Sources of Evidence

- Slack, Free, Swap, Recycle Bin
- Event logs
- Registry
- Application files, temp files
- E-mail
- Browser history and cache
- Spool

Procedure

- Review logs (jobs run, logins, processes started, etc)
- Search suspected areas with criteria defined by criminal suspicions
- Identify unauthorized accounts
- Identify unauthorized access

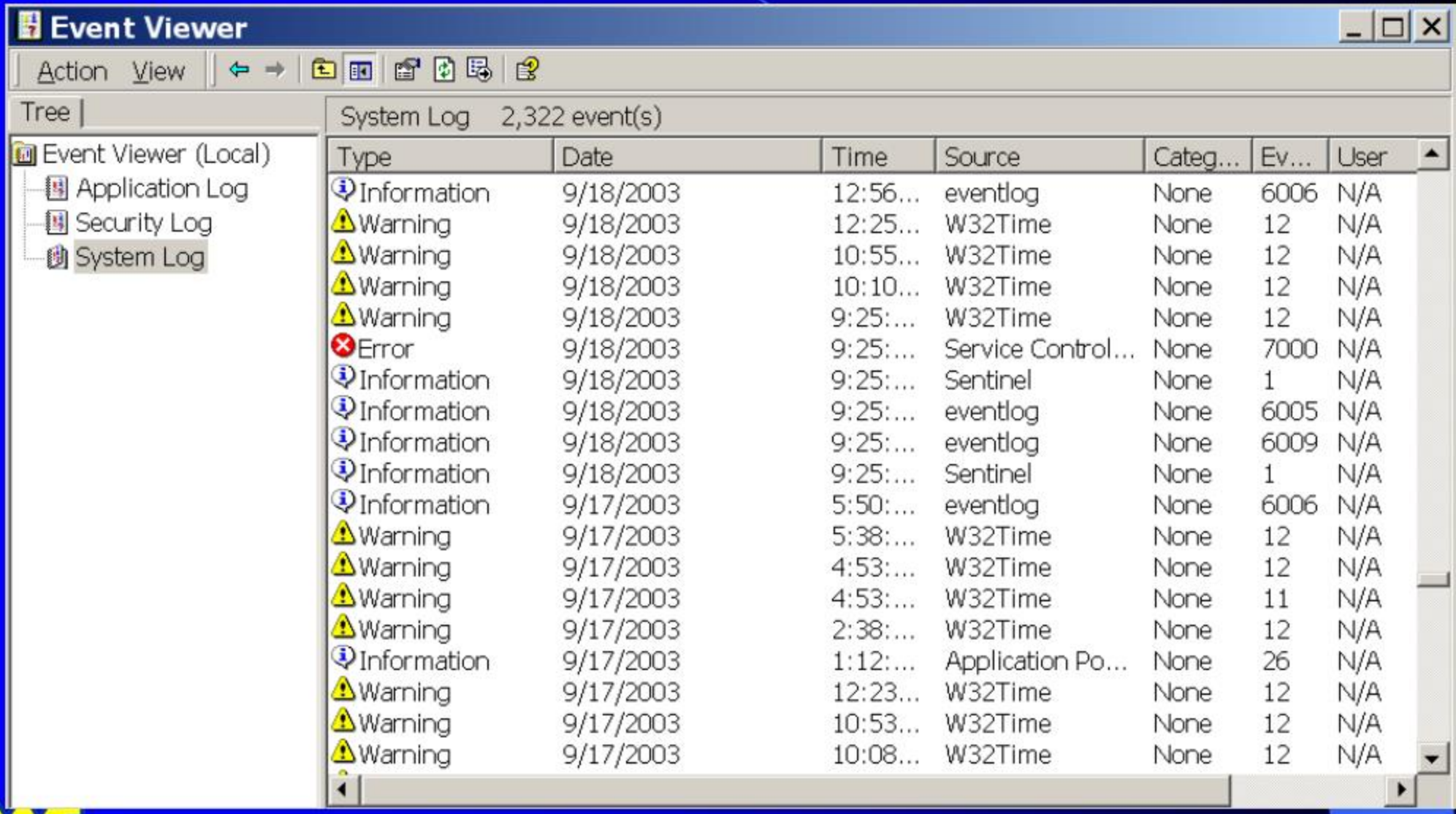
Log Files

- Start → Settings → Control Panel → Administrative Tools → Event Viewer
- View the Application Log, Security Log, and System Log
- Ex. Application Log
  - App installation, updates, Services started (backup, copy, Anti-virus, file system check, Defrag,) etc

Log Files

- Ex. System Log
  - Plugging in a device like USB thumb drive, stopping a service like Event log, print notification from spooler time and job size, network logon, automatic update notices, bad blocks on disk, etc.

System Log Example



Setting the System to Monitor

- Start → Settings → Control Panel → Administrative Tools → Local Security Policy
- Turn on (by default they are off!) Security Settings→ Local Policies → Audit Policy
  - Audit logon events
  - Audit object access
  - Audit process tracking

Setting the System to Monitor

- Corporate policies may permit you to monitor an employee's use of the computer thus, if there is any suspicion.

Offline examination of Log files

- Requires copies of the files from the suspect computer
  - AppEvent.Evt
  - SecEvent.Evt
  - SysEvent.Evt

  Contained in C:\WINNT\system32\config
- They can be viewed in the forensic workstation's Event Viewer by opening the log files extracted above.

Performing Keyword Searches

- Use tools (e.g. from NTI http://www.forensics-intl.com/intro.html) for harvesting various important areas (slack, free, swap, etc.) into files
- Look in them (use a narrow window to be legal) for codewords, relevant words in the crime context, names, etc.

Performing Keyword Searches

- Prioritize search words, and use tighter criteria to get fewer hits
- Use Viewers like Quick View Plus that can look inside many file types without being fooled by the extension

Further Detective Work

- Firewalls (particularly software firewalls on hosts, like Zone Alarm) leave all traces of connections
- Useful to determine who connected to what application when and transferred how many bytes

Further Detective Work

- Files changed during the time of such connections should be looked at carefully for evidence (time-stamps)
- You may pick up the presence of a Virus, and if it is in a directory like C:\Inetpub\scripts it may indicate a Web server hack took place.

E-mail Files

- They are files with proprietary formats
- In Netscape
  - each mail folder is stored as a single file (could be 100's of MBs)
  - Find these in \Program Files\Netscape\Users\<*User Account*>\Mail
  - The file names are Inbox and Sent . View them using Messenger

E-mail Files

- In Outlook
  - Find the mail in \Documents and Settings\<*User Account*>\Local Settings\Application Data\Microsoft\Outlook
  - The *.pst files contain the archives of all the folders of Outlook data for each user account
  - View them using the Outlook Client with Select File → Open → Personal Folders and point to the .pst file you want.

Deleted Files

- Use a good 'undelete' application like Norton or File Scavenger to recover deleted files
- You have to do it sooner so the areas released by deletion are not re-used
- Look at the *.temp files
- Look at backup tapes to discover what may have been deleted; that provides clues

Registry – a database of all that is installed

- Evidence of suspicious software installed can be found here
- E.g., Steg tools, password cracking tools, sniffer programs, etc

Registry – a database of all that is installed

- Use Regedit to view the Registry. Import the Registry Hive files from C:\WINNT\System32\Config
- Look for any uninstalls because App Uninstalls do not clean the Uninstall sub key in My Computer\HKEY_LOCAL_MACHINE\SOFTWARE

Network Forensics

- NF is the process of finding the evidence of unauthorized activity by
  - examining network traffic and
  - Looking at the activity traces left on a computer (server usually) after a break-in has occurred
- NF includes
  - Post facto analysis of transaction logs
  - Real-time analysis by network monitoring with Sniffers and real-time tracing

Issues

- Systems are huge and complex, changing rapidly
- Things can hide anywhere
- Software does not provide a lot of interpretation
- Knowledge & experience are essential
- Gathering data is easy, analysis is much harder (and far more time-consuming)

Some tips

- Be deliberate and slow (acting fast != typing fast)
- Preserve an authentic original copy
- Document everything as you go in a notebook
- Isolate the system (from network, users). If possible, remove the hard drive. Else image it.
- Normal operation can destroy evidence lurking in unallocated space, file slack or in the swap file

More tips

- Run a coroner's tool (like IRCR) to record the system state (http://ircr.tripod.com/)
- Use only verified executables (also ensure verified shared library files)
- Use extreme care while handling data so you don't change what you want to observe
- Check data in the order of volatility
  - Registers
  - Memory
  - Network state
  - Running processes
  - Disk
  - Floppies
  - CDROMs, printouts, etc.

IRCR Incident Response Collection Report

- A collection of tools that gathers and/or analyzes forensic data on a Microsoft Windows system.
- A snapshot of the system in the past.
- Tools are oriented towards data collection rather than analysis.
- The idea of IRCR is that anyone could run the tool and send the output to a skilled Windows forensic security person for further analysis
- Similar to The Coroner's Toolkit (TCT) by Dan Farmer & Wietse Venema of IBM

Download from http://www.securityfocus.com/tools/2024

IRCR Reports

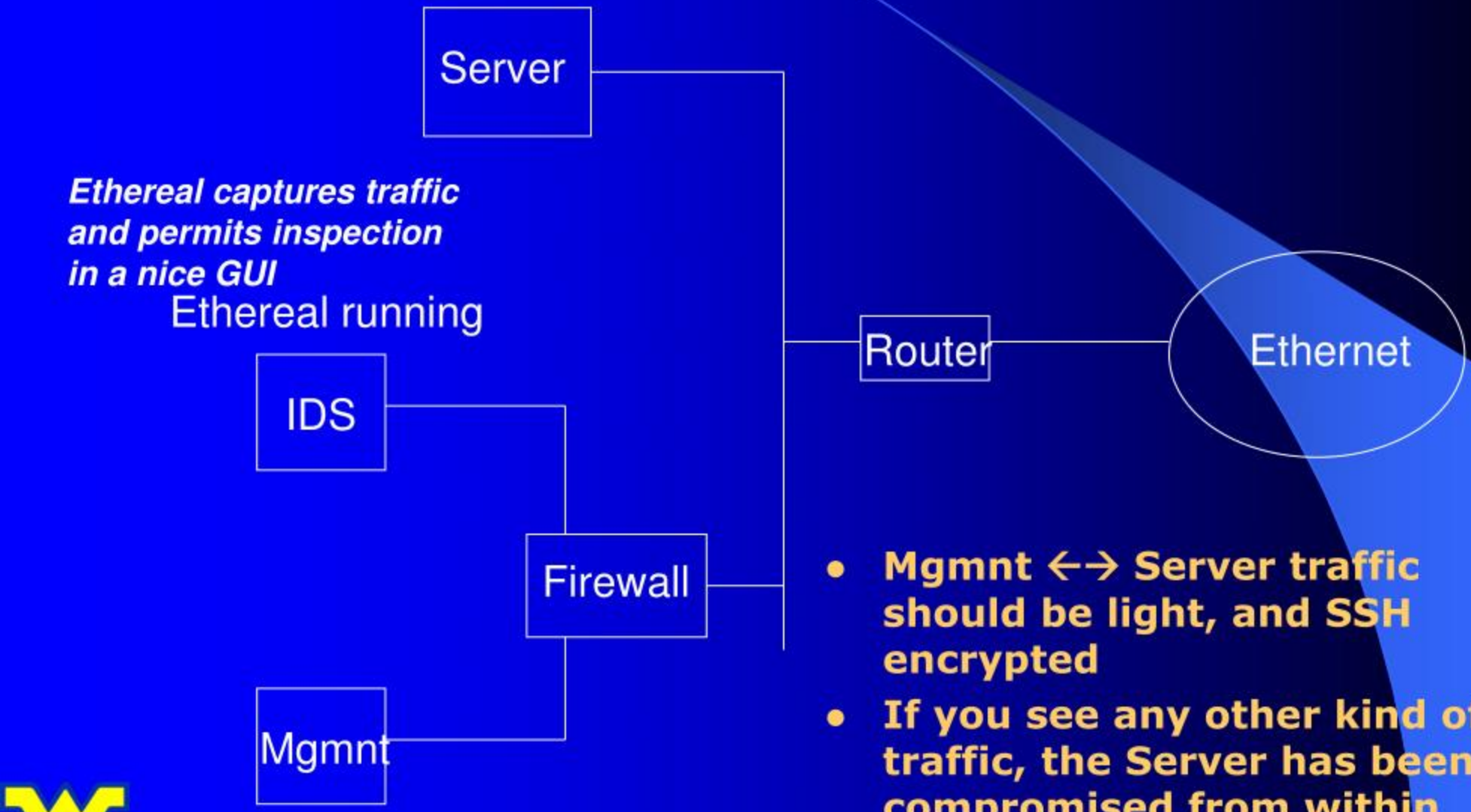
- Execute ircnt.exe and obtain about 25 text report files, such as
  - *md5chk* (verifying important .exe files),
  - *netstat* (network connections and protocols),
  - *evtlog* (log of events by system),
  - *filelist* (all files touched),
  - *netstart* (windows services started),
  - *syslog* (Windows system log), etc.
- Take report files on a FD.

As an exercise you may download and run ircr

To Detect Potential Intrusion

- In advanced enterprise systems you will have many security methods and hardware to protect the systems
- An IDS (Intrusion Detection System) is such a tool
- You can buy an IDS ready-built
- Large volume of traffic on unexpected channels is an indicator
- Unexpected traffic types is another indicator
- Need to characterize the normal traffic with tools such as Ethereal
- And then monitor continuously

Example



- **Mgmnt ←→ Server traffic should be light, and SSH encrypted**
- **If you see any other kind of traffic, the Server has been compromised from within**

To Identify

- What occurred
- How was the system compromised
- How serious is the damage
- How to recover
- How to eliminate vulnerability
- How to report
- How to capture evidence

Tools

- Major server OSes are variants of Unix and Linux; and Windows
- Tools are most developed for Unix/Linux
- But lots of Windows tools now
- Capture
  - Communications
  - Volatile info
  - Non-volatile info

Communications Tools

- Netcat is a fine tool, does many things
- It listens on ports and concatenates the packets
- Set it up on the forensics workstation to collect info in a file from the server which may be attacked

Communications Tools

- On the server (potential victim)
  - **netstat -s | nc 192.168.0.3 1234**
  - 1234 is the portnumber on which to send to the forensics workstation whose address is here 192.168.0.3
  - netstat reports the protocol statistics

- On the forensic workstation
  - **nc -l -p 1234>test.txt**
  - listen on 12345 port number and write protocol statistics collected to a file test.txt

Communications Tools

- On the server (potential victim)
  - **windump -i 2 | nc 192.168.0.3 1234**
  - what is sent continuously are the packets collected by the windump utility(equivalent of tcpdump on Unix)
  - http://home.wanadoo.nl/lc.staak/windump.htm for windump reference

- On the forensic workstation, as before
  - **nc -l -p 1234>test2.txt**
  - The dumped packets are written to test2.txt

Cryptcat is an encrypted version of netcat for added security

Volatile Info

- Processes – can be collected by using *Pslist.exe* from Sysinternals (processes, ProcessIDs, time usage, memory usage, etc.)
- *Fport.exe* from Foundstone reveals the PID, the process, and path to the Application that is using the port, for all open TCP and UDP ports
- *Psloggedon.exe* gives users logged on to the victim locally or remotely
- *Pclip.exe* sends the clipboard contents to stdout and from there can be piped to to the forensics workstation by *netcat*

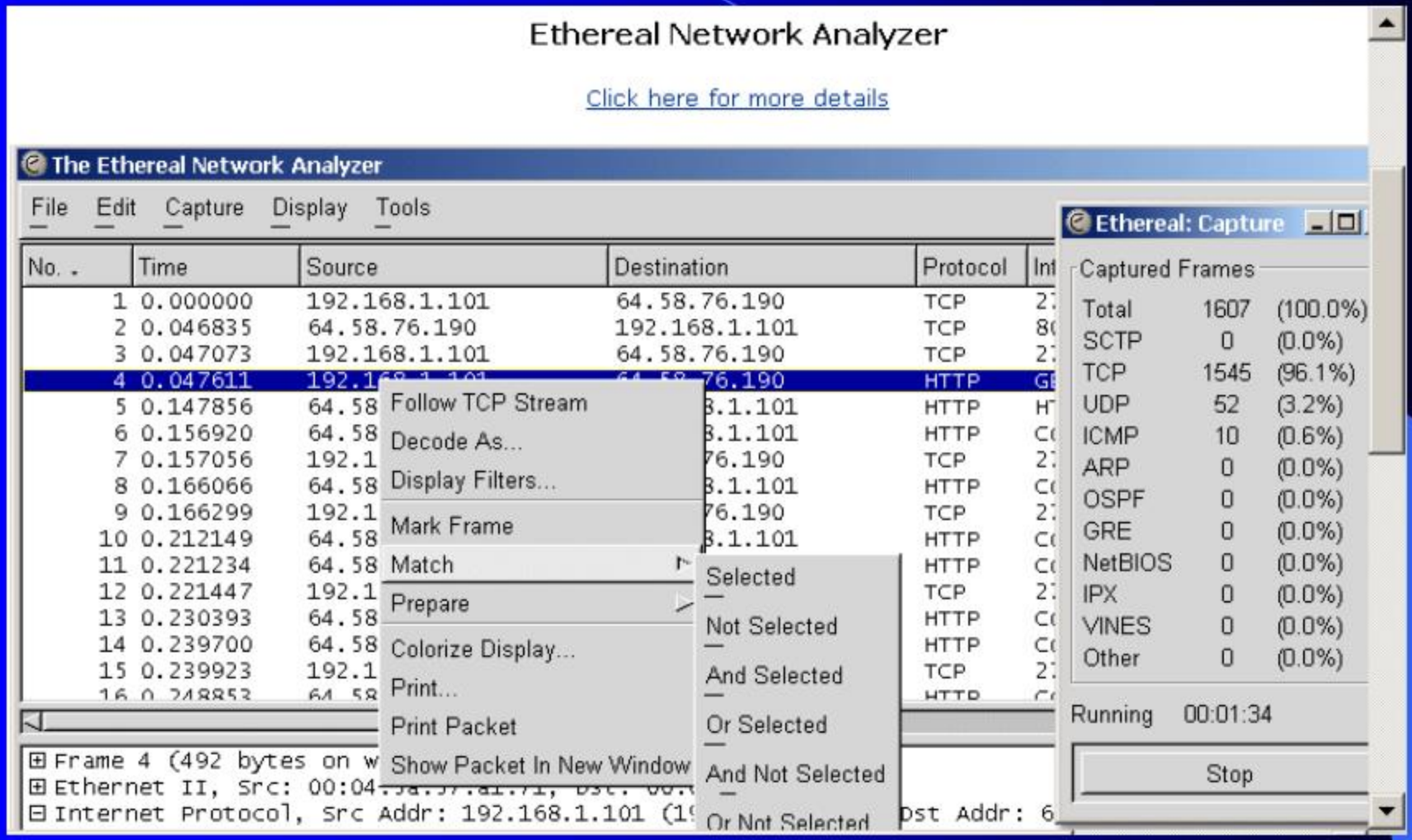
Volatile Info

- Network connections is another important info
- *Netstat* is the utility here to massage that info.
  - *Netstat –c* gives the state of all connections, the source and destination address, and
  - *Netstat –e* provides statistics of bytes sent and received

- As before you can capture the info on the victim; and *netcat* it for capture in a file on a forensics workstation
- *Nbtstat* tells who is logged on on a remote machine by using the *-a* option and the IPaddress or name of the remote computer

Volatile Info

- Network traffic is also very important in intrusions
- The recommended utility (many exist) is *Ethereal* because it not only captures the traffic, but has a nice GUI to inspect it.
- *Snort* is another famous utility; snort output can be inspected in Ethereal.


Ethereal Network Analyzer
Click here for more details
The Ethereal Network Analyzer
File Edit Capture Display Tools
No. Time Source Destination Protocol
1 0.000000 192.168.1.101 64.58.76.190 TCP
2 0.046835 64.58.76.190 192.168.1.101 TCP
3 0.047073 192.168.1.101 64.58.76.190 TCP
4 0.047611 HTTP
5 0.147856 HTTP
6 0.156920 HTTP
7 0.157056 TCP
8 0.166066 HTTP
9 0.166299 TCP
10 0.212149 HTTP
11 0.221234 HTTP
12 0.221447 TCP
13 0.230393 HTTP
14 0.239700 HTTP
15 0.239923 TCP
Follow TCP Stream
Decode As...
Display Filters...
Mark Frame
Match
Prepare
Colorize Display...
Print...
Print Packet
Show Packet In New Window
Selected
Not Selected
And Selected
Or Selected
And Not Selected
Or Not Selected
Frame 4 (492 bytes on w
Ethernet II, Src: 00:04
Internet Protocol, Src Addr: 192.168.1.101
Ethereal: Capture
Captured Frames
Total 1607 (100.0%)
SCTP 0 (0.0%)
TCP 1545 (96.1%)
UDP 52 (3.2%)
ICMP 10 (0.6%)
ARP 0 (0.0%)
OSPF 0 (0.0%)
GRE 0 (0.0%)
NetBIOS 0 (0.0%)
IPX 0 (0.0%)
VINES 0 (0.0%)
Other 0 (0.0%)
Running 00:01:34
Stop

Non-Volatile Info

- Use the output of IRCR
- Examine Event logs
- Check MAC times – modify, access, creation times – for files on the victim system
- *Afind.exe* from Foundstone is a tool to use here for last access times (so will Filelist)
- If MAC times show something suspicious, then you can examine the victim system for Alternate Data Streams attached to files in the NTFS file system. A tools here is LADS and another is Ads.pl
- A Perl script called mc.pl yields a comma delimited file with the 3 times

MAC Times

- MACtime is a shorthand way to refer to the three (or in some versions of Linux, four) time attributes -- mtime, atime, and ctime
- Microsoft refers to it as LastWriteTime, LastAccessTime, and CreationTime

Non-Volatile Info

- If suspicious files are found record the MAC times and the permissions(use a tool called cacls.exe included on Win2K systems)
- Use Md5sum.exe to establish the integrity of the files before and after copying
- You can also use Md5sum to verify critical files of the OS have not changed
- Strings.exe from Sysinternals allows searching for strings inside any file

Non-Volatile Info - Registry

- The Registry is a mine of information
- Look under HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- Trojans and other malware will leave traces here since they want to run across reboots and logins
- Look also under RunOnce, RunOnceEx, and RunServices
- A tool called autoruns.exe from Sysinternals tells what Registry keys are examined during Startup and user Logon
- Virus sites like F-Secure Virus Information record the sites in the Registry that get infected by various malware

Non-Volatile Info - Registry

- Maintain a good baseline of the Registry to compare against when incidents occur
- Other positions in the Registry record the most recently used files, URLs visited by IE, etc. Examine them.
- Examine HKEY_CURRENT_USER\Software\Microsoft\Telnet to see if which Hosts and Ports have been connected to by Telnet

What to do

- Before attack:
  - Create action plan (what to do when attack occurs)
  - Have a security policy in place
  - Identify who is in charge, points of entry (e-mail, net access), support options, law enforcement

What to do

- During attack:
  - Determine what is being attacked
  - Log activity
  - Take action, if possible without alerting the attacker
  - Isolate LAN/WAN traffic
  - Re-direct traffic
  - Clean OS

What to do

- After attack:
  - Save log files
  - Report attack (based on company policy – check higher up)
  - Clean systems
  - Re-examine the Firewall, Router, etc.
  - Communicate with others to prevent similar occurrences – what steps to take
  - Use occasion to train users and security staff

Ten Steps to Security

1. Use an Internet Firewall
2. Keep the System files, Application files and OS up-to -date with Patches, etc
3. Use Anti-virus software and ensure virus signatures are up-to-date
4. Use STRONG passwords
5. Keep your guard over physical security
6. Browse the Web with caution
7. Beware of Peer-to-peer networks
8. Use e-mail safely
9. Back up regularly
10. Connect to remote users securely
11. Lock down wireless networks

A Powerful Security Scanner

- Sunbelt Software makes a security scanner
- Download the current version Version 1.6.20.0 from http://www.sunbelt-software.com/product.cfm?page=download&id=987
- See presentation at http://www.sunbelt-software.com/rd/rd.cfm?id=040818WC-SNSI
- Comprehensive up-to-date Database of 2,300+ Windows vulnerabilities
- Scans and analyzes an entire network domain or a single machine
- Multiplatform – SNSI can now scan Windows, Linux, Solaris, HP UX, Cisco Routers, and HP Printers.
- Recommended solutions with links to related websites

As an exercise you may download (35MB!) and run SNSI

Sample Scan

Severe

- W0064
  - File Allocation Table (FAT) file system is less secure than an NT
    - Solution: Convert to NTFS
- W0100
  - Password cracker L0phtcrack detected: is a publicly available Windows NT password cracker and can crack brute-force hashed passwords.
    - Solution: Delete it

Sample Scan

Medium

- W0563
  - The SecEvent.Evt Security Event Log file permissions should only allow Administrators and system access. If this log is not secured, evidence of unauthorized activity can be erased.
    - Solution: Use File Properties and Set Permissions so only Administrator has: Full Control and System: Full Control
- W2084
  - Earlier versions of Mozilla contain vulnerabilities. The IMAP client for Mozilla 1.3 and 1.4a allows remote malicious IMAP servers to cause a denial of service and possible execute arbitrary code.
    - Solution: Download latest version 1.7 of Mozilla from mozilla.org/downloadW0100

Sample Scan

Low

- W0349
  - One or more of the following several Peer-to-Peer (P2P) clients was found on this system. P2P networks provide an ideal environment for viruses and other malicious software to be distributed.
    - Solution: Remove the P2P software from the machine and purge any files which may have been obtained illegally over a P2P network. ("AutoFix" NOT Available)

Sample

Warning

- W1953
  - AOL Instant Messenger Detected: Instant messaging (IM) software allows users to chat with other members. Most IM clients also have the capability transfer files across the Internet. Furthermore, the use of IM software may be in violation of company policy due to: - Misuse of network resources -Employee productivity factors -Company intellectual property protection issues.
    - Solution: Remove the AIM instant messaging software from the machine, using the Add/Remove Programs wizard to uninstall the application.

Resources

- WWW.SANS.ORG
  - Systems Administration, Network Security, founded in 1989 offers seminars, training, FAQ's
- WWW.INTRUSIONS.ORG
  - Intrusion Detection analysts and incident handlers
- WWW.CERT.ORG
  - Major reporting center for Internet security vulnerabilities, founded in 1988
- WWW.INFRAGARD.NET
  - FBI and private industry partnership – local chapters in most major cities