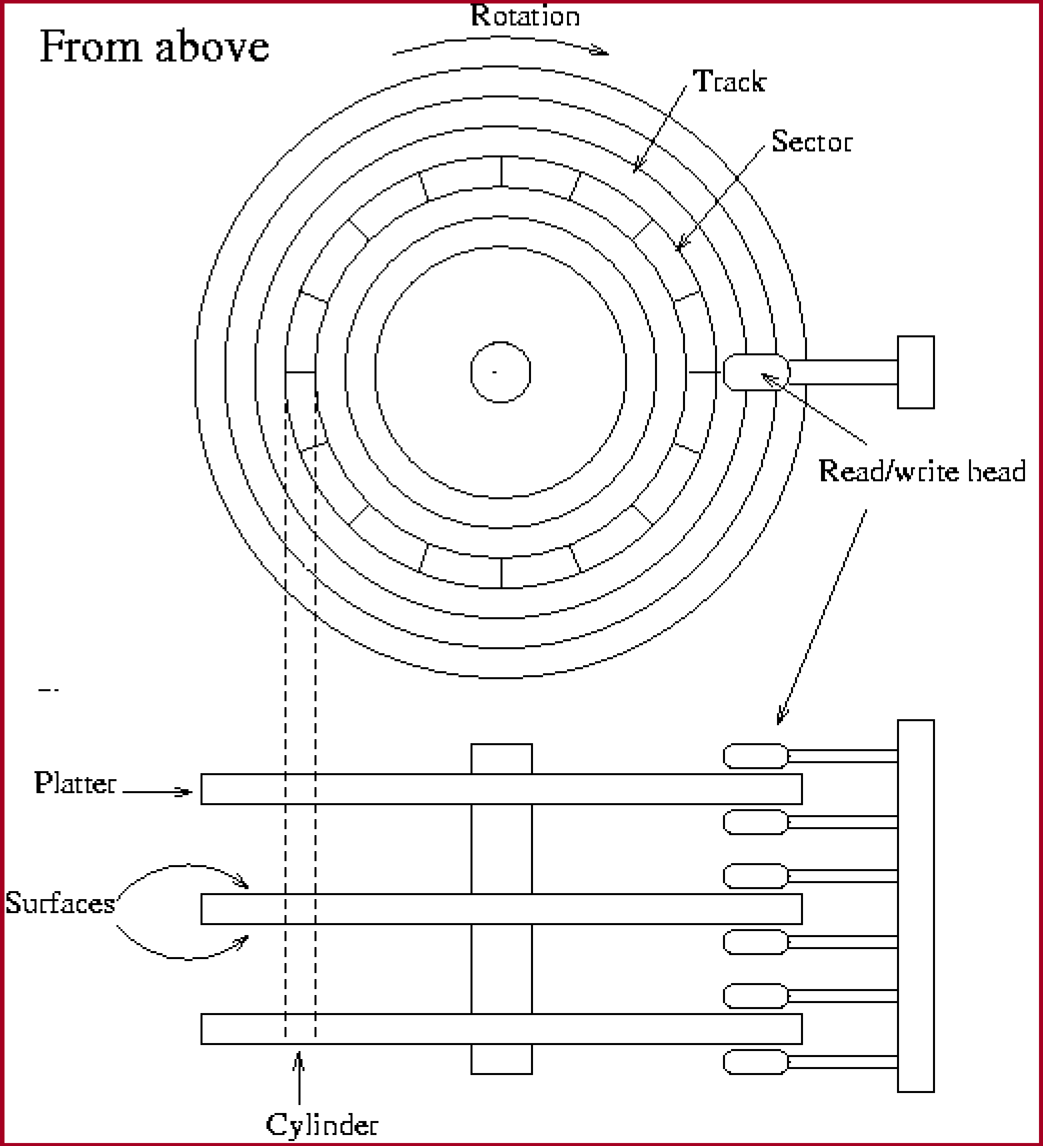
FS Layers : Physical

- No matter what, this layer is always present. The bits have to actually be located somewhere.
- Absolute sectors are numbered 0 and up.
- Most OS's read and write in chunks of 512 bytes.
- Some hardware actually allow access via Cylinder, head and sector values

FS Layers: Physical



FS Layers: Physical



FS Layers: Data Classification

- Just above the physical layer
- Partitioning scheme set up by the OS
- Basically allows for segmentation of data
  - Security
  - Logical organization
  - Speed
  - Means to an end

FS Layers: Data Classification

- Host Protected Access
- Usually used by vendors as part of a restoration process
- Not accessable by the OS
  - Or by earlier versions of encase/safeback/etc

FS Layers: Data Classification

- One byte FS identifier code – used for mounting. Some OSes allow this to be specified.

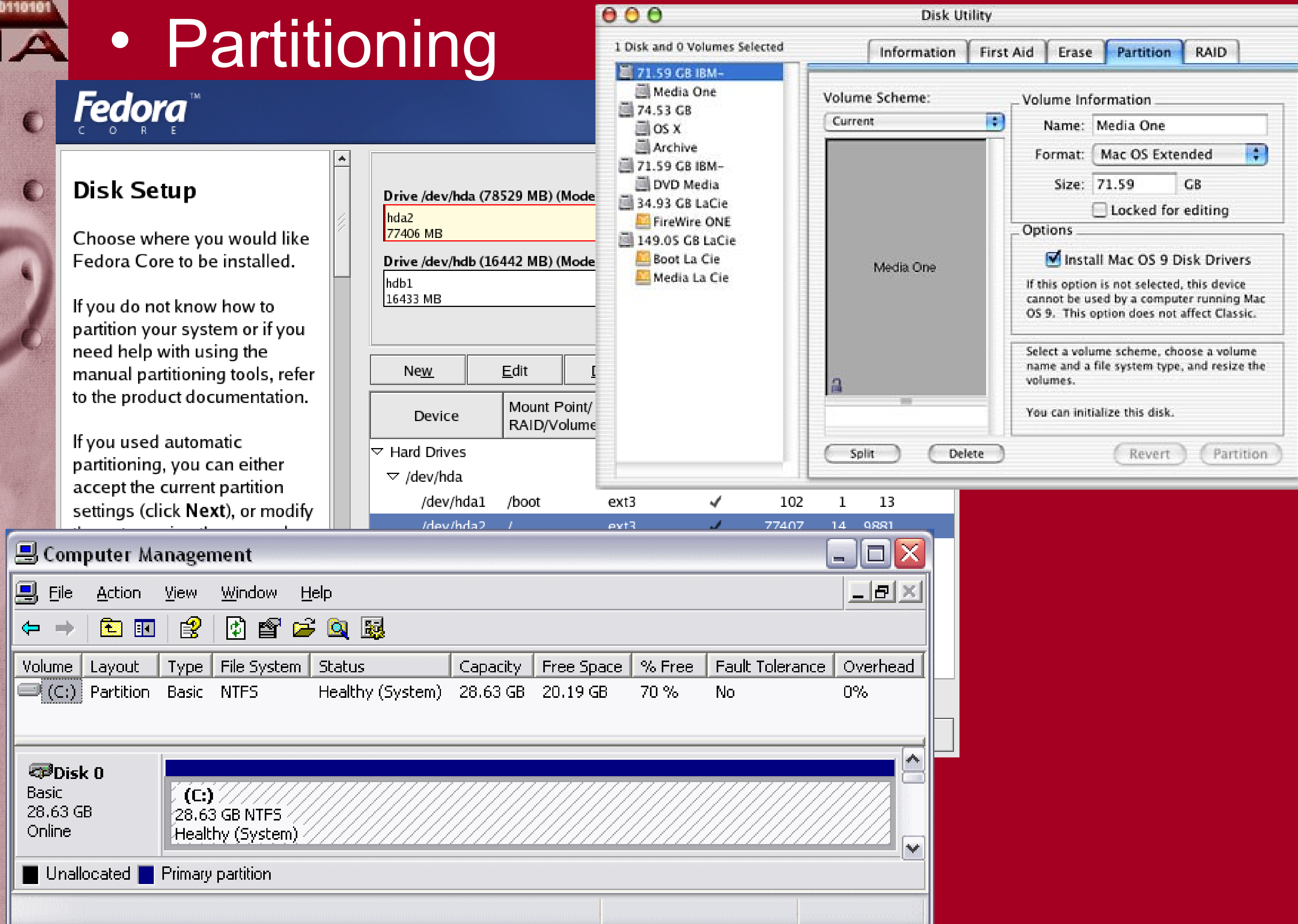
00 Empty
01 DOS 12-bit FAT
02 XENIX root
03 XENIX /usr .
04 DOS 3.0+ 16-bit FAT (up to 32M)
05 DOS 3.3+ Extended Partition
06 DOS 3.31+ 16-bit FAT (over 32M)
07 OS/2 IFS (e.g., HPFS)
07 Windows NT NTFS
07 Advanced Unix
07 QNX2.x pre-1988
08 OS/2 (v1.0-1.3 only)
08 AIX boot partition
08 SplitDrive
08 Commodore DOS
08 DELL partition spanning multiple drives
08 QNX 1.x and 2.x ("qny")
09 AIX data partition
09 Coherent filesystem
09 QNX 1.x and 2.x ("qnz")
0a OS/2 Boot Manager
0a Coherent swap partition
0a OPUS
0b WIN95 OSR2 FAT32
0c WIN95 OSR2 FAT32, LBA-mapped
0e WIN95: DOS 16-bit FAT, LBA-mapped
0f WIN95: Extended partition, LBA-mapped
10 OPUS (?)
11 Hidden DOS 12-bit FAT
11 Leading Edge DOS 3.x
12 Configuration/diagnostics partition
14 Hidden DOS 16-bit FAT <32M
14 AST DOS with
16 Hidden DOS 16-bit FAT >=32M
17 Hidden IFS (e.g., HPFS)
18 AST SmartSleep Partition
19 Unused
1b Hidden WIN95 OSR2 FAT32
1c Hidden WIN95 OSR2 FAT32, LBA-mapped
1e Hidden WIN95 16-bit FAT, LBA-mapped
20 Unused
21 Reserved
21 Unused
22 Unused
23 Reserved
24 NEC DOS 3.x
26 Reserved
31 Reserved
32 NOS
33 Reserved
34 Reserved
35 JFS on OS/2 or eCS
36 Reserved
38 THEOS ver 3.2 2gb partition
39 Plan 9 partition
39 THEOS ver 4 spanned partition
3a THEOS ver 4 4gb partition
3b THEOS ver 4 extended partition
3c PartitionMagic recovery partition
3d Hidden NetWare
40 Venix 80286
41 Linux/MINIX (sharing disk with DRDOS)
41 Personal RISC Boot
41 PPC PReP (Power PC Reference Platform) Boot
42 Linux swap (sharing disk with DRDOS)
42 SFS (Secure Filesystem)
42 Windows 2000 dynamic extended partition marker
43 Linux native (sharing disk with DRDOS)
44 GoBack partition
45 Boot-US boot manager
45 Priam
5c Priam EDisk
61 SpeedStor
63 Unix System V (SCO, ISC Unix, UnixWare, ...), Mach, GNU Hu
64 PC-ARMOUR protected partition
64 Novell Netware 286, 2.xx
65 Novell Netware 386, 3.xx or 4.xx
66 Novell Netware SMS Partition
82 Solaris x86
82 Linux swap
83 Linux native partition
84 OS/2 hidden C: drive
84 Hibernation partition
85 Linux extended partition
86 Old Linux RAID partition superblock
86 NTFS volume set
87 NTFS volume set
8a Linux Kernel Partition (used by AiR-BOOT)
8b Legacy Fault Tolerant FAT32 volume
8c Legacy Fault Tolerant FAT32 volume using BIOS extd INT 13h
8d Free FDISK hidden Primary DOS FAT12 partitition
8e Linux Logical Volume Manager partition
90 Free FDISK hidden Primary DOS FAT16 partitition
91 Free FDISK hidden DOS extended partitition
92 Free FDISK hidden Primary DOS large FAT16 partitition
93 Hidden Linux native partition
a0 Laptop hibernation partition
a1 Laptop hibernation partition
a1 HP Volume Expansion (SpeedStor variant)
a5 BSD/386, 386BSD, NetBSD, FreeBSD
a6 OpenBSD
a9 NetBSD
ab Mac OS-X Boot partition
c2 Hidden Linux
c3 Hidden Linux swap

FS Layers: Data Classification

- Most mainstream OS's have partitioning software built in (most even graphical)
- 3rd party vendors sell things like partition magic

FS Layers: Data Classification

- Partitioning



FS Layers: Allocation

- Allocations units (blocks) depend on:
  - FS Type
  - Partition Size
  - System Admin
- Particular applications can perform better or worse depending on the size of an allocation unit
- Things like databases, and video have known performance relations with block size.

FS Layers: Allocation

Hard Disk Size	FAT12	FAT16	FAT32	NTFS	Ext2
0 to 16MB	4,096 bytes	2,048 bytes	512 bytes	512 bytes	4,096 bytes
16 to 128MB	n/a	2,048 bytes	512 bytes	512 bytes	4,096 bytes
128 to 256MB	n/a	4,096 bytes	512 bytes	512 bytes	4,096 bytes
256 to 512MB	n/a	8,192 bytes	4,096 bytes	512 bytes	4,096 bytes
512 to 1,024MB	n/a	16,384 bytes	4,096 bytes	1,024 bytes	4,096 bytes
1,024 to 2,048MB	n/a	32,768 bytes	4,096 bytes	4,096 bytes	4,096 bytes
2,048 to 6,128MB	n/a	n/a	4,096 bytes	4,096 bytes	4,096 bytes

- Why are there N/A's?

FS Layers: Management

- Space Management
  - This layer logically keeps track of all the blocks from the Allocation layer below.
- FAT (file allocation table) uses…a table …to track all the allocation units….in the file system…

FS Layers: Management

- Files that are larger than a single allocation unit span multiple units
- The FAT table has an entry for each block possible values are
  - Address for next block of the file (contiguous or not)
  - EOF
  - Bad Block

The inode

- The Ext2 file system until recently could easily be argued to be the most used FS in linux. Now more an more FS's are being used, (Ext3, XFS, Reiserfs….)

The inode

- Inodes contain meta-data for files
- One piece of data is a link-count
  - Every link to the file ups the count
  - Every deletion of a link to the file decrements
  - If the count is 0 – the file is ‘deleted’

The inode

- The Inode contians:
  - Mode of the file (everything is a file)
  - Link-count
  - UID
  - GID
  - Size
  - Access time
  - Mod time
  - Address for the file (data portion)
  - Number of blocks
  - version

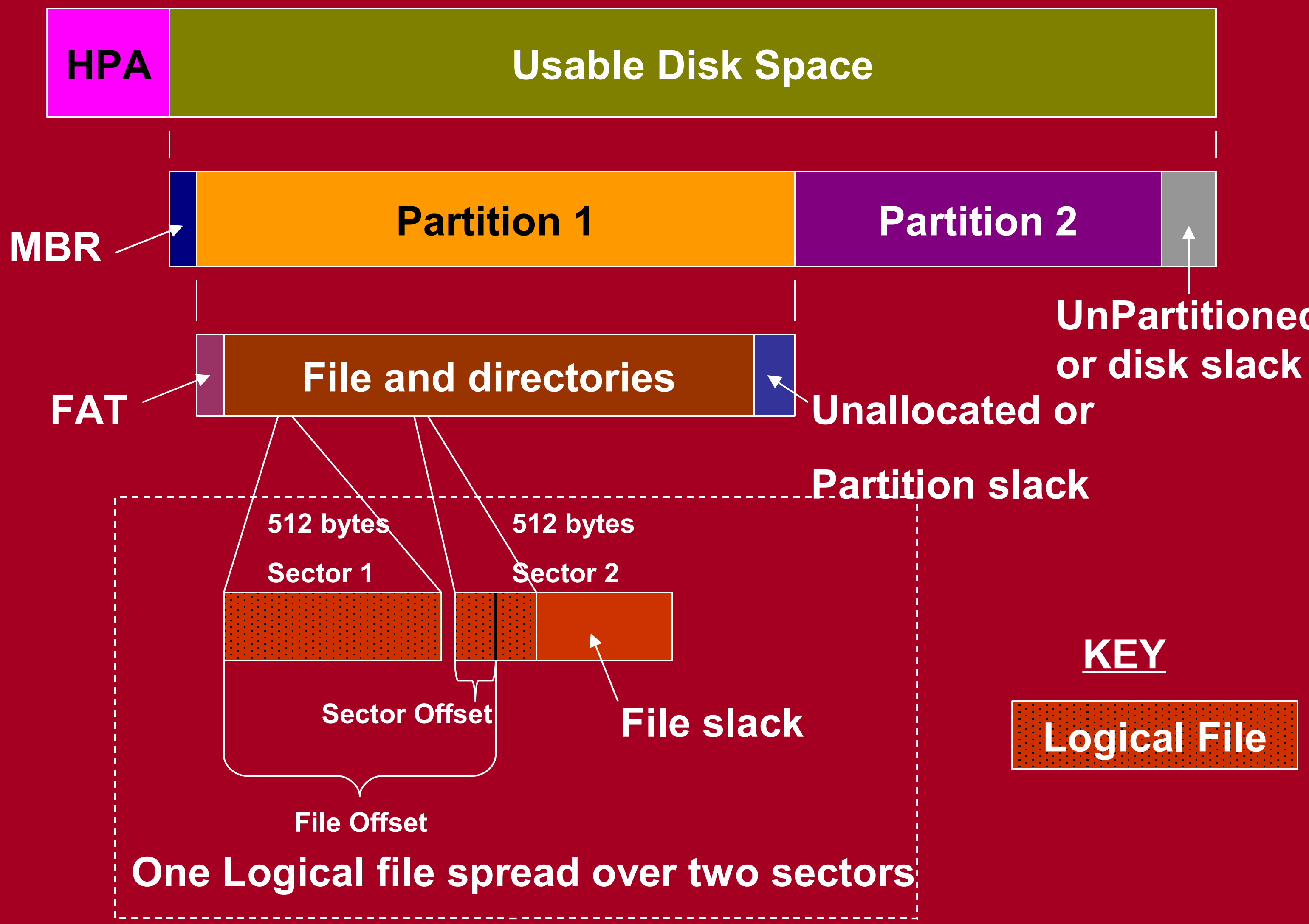
Inode

- Unlike FAT, the inode keeps pointers to the blocks that contain the information for the file.
  - Up to three (or so) levels of pointers:
    - Direct (original 13 pointers)
    - Indirect (first ptr layer – 128 more ea)
    - Double indirect (128 more ea)
    - Triple indirect (128 more ea)

FS Layers: Directories / files

- Logically used by users to segment data.
- Some systems have very little to distinguish between a file and a directory
- Most files will have metadata about the file itself – much like a header in network data structures or email

Graphically…



Partition finding

- Look for strings like MSWIN4.1 or NTFS to locate the beginning of FAT/NTFS partitions (existing or deleted)

Logical file systems

- Windows
  - A:
  - C:
    - Docs n set..
    - Windows
      - Sys32
        - drivers
      - sys
  - D:
  - E:

- Linux
  - /
    - Bin
    - Etc
      - fstab
    - Dev
      - sda1
    - Boot
    - Home
    - Initrd
    - Mnt
      - Floppy
      - usb
    - Usr
    - var

Drives

- Drives are files too
  - /dev/hda   /dev/hdb
- Partitions are part of drives
  - /dev/hda1   /dev/hda2
- SCSI (and firewire, and usb …)
  - /dev/sda

Linux Topics

ls –al

Sticky bit

Set uid

Set gid

Permission bits

mke2fs

e2fsck

badblocks

mount

CERTConf2005

Tracking Email

Email

- Just like anything else we've talked about in this class, email is just a series of bits
- These bits happen to be designed to route from one computer on a network to another
- Just a file exchange

Email

- There are a variety of protocols associated with email…
  - Smtp
  - Pop3
  - Imap
- SMTP, simple mail transfer protocol, handles most of the email exchange today

Email – Postal Example

- Lets consider a 'physical world' example – the US Postal System
- Peter Parker writes a letter the Aunt May.
- He folds the letter and packages it in an envelope.
- On the envelope he writes information the postal system needs:
  - To: name, street address, zip code etc
  - From: Name, street, zip
  - And of course postage
  - Once at the post office the postage is inked to prevent re-use – this stamp contains more information about the accepting posting office and possibly unique codes for the letter

Email – Postal Example

- So then depending on the destination the letter takes different paths… for example:
  - Peter's Mailbox, Peter's Mail Carrier, Local Post Office, Truck, Regional Post office, Plane, Regional Post office, truck, Local Post Office, Aunt May's Mail Carrier, Aunt May's Mailbox
  - Local mail may only read the local post office, then be sent out for delivery

Email

- In the digital world, transmission happens very similarly
- “Local mail” will never leave your network and may go directly between two computers
- “Internet mail” (typical mail) will touch at least 4 computers:
  - Senders computer, senders mail server, receivers mail server, receiver's computer

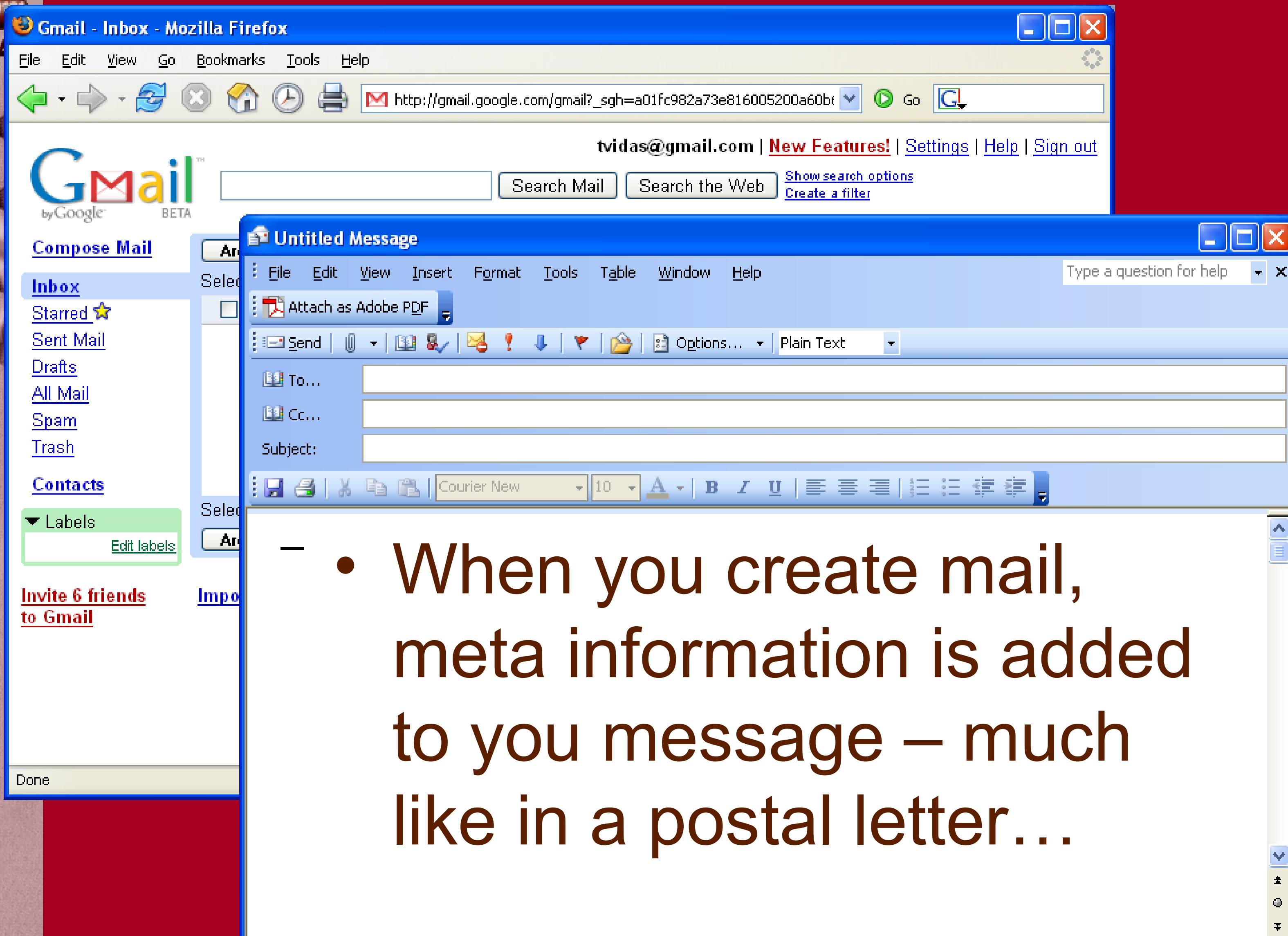
Email

- At each location the email is cached in it’s entirety and forwarded on to another server
- ISP’s and corporations tend to do ‘funny’ things with email and typically your email will travel through more than 4 computers
  – Spam, virus, proxy

Email

- So, Aunt May sends Peter a response via email…
- She has a internet access at home and uses Outlook, but to thwart spam her ISP does not allow any traffic on port 25 (smtp) so she can't use her email providers smtp server
- Peter is at work and also uses outlook, but his is tied to an exchange server
- So the path of the email will likely be:
  - May's computer, May's ISP's smtp server, Peter's companies antivirus/spam filter,

Email



– • When you create mail, meta information is added to you message – much like in a postal letter…

Email – 1 - creation

- When Aunt May creates the email, some initial header information is added:

  From: “May Parker" <mparker@someISP.com>
  To: <pparker@someCompany.com>
  Subject: Dinner on Thursday
  Date: Sat, 20 Nov 2003 18:52:59 -0600
  X-Mailer: Microsoft Office Outlook, Build 11.0.5510

- This is interesting to note, but not very trustworthy – this information is fairly straightforward for anyone to forge
- For example the “from” is whatever you type in when you create an email account, or install outlook…

Email – 2 – ISP mailserver

- Once the mail reaches the first mailserver, a “received” header is added, notice that generally, most recent headers are at the top

Received: from 68.225.185.16 by Mailserver1.someISP.com (InterMail vM.6.01.04.00) with ESMTP id <20041123025259.ORWK14730. Mailserver1.someISP.com@ 68.225.185.16 > for <pparker@someCompany.com>; Sat, 20 Nov 2003 19:52:59 -0500
From: “May Parker" <mparker@someISP.com>
To: <pparker@someCompany.com>
Subject: Dinner on Thursday
Date: Sat, 20 Nov 2003 18:52:59 -0600
Message-ID: <UEAALKJGJKd33AA@someISP.com>
X-Mailer: Microsoft Office Outlook, Build 11.0.5510

Email - 3 - Company mailsvr

- Once the mail reaches the last mailserver, a final “received” header is added – after this, the email is read

Received: from Mailserver1.someISP.com (Mailserver1.someISP.com [67.234.241.34]) by mx.somecompany.com with ESMTP id 61si133770rr for pparker@somecompany.com; Sat, 20 Nov 2003 16:53:01 -0800 (PST

Received: from 68.225.185.16 by Mailserver1.someISP.com (InterMail vM.6.01.04.00) with ESMTP id <20041123025259.ORWK14730. Mailserver1.someISP.com@ 68.225.185.16 > for <pparker@someCompany.com>; Sat, 20 Nov 2003 19:52:59 -0500
From: “May Parker" <mparker@someISP.com>
To: <pparker@someCompany.com>
Subject: Dinner on Thursday
Date: Sat, 20 Nov 2003 18:52:59 -0600
Message-ID: <UEAALKJGJKd33AA@someISP.com>
X-Mailer: Microsoft Office Outlook, Build 11.0.5510

Email - headers

Received: from Mailserver1.someISP.com (Mailserver1.someISP.com [67.234.241.34]) by mx.somecompany.com with ESMTP id 61si133770rnb for pparker@somecompany.com; Sat, 20 Nov 2003 16:53:01 -0800 (PST)
Received: from 68.225.185.16 by Mailserver1.someISP.com (InterMail vM.6.01.04.00) with ESMTP id <20041123025259.ORWK14730. Mailserver1.someISP.com@ 68.225.185.16 > for <pparker@someCompany.com>; Sat, 20 Nov 2003 19:52:59 -0500
From: “May Parker" <mparker@someISP.com>
To: <pparker@someCompany.com>
Subject: Dinner on Thursday
Date: Sat, 20 Nov 2003 18:52:59 -0600
Message-ID: <UEAALKJGJKd33AA@someISP.com>
X-Mailer: Microsoft Office Outlook, Build 11.0.5510

The second-to-last machine communicating with the final destination. The name the server gives, and the IP (so can verify that the IP matches the DNS name)

The receiving server often includes things like version numbers here also

The ESMTP id – which is just an internal number for the server to keep track of that message – but this can be useful if you need to ask (subpeona) the administrator for help

The address for deliver (this is different that the original “To:”)

And the delivery timestamp

Email - headers

Received: from Mailserver1.someISP.com (Mailserver1.someISP.com [67.234.241.34]) by mx.somecompany.com with ESMTP id 61si133770rnb for pparker@somecompany.com; Sat, 20 Nov 2003 16:53:01 -0800 (PST)
Received: from 68.225.185.16 by Mailserver1.someISP.com (InterMail vM.6.01.04.00) with ESMTP id <20041123025259.ORWK14730. Mailserver1.someISP.com@ 68.225.185.16 > for <pparker@someCompany.com>; Sat, 20 Nov 2003 19:52:59 -0500
From: “May Parker" <mparker@someISP.com>
To: <pparker@someCompany.com>
Subject: Dinner on Thursday
Date: Sat, 20 Nov 2003 18:52:59 -0600
Message-ID: <UEAALKJGJKd33AA@someISP.com>
X-Mailer: Microsoft Office Outlook, Build 11.0.5510

Note the difference in timestamps, this can reflect different timezones that servers are physically located in or just server configurations.

The –0X00 is hours behind Greenwich mean time…

So even though it at first glance appears the email was written at 6:52, then took an hour to reach May’s ISP at 7:52, then finally arrived to Peter about 2 hours before she wrote it(4:53) it really just took a few seconds to deliver

Email - headers

Received: from Mailserver1.someISP.com (Mailserver1.someISP.com [67.234.241.34]) by mx.somecompany.com with ESMTP id 61si133770rnb for pparker@somecompany.com; Sat, 20 Nov 2003 16:53:01 -0800 (PST)
Received: from 68.225.185.16 by Mailserver1.someISP.com (InterMail vM.6.01.04.00) with ESMTP id <20041123025259.ORWK14730. Mailserver1.someISP.com@ 68.225.185.16 > for <pparker@someCompany.com>; Sat, 20 Nov 2003 19:52:59 -0500
From: “May Parker" <mparker@someISP.com>
To: <pparker@someCompany.com>
Subject: Dinner on Thursday
Date: Sat, 20 Nov 2003 18:52:59 -0600
Message-ID: <UEAALKJGJKd33AA@someISP.com>
X-Mailer: Microsoft Office Outlook, Build 11.0.5510

X-Mailer: is added by the application used to create the email.

As mentioned before, all the initial headers should be considered less trustworthy

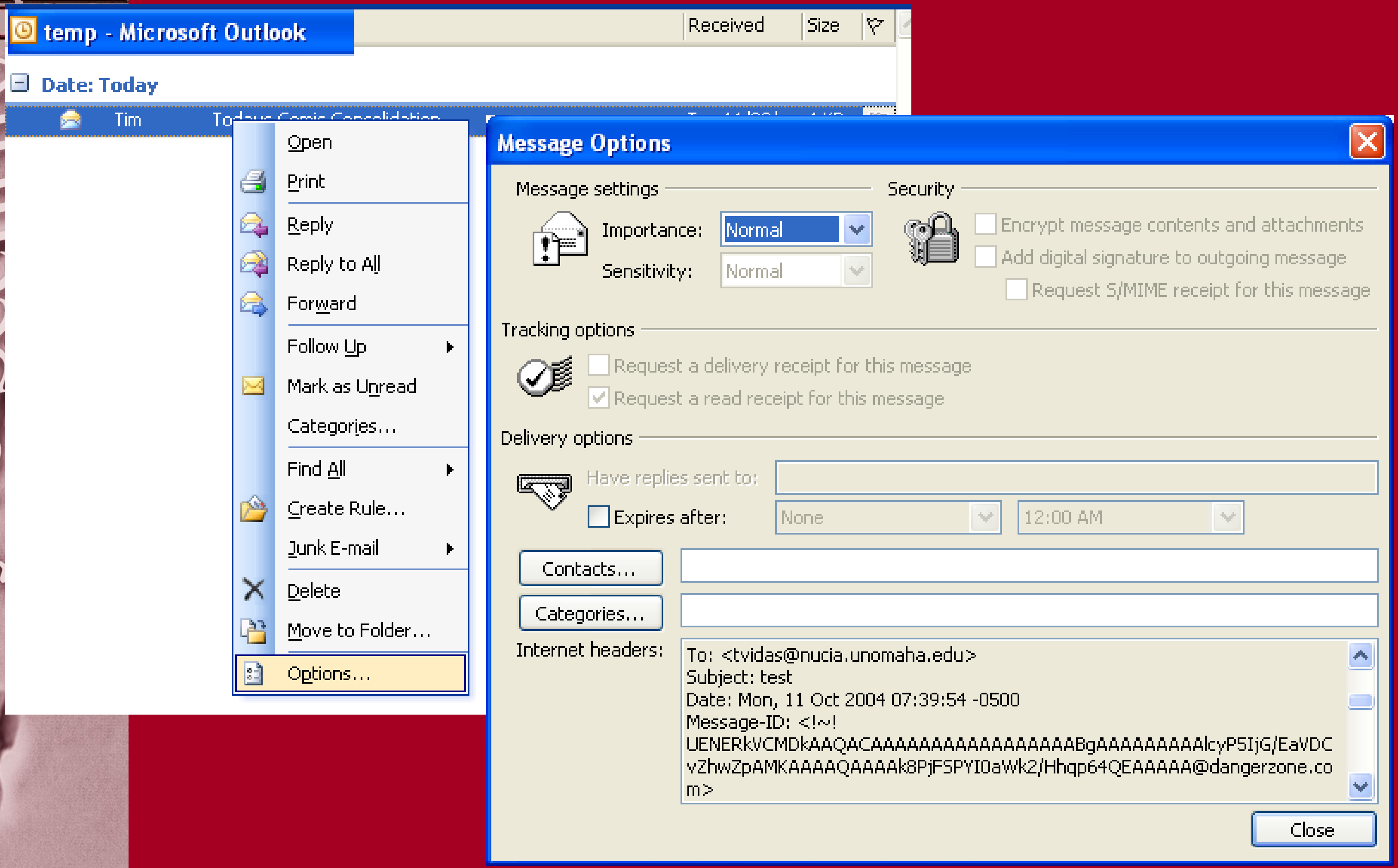
Additionally any header starting with “X-” are *optional* headers, and may or may not be present in any arbitrary email

The Message-ID is similar to the ESMTP id, except the Message-ID is a unique tag for the email, not a particular file on a server…so this ID exists on all instances of this message on all servers…

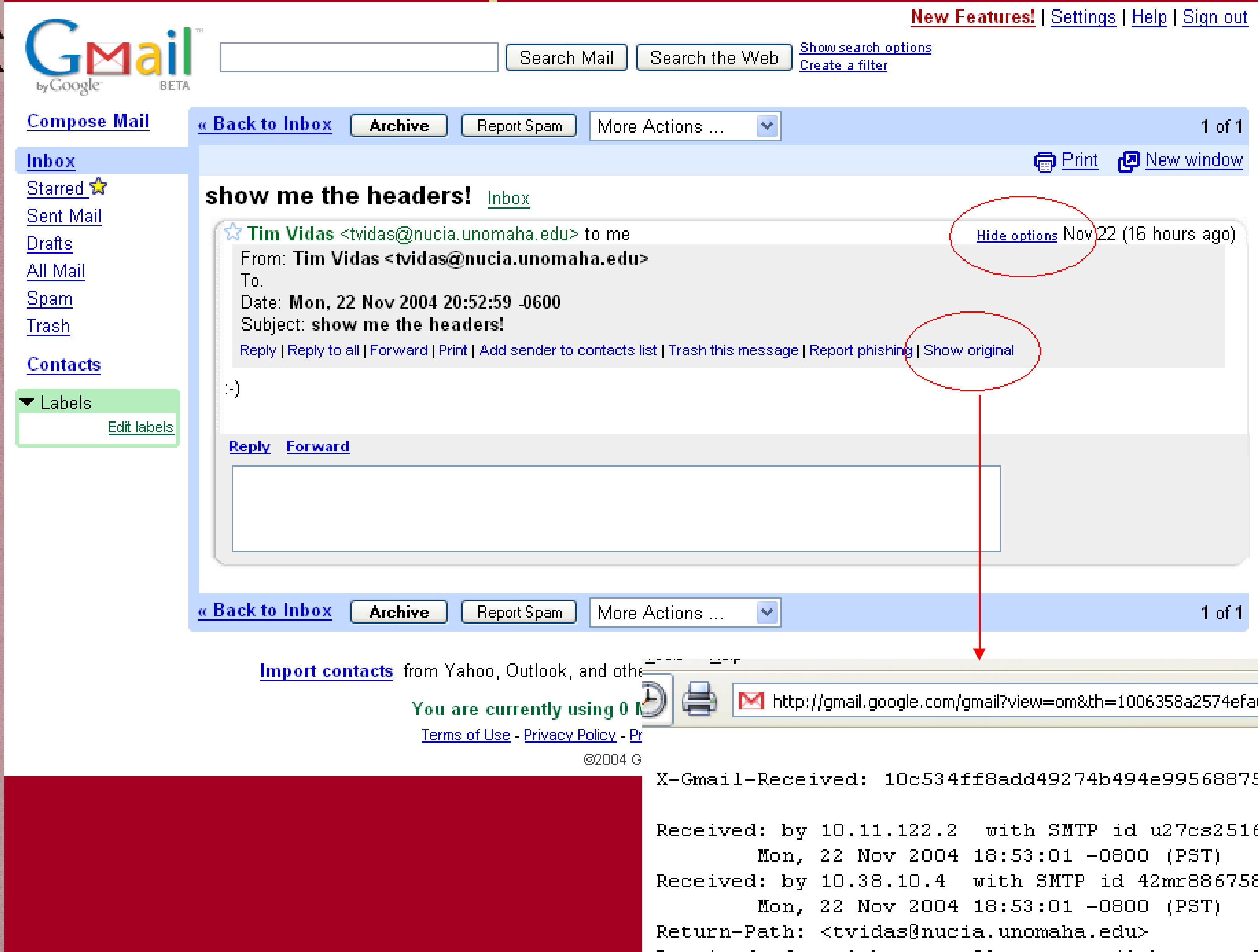
OK..so how do I do it?

- How to see the headers of your email varies based on the ‘client’ you use to view your email – often it’s an ‘advanced’ option or a field under ‘properties’
- If your ‘client’ is a web site, then you can only view headers if the site allows you to…

Examples - Outlook



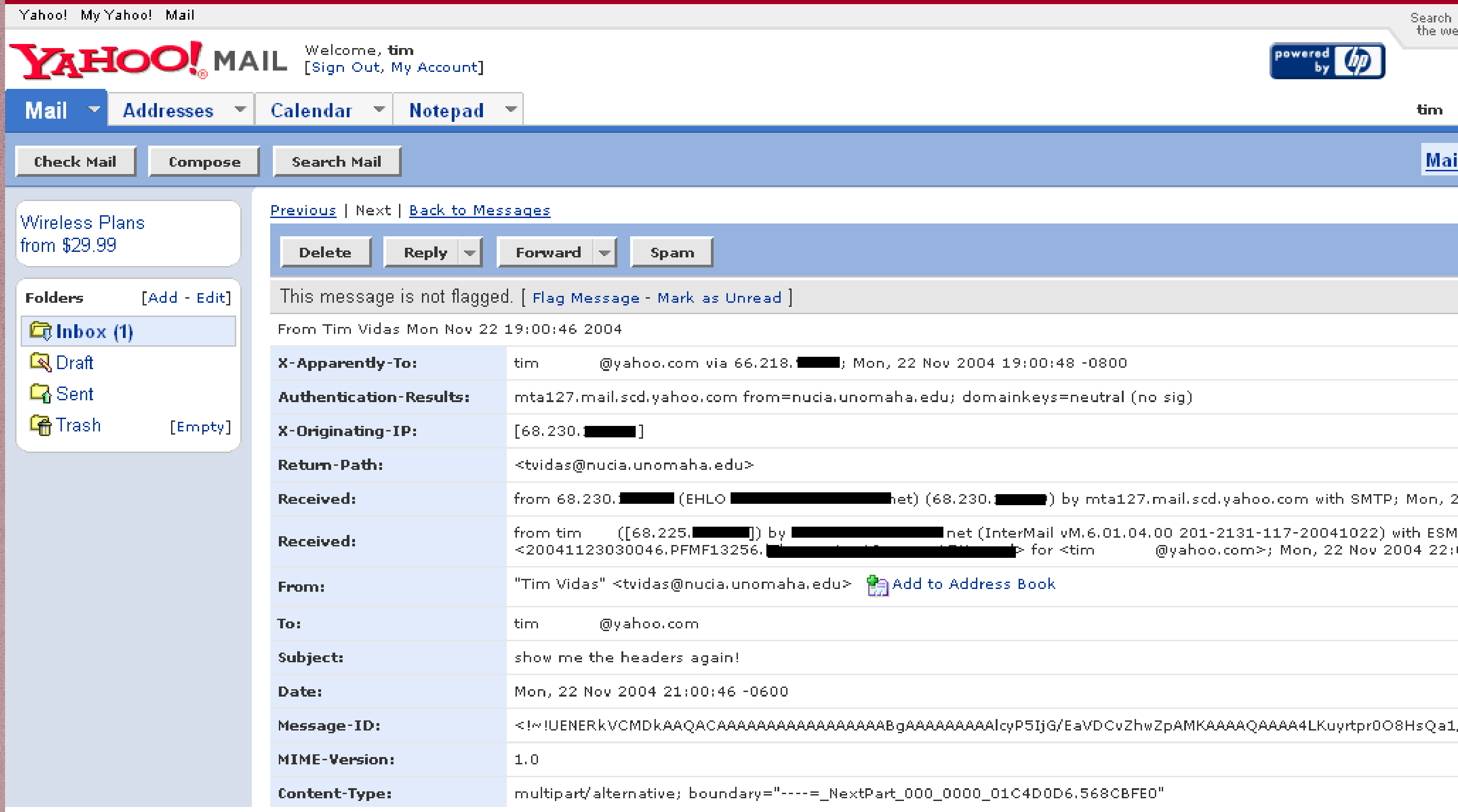
Examples - Gmail



NUCIA

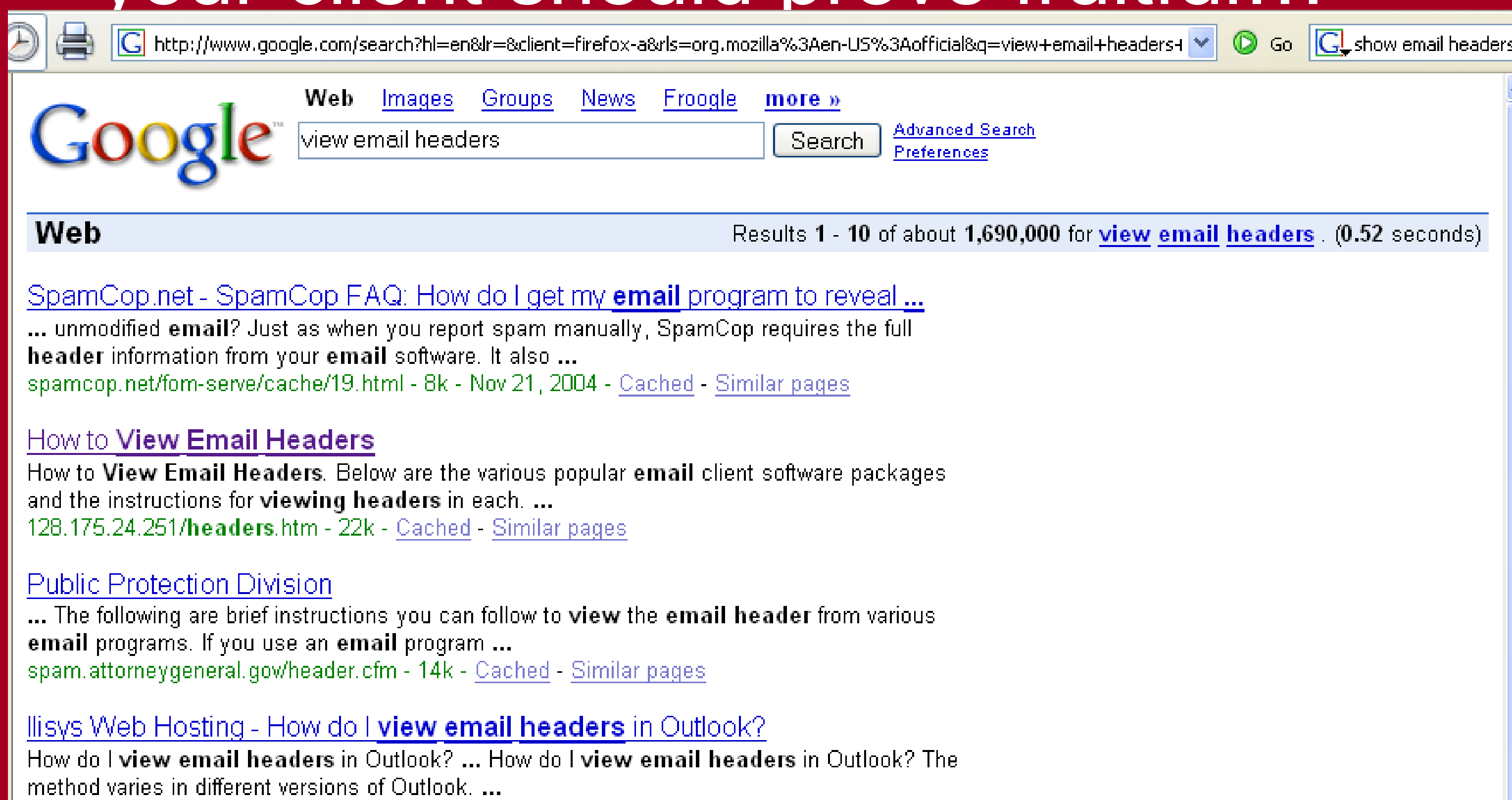
Your Key to Security

Examples - Yahoo



Examples - other

- Most clients are now able to display headers…a web search for your client should prove fruitful…



Other Popular Headers:

- **Apparently-To:** normally a sign of a mailing list (old style)
- **Bcc:** If you see this header on incoming mail, something is wrong. Why? Uhm, it's BLIND carbon copy…your emailer program should send out multiple emails to your bcc recipients..
- **Cc:** This header is sort of an extension of "To:"; it specifies additional recipients. Not much different between CC and To, mainly the difference is in your email program

Other Popular Headers:

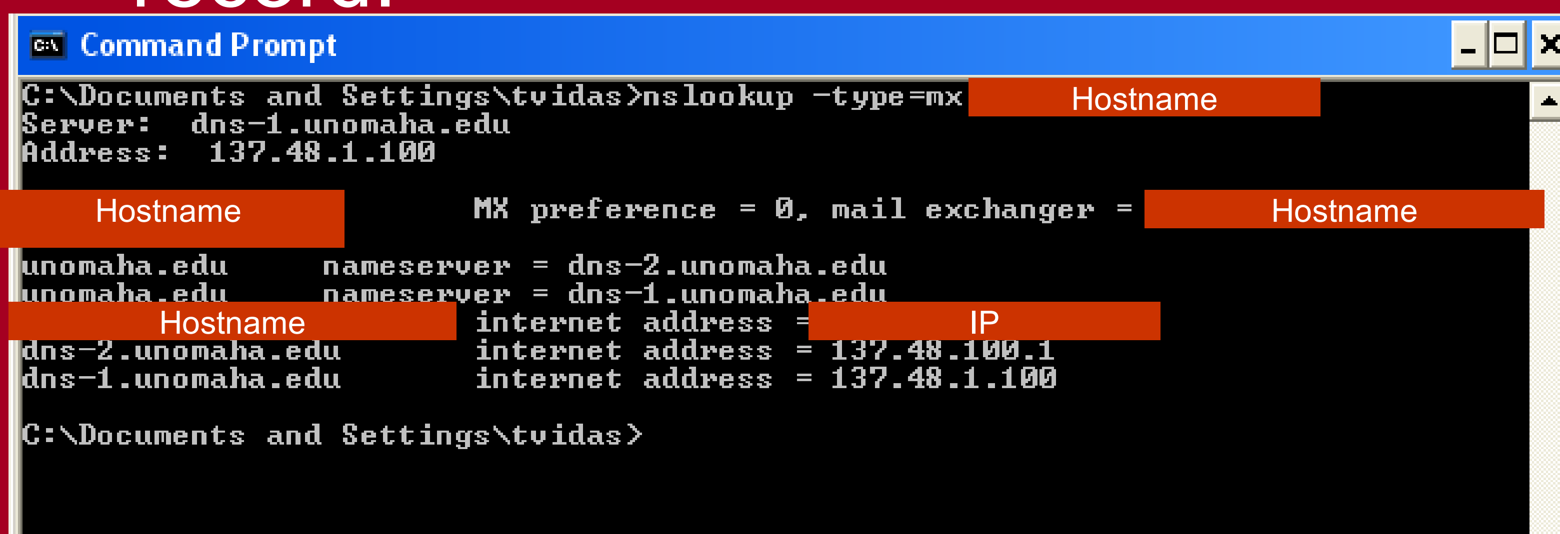
- **Content-Type:** tells MIME-compliant mail programs what type of content to expect in the message.
- **Priority:** assigns a priority to the mail. Most software ignores it. It is often used by spammers
- **Reply-To:** Specifies an address for replies to go to. Though this header has many legitimate uses (perhaps your use multiple addresses), it is also widely used by spammers.
- And many more….

SMTP – Example

- SMTP – what actually gets the message from one point to another
- The example on the next slide shows an actual connection made – some SMTP servers do ‘additional non-standard things’ like:
  - Verify that the sender’s domain exists
  - Or only allow SMTP to certain users/computers
  - Or any number of freaky things…

SMTP Example

- First you need to figure out 'where' the mail server is. You can use something like nslookup or a web based tool to find the DNS "mx" record:



SMTP Example

Command Prompt

```
C:\Documents and Settings\tvidas>telnet Hostname u 25_
```

Command Prompt

```
220 I Hostname Microsoft ESMTP MAIL Service, Version: 6.0.3790.211 r
eady at  Tue, 23 Nov 2004 13:45:11 -0600
HELO Hostname
250 Hostname Hello IP
MAIL FROM: tim@adsfasdf.com
250 2.1.0 tim@adsfasdf.com....Sender OK
RCPT TO: tvidas@nucia.unomaha.edu
250 2.1.5 tvidas@nucia.unomaha.edu
DATA
354 Start mail input; end with <CRLF>.<CRLF>
Received: from fake.computer.edu (fake.computer.edu [111.111.1.11]) by mail.othe
rfake.edu (8.8.5) id 0334A21; Tue, Mar 18 1997 14:36:17 -0800 (PST)
From: thisone@guy.edu (One Guy)
To: tvidas@nucia.unomaha.edu
Date: Tue, Mar 18 1997 14:36:14 PST
Message-Id: <rth031897143614-00000298@fake.computer.edu>
X-Mailer: Tim's fancy email editor
X-other-header:  Just added one for fun
Subject: SMTP TEST

This is an example of mail recieved via SMT

-t
.
250 2.6.0  <rth031897143614-00000298@fake.c
QUIT
500 5.3.3 Unrecognized command
QUIT
221 2.0.0 Hostname Service cl


Connection to host lost.

C:\Documents and Settings\tvidas>_
```

One Guy | SMTP TEST

SMTP TEST

One Guy [thisone@guy.edu]

To: Tim Vidas

```
This is an example of mail recieved via SMTP.

-t
```

Internet headers:

Received: from Hostname ([137.48.]) by Hostname with Microsoft SMTPSVC(6.0.3790.211);
Tue, 23 Nov 2004 13:35:20 -0600
Received: from fake.computer.edu (fake.computer.edu [111.111.1.11]) by mail.otherfake.edu (8.8.5) id 0334A21; Tue, Mar 18 1997 14:36:17 -0800 (PST)
From: thisone@guy.edu (One Guy)

Close

NUCIA

Your Key to Security

Significance

- The whole purpose is to attempt to trace an email back to the originator
- Obtaining the originators email address or better yet the IP address of the machine is the goal
- To do this you may need to search around with nslookup, whois, and similar tools.

Significance

- If your search ends with an ISP or you need information from “middle” ISPs you can order a freeze via 18 USC Sec. 2703 (f) – Requirement to Preserve Evidence.
- This works for 90 days
- However as far as the ISP is concerned, their hands are not tied
  - Terminate account b/c of publicity
  - Notify the user that the account is in question

problems

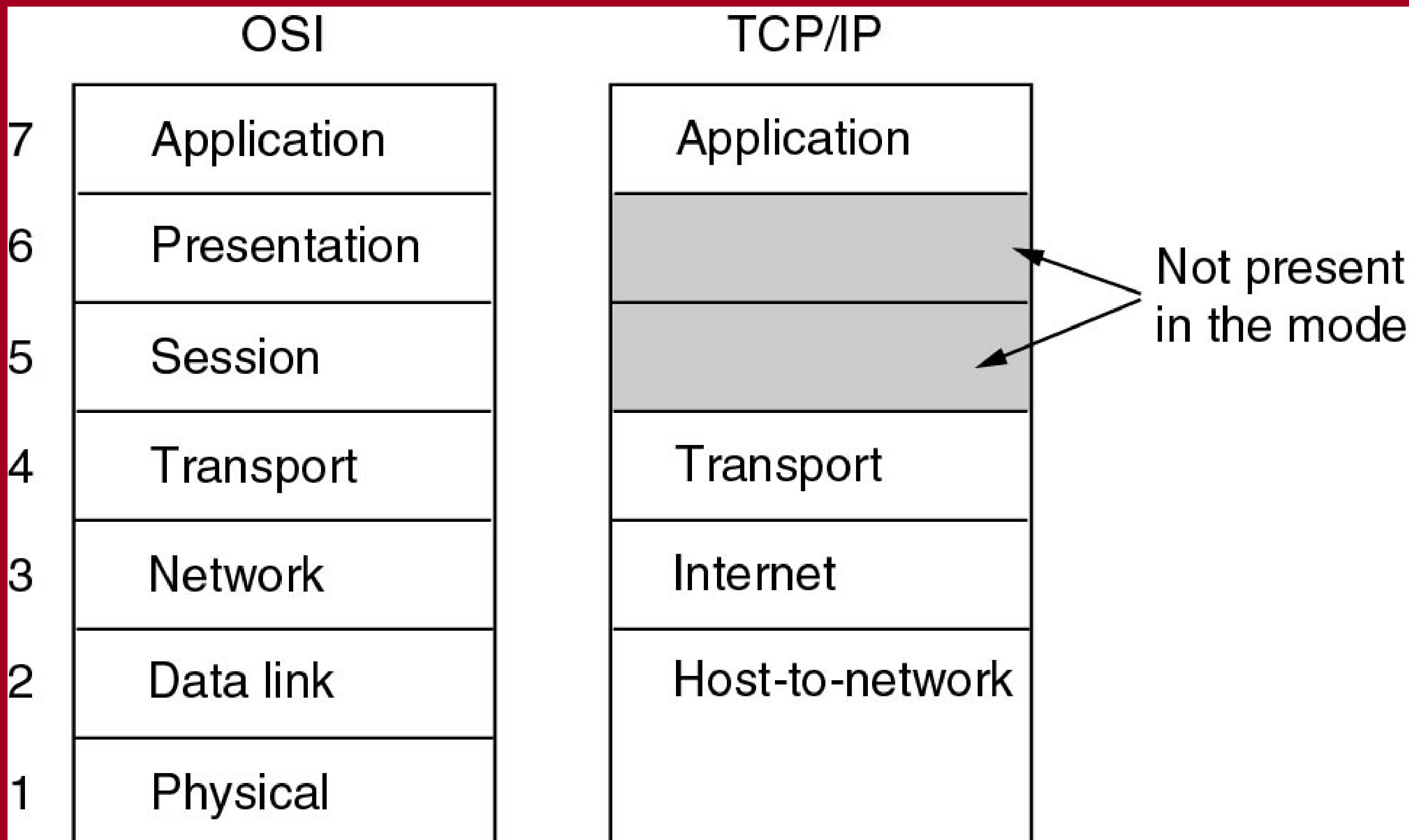
- And of course, none of this matters when you consider remailers / anonymizers :-)
- What about encrypted email?

Resources

- www.arin.net/
- www.samspade.org
- http://www.spamcop.net/
- Nslookup
- Tracert / traceroute
- http://uscode.house.gov/search/crit
- http://www.infobin.org/

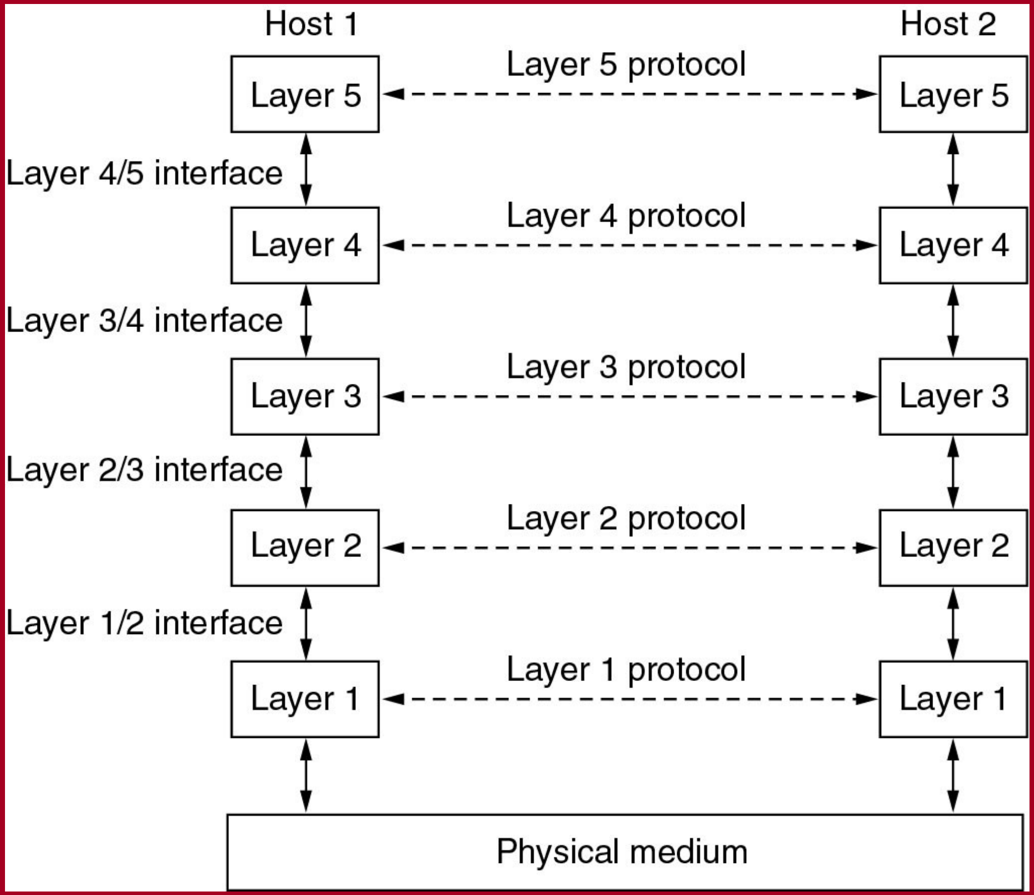
Cyberforensics Networking Review

Reference Models



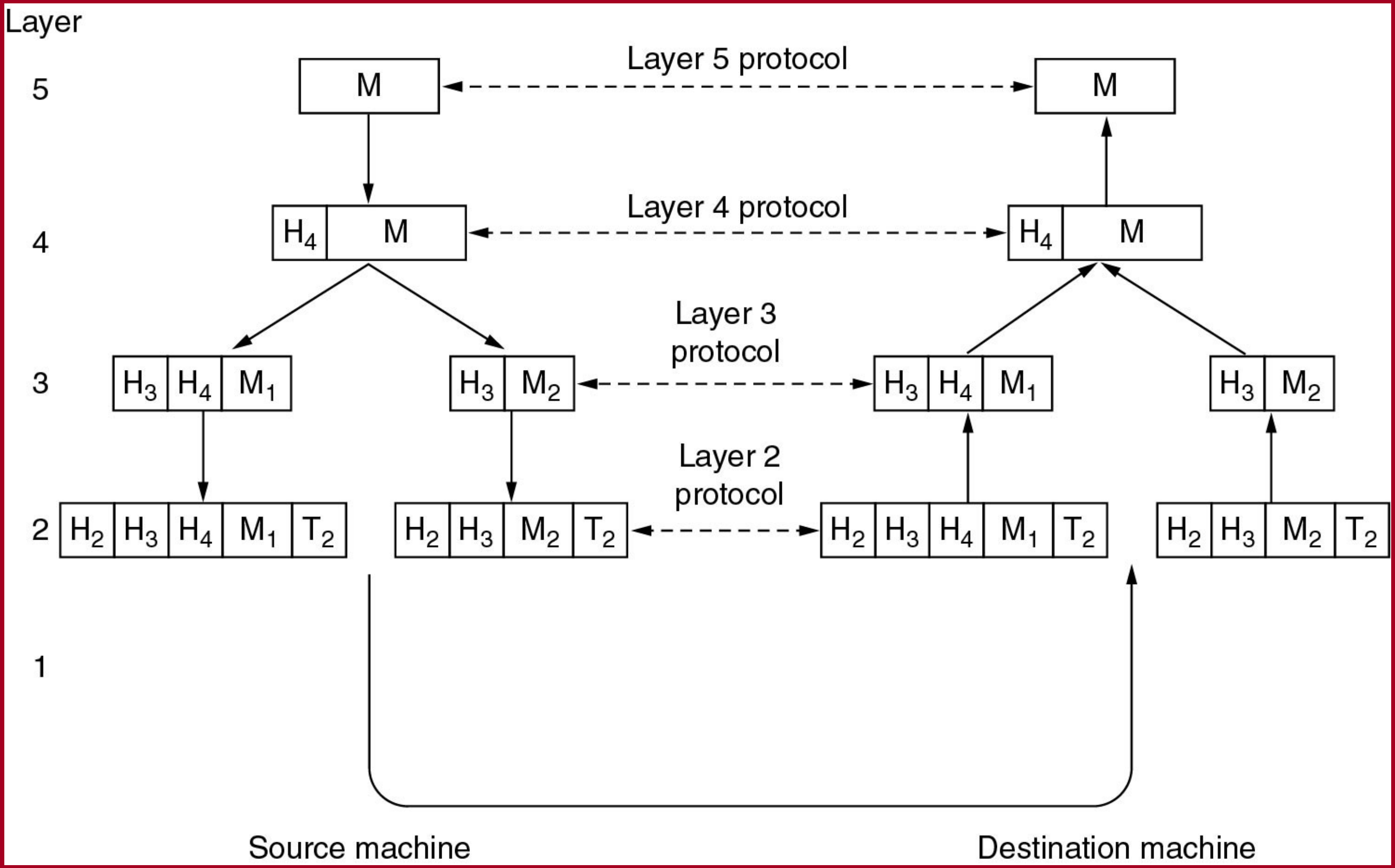
- The TCP/IP reference model.

Network Software
Protocol Hierarchies



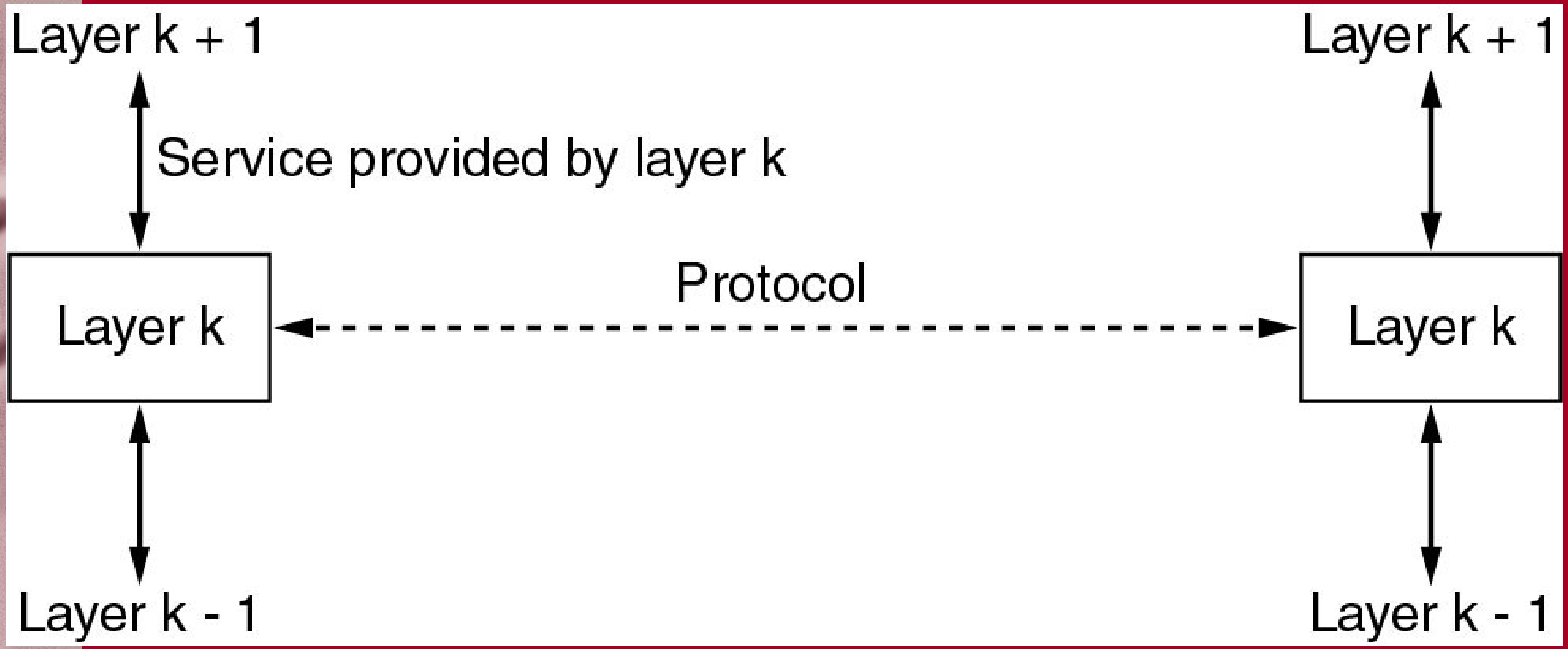
- Layers, protocols, and interfaces.

Protocol Hierarchies



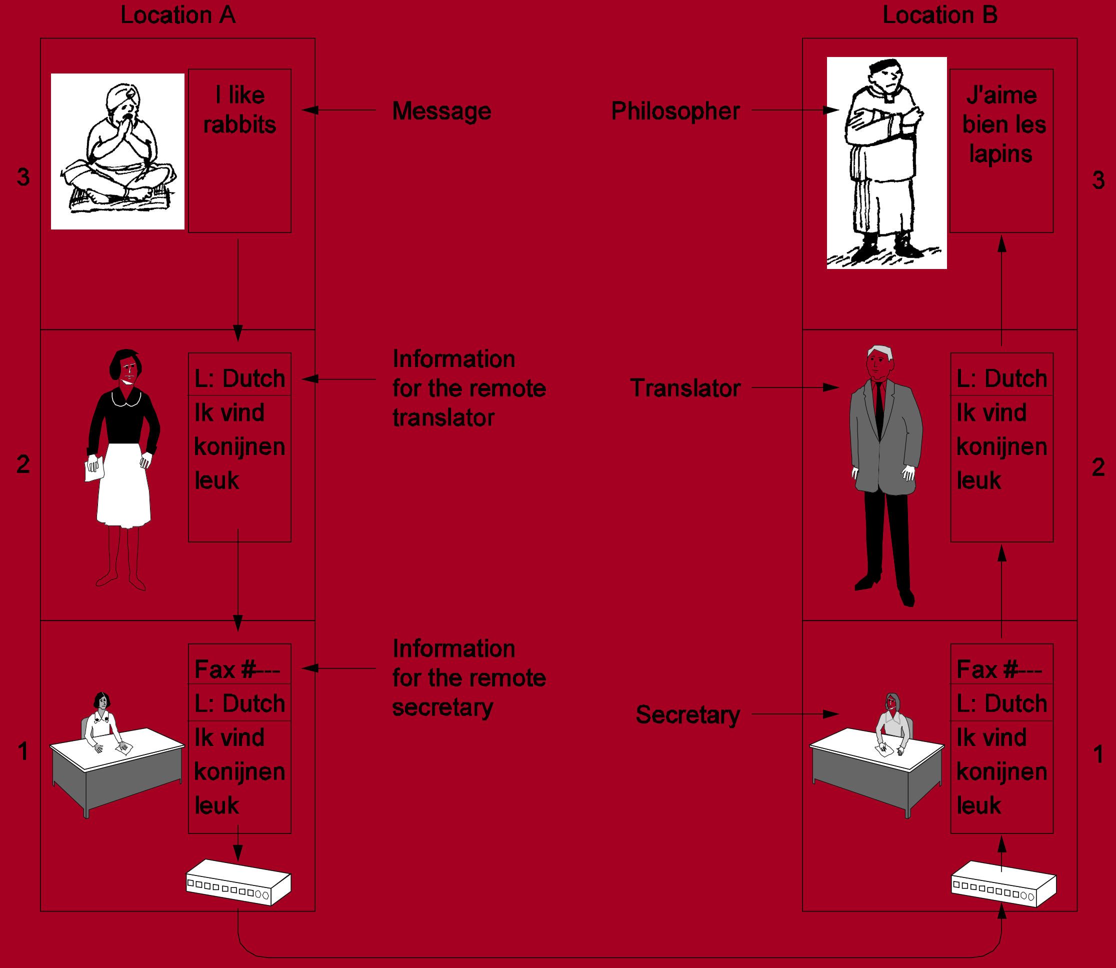
- Example information flow supporting virtual communication in layer 5.

Services to Protocols Relationship



- The relationship between a service and a protocol.

Protocol Hierarchies



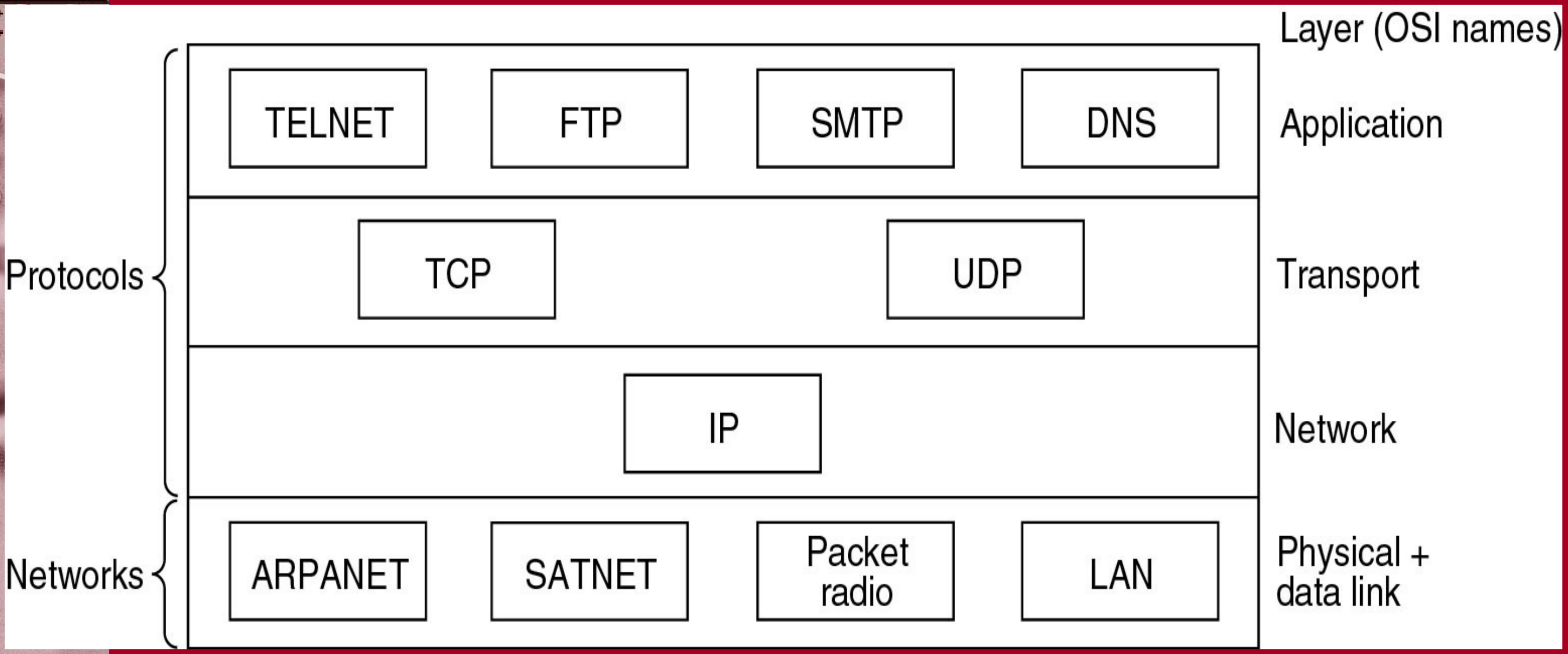
- The philosopher-translator-secretary architecture.

Service Primitives

Primitive	Meaning
LISTEN	Block waiting for an incoming connection
CONNECT	Establish a connection with a waiting peer
RECEIVE	Block waiting for an incoming message
SEND	Send a message to the peer
DISCONNECT	Terminate a connection

- Five service primitives for implementing a simple connection-oriented service.

Reference Models



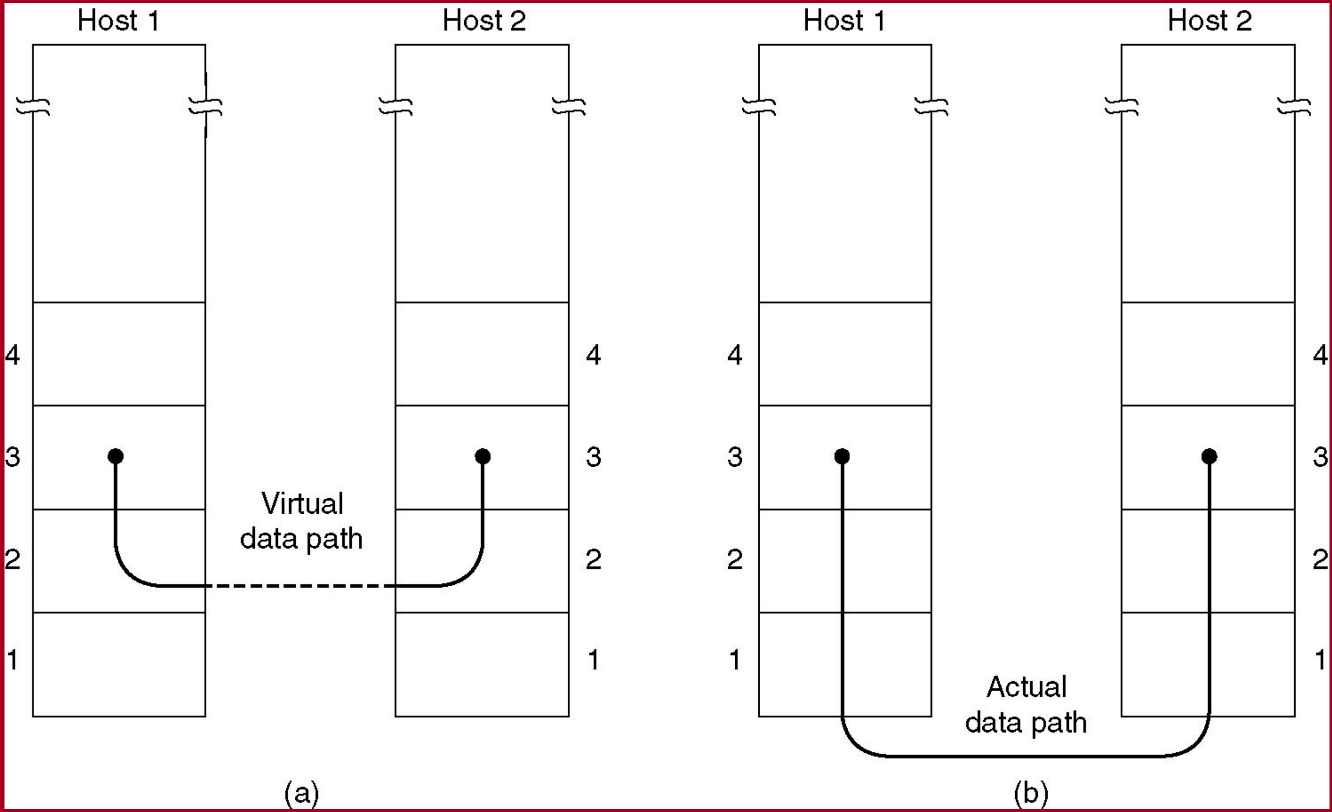
- Protocols and networks in the TCP/IP model initially.

IEEE 802 Standards

Number	Topic
802.1	Overview and architecture of LANs
802.2 ↓	Logical link control
802.3 *	Ethernet
802.4 ↓	Token bus (was briefly used in manufacturing plants)
802.5	Token ring (IBM's entry into the LAN world)
802.6 ↓	Dual queue dual bus (early metropolitan area network)
802.7 ↓	Technical advisory group on broadband technologies
802.8 †	Technical advisory group on fiber optic technologies
802.9 ↓	Isochronous LANs (for real-time applications)
802.10 ↓	Virtual LANs and security
802.11 *	Wireless LANs
802.12 ↓	Demand priority (Hewlett-Packard's AnyLAN)
802.13	Unlucky number. Nobody wanted it
802.14 ↓	Cable modems (defunct: an industry consortium got there first)
802.15 *	Personal area networks (Bluetooth)
802.16 *	Broadband wireless
802.17	Resilient packet ring

The 802 working groups. The important ones are marked with *. The ones marked with ↓ are hibernating. The one marked with † gave up.

Services Provided to Network Layer



(a) Virtual communication.

(b) Actual communication.

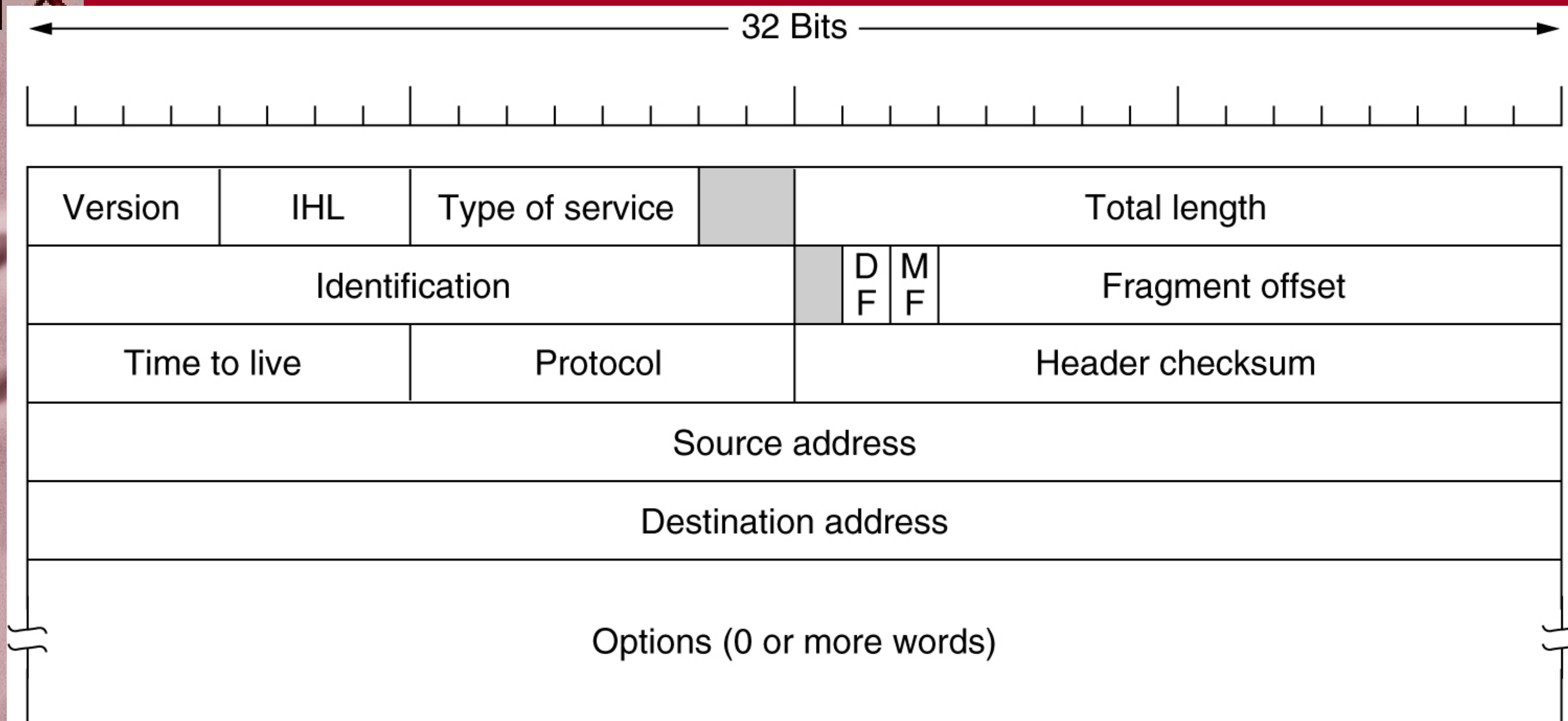
MAC - Ethernet

- Hardware address

  00 0F 1F 14 04 FA

Preamble	SoF	Destination address	Source address	Length	Data	Pad	Check-sum

The IP Protocol



The IPv4 (Internet Protocol) header.

IP

- IPv4 address

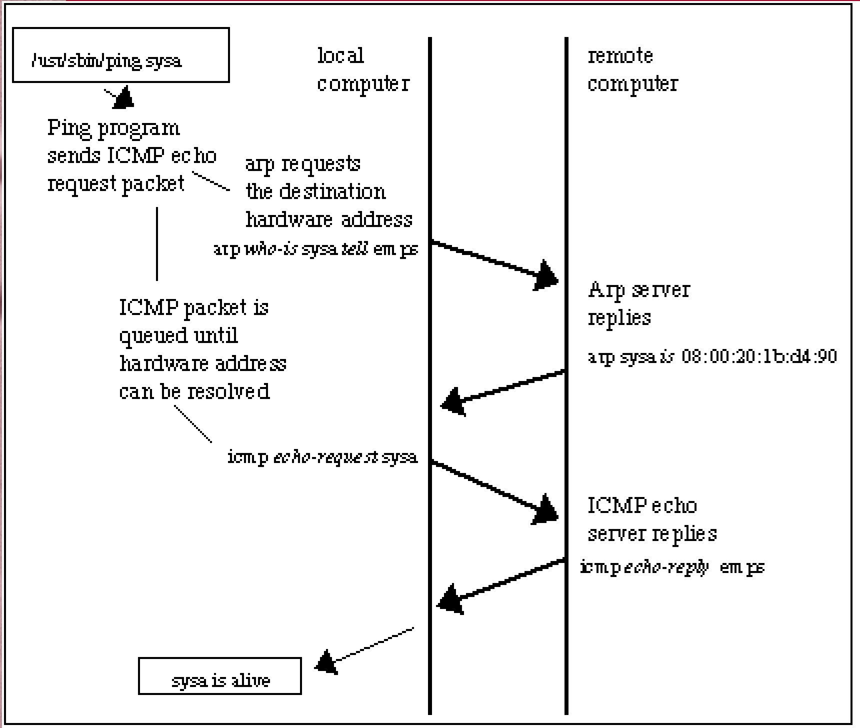
192.168.100.24	local addy
255.255.255.255	broadcast
127.0.0.1	loopback

Different classes…

Subnet masking…

…not going to be covered now

ARP

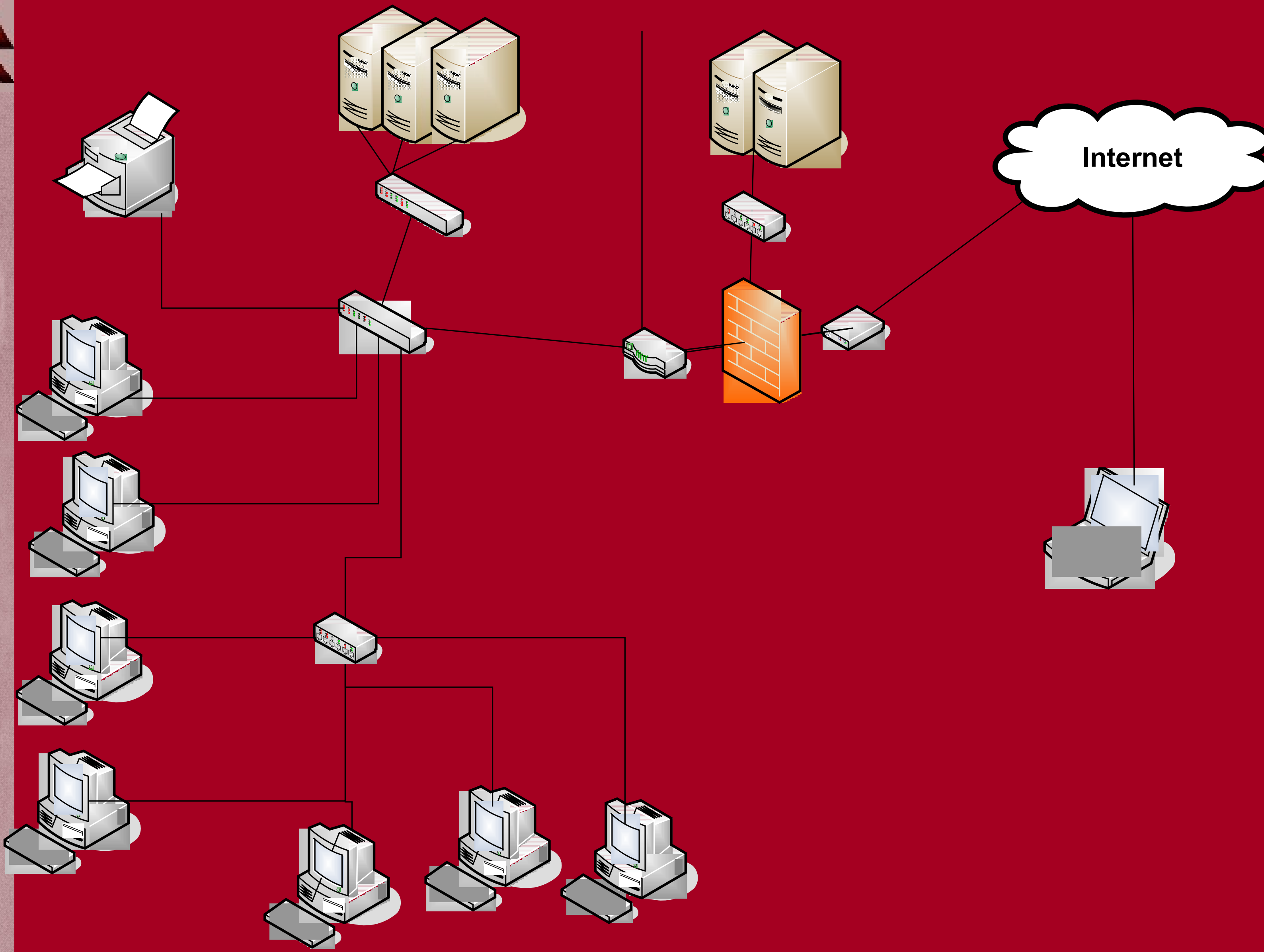


Who is 192.168.100.24?

It's 08:00:20:1b:d4:90

RARP is the other way.   DHCP is more common…..

Generic Network



Methodologies: Tootsie Pop

- Most networks are created after the tootsie pop model:
  - Hard crunchy outside
  - Soft squishy inside
- Notions such as “untrusted network”, firewall, edge router, etc lend themselves to this model
- Historically networks are “supposed to be Open and Accessible”
- Once the perimeter is broken, and intruder is free to peruse the ‘soft’ inside at will

Methodologies: Jaw Breaker

- Networks should be Jaw Breakers
- Evenly secure throughout
- Unfortunately
  - Higher overhead
  - Harder to obtain / troubleshoot
  - Costs more
    - probably indirectly through time / people
    - May be directly through incompatible software / devices

Research Topics

- TCP
- UDP
- ARP
- RARP
- MAC
- NAT
- IP
- ETHERNET
- ROUTING
- FRAME
- PACKET
- PORT

Cyberforensics
Network Forensics

Terminology

- Vulnerability
  - Weakness of some sort – software, hardware, wetware, physical…
- Threat
  - An event (possibly malicious) that may compromise an asset
- Exploit
  - Basically the combination of a threat and a vulnerability.

Hacking Methodology?

- By definition there is no methodology for hacking
  - Historically it goes something like:
    - Obtain insider info
    - Passively obtain more info
    - Possibly actively obtain more info
    - Attack
    - Optionally cover tracks

Setup is key

- Before the incident occurs
  - What is the "default" logging
  - What is your policy
  - Are the logs volatile
  - Are the logs accessible…

    …are you ready to share your logs?

Attack Types

- Passive
  - Eavesdropping / monitoring
  - Traffic analysis / pattern matching
  - Detectable?
- Active
  - Masquerade
  - Replay
  - Modification
  - DOS

Promiscuity

- On a network using a hub, all traffic is broadcast to all hosts
- A host listens to all traffic but only uses/acknowledges traffic where it's address is the destination address…
  - …unless your NIC is in 'promiscuous' mode

Promiscuity

- The promisc option

```
IFCONFIG(8)                Linux Programmer's Manual               IFCONFIG(8)

NAME
       ifconfig - configure a network interface

SYNOPSIS
       ifconfig [interface]
       ifconfig interface [aftype] options | address ...

OPTIONS
       interface
              The  name  of the interface.  This is usually a driver name fol-
              lowed by a unit number, for example eth0 for the first  Ethernet
              interface.

       up     This  flag  causes the interface to be activated.  It is implic-
              itly specified if an address is assigned to the interface.

       down   This flag causes the driver for this interface to be shut  down.

       [-]arp Enable or disable the use of the ARP protocol on this interface.

       [-]promisc
              Enable or disable the promiscuous mode  of  the  interface.   If
              selected,  all  packets  on  the network will be received by the
              interface.
```

Promiscuity

- On a switched network, when a single host is connected to a physical port on the switch, the switch only sends traffic destined for that host through that particular physical port.
- Which host is connected to which port is held in a table on the switch

Passive: Sniffing

- On a non-switched network you can sniff the traffic of all hosts
- On a switched network you can only sniff traffic you sent and traffic the switch deems destined for you

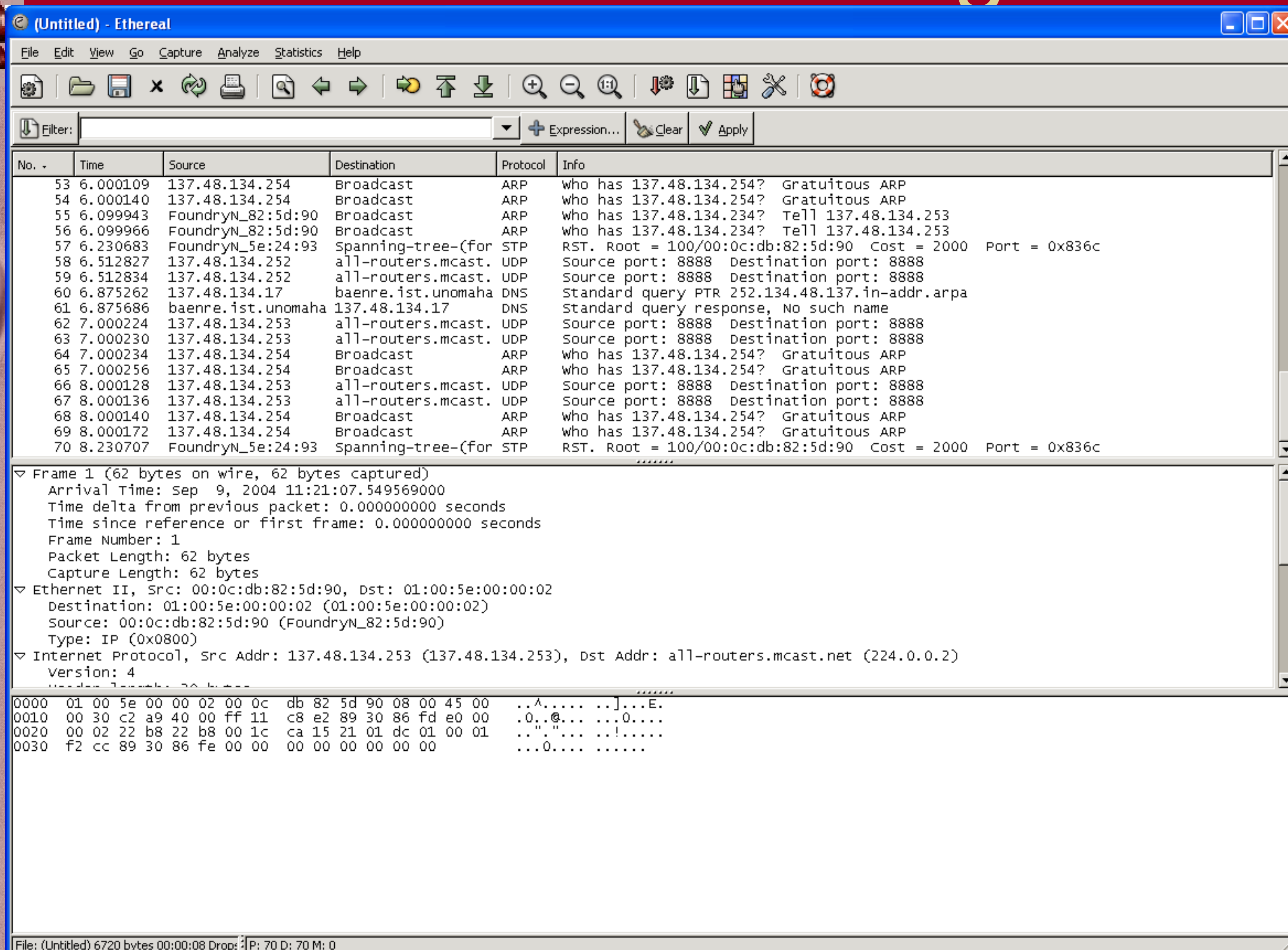
What if the table on the switch is full?

What if you spoof (lie) about your MAC address)?

What about wireless networks (no physical port on the switch)

As a Network Admin how do you do this?

Passive: Sniffing



The Biggest Sniffer of all?

- Carnivore
  - DCS1000
- Altivore
- Echelon

Uhm…just use google.

Active: Scanning

- Typically specific hosts or specific network ranges are scanned
- This is actually a fairly large spectrum
  - Hosts alive
  - Server banners
  - Ports open / close / obfuscated
- Used for network troubleshooting

Trap n Trace

- Basically “sniffing over time”
- Considered Non-intrusive
  - Not inspecting the data portion itself just the ‘auxiliary information’
  - Curbs privacy concerns
- Network shaping, DOS, etc

- tcpdump   windump

```
localhost$> tcpdump > dumpfile.dat
```

Content Monitoring

- Still “sniffing over time”
- Actually looking at data now, not just the “extra info” – so privacy issues

```
[                ]# /usr/sbin/tcpdump --help
tcpdump version 3.8
libpcap version 0.8.3
Usage: tcpdump [-aAdDeflLnNOpqRStuUvxX] [-c count] [ -C file_size ]
                [ -E algo:secret ] [ -F file ] [ -i interface ] [ -M secret ]
                [ -r file ] [ -s snaplen ] [ -T type ] [ -w file ] [ -W filecount ]
                [ -y datalinktype ] [ -Z user ]
                [ expression ]
```

- Something like:

```
tcpdump -n -s 1514 -w /home/user/logfile.dat &
```

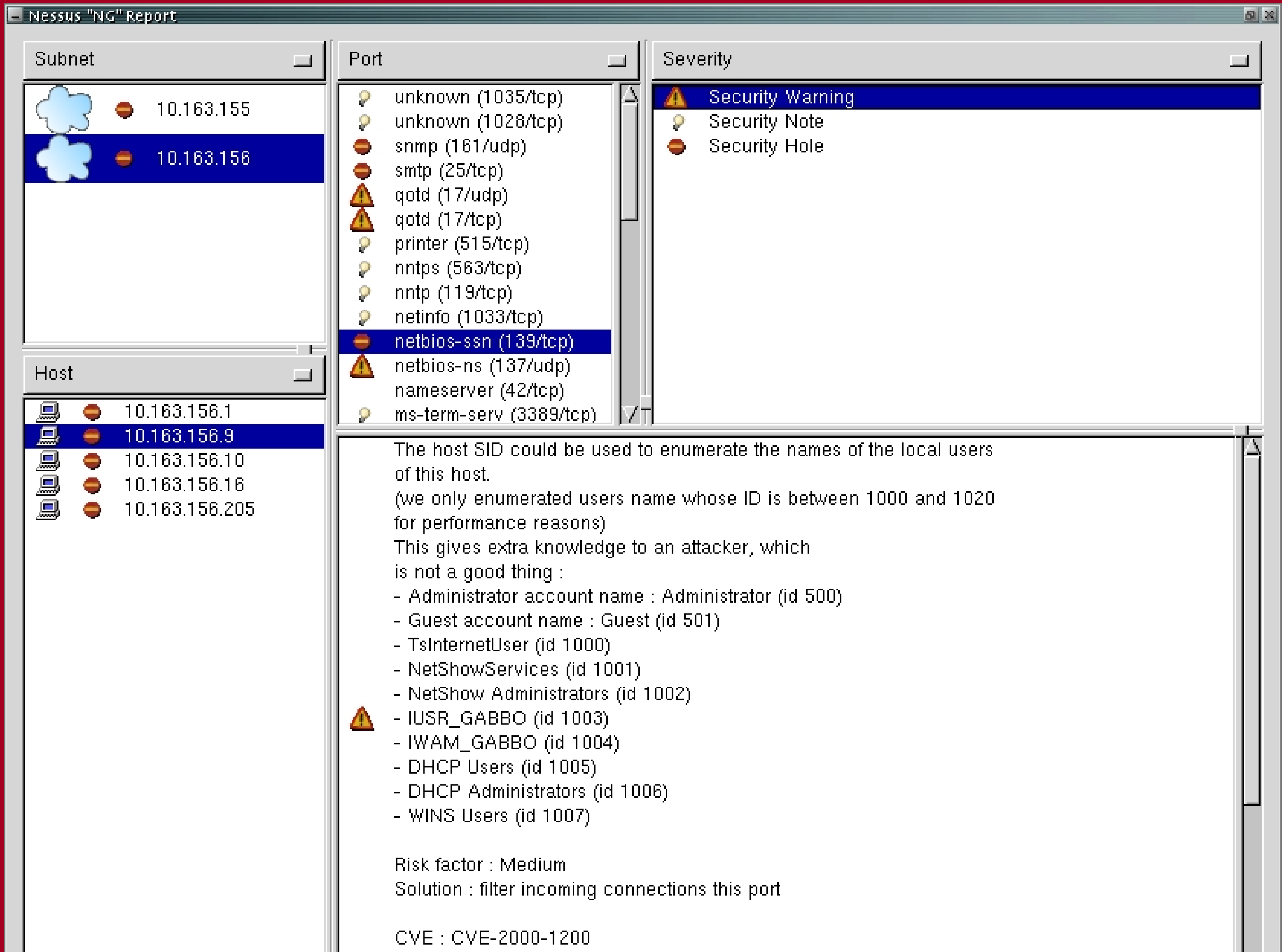
Creating Traffic…

- So just for the sake of argument let's move to the offensive.
- In addition to scanning for things like open ports you can search for known vulnerabilities:
  - Nessus

  Or be tricky / thorough on the scan:

  - nmap

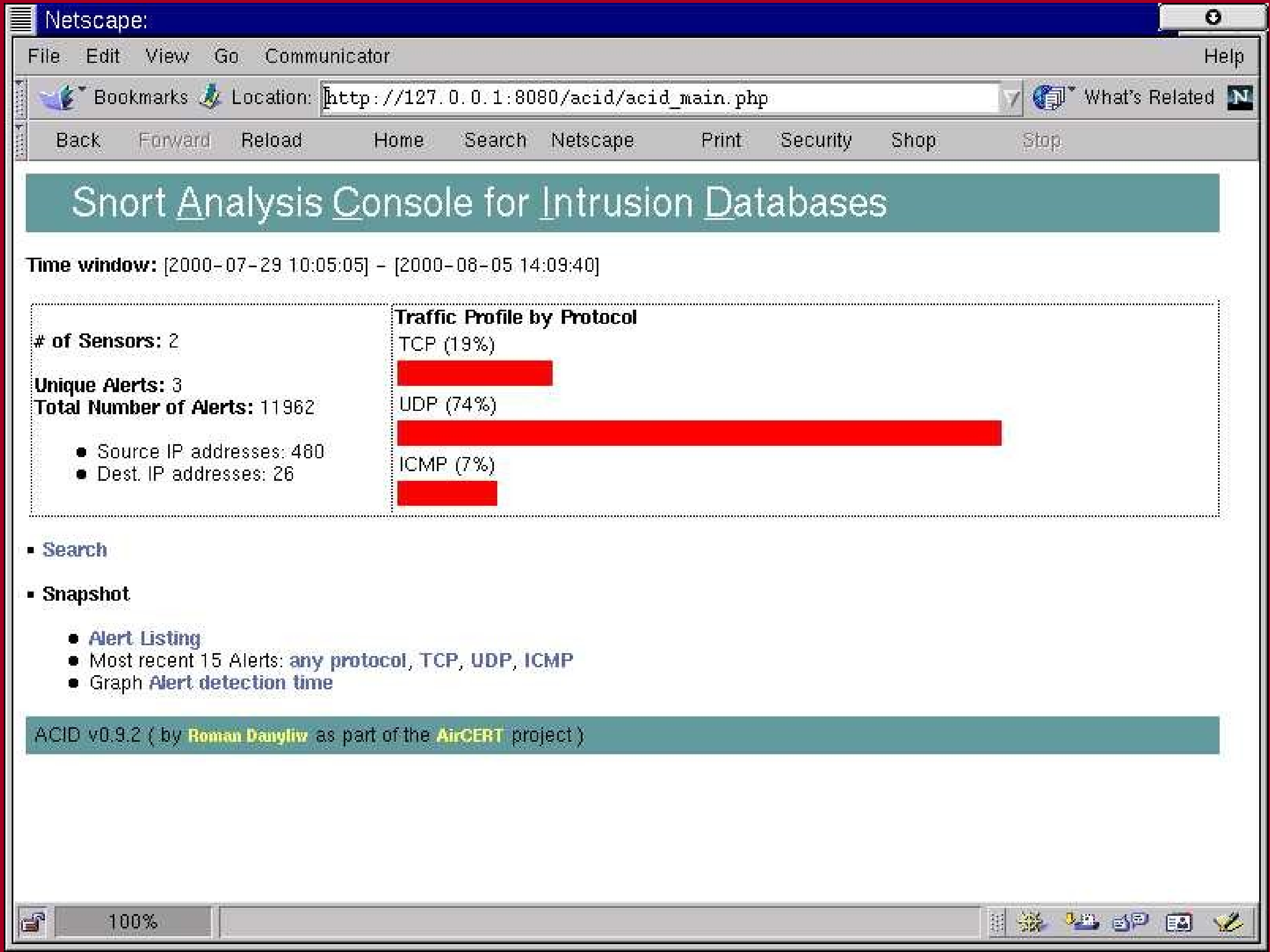
Vulnerability Scanning



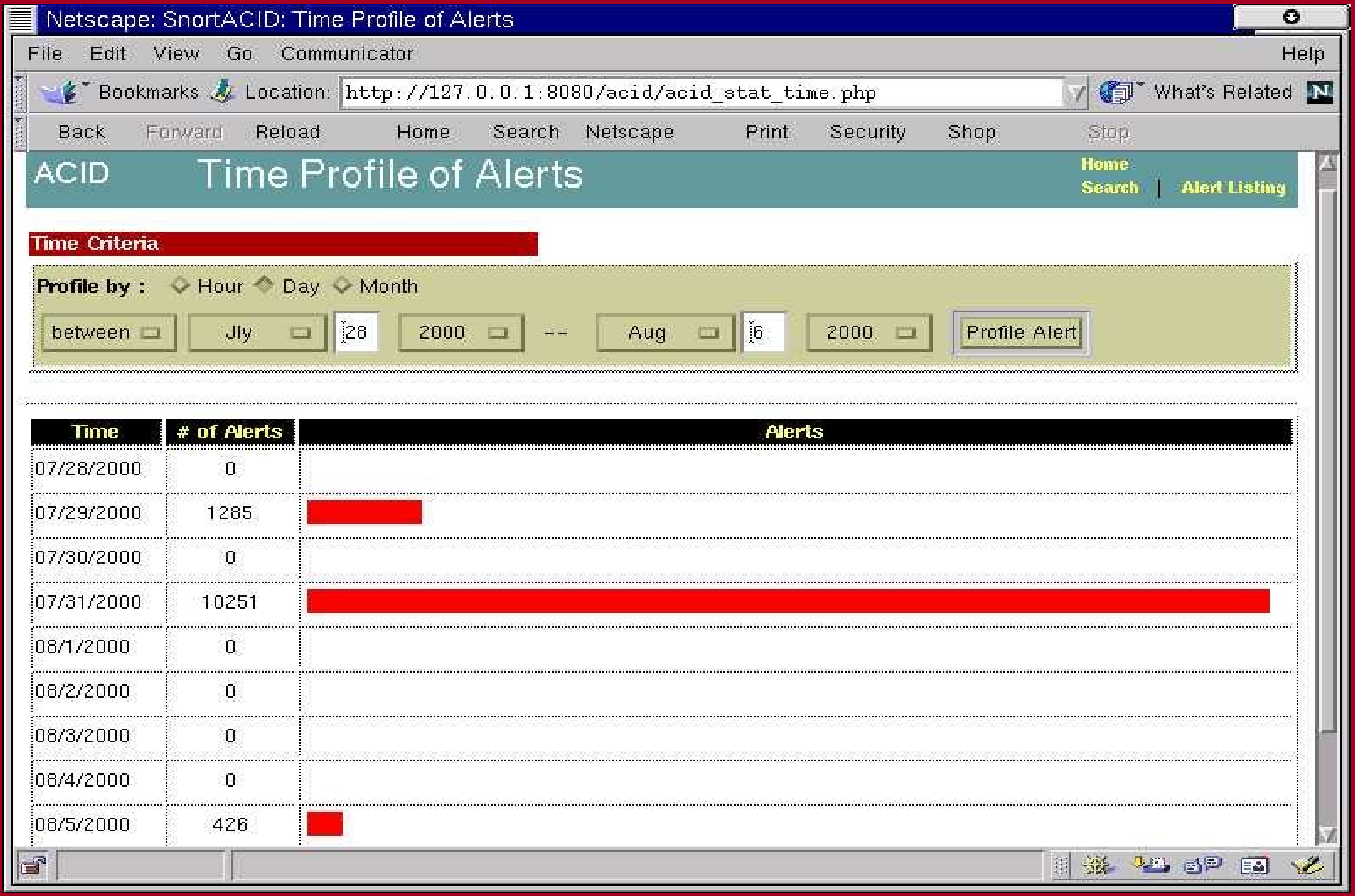
IDS: Detecting this stuff

- Open source stuff
  - Snort – the actual IDS
  - Acid – a good GUI to get started with
- Essentially listens for certain events which may or may not trigger actions
  - Like sending email, pager, beeping
  - Or dropping the connection for a time period, or permanently (reactive passive)
  - Or attacking the attacker back (reactive aggressive)

IDS


Netscape:
File Edit View Go Communicator Help
Bookmarks Location: http://127.0.0.1:8080/acid/acid_main.php What's Related
Back Forward Reload Home Search Netscape Print Security Shop Stop
Snort Analysis Console for Intrusion Databases
Time window: [2000-07-29 10:05:05] - [2000-08-05 14:09:40]
# of Sensors: 2
Unique Alerts: 3
Total Number of Alerts: 11962
Source IP addresses: 480
Dest. IP addresses: 26
Traffic Profile by Protocol
TCP (19%)
UDP (74%)
ICMP (7%)
Search
Snapshot
Alert Listing
Most recent 15 Alerts: any protocol, TCP, UDP, ICMP
Graph Alert detection time
ACID v0.9.2 (by Roman Danyliw as part of the AirCERT project)
100%

IDS


Netscape: SnortACID: Time Profile of Alerts
File Edit View Go Communicator Help
Bookmarks Location: http://127.0.0.1:8080/acid/acid_stat_time.php
What's Related
Back Forward Reload Home Search Netscape Print Security Shop Stop
ACID Time Profile of Alerts
Home
Search | Alert Listing
Time Criteria
Profile by : Hour Day Month
between Jly 28 2000 -- Aug 6 2000 Profile Alert
Time # of Alerts Alerts
07/28/2000 0
07/29/2000 1285
07/30/2000 0
07/31/2000 10251
08/1/2000 0
08/2/2000 0
08/3/2000 0
08/4/2000 0
08/5/2000 426

Side note: Getting tricky

- Some scanners have options to make things more clandestine…

```
NMAP(1)                                                          NMAP(1)

NAME
       nmap - Network exploration tool and security scanner

SYNOPSIS
       nmap [Scan Type(s)] [Options] <host or net #1 ... [#N]>

DESCRIPTION
       Nmap is designed to allow system administrators and curious individuals
       to scan large networks to determine which hosts are up  and  what  ser-
       vices  they  are  offering.   nmap  supports a large number of scanning
       techniques such as: UDP, TCP connect(), TCP SYN (half open), ftp  proxy
       (bounce attack), Reverse-ident, ICMP (ping sweep), FIN, ACK sweep, Xmas
       Tree, SYN sweep, IP Protocol, and Null scan.  See the Scan  Types  sec-
       tion  for more details.  nmap also offers a number of advanced features
       such as remote OS detection via TCP/IP  fingerprinting,  stealth  scan-
       ning, dynamic delay and retransmission calculations, parallel scanning,
       detection of down hosts via parallel pings, decoy scanning,  port  fil-
       tering  detection,  direct (non-portmapper) RPC scanning, fragmentation
       scanning, and flexible target and port specification.

 -sF -sX -sN
        Stealth FIN, Xmas Tree, or Null scan modes: There are times when
        even  SYN  scanning isnât clandestine enough. Some firewalls and
        packet filters watch for SYNs to restricted ports, and  programs
        like Synlogger and Courtney are available to detect these scans.
        These advanced scans, on the other hand, may  be  able  to  pass
        through unmolested.
```

Tools

- Ntop
- Tcpdump - windump
- Tcptrace
- Snort
- Ethereal
- Nmap
- Nessus

Cyberforensics
Information Hiding

IF: Intro

- Greeks used wax covered tablets
- Tattooing the shaved head of a slave
- Invisible ink in WW2
- “reading between the words”
- Microdots

IF: Intro

- So information hiding has existed for a long, long time
- But has received recent attention in past few years in the computer community – there has actually somewhat been a shift from cryptography to information hiding

IF: intro

- Information hiding is not simply hiding messages for clandestine transmission:
  – Watermarking
  – Digital rights management
  – Fingerprinting
- Steganography
  – Hiding data in unused space of other files… typically pictures, but mp3s and others can be used also.
- Compression
  – Compression algorithms to much to hide the actual content of the compressed files.

Information Hiding

- So information hiding by itself general provides little security
- This goes back to the whole ‘security through obscurity’ argument
- Because of this, it is not uncommon to encrypt the data that is to be hidden before hiding it
- The encryption provides a layer of security and the information hiding provides a layer of obfuscation
- Of course encrypting will create larger files that now needs to be hidden

Bit Shift

- So if a certain set of bits represents readable characters:

  `48 65 6C 6C 6F          ->  Hello`
- in BIN: `01011000 01100101 01101101 01101101 01101111`
- What if you move each bit "one left"?
- `0101100001100101011011010110110101101111`
- `10110000 11001010 11011010 11011010 11011110`
- Now decode it…
- `B0 CA DA DA DE ->  ?`
- It is no longer readable – it may actually appear to be binary data now!

Stego

- Some files, such as a bitmap, technically are more suitable for hiding information
- This can be due to file structure, conventions, typical applications or lenience in a standard

Bitmap

- So a bit map is a digital representation of a picture using X bits to represent a single picture.
- For monochrome images X may be 1, but for color images X may be many bits
- These X bits are translated into color information for display on screen or for printing
- This is known as “bit-depth”, so 4 bit color can represent 16 colors:
  - 0000, 0001, 0010 … 1110, 1111

Bitmap

- In addition to bit-dept, computer graphics depend upon resolution, most monitors operate at 72dpi (resolution also sometimes means total pixels – like 1024x768)
- Printers come in a variety of resolutions…150, 300, 600, 1200, 2000

Bitmap

- The colors your eye actually sees, depends on the bit depth of the picture and monitor in addition to the picture and monitor's resolution.

Bitmap

- The actual file structure of a bitmap has four parts

File Header
Info Header
RGBQuadArray
ColorIndexArray

Bitmap – File Header

start	size	function
1	2	‘BM’ tag
3	4	File size
7	2	Reserved
9	2	Reserved
11	4	Offset to bitmap data

Bitmap – Info Header

start	size	function
15	4	Size of info header
19	4	Width
23	4	Height
27	2	Planes – 0
29	2	Bits per pixel
31	4	Compression – 0
35	4	Size of image – 0
39	4	Horizonal pixels on device -0
43	4	Vertical pixels on device – 0
47	4	Colors used, if 0 calc from bits
51	4	Specifies ‘important’ colors

Bitmap – RGB Quad

There is an array of these structures…

Start	Size	Function
1	1	Blue
2	1	Green
3	1	Red
4	1	reserved

Bitmap

- So there are many methods of storing additional information in a bitmap…
  - LSB of each color in each ‘Quad’
  - Change bitmap data offset
  - Unused ‘colors’
  - ‘messing’ with compression bits

Bitmap - LSB

- One of the simplest ways to hide information is using the Least Significant Bit
- If it’s a 24-bit bitmap, then each pixel is represented by 3 bytes, if you use the LSB of each byte, a 1024 x 768 image would have 2359296 b = 294912 B ~= 288 kb of space to hide information

Bitmap – LSB - example

- 3 pixels in an image; 9 bytes

11001100 11111011 11111011
11111101 10100000 10101110
00000100 11111011 10111110

- So 9 bits to hide information in…

11001100 11111011 11111011
11111101 10100000 10101110
00000100 11111011 10111110

- Enough to hide a byte..

Bitmap – LSB - example

- If we would like to hide the value for an "H"….01001000

  11001100 11111011 11111011

  11111101 10100000 10101110

  00000100 11111011 10111110

- Becomes :
  11001100 11111011 11111010

  11111100 10100001 10101110

  00000100 11111010 10111110

On average, only ½ of the LSBs will actually change.

Bitmap – LSB

- Actual implementation of this is varied and somewhat different
- For 8 bit images, adjacent bytes may be joined together for stego purposes
- Some tools alter the palette order or the actual colors slightly to make the image more amenable to information hiding

Bitmap - LSB

- Simple conversion of the image will likely loose all hidden messages
- Works best with pallets of similar colors (gradients) - likewise works worst with pallets of solid, different colors

Bitmap

- So how do you get the information out?
  - – Proprietary
    - Similar to a crypto key, there may be a "stego-key" – for example the process required to extract the hidden information
  - – If you don't know which bits are being used for information and which are being used for color representation, this is a fairly arduous task

Stego

- Other files, such as jpg, may not be the most suitable, but are the most desirable because they are the most prevalent
- Jpgs are compressed at various levels – sometimes a simple ‘save-as’ will alter the contents of a file
- Because they are compressed they don’t have as much unutilized space as a bitmap - this is also due to the lossless versus lossy formats

NUCIA

Your Key to Security

WaterMarks

- Technically not stego
- Stego conceals information
- Watermarks extend information
  - A characteristic of the image
- Masking is when ‘watermark-like’ methods are used to hide information

Stego

- MP3’s are also fairly prevalent and have a file size much larger than jpgs (typically)
- Because of the file structure there are ample places to store additional information
  - Before/after mp3 id tags for example
  - Actually encoding information into the mp3 when creating the file

Stego

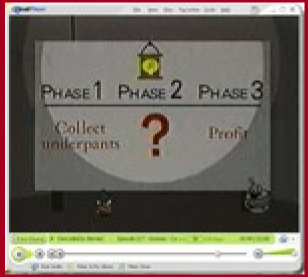
- Of course different encoders and algorithms have different results, so the exact file size of an encoded mp3 is largely unpredictable
- Therefore the notion of a “slightly large” mp3 doesn’t have merit

Stego

- Encoding small amounts of information into the music itself will only marginally increase the file size, manipulating the bitrate (Variable bit rate?!), ceiling /floor, or the number of channels etc can reduce the file size back to near original.
- Of course re-sampling the music will obliterate your hidden information

Cyberforensics
Attack Artifacts (footprints)

Objectives



1. Attain a working knowledge cyber incident response
2. ?
3. Profit!

U.S. DEPARTMENT OF ENERGY

Office of the Chief Information Officer
Office of Cyber Security

CIAC
CIAC@ciac.org
Computer Incident Advisory Capability
"Keeping DOE Secure"

NUCIA

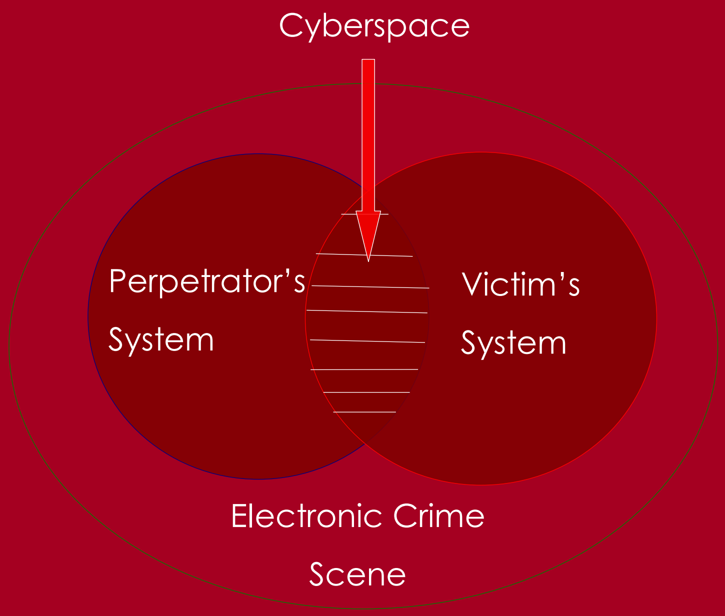
Your Key to Security

"Almost all attacks leave detectable remnants that may be uncovered and used in an investigation."

http://ciac.llnl.gov

Crimescene

- Where is the crime scene?
- In traditional cases, a crime scene is taped off to prevent outside alteration
- In the digital world there isn't a place to tape



What are the signs of an inexperienced attacker?

Signs of an inexperienced attacker *can* be:

- Deletes or corrupts data
- Downs the machine
- Gives out the compromised passwords to people
- Can be identified with automated tools
- Shares his account with others

What are the signs of an experienced attacker?

Signs of an experienced attacker *can* be:

- Alters logs rather than deletes them
- Alters all relevant logs
- You cannot easily determine how original access was attained
- New/unseen techniques were used
- Hacker installed trojanized code to avoid detection
- On and off quickly
- No bragging or sharing of account

Signs of an experienced hacker

can be:

Logs may not contribute much added value to an investigation. The omission of helpful logs in itself is a good clue:

The hacker has the access and wants to *keep* it

Curveball

- What about the experienced attacker trying to appear like an inexperienced attacker?

Step One

- Was there really a breach?
  - Find out who manages the systems in question, s/he will have more intimate knowledge of the system than anyone else

Was there a Computer Intrusion?

- What system(s) was attacked?
- What technique(s) was used to perform the attack?
- When did the attack occur?
- Where was the attack initiated from?
- What damage (if any) was caused by the intrusion?
- How was the incident discovered?
- Is the system(s) now secure?
- Who else knows about the compromise?

The SA is your friend

- It does no good to make the SA an enemy.
- s/he will be able to answer your questions faster and better than others
  - Sometimes (often?) this will be your only avenue for answers
- Ask questions about things that will help answer the previous questions…

The SA is your friend

- New or modified accounts in the /etc/passwd and /etc/shadow file
- New or modified entries in the crontab files / folders
- The sensitivity of the data on the system
- What logs are kept
  - and where
  - and for how long
  - And backup strategies..
- The configuration of the Network
- Did the hacker know exactly where to go to get files?

NUCIA

Your Key to Security

Step Two

- If possible Obtain / create a forensic duplicate
- Ideally this can be done before any live (hands on) work is done
- What are the implications of “pulling the plug” of a powered on machine?

Live system consequences

- Running processes
- Active network connections, activities
- Logged in users
- Encryption
- Viruses (one-half)

Simple Steps

- Several commands can be used to start understanding the current system's state
  - The "w" command
  - The "finger" command
  - The "who" command
  - The "netstat" command

The “w” Command

If you are suspicious that an intruder is on the system, perform the “w” command to see a listing of the users currently logged in

“w” shows you who is *currently logged in* and *what they are currently doing*

The “w” Command

```
Prompt % w
3:47pm      up       18 days,     3:02,     7 users,         load
average:    0.02, 0.00,0.00
User        tty      login@     idle       JCPU       PCPU       what
User1       ttyp0    25Mar94    2:08       39:15      4          -tcsh
user2 ttyp1 5Apr94   8          5:51       5:28       emacs
user2 ttyp2 3:46pm                                    w
user3 ttyp3 Mon 2pm             2:04       1          -csh
user3 ttyp4 Mon 3pm  41         21                    -csh
user2 ttyp6 5Apr94   3          1:38       6          -tcsh
user2 ttyp7 Wed 2pm  5:31       17         1          -tcsh
Prompt %
```

Verify

- All users are valid users
- Users have not been logged on for an abnormal length of time
- Users are not currently running ‘suspicious’ programs
- What constitutes a ‘suspicious’ program?

The "w" Command

What if….

- The output of "w" is not reliable
- The output of a "w" is modified by the hacker immediately after his initial access
- Modified utmp log affects output

The "finger" Command

"finger" shows you who is *currently logged in* and *where they are currently logged in from*

The "finger" Command

Prompt % finger

Login	Name	TTY	Idle	When	Where
user1	user name	p0	26	Fri 11:46	host1.sub.domain
User2	user name	p1	34	Tue 10:42	host2.sub.domain
user4	user name	p2		Mon 14:04	host3.sub.domain
User3	user name	p3	44	Mon 14:06	host5.sub.domain
user2	user name	p4		Mon 16:43	host4.sub.domain
User2	user name	p6	3:45	Tue 11:06	host2.sub.domain
user2	user name	p7	1	Wed 14:47	host2.sub.domain
user3	user name	p8	3:04	Thu 11:04	host5.sub.domain
user3	user name	p9	1:02	Fri 13:52	host5.sub.domain

Prompt %

Verify

- All users are valid users
- Users have not been logged on for an abnormal length of time
- Users are not currently logged in from suspicious places

The "finger" Command

- The output of the "finger" command is not reliable
- Modified utmp log affects output

The “who” Command

“who” shows you who is *currently logged in* and *where they are currently logged in from*

The “who” Command

```
Prompt % who
user1   ttyp0   Mar   25   11:46   (host1.sub.domain)
User2   ttyp1   Apr   5    10:42   (host2.sub.domain)
user4   ttyp2   Apr   18   14:04   (host3.sub.domain)
User3   ttyp3   Apr   11   14:06   (host5.sub.domain)
user2   ttyp4   Apr   18   16:43   (host4.sub.domain)
User2   ttyp6   Apr   5    11:06   (host2.sub.domain)
user2   ttyp7   Apr   6    14:47   (host2.sub.domain)
user3   ttyp8   Apr   14   11:04   (host5.sub.domain)
user3   ttyp9   Apr   15   13:52   (host5.sub.domain)
Prompt %
```

Verify

- All users are valid users
- Users have not been logged on for an abnormal length of time
- Users are not currently logged in from suspicious places

The "who" Command

- The output of "who" is not reliable
- The source of the information for the "who" command is the utmp log, which is easily modified

See any patterns here?

The MAN page says:

The **utmp** file allows one to discover information about who is currently using the system. There may be more users currently using the system, because not all programs use utmp logging.

Warning: utmp must not be writable, because many system programs (foolishly) depend on its integrity. You risk faked system logfiles and modifications of system files if you leave **utmp** writable to any user.

The "netstat" Command

"netstat" shows you who is *currently logged in* and *where they are currently logged in from*

The "netstat" Command

Active Internet connections (w/o servers)

Proto	Race-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	2	nazgul.sso.sytex:telaet	207.196.92.162:1747	ESTABLISF£D
udp	0	0	localhost:759	localhost:1023	ESTASLISh£O
udp	0	0	localhost:ntp	*:*	
udn	0	0	nazgul.sso.sytexinc:ntp	*:*	

Active UNIX domain sockets (w/o servers)

Proto	Ra£Cnt	Flags	Type	State	I-Node	Path
unix	2	[ ]	STREAM	CONNECTED	366	
unix	2	[ ]	STREAM		367	/dev/log
unix	2	[ ]	STREAM	CONNECTED	401	
unix	2	[ ]		CONNECTED	523	
unix	2	[ ]	STREAM		440	/dev/log
unix	2	[ ]	STREAM		400	/dev/log
unix	2	[ ]	STREAM	CONNECTED	519	
unix	2	[ ]	STREAM	CONNECTED	555	
unix	2	[ ]	STREAM		564	/dev/leg
unix	2	[ ]	STREAM		566	/dev/log
unix	2	[ ]	STREAM	CONNECTED	591	
unix	2	[ ]	STREAM		592	/dev/log

The "netstat" Command

- Much more reliable results than a "w", "who", or "finger"
- Compare the results of "netstat" to "w", "who", and "finger"
- Compromised systems have been found to contain trojanized versions of "netstat" which does not display the intruder's connections (rootkit)
- We'll talk later about rootkit detection methods

lsof

- List open files
- Since "everything in linux is a file"….
- Usefule optoins:
  - -i all internet sockets
  - -u comma delimited list of users
- Lsof can be a very valuable tool

Lsof output

```
Prompt# /usr/sbin/lsof
COMMAND      PID   USER   FD    TYPE     DEVICE      SIZE       NODE NAME
init           1   root   cwd    DIR       8,17      4096          2 /
init           1   root   rtd    DIR       8,17      4096          2 /
init           1   root   txt    REG       8,17     35344    3662904 /sbin/init
init           1   root   mem    REG       8,17    105708    3597454 /lib/ld-2.3.3.so
init           1   root   mem    REG       8,17   1451868    3597555 /lib/tls/libc-2.3.3.so
init           1   root   mem    REG       8,17     59400    3597500 /lib/libselinux.so.1
init           1   root   10u   FIFO       8,17               2198815 /dev/initctl
syslogd     1153   root   txt    REG       8,17     31604    3662883 /sbin/syslogd
syslogd     1153   root    0u   unix 0x0fb65980                 2253 /dev/log
syslogd     1153   root    2w    REG       8,17     20600    1308358 /var/log/messages
sshd        1528   root   cwd    DIR       8,17      4096          2 /
sshd        1528   root   rtd    DIR       8,17      4096          2 /
sshd        1528   root   txt    REG       8,17    269128     392747 /usr/sbin/sshd
sshd        1528   root   mem    REG       8,17     28008    3597515 /lib/libpam.so.0.77
sshd        1528   root   mem    REG       8,17     13988    3597490 /lib/libutil-2.3.3.so
sshd        1528   root   mem    REG       8,17    971652    3597507
/lib/libcrypto.so.0.9.7a
httpd       1644   root   cwd    DIR       8,17      4096          2 /
httpd       1644   root   rtd    DIR       8,17      4096          2 /
httpd       1644   root   txt    REG       8,17    263640     392703 /usr/sbin/httpd
httpd       1644   root   mem    REG       8,17     74844    3597484 /lib/libresolv-2.3.3.so
httpd       1644   root   mem    REG       8,17     64040     359838
/usr/lib/libz.so.1.2.1.1
crond       1654   root   txt    REG       8,17     27472     392600 /usr/sbin/crond
crond       1654   root   mem    REG       8,17    105708    3597454 /lib/ld-2.3.3.so
crond       1654   root   mem    REG       8,17   1451868    3597555 /lib/tls/libc-2.3.3.so
crond       1654   root   mem    REG       8,17     59400    3597500 /lib/libselinux.so.1
```

Lsof cont'd output

```
sshd     14838  joeuser  cwd   DIR   8,17     4096        2 /
sshd     14838  joeuser  rtd   DIR   8,17     4096        2 /
sshd     14838  joeuser  txt   REG   8,17   269128   392747 /usr/sbin/sshd
sshd     14838  joeuser  mem   REG   8,17    28008  3597515 /lib/libpam.so.0.77
sshd     14838  joeuser  mem   REG   8,17    13988  3597490 /lib/libutil-2.3.3.so
sshd     14838  joeuser  mem   REG   8,17   971652  3597507 /lib/libcrypto.so.0.9.7a
sshd     14838  joeuser  mem   REG   8,17  1451868  3597555 /lib/tls/libc-2.3.3.so
su       14876  root   cwd   DIR   8,17     4096  1880662 /home/joeuser
su       14876  root   rtd   DIR   8,17     4096        2 /
su       14876  root   txt   REG   8,17   101390  3450324 /bin/su
su       14876  root   mem   REG   8,17     8332  3597516 /lib/libpam_misc.so.0.77
su       14876  root   mem   REG   8,17    11160   294366 /lib/security/pam_selinux.so
su       14876  root   mem   REG   8,17    10776   294463 /lib/security/pam_env.so
su       14876  root   mem   REG   8,17    48740   294372 /lib/security/pam_unix.so
bash     14877  root   cwd   DIR   8,17     4096  1880662 /home/joeuser
bash     14877  root   rtd   DIR   8,17     4096        2 /
bash     14877  root   txt   REG   8,17   587620  3450275 /bin/bash
bash     14877  root   mem   REG   8,17    15008  3597472 /lib/libdl-2.3.3.so
cupsd    18084  root   txt   REG   8,17   250532   392764 /usr/sbin/cupsd
cupsd    18084  root   mem   REG   8,17    50944  3597539 /lib/libnss_files-2.3.3.so
cupsd    18084  root   mem   REG   8,17    22172  3597524 /lib/libnss_dns-2.3.3.so
httpd    18350 apache  cwd   DIR   8,17     4096        2 /
httpd    18350 apache  rtd   DIR   8,17     4096        2 /
httpd    18350 apache  txt   REG   8,17   263640   392703 /usr/sbin/httpd
httpd    18350 apache  mem   REG   8,17    74844  3597484 /lib/libresolv-2.3.3.so
httpd    18350 apache  mem   REG   8,17    64040   359838 /usr/lib/libz.so.1.2.1.1
```

lsmod

- List loaded modules in the kernel
- Intimately related to insmod, depmod, modprobe, etc
- Can give you insight into the hardware of the machine

lsmod

```
Prompt# /sbin/lsmod
Module                  Size  Used by
snd_pcm_oss            40740  0
snd_pcm                68872  1 snd_pcm_oss
snd_page_alloc          7940  1 snd_pcm
snd_timer              17156  1 snd_pcm
snd_mixer_oss          13824  1 snd_pcm_oss
snd                    38372  4 snd_pcm_oss,snd_pcm,snd_
soundcore               6112  1 snd
ipv6                  184288  14
parport_pc             19392  0
lp                      8236  0
parport                29640  2 parport_pc,lp
autofs4                10624  0
sunrpc                101064  1
e1000                  68492  0
ipt_REJECT              4736  1
ipt_state               1536  6
ip_conntrack           24968  1 ipt_state
iptable_filter          2048  1
ip_tables              13440  3 ipt_REJECT,ipt_state,ipt
floppy                 47440  0
sg                     27552  0
microcode               4768  0
dm_mod                 33184  0
ohci_hcd               14748  0
button                  4504  0
battery                 6924  0
asus_acpi               8472  0
ac                      3340  0
ext3                  102376  2
jbd                    40216  1 ext3
aic7xxx               135864  3
sd_mod                 16384  5
scsi_mod               91344  3 sg,aic7xxx,sd_mod
```

```
Prompt# /sbin/lsmod
Module                  Size  Used
iptable_filter          2316   0  (a
ip_tables              15072   1  [i
es1371                 27788   0
ac97_codec             15828   0  [e
soundcore               6340   0  [e
gameport                3268   0  [e
nfsd                   75280   8  (a
af_packet              14856   1  (a
ip_vs                  70188   0  (a
floppy                 55932   0
3c59x                  29680   1  (a
supermount             84032   3  (a
usb-uhci               25136   0  (u
usbcore                74988   1  [u
rtc                     9004   0  (a
ext3                   60048   4
jbd                    39264   4  [e
```

Ten Steps to Take After Intrusions

1. Examine Log Files and Backups
2. Examine All Files Run by “cron” and “at”
3. Examine the “/etc/passwd” (shadow) File for Alterations
4. Check Systems for Unauthorized Services
5. Check Systems for Sniffer Programs
6. Check Systems for Trojanized Programs
7. Look for “setuid” and “setgid” Files
8. Look for “+” Entries and Non Local Host Names in Certain Files
9. Look for Unusual and Hidden Files
10. Review All Processes Currently Running on System

Examine Log Files

- History Log of Compromised Account(s)
- Messages Log
- Look at logs created by "syslog"
- Look at logs maintained by firewalls or routers
- What do inconsistencies between two logs mean?
- How do you know if the system in question uses syslog or log files or…
.

Examine the WTMP File(s)

- This is may be among the most important file when tracking an intruder
- Use the “last” command to access information in the WTMP file
- Use “last <userid>” to view the previous logins to a specific account
- Use “last -<number> <userid>” to view a certain number of logins from a specific account
- You’ll need the userid obviously

Examine the WTMP File(s)

```
smith    pts/1        Mon Aug  8 10:01    gone - no logout  136.48.111.1
smith    pts/1        Mon Aug  8 08:16 - 08:24  (00:08)    ip68-13-121-33.om.cox.net
smith    pts/0        Mon Aug  8 05:53    gone - no logout  ip68-13-121-33.om.cox.net
smith    pts/0        Sun Aug  7 23:49 - 05:52  (06:03)    ip68-13-121-33.om.cox.net
smith    pts/1        Sun Aug  7 17:50 - 18:46  (00:56)    136.48.111.1
smith    pts/0        Sun Aug  7 15:47 - 19:48  (04:00)    136.48.111.1
root     pts/0        Sun Aug  7 15:08 - 15:08  (00:00)    ispnet-logan-181.ispnet.net
reboot   system boot  Sun Aug  7 14:46          (22:56)    0.0.0.0
smith    pts/1        Sat Aug  6 11:13 - 12:05  (00:51)    ip68-13-121-33.om.cox.net
smith    pts/0        Sat Aug  6 10:33 - crash (1+04:12)   ip68-13-121-33.om.cox.net
smith    pts/7        Sat Aug  6 10:21 - 10:26  (00:04)    ip68-13-121-33.om.cox.net
smith    pts/6        Thu Aug  4 23:32 - 01:44  (02:11)    ip68-13-121-33.om.cox.net
smith    pts/6        Thu Aug  4 19:49 - 19:49  (00:00)    136.48.111.1
smith    pts/6        Thu Aug  4 17:33 - 17:35  (00:01)    136.48.111.33
smith    pts/1        Tue Aug  2 17:05 - 09:58 (1+16:52)   136.48.111.1
root     pts/1        Tue Aug  2 16:02 - 16:04  (00:01)    somecorp.com
don      pts/6        Tue Aug  2 14:29 - 15:27  (00:58)    somecorp.com
don      pts/6        Tue Aug  2 13:44 - 14:06  (00:21)    somecorp.com
don      pts/1        Tue Aug  2 12:04 - 14:33  (02:29)    somecorp.com
root     pts/1        Mon Aug  1 20:15 - 20:35  (00:19)    dns2.ispnet.net
root     pts/1        Mon Aug  1 18:18 - 18:36  (00:18)    dns2.ispnet.net
don      pts/1        Mon Aug  1 16:29 - 16:33  (00:04)    somecorp.com
don      pts/1        Mon Aug  1 14:33 - 14:51  (00:17)    somecorp.com
don      pts/1        Mon Aug  1 14:21 - 14:22  (00:00)    somecorp.com
don      pts/6        Mon Aug  1 13:26 - 13:54  (00:27)    somecorp.com
smith    pts/2        Mon Aug  1 13:16 - 16:21 (1+03:05)   136.48.111.1
smith    pts/2        Mon Aug  1 12:41 - 13:12  (00:30)    136.48.111.1
don      pts/7        Mon Aug  1 12:25 - 13:05  (00:40)    somecorp.com
smith    pts/2        Mon Aug  1 12:16 - 12:27  (00:11)    136.48.111.1
root     pts/6        Mon Aug  1 12:11 - 12:26  (00:15)    somecorp.com
smith    pts/2        Mon Aug  1 12:09 - 12:15  (00:06)    136.48.111.1
smith    pts/1        Mon Aug  1 11:17 - 13:57  (02:40)    136.48.135.50
smith    pts/1        Mon Aug  1 09:07 - 09:40  (00:32)    136.48.111.1
```

WTMP File(s)

- The files wtmp and btmp are only logged to if they already exist.
  - This is by design.
- If the SA wants to use them they need to be created
  - Something like: `touch /var/log/wtmp`
  - This is fairly common

What to Look For

- When you do not know the compromised account

Look For

- Log entries around the time of the intrusion
- Accounts that have become active after being dormant for long periods of time
- Logins from unexpected locations
- Logins at unusual times
- Very short login times
- Gaps in the WTMP file

Examine the History File

- Check the suspected account's history file to view the last commands run by that user account
- The history file displays the most recent commands used by that specific account
- The history file is easily disabled
- How many of you disable your history file? Pros? Cons?

Examine the History File

- The history file lives along with other ‘nice’ logging files
- Buffer overflows will not appear (nor likely the occurrence of one)
- Requires things like ‘graceful’ exits
- etc

Examine the Messages Log

- Can examine failed login attempts
- Can examine root logins
- Can examine attempts to “su” to root
- Simple greps

Don't Forget Backups

Most system administrators have weekly backups created for their systems

I.E. The crontab file actually has a variable MAILTO=root to actually mail logs to the sysadmin

"networkified logging"

Backups

- Crucial evidence may exist in backups
- At least this gives you a point to compare against
  - Manually
  - diff
  - Custom tools

Backups

- PAYNE GPG script

Examine All Files Run by "cron" and "at"

- System Administrators almost always automate the logging process
- "cron" is the utility which handles periodic execution of processes

FYI: Most anything that can be done by hand can be automatically handled by the "cron" utility at specified times

Examine All Files Run by “cron” and “at”

Hackers may use cron to periodically perform processes for them

(I.E. Mail a sniffer file, then deletes its contents)

Examine All Files Run by "cron" and "at"

- "cron" uses tables or "crontab" files to know what to do and when
- Usually there are "crontab"s for root as well as each user

Examine All Files Run by "cron" and "at"

The format for cron tables (crontab files) is:

minute hour day month

weekday username command

Field	Description	Range
Minute	Minute of the Hour	0-59
Hour	Hour of the Day	0-23
Day	Day of the Month	1-31
Month	Month of the Year	1-12
Weekday	Day of the Week	0-6

Examine All Files Run by "cron" and "at"

- Each of the time related fields can contain:
  - An "*", which matches anything
  - A single integer, which matches exactly
  - Integers separated by commas, matching all listed values
  - Two integers separated by a hyphen, which matches the specified range of values

Examine All Files Run by "cron" and "at"

minute hour day month

weekday username command

1 10 * * 1-5

"10:45 a.m., Monday Through Friday

0,30 * 13 * 5

"Every Half Hour on Friday, and every half hour on the Thirteenth of the month

Examine the "/etc/passwd" file

- The 'old style' contains the encrypted password of all users
- Is a world readable file
- If someone has attained the "/etc/passwd" file, they can run a password cracking program to inevitably determine the passwords
- Many, more secure systems use "shadowed" password files…in fact, just plain 'most systems' used this now

Examine the "/etc/passwd" file

- The etc passwd file contains seven fields separated by colons:
  - Login Name
  - Encrypted Password
  - UID Number
  - Default GID Number
  - "GECOS" or Personal Information
  - Home Directory
  - Login Shell

Examine the "/etc/passwd" file

- Look for alterations to the "/etc/passwd" file
  - A Blank or Empty password Field
  - New Accounts
  - Inappropriate GID of "0"
    - Proper way to this is…..?

mandia::144:12:Mandia Kevin, Bldg 433:/home/staff/mandia:/bin/csh

mandia:gfds5432fdsa:144:**0**:Mandia Kevin:/home/staff/mandia:/bin/csh

Examine the "/etc/passwd" file

Login ID

GID

Home Directory

mandia:gfsdafgdsa:144:12:Mandia Kevin:/home/staff/mandia:/bin/csh

Encrypted Password

UID

GECOS Info

Login Shell

Check Systems for Unauthorized Services

- Backdoor versions of finger, rsh, rlogin, ftp, and many other services are available
- One of these backdoor services may be added to the inetd as an additional and unwanted service being offered by the victim machine
- The best way to find unauthorized services is run a trusted “netstat -a” command (what does the ‘trusted’ mean)

What to Look For

Look For

- Inspect the "/etc/inetd.conf" for unauthorized additions and changes
- Look for entries that execute a shell program
- Look at the "init" files or "rc" files (i.e. /etc/rc.d/rc.local)
- Run a trusted "netstat –a" command

Check System for Trojanized Programs

- Look for evidence that rootkit was executed
- History File in hacked account shows the compiling and/or executing of the following:

-	z2	Overwrites the utmp, wtmp, and lastlog
-	Ic	Installs trojanized ifconfig utility
-	Ps	Installs trojanized ps utility
-	Ns	Installs trojanized netstat ability

Check System for Sniffer Programs

First Clue:

You usually can infer that hacker has installed a sniffer somewhere because he/she continually uses accounts with "unguessable" or "uncrackable" passwords

Check Systems for Sniffer Programs

- Run a trusted version of IFCONFIG on victim system to determine if the network adapter is running in promiscuous mode
- Look for sniffer logs (files with odd names)
- Look at the currently running processes for suspicious programs

```
find / -mtime -4 | more
find / -mtime -3 -ls | more
```

Look for "Setuid" and "Setgid" Files

A hacker who has attained access often will create private setuid shells and utilities that allow root access

What to Look For

Look For

- Look for “setuid” and “setgid” files on the system
- Focus on “setuid” copies of “/bin/sh” which allow intruders shell or root access at a later time
- Use the following commands to find “setuid” root files

  find / -perm +4000 -ls

Look For "+" Entries and Non Local Entries in Certain Files

- Check the following files (equivalents) for inappropriate host names (computers) and "+" signs
  - /etc/hosts.equiv
  - /etc/hosts.lpd
  - And all .rhosts files
- A "+" signifies all incoming connections are from trusted computers

Remote Commands

- There are a number of commands for executing commands on remote hosts
  - rlogin
  - rsh
  - rcp
  - rcmd

Remote Commands

- The client needs to have an account on the host where the command will be executed
- Thus rlogin, rsh, rcmd, and rcp perform an authorization procedure unless…

There is an entry in the /etc/hosts.equiv file or a users .rhosts file

Remote Commands

People use .rhosts and hosts.equiv files when they frequently have to log into other machines on the LAN, and they want to relax authentication checks for themselves and other specific users

hosts.equiv

This file is used to disable authentication and lists machines (and user IDs) trusted by the computer

rhosts

If a user has a .rhost file in his home directory, it allows him (or others) to run programs on that machine remotely

rhosts

.rhost file on satcom.fbiclass.net

mandiak,cs.lafayette.edu kmandia

foobar.cs.harvard.edu speedy

These lines mean you could run a program on mandiak.cs.lafayette.edu and have the output go to satcom.fbiclass.net without ever logging on

SSH

- Many of these ‘remote’ commands have been replaced with SSH / SCP sessions and scripts
- ..but the remote tools usually still exist and can be used

Looking for Unusual or Hidden Files

- Intruders may attempt to conceal their presence by hiding files and directories

"…"	(dot dot dot)
". . "	(dot dot space)
". . ^G"	(dot dot cntrl-G)
".test"	
".sh"	
" "	(" <alt>32 ")

Looking for Unusual or Hidden Files

- Look at files created / modified since the time of the first known intrusion

```
find / -mtime n -ls
```

where n = the number of days prior to the present time

Reviewing All Processes Currently Running on the System

- The *ps* command on most Unix systems is the tool used to monitor processes
- The output of the *ps* command allows you to determine:
  - What processes are running on your system
  - How much CPU time and memory these processes are using
  - Who owns each process

Reviewing All Processes Currently Running on the System

ps -aux

USER	PID	%CPU	%MEM	VSZ	RSS	TT	STAT	START	TIME	COMMAND
root	137	5.5	0.0	3832	2140	co	S	7:22PM	3:54.12	**talkd**
mandia	144	3.0	0.0	172	16	p0	S	7:22PM	0:00.00	(xterm)
root	0	0.0	0.0	0	0	??	DLs	7:10PM	0:00.06	(swapper)
Mandia	43	33.0	0.0	160	112	p0	0	7:20PM	6.01.45	progx
root	66	0.0	0.0	228	152	??	I	7:21PM	0:00.23	cron

The ps -aux provides a detailed overview of processes running on the system

What to Look For

- Use the *ps* command to identify:
  - Hung Processes
    - User Processes Using Excess CPU Time
    - System Processes Gone Berserk
  - Unidentifiable Processes (Unusual Names)
    - Possible Evidence of Unauthorized Activity
  - Unusual Start Times
  - A process that uses an extremely high % of CPU time - sniffer

Reviewing All Processes Currently Running on the System

% ps -aux (Hung Processes)

USER	PID%	CPU	%MEM	VSZ	RSS	TT	STAT	START	TIME	COMMAND
root	137	5.5	0.0	3832	2140	co	S	7.22PM	3:54.12	talkd
mandia	144	3.0	0.0	172	16	p0	S	7:22PM	0:00.00	(xterm)
root	0	0.0	0.0	0	0	??	DLs	7:10PM	0:00.06	(swapper)
mandia	43	0.0	0.0	160	112	p0	O	7:20PM	6.01.45	progx
root	66	0.0	0.0	228	152	??	I	7:21PM	0:00.23	cron
root	1532	0.0	0.0	332	224	pa	R+	7:46PM	0:00.04	ps -aux

Reviewing All Processes Currently Running on the System

% ps -aux (Unidentifiable Processes)

USER	PID%	CPU	%MEM	VSZ	RSS	TT	STAT	START	TIME	COMMAND
root	137	5.5	0.0	3832	2140	co	S	7.22PM	3:54.12	talkd
mandia	144	3.0	0.0	172	16	p0	S	7:22PM	0:00.00	(xterm)
root	0	0.0	0.0	0	0	??	DLs	7:10PM	0:00.06	(swapper)
root	43	0.0	0.0	160	112	??	S	7:20PM	0:07.22	/bin/ .z
root	66	0.0	0.0	228	152	??	I	7:21PM	0:00.23	cron
root	1532	0.0	0.0	332	224	pa	R+	7:46PM	0:00.04	ps -aux

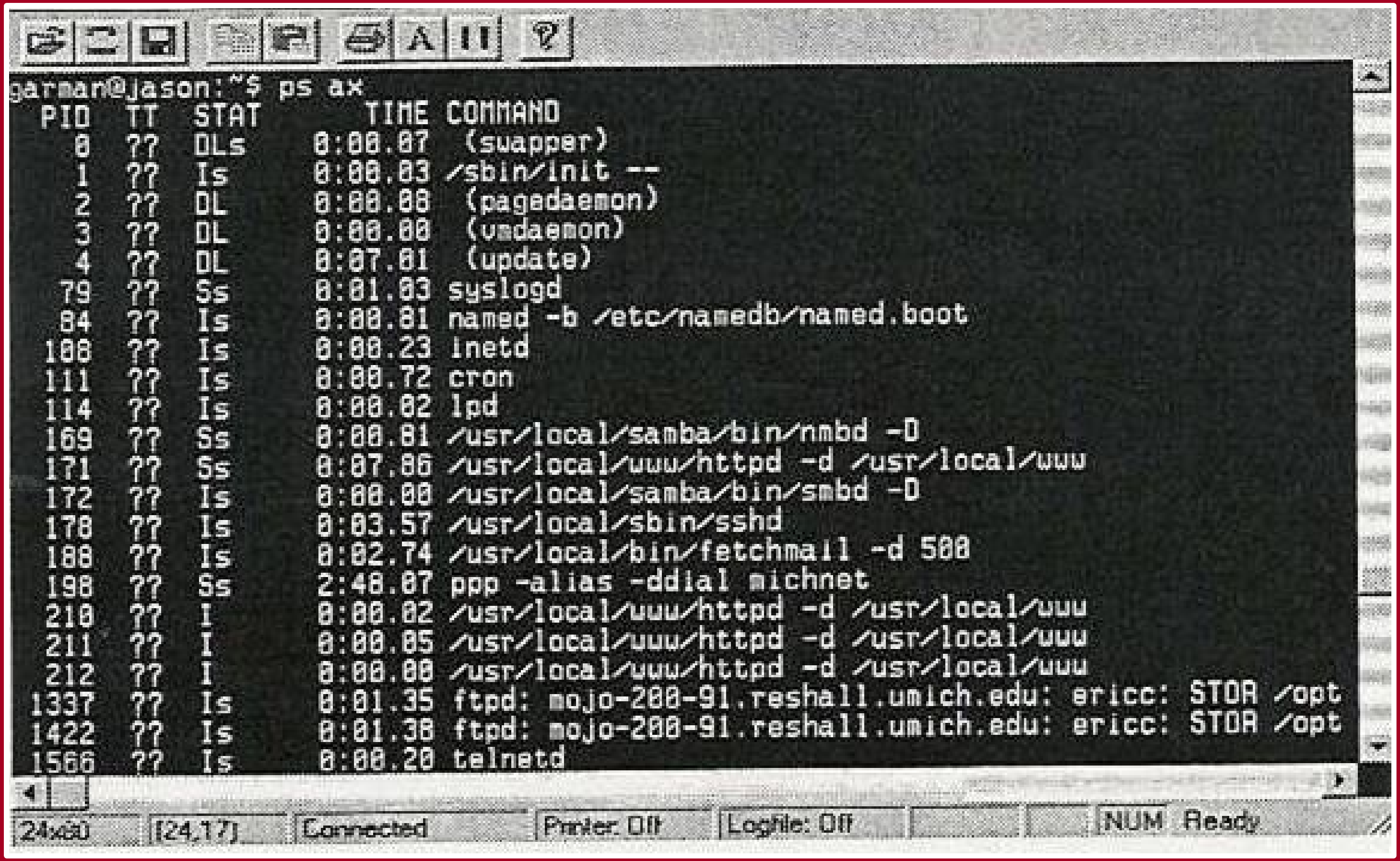
Points to Note

- Compromised systems have been found to contain trojanized versions of “ps” which does not display the intruder’s processes
- Trojanized “ps” is commonly installed by running a Rootkit

Points to Note

- Intruders also run sniffer programs under names such as “sendmail” and “inetd”, making them hard to find when scanning the output of “ps”

Reviewing All Processes Currently Running on the System



*Ten Steps to Take After Intrusions (**Recap**)*

1. Examine Log Files and Backups
2. Examine All Files Run by "cron" and "at"
3. Examine the "/etc/passwd" File for Alterations
4. Check Systems for Unauthorized Services
5. Check Systems for Sniffer Programs
6. Check Systems for Trojanized Programs
7. Look for "setuid" and "setgid" Files
8. Look for "+" Entries and Non Local Host Names in Certain Files
9. Look for Unusual and Hidden Files
10. Review All Processes Currently Running on System

NUCIA

Your Key to Security

Windows

Ask the admin….

2. What happened?
3. What actions did you take after you noticed the intrusion?
4. Have you enabled audit logging?
   - How much logging?
   - How long are the logs kept?
4. Do you have back-ups?

Windows

1. Who has Administrator privileges?
2. What was the latest Service Pack you installed?
3. What Hot-Fixes have you installed?
4. What Internet Services do you offer? (internet exposure)
5. Is the attacked system a Primary Domain Controller, member

Windows Logs

- There are three standard NT Logs
  - APPEVENT.EVT Application log
  - SECEVENT.EVT Security log
  - SYSEVENT.EVT System log
- Logs are usually stored in the directory: **C:\WINNT\System32\config**

Your Key to Security

Event Viewer

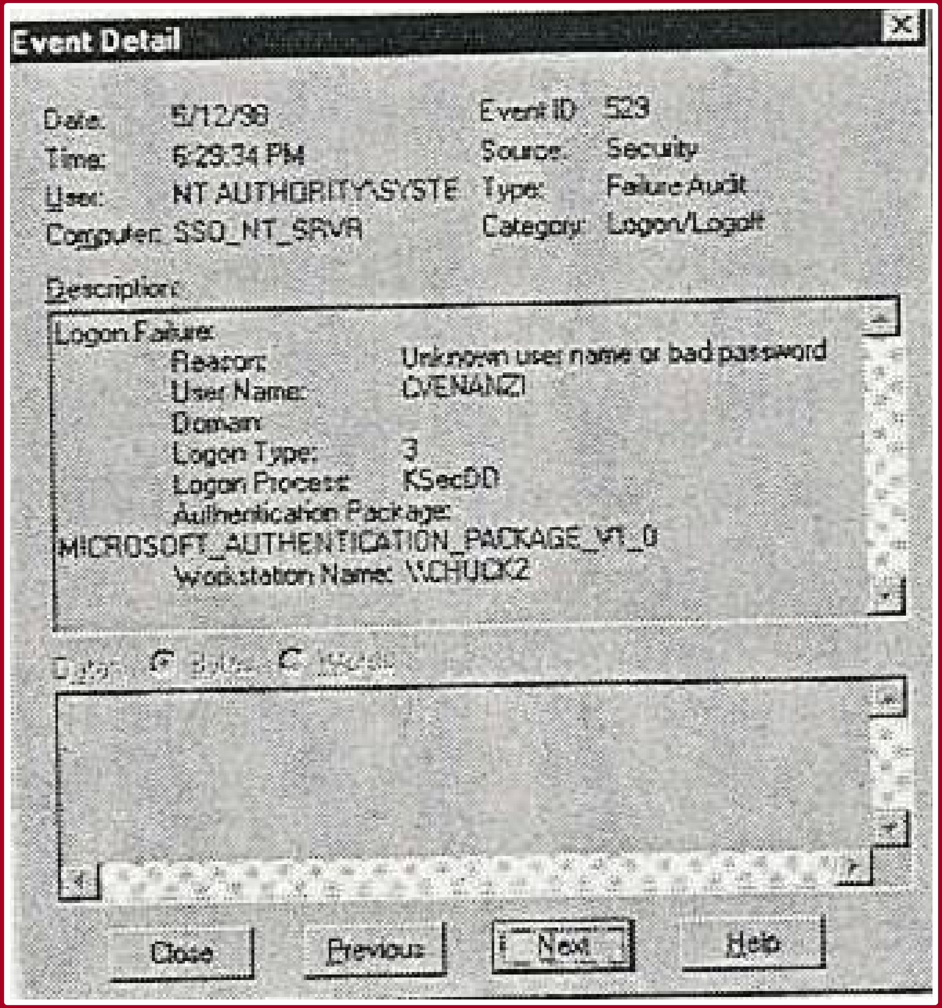
Event Viewer - Security Log on \\SSO_NT_SRVR

Log View Options Help

Date	Time	Source	Category	Event	User	Computer
5/13/98	8:09:29 PM	Security	Detailed Tracking	592	crose	SSO_NT_SRVR
5/13/98	8:09:01 PM	Security	Detailed Tracking	592	crose	SSO_NT_SRVR
5/13/98	8:08:47 PM	Security	Detailed Tracking	593	crose	SSO_NT_SRVR
5/13/98	8:08:36 PM	Security	Detailed Tracking	592	crose	SSO_NT_SRVR
5/13/98	8:08:13 PM	Security	Detailed Tracking	593	SYSTEM	SSO_NT_SRVR
5/13/98	8:08:13 PM	Security	Detailed Tracking	592	SYSTEM	SSO_NT_SRVR
5/13/98	8:07:25 PM	Security	Detailed Tracking	593	crose	SSO_NT_SRVR
5/13/98	8:07:23 PM	Security	Detailed Tracking	592	crose	SSO_NT_SRVR
5/13/98	8:07:22 PM	Security	Detailed Tracking	592	crose	SSO_NT_SRVR
5/13/98	8:06:44 PM	Security	Detailed Tracking	593	SYSTEM	SSO_NT_SRVR
5/13/98	8:06:44 PM	Security	Detailed Tracking	592	SYSTEM	SSO_NT_SRVR
5/13/98	8:05:19 PM	Security	Detailed Tracking	593	SYSTEM	SSO_NT_SRVR
5/13/98	8:05:18 PM	Security	Detailed Tracking	592	SYSTEM	SSO_NT_SRVR
5/13/98	8:05:18 PM	Security	Detailed Tracking	593	SYSTEM	SSO_NT_SRVR
5/13/98	8:05:18 PM	Security	Detailed Tracking	592	SYSTEM	SSO_NT_SRVR
5/13/98	8:04:22 PM	Security	Detailed Tracking	593	SYSTEM	SSO_NT_SRVR
5/13/98	8:04:22 PM	Security	Detailed Tracking	592	SYSTEM	SSO_NT_SRVR
5/13/98	8:03:32 PM	Security	Detailed Tracking	593	SYSTEM	SSO_NT_SRVR
5/13/98	8:02:56 PM	Security	Detailed Tracking	593	SYSTEM	SSO_NT_SRVR
5/13/98	8:02:56 PM	Security	Detailed Tracking	592	SYSTEM	SSO_NT_SRVR
5/13/98	8:02:56 PM	Security	Detailed Tracking	593	SYSTEM	SSO_NT_SRVR
5/13/98	8:02:56 PM	Security	Detailed Tracking	592	SYSTEM	SSO_NT_SRVR
5/13/98	8:02:56 PM	Security	Detailed Tracking	592	SYSTEM	SSO_NT_SRVR
5/13/98	8:00:11 PM	Security	Detailed Tracking	593	SYSTEM	SSO_NT_SRVR
5/13/98	8:00:11 PM	Security	Detailed Tracking	592	SYSTEM	SSO_NT_SRVR
5/13/98	7:55:54 PM	Security	Detailed Tracking	593	SYSTEM	SSO_NT_SRVR
5/13/98	7:55:54 PM	Security	Detailed Tracking	592	SYSTEM	SSO_NT_SRVR
5/13/98	7:54:23 PM	Security	Detailed Tracking	593	SYSTEM	SSO_NT_SRVR
5/13/98	7:54:23 PM	Security	Detailed Tracking	592	SYSTEM	SSO_NT_SRVR
5/13/98	7:52:49 PM	Security	Detailed Tracking	592	SYSTEM	SSO_NT_SRVR
5/13/98	7:48:35 PM	Security	Privilege Use	576	bdykstra	SSO_NT_SRVR
5/13/98	7:48:35 PM	Security	Logon/Logoff	528	bdykstra	SSO_NT_SRVR

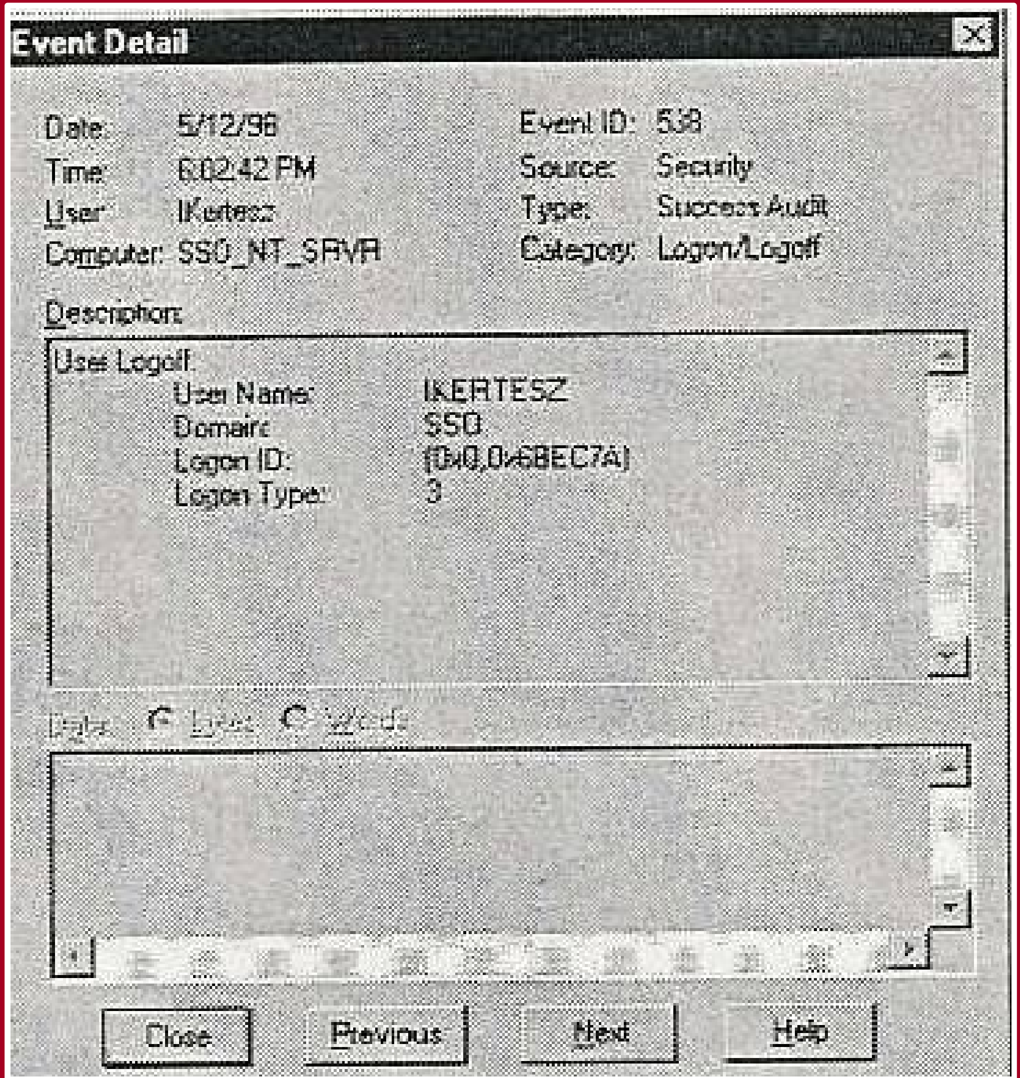
Things to Look For In NT Logs

Hacker-type break-in using random passwords



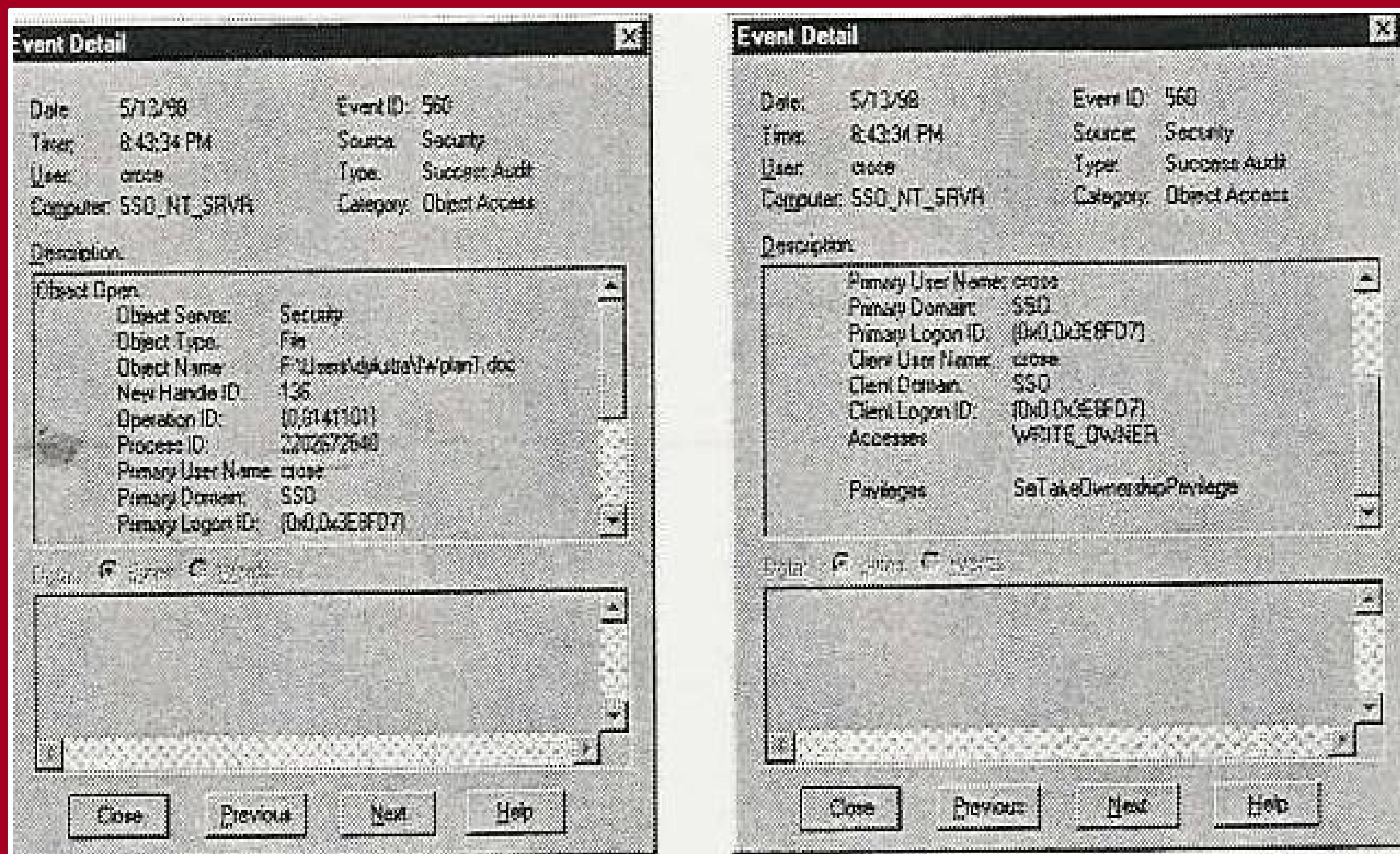
Things to Look For In NT Logs

Break-in using a stolen account



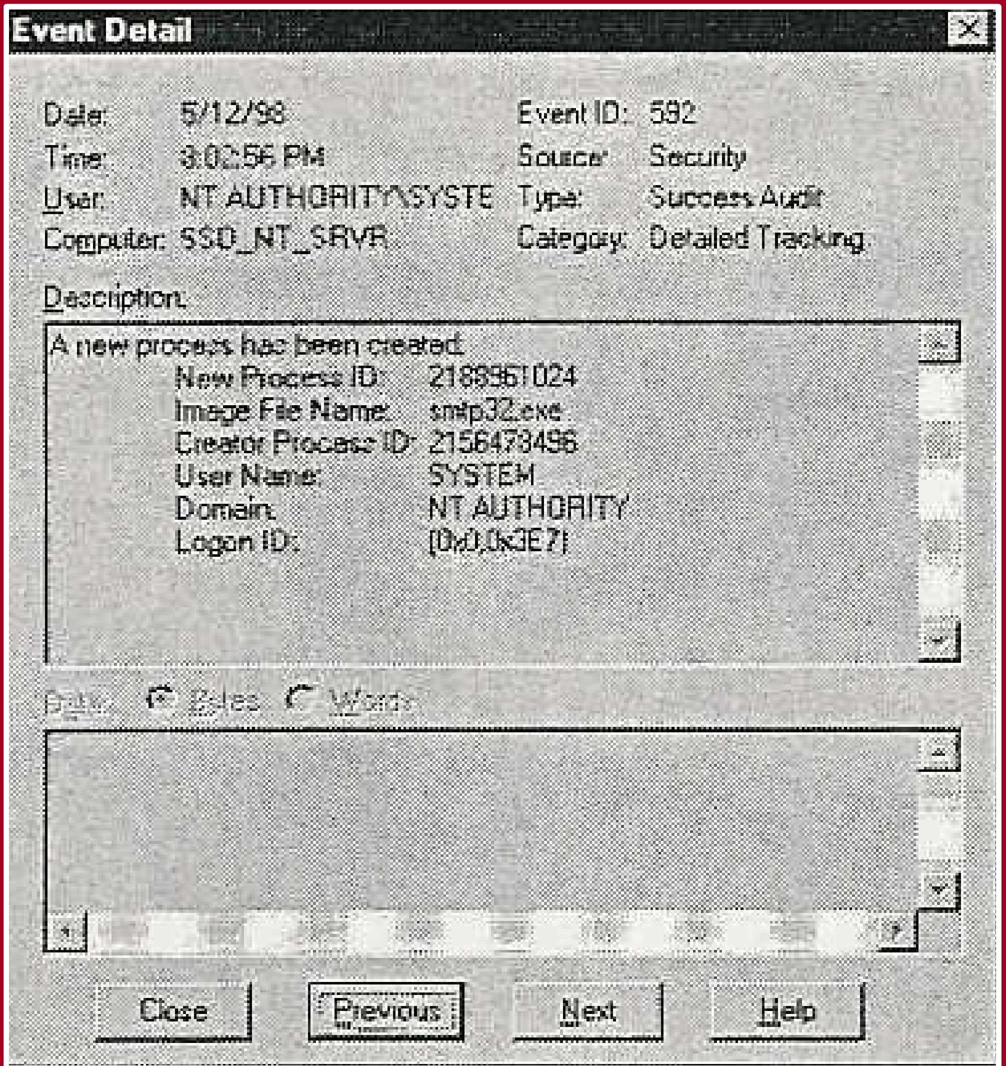
Things to Look For In NT Logs

Misuse of administrative privileges by an authorized user

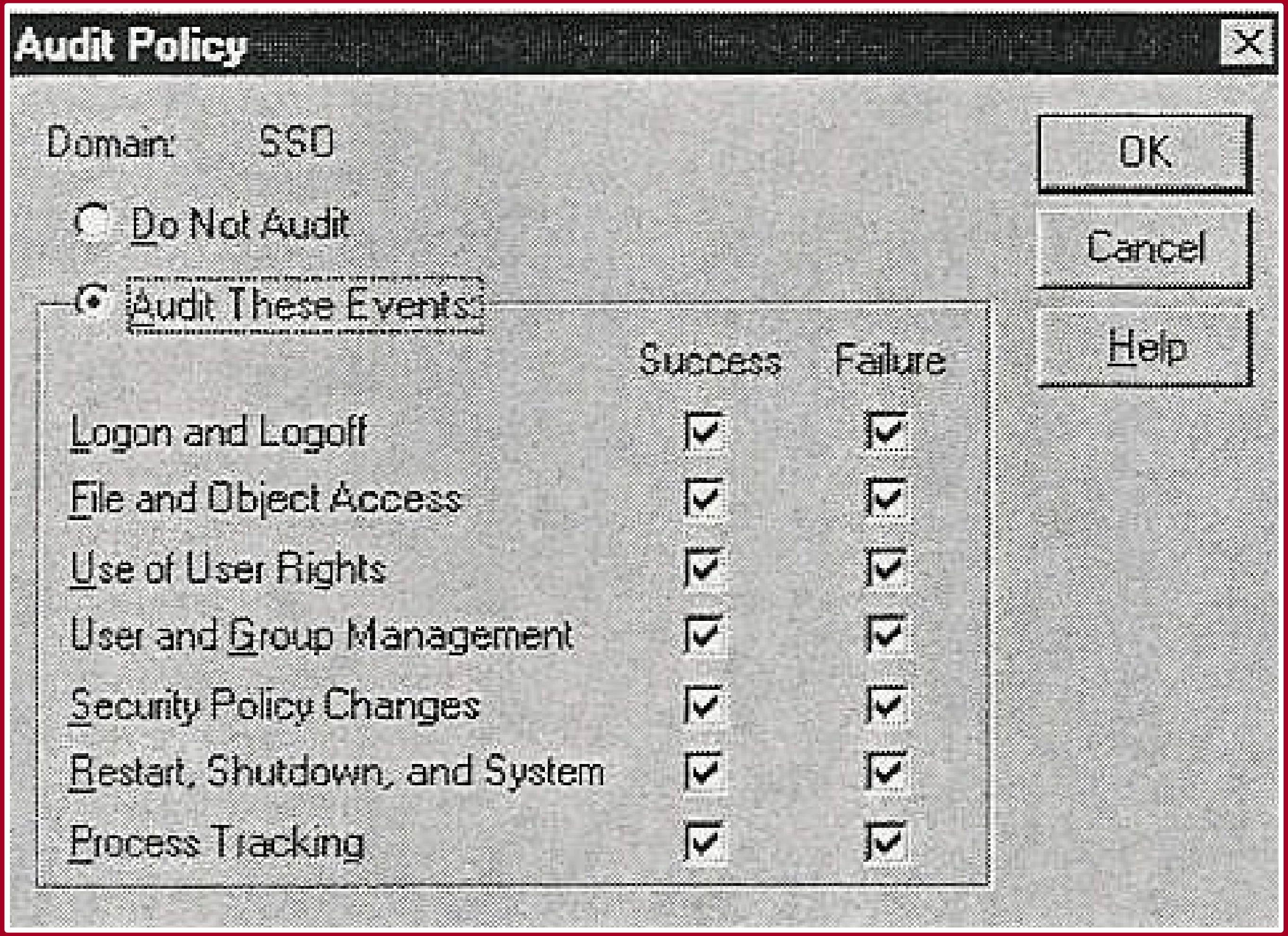


Things to Look For In NT Logs

Running system processes

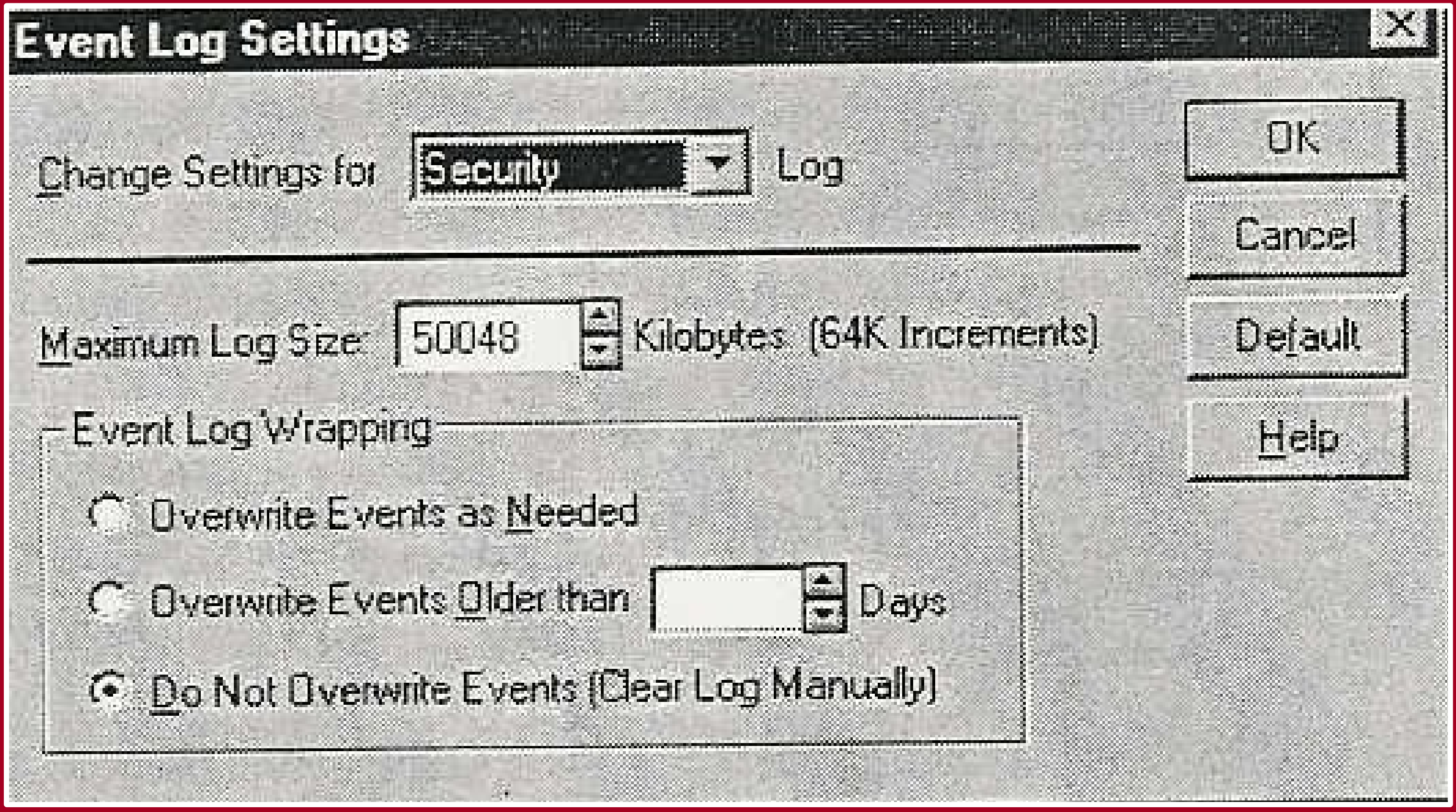


The NT Audit Policy



NT Audit Log Settings

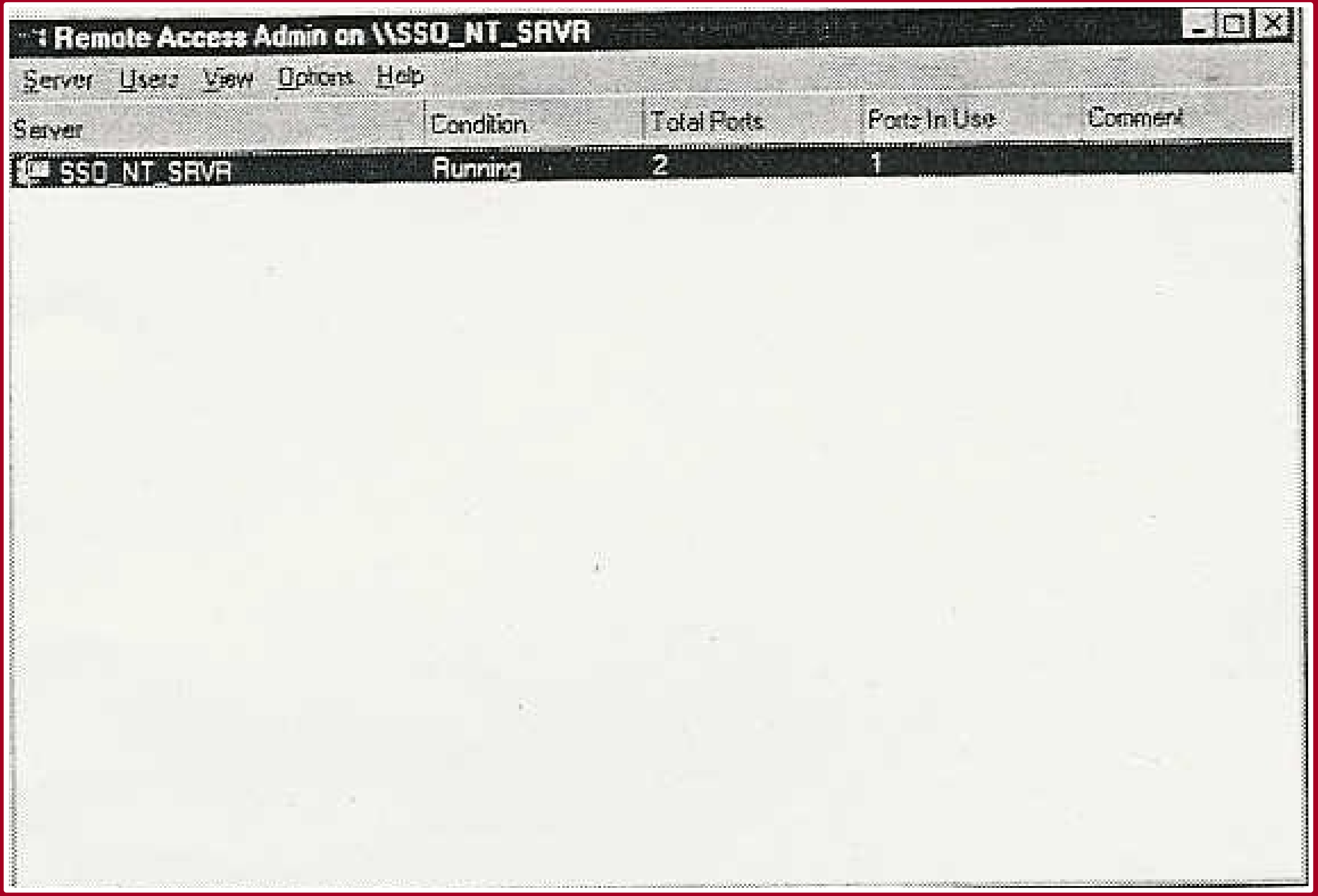
The default log size is 512k with Overwrite Events Older than 7 Days



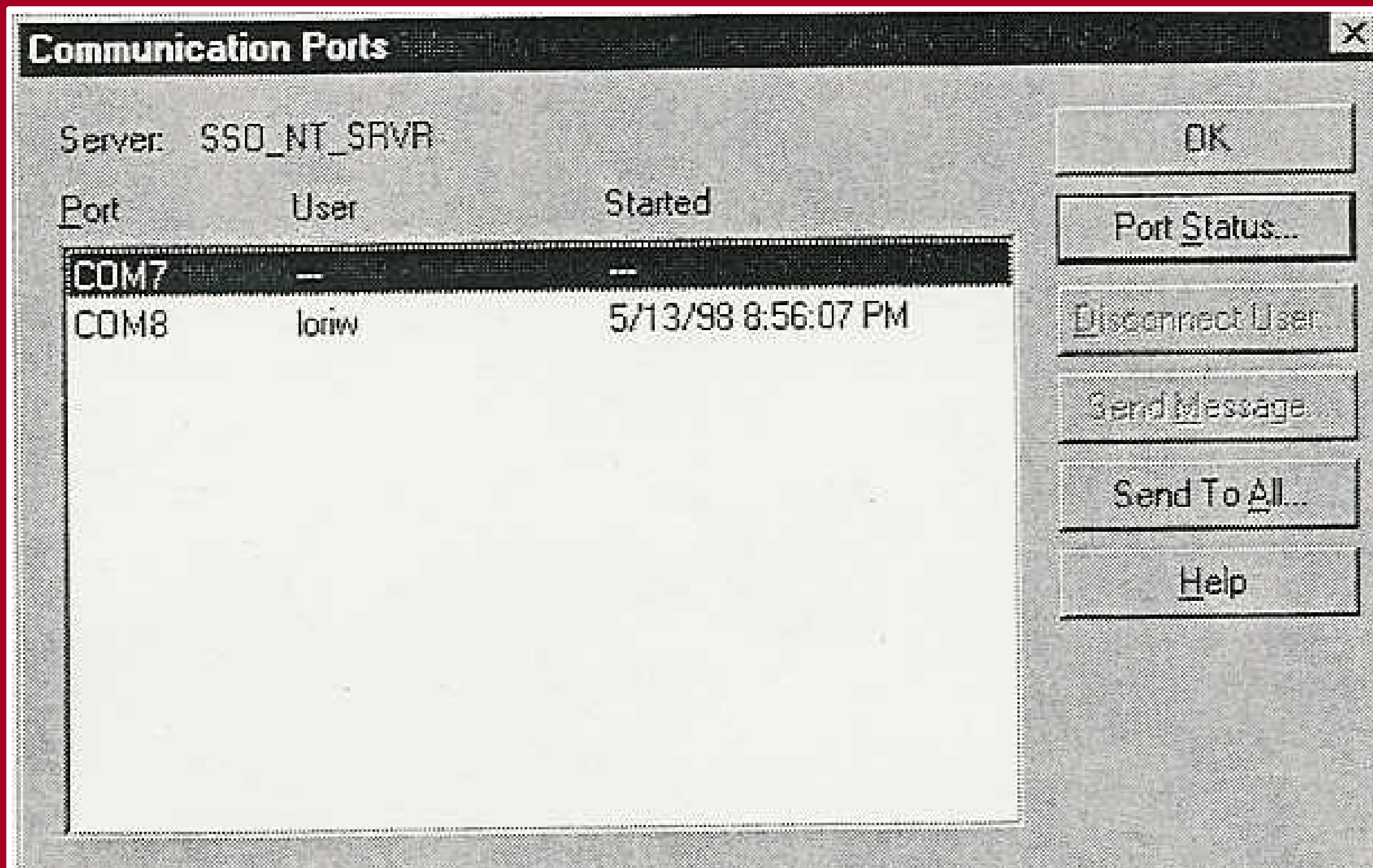
Other Useful Functions

- Remote Access Administrator
- Performance Monitor
- The NET Commands
- ARP

Remote Access Administrator

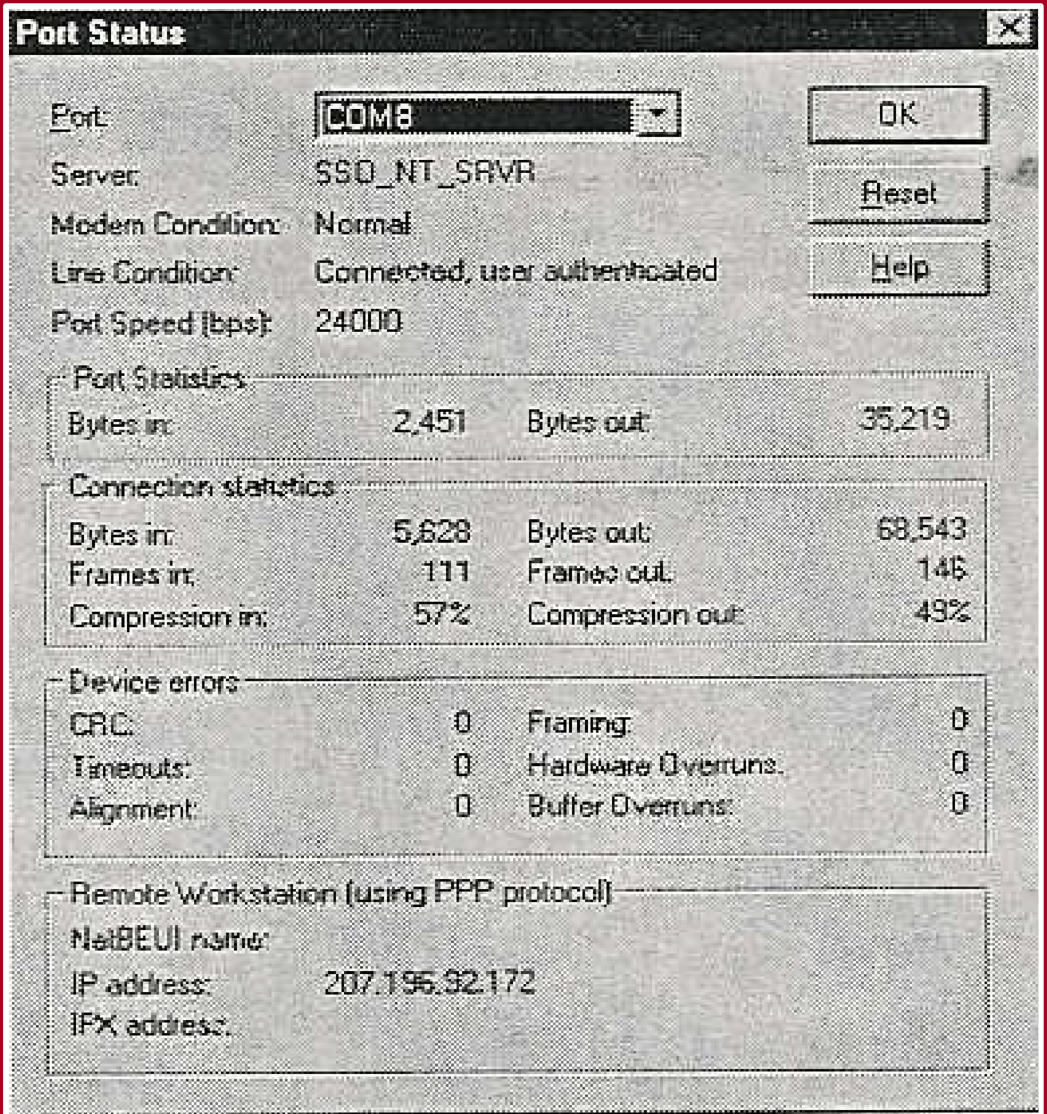


Remote Access Administrator

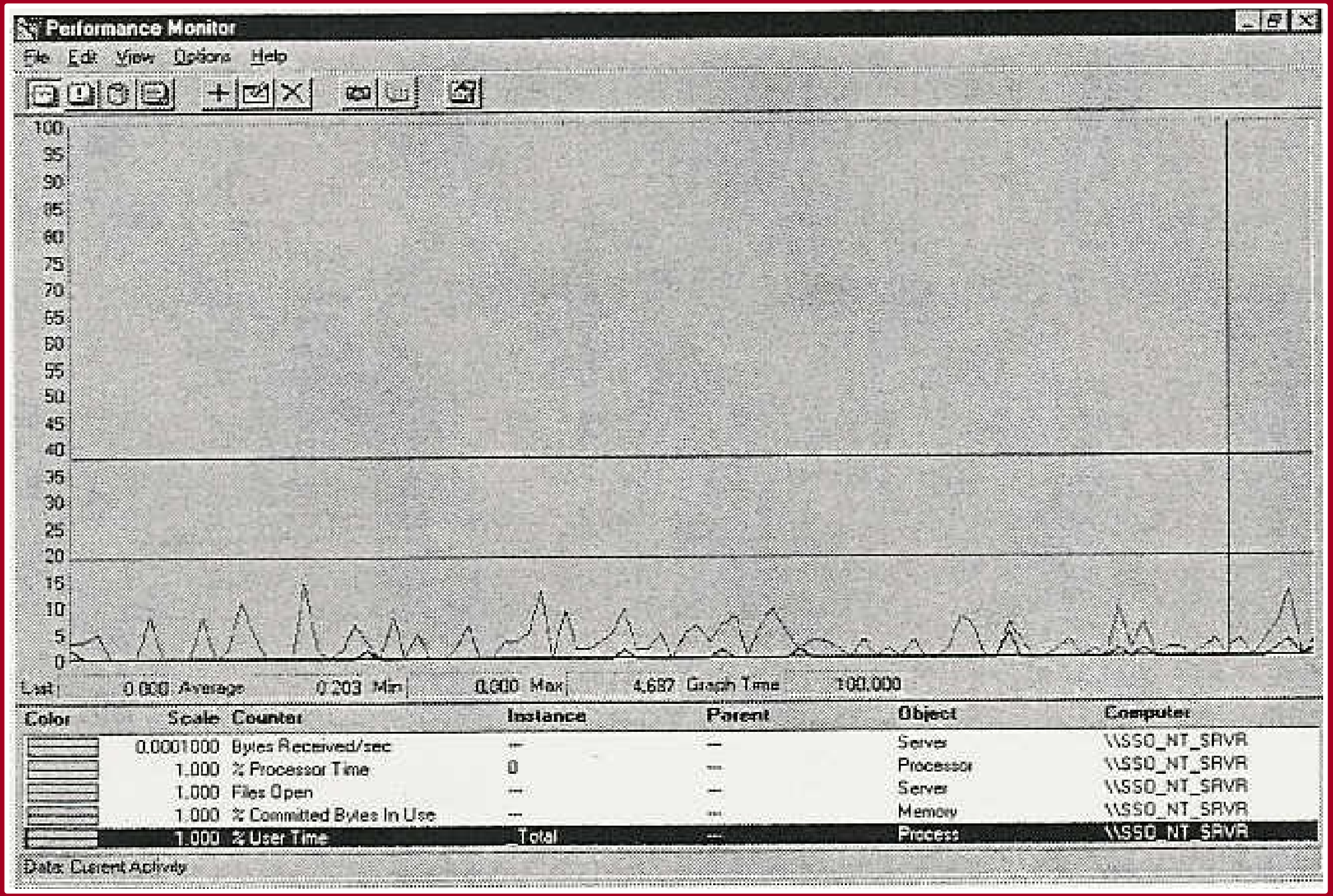


Remote Access Administrator

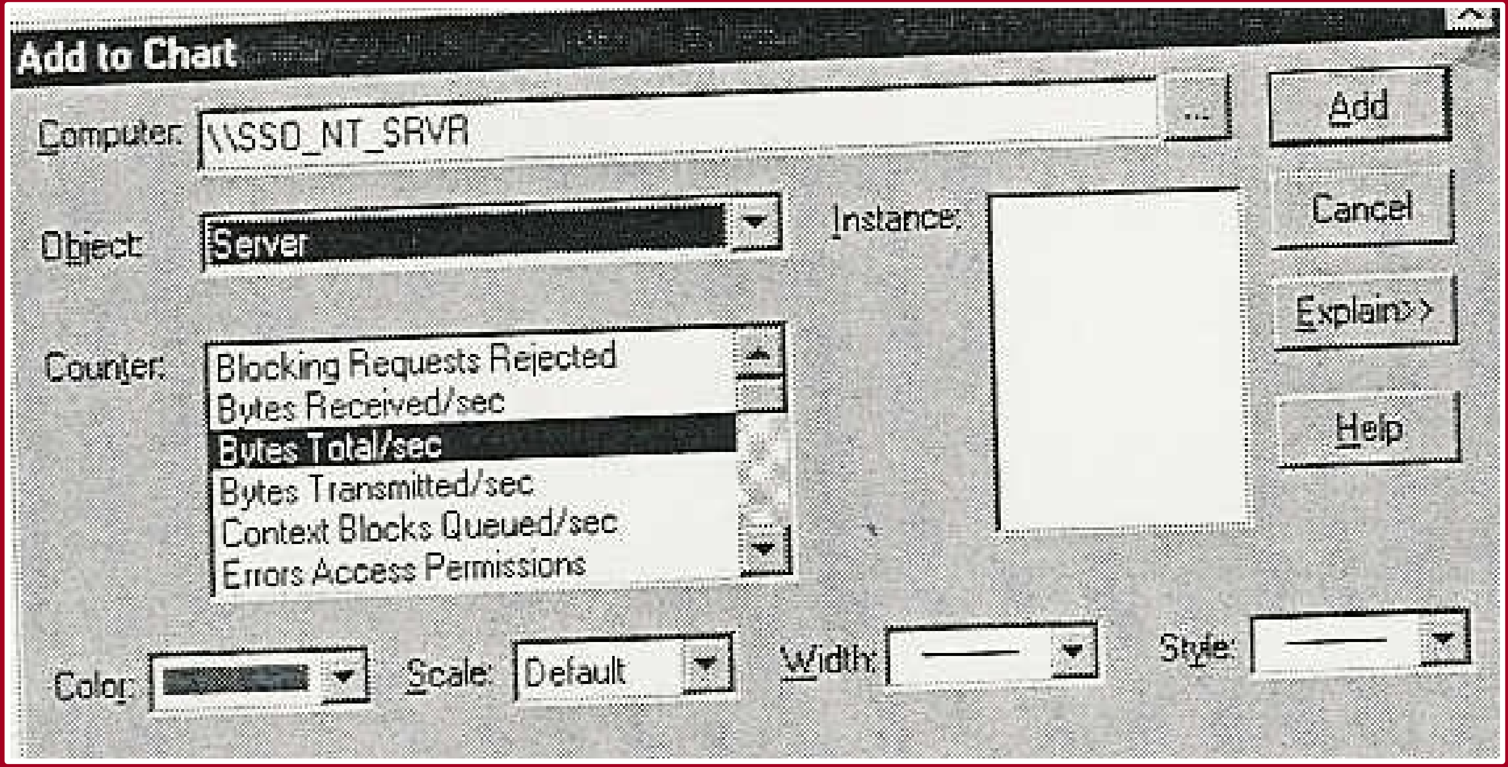
Also displayed in The SYSTEM log



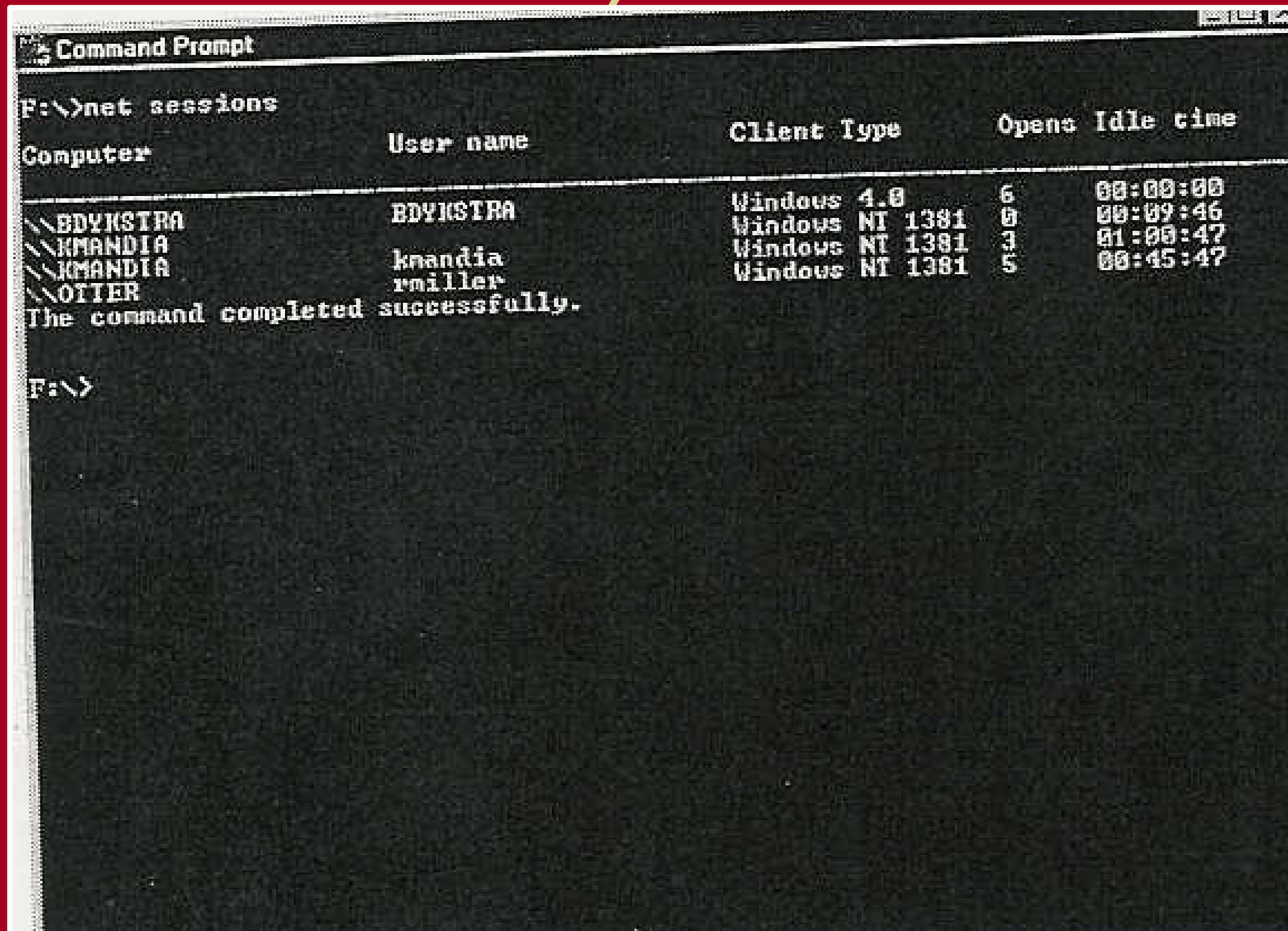
Performance Monitor



Setting Performance Monitor



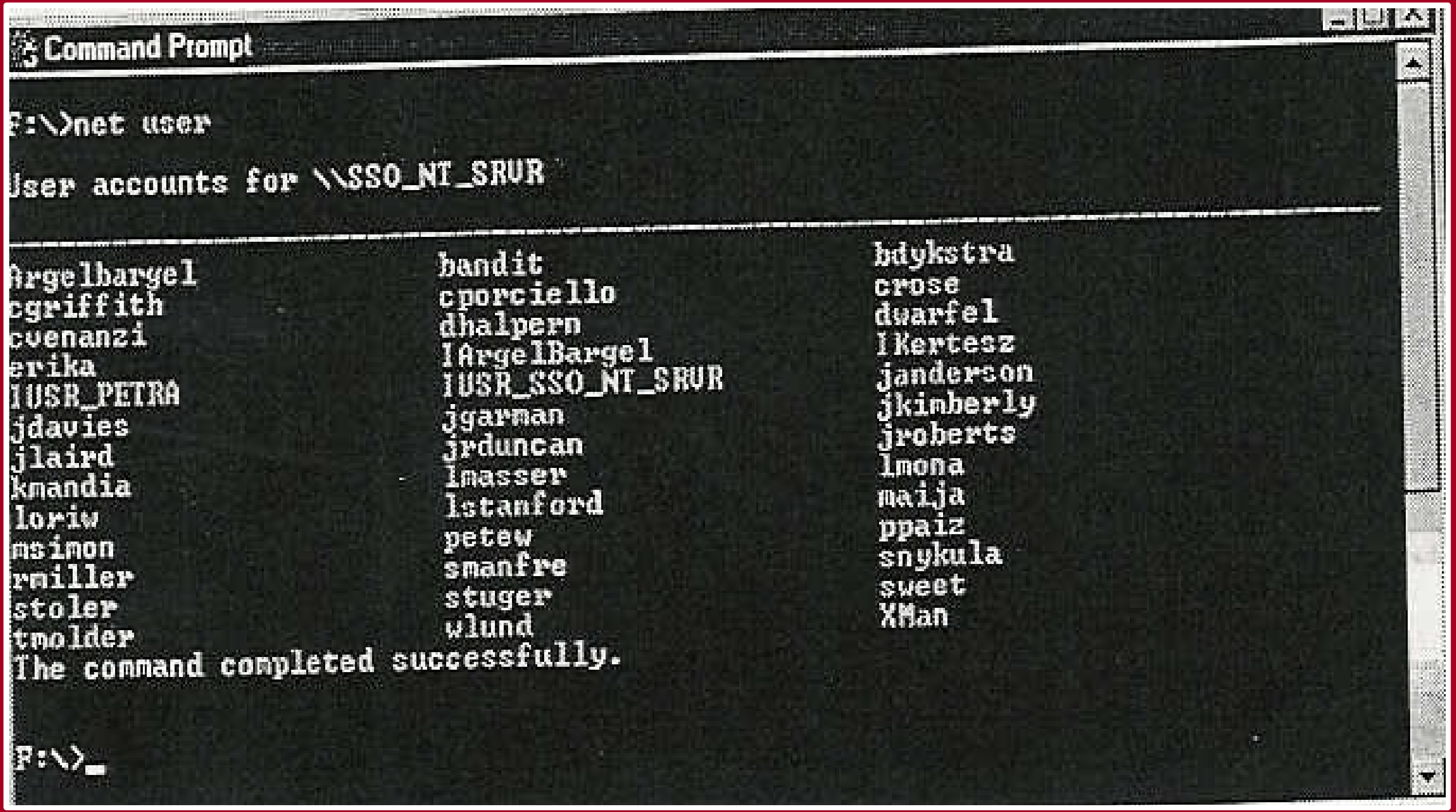
Viewing Active Systems



NET SHARE Command

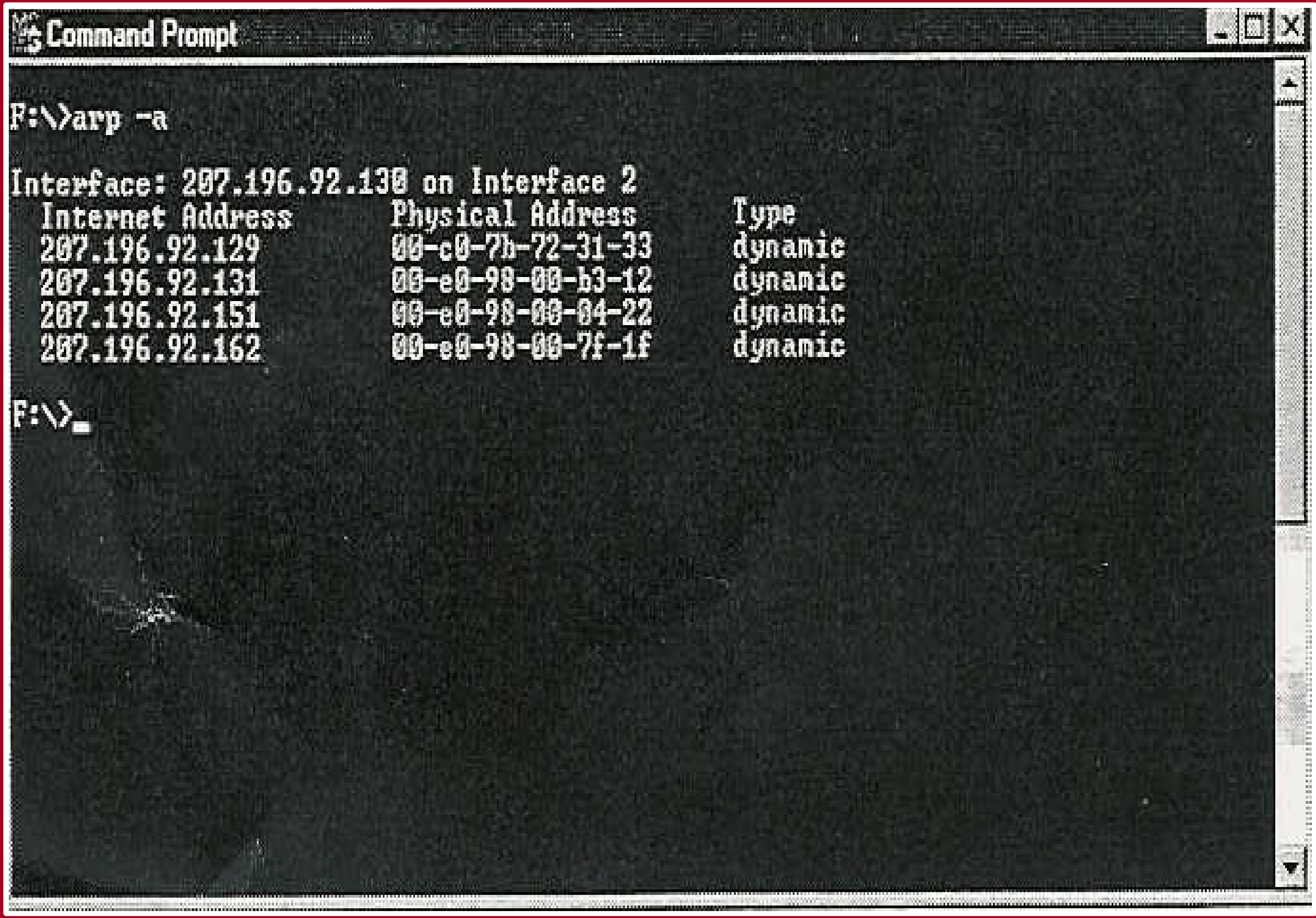
```
Command Prompt
                                                            Remote IPC
IPC$                                                        Default share
F$            F:\                                           Default share
C$            C:\                                           Remote Admin
ADMIN$        C:\WINNT
REPL$         C:\WINNT\system32\Repl\Export
D$            D:\                                           Default share
print$        C:\WINNT\system32\spool\drivers               Printer Drivers
A             A:\
crose         F:\Users\crose
davies        F:\Users\davies
dykstra       F:\Users\dykstra
E             E:\
erika         F:\Users\erika
ftp           D:\ftp
garman        F:\Users\garman
halpern       F:\Users\halpern
iwce          D:\iwce
kertesz       F:\Users\ikertesz
laird         F:\Users\laird
maija         F:\Users\maija
mandia        F:\Users\mandia
manfre        F:\Users\manfre
masser        F:\Users\masser
miller        F:\Users\miller
molder        F:\Users\molder
NETLOGON      C:\WINNT\system32\Repl\Import\S Logon server share
OSI           D:\OSI Class
simon         F:\Users\simon
stanford      F:\Users\stanford
sweet         F:\Users\sweet
venanzi       F:\Users\venanzi
warfel        F:\Users\warfel
wells         F:\Users\wells
woehler       F:\Users\woehler
wood          F:\Users\wood
LexLaser      207.196.92.141          Spooled   Lexmark Optra R Plus Series
LexmarkO      LexmarkSC               Spooled   Lexmark Optra SC 1275
The command completed successfully.

F:\>
```

Viewing All NT Accounts



```
Command Prompt

F:\>net user

User accounts for \\SSO_NT_SRVR

-------------------------------------------------------------------------------
Argelbargel              bandit                   bdykstra
cgriffith                cporciello               crose
cvenanzi                 dhalpern                 dwarfel
erika                    IArgelBargel             IKertesz
IUSR_PETRA               IUSR_SSO_NT_SRVR         janderson
jdavies                  jgarman                  jkimberly
jlaird                   jrduncan                 jroberts
kmandia                  lmasser                  lmona
loriw                    lstanford                maija
msimon                   petew                    ppaiz
rmiller                  smanfre                  snykula
stoler                   stuger                   sweet
tmolder                  wlund                    XMan
The command completed successfully.

F:\>_
```

Address Resolution Protocol



ISO Reference Model vs. TCP/IP

• Application	Application
• Presentation	
• Session	
• Transport	H to H Transport
• Network	Internet
• Data Link	Network Interface
• Physical	

TCP/IP Protocol Suite

- Application – FTP, HTTP, SMTP
- Host to Host Transport – TCP, UDP
- Internet – IP, ICMP
- Network Interface – Ethernet, Token Ring, X.25.

References

- Sytex Corp
- Incident Response and Computer Forensics; Mandia, Kevin.