Network and Text Logs

NBE (Network Based Evidence)

Text based logs

Analysing and working with logs

Typer av loggar

- Nätverks device loggar
  - Routrar, switchar etc.
- Firewall loggar
  - Ingående, utgående och droppade paket
- IDS (Intrusion Detection System) loggar
  - Suspekta paket, attacker
- Server loggar
  - WWW, MTA, FTP, DBMS etc.
  - Access, error, connection status, queues, logins, activity, executed commands, etc.
- IPS (Intrusion Prevention System) loggar
  - System anrop loggar etc.
- Klient/system loggar
  - Security, application, system

System loggar

- Windows XP och Vista/7
  - Binära och låsta (.evt, .evtx)
  - Lagrar loggar i C:\Windows\system32\config\ eller C:\windows\system32\winevt\Logs\
    - **Appevent.evt(x)** - Contains a log of application usage
    - **Secevent.evt(x)** - Records activities that have security implications such as logins
    - **Sysevent.evt(x)** - Notes system events such as shutdowns
  - Det mesta av loggningen är avslagen som default
  - Verktyg som tex. MS dumpel och MS Log Parser (klarar fler format) kan användas för att parsa loggarna samt Event Viewer
- UNIX/Linux
  - ASCII
  - /etc/syslog.conf talar om var loggarna finns
    - Under /var/log ligger det mesta ang. systemet normalt
  - History etc. finnas i /home/<user> mappen, tex.
    - .shellName_history

NBE (Network Based Evidence) and NSM

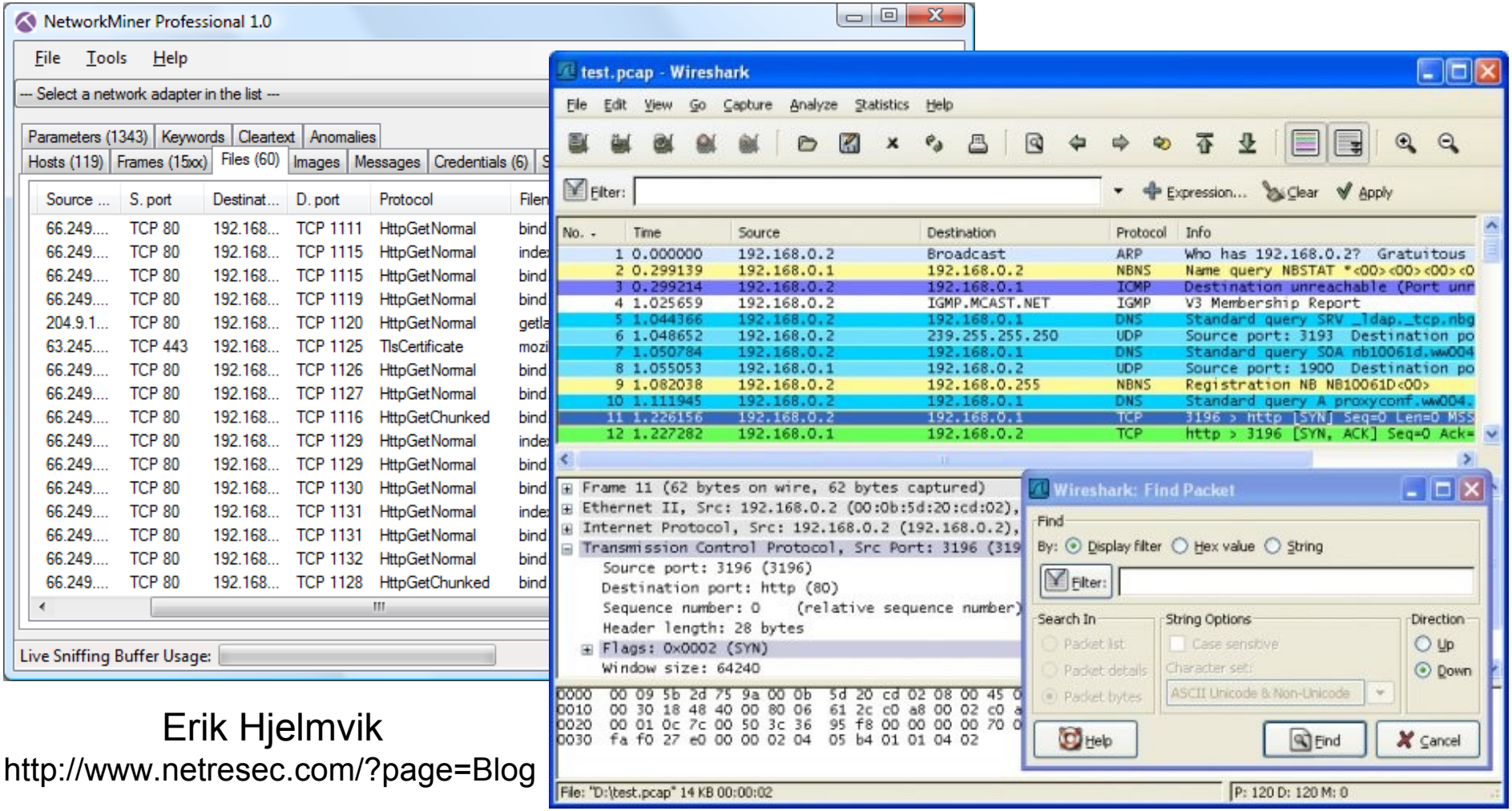
- Full content data
  - Records everything – lots of disk space may be needed
  - Tcpdump/windump/dumpcap, wireshark, ngrep, networkminer...
- Session data

libpcap/WinPcap

  - Records just the session: time stamp, pid, start/stop, type, IP-source/destination port and state, etc., **usually built-in**
  - Microsoft Port Reporter (and port reporter parser) tool - http://support.microsoft.com/kb/837243
  - Argus - http://www.qosient.com/argus/
  - Tcptrace - http://tcptrace.org/
- Alert data
  - Analyze the NBE for predefined items of interest with rules or signatures
  - Normally done by a network IDS/IPS as Snort or Bro Intrusion Detection System etc.

NetworkMiner and Wireshark

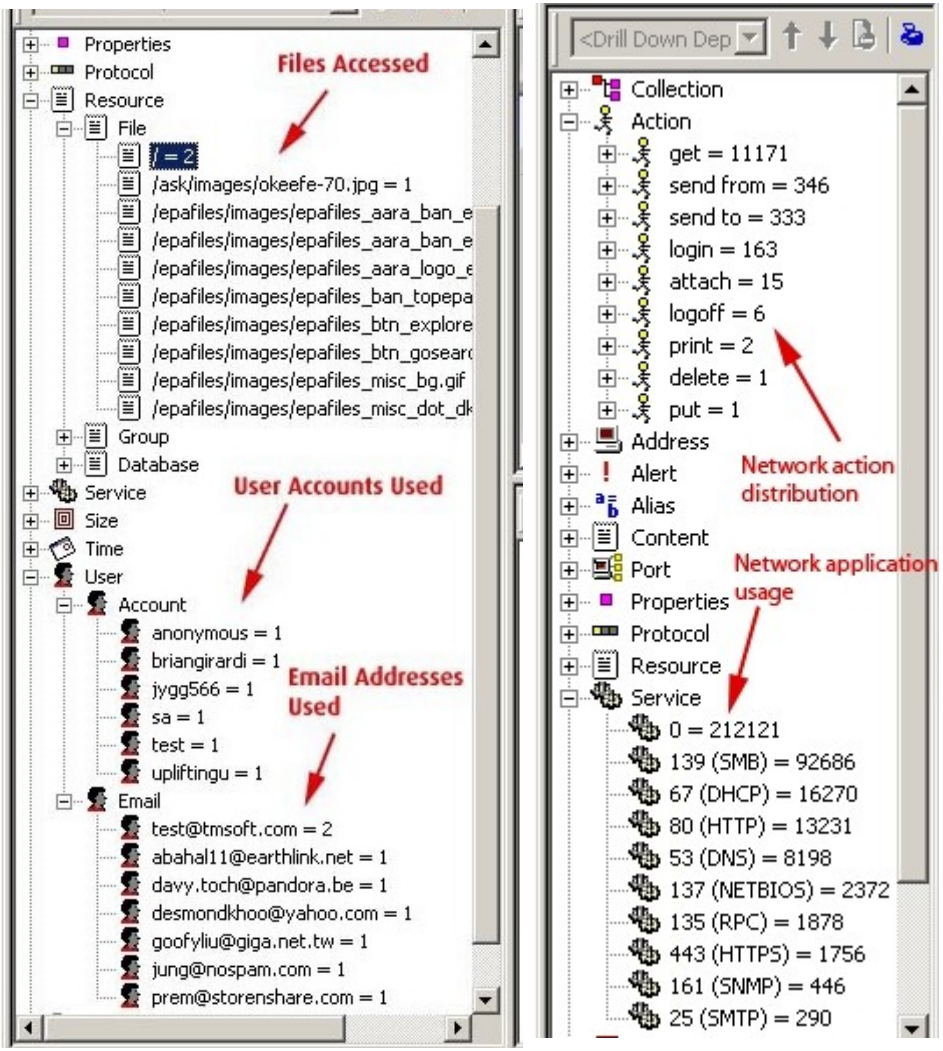
Jonathan James - [server]\training_forensics_networkanalysis\
youtube.com-user-techworldsverige\Kontrollera ditt nätverk med Wireshark



Erik Hjelmvik
http://www.netresec.com/?page=Blog

NBE (Network Based Evidence) and NSM

- Statistical data
  - Perform different types of traffic analysis as Top talkers etc.
  - tcpdstat, tcpstat, ntop, trafshow etc.
  - Analog (www)
- Advanced Network Security Monitoring (NSM) solutions as SGUIL, Snort etc. and NetWitness NextGen Investigator or NIKSUN NetDetector can do most of the above



NetWitness NextGen Investigator

Analog: WWW logfile analysis

Web Server Statistics for [...

file:///C:/data/kurs/analys_och_sparning/New%20tools/loggers/analog/analog%206.0/Report.html

Freja och Embla - | iGoogle | Synonymer.se - Lexi... | Språkrådet - Lexin | xda-developers | Android Developers | Metasploit Unleashe... | Geodataportalen | Other bookmarks

Web Server Statistics for [my organisation]

Program started at Fri-22-Apr-2011 00:29.
Analysed requests from Fri-31-Dec-1999 10:11 to Tue-04-Jan-2000 13:11 (4.13 days).

General Summary

(**Go To**: Top | General Summary | Monthly Report | Daily Summary | Hourly Summary | Domain Report | Organisation Report | Search Word Report | Operating System Report | Status Code Report | File Size Report | File Type Report | Directory Report | Request Report)

This report contains overall statistics.

Successful requests: 46
Average successful requests per day: 10
Successful requests for pages: 44
Average successful requests for pages per day: 10
Failed requests: 2
Redirected requests: 2
Distinct files requested: 4
Distinct hosts served: 2
Data transferred: 48.75 kilobytes
Average data transferred per day: 11.82 kilobytes

Monthly Report

(**Go To**: Top | General Summary | Monthly Report | Daily Summary | Hourly Summary | Domain Report | Organisation Report | Search Word Report | Operating System Report | Status Code Report | File Size Report | File Type Report | Directory Report | Request Report)

This report lists the activity in each month.

Each unit (▬) represents 1 request for a page.

month	reqs	pages	
Dec 1999	11	11	
Jan 2000	35	33	

Busiest month: Jan 2000 (33 requests for pages).

Daily Summary

(**Go To**: Top | General Summary | Monthly Report | Daily Summary | Hourly Summary | Domain Report | Organisation Report | Search Word Report | Operating System Report | Status Code Report | File Size Report | File Type Report | Directory Report | Request Report)

NBE/NSM standard intrusion scenario 1

The CIO (Chief Information Officer) wants to know the following questions answered!

1. Is the Web server etc. definitely compromized?
2. If yes, what did we lose on the Web server etc.?
3. Where else did the intruder go?
4. Is the intruder back today?

Full content data

1. Could reveal all or some of the intruders activities depending on the use of encryption etc. however later steps (pillage) in the attack may be more visible
2. Again depending on encryption...
3. Encryption cant help the intruder here (inside our network)
4. Depending on the backdoor it could be very hard to recognize a stateless backdoor together with millions of other packets

NBE/NSM standard intrusion scenario 2

Session data

1. Looking on the connections one could determine if it is compromized if the connections not are normal
2. Analyzing traffic patterns may reveal an intruder
3. Transaction logging/session data etc. should give a good base
4. This should also be possible to answer with transaction logging/session data etc.

Alert data

1. Assuming a signature exist for the attack, probably yes, otherwise no
2. Unless the IDS search for data information signatures, no
3. If the intruder perform further attacks against monitored systems, yes
4. If it exist a signature for the backdoor, yes

Statistical data

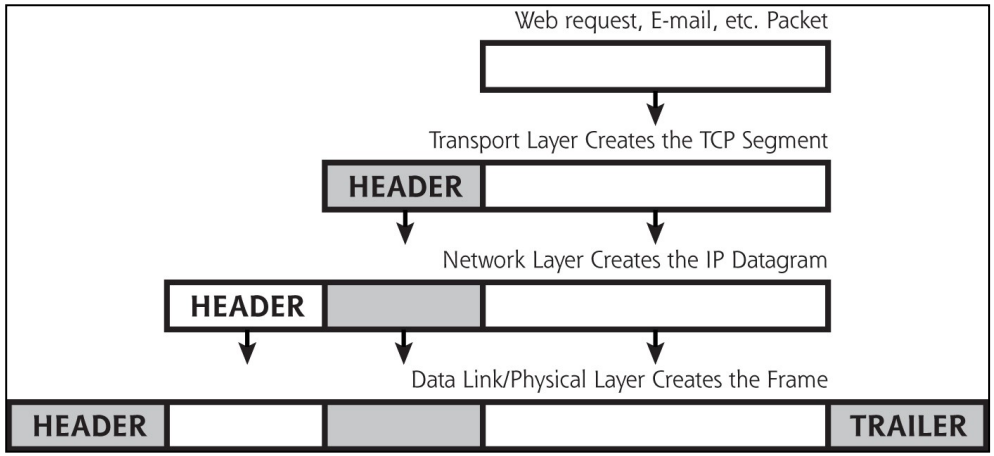
None of the CIOs questions can be answered but patterns can be seen!

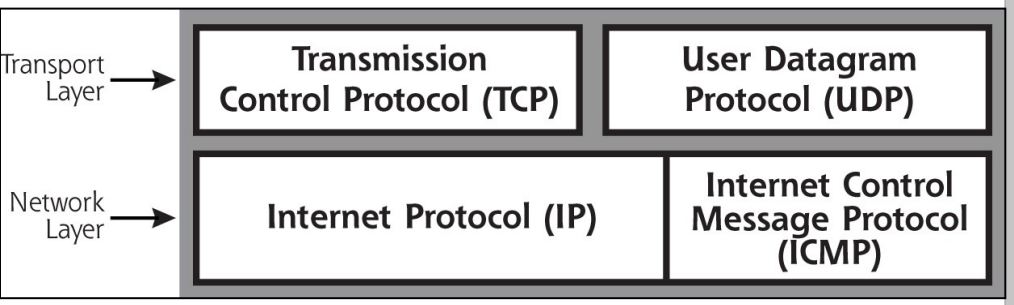
Några vanliga TCP/IP protokoll

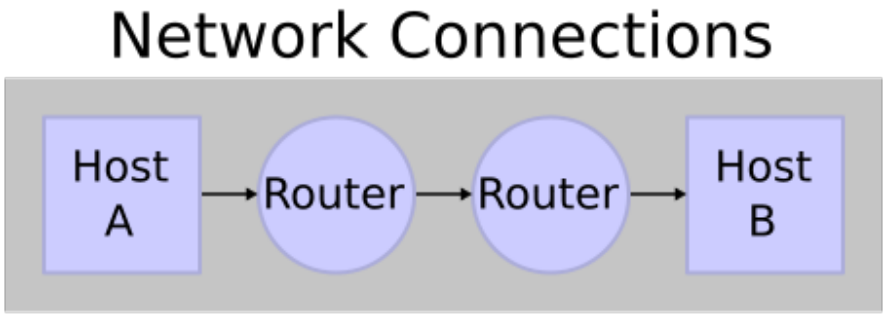
- IP (Internet Protocol)
  - Adresserar och routar paket mellan värddatorer (hosts)
- ARP (Adress Resolution Protocol)
  - Översätter hårdvaruadresser till IP-adresser
- ICMP (Internet Control Message Protocol)
  - Kontrollerar att paketleverans fungerar
- IGMP (Internet Group Management Protocol)
  - Hanterar hostar som är med i multicast grupp, kräver stöd från router, motsatsen till unicast
- TCP (Transmisson Control Protocol)
  - Pålitligt förbindelseorienterat, sekvens nummer skickas, använder portar
- UDP (User Datagram Protocol)
  - Opålitligt förbindelselöst (ej ACK), använder portar, snabbare än TCP

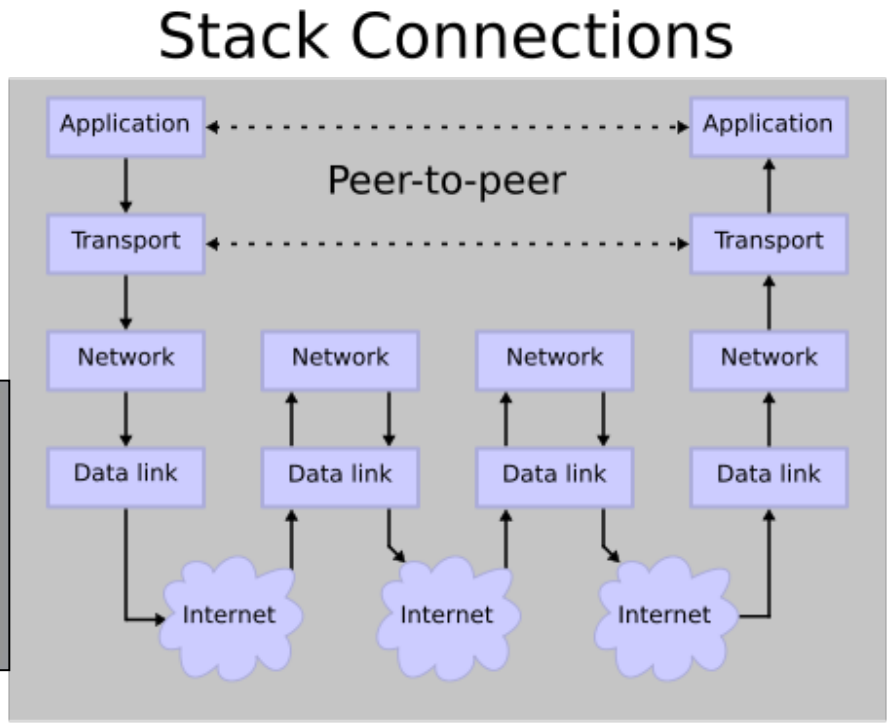
Networking TCP/IP

- Basic function of TCP/IP





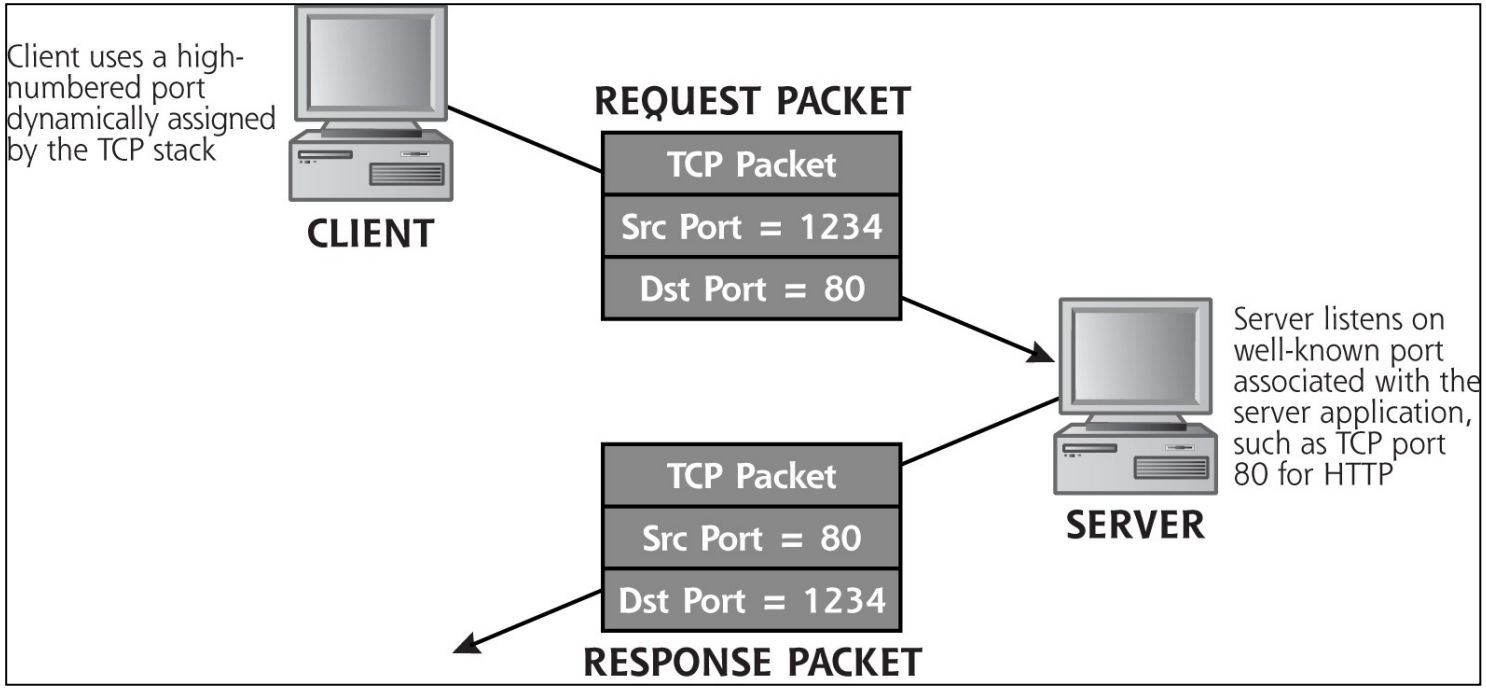




Nätverkstjänster

- För att fungera i nätverk måste OS ha vissa nätverkstjänster igång
  - Man bör sträva efter att **endast** ha de **nödvändiga** igång
- Standardtjänster har vissa ”portnummer” tilldelade
  - Portar, kan jämföras med TV eller radiokanaler, 65536 st.
  - Med kommandot netstat kan man se vilka portar som är aktiva
  - Vissa protokoll/applikationer kräver en viss port tex. HTTP (WWW) = 80, FTP (File Transfer Protocol)= 21, SMTP = 25, DNS = 53 (Domain Name System) samma funktion som vita sidorna i telefonkatalogen, se fullständig lista: http://www.iana.org/assignments/port-numbers
  - Well-known ports < 1024 vs. registered ports 1024 – 49151 vs. dynamic/private ports 49152 - 65535

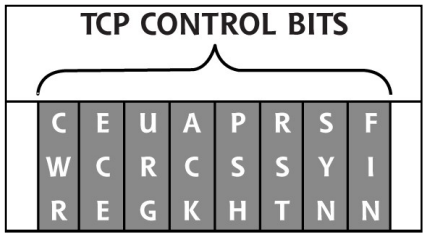
TCP packet and states

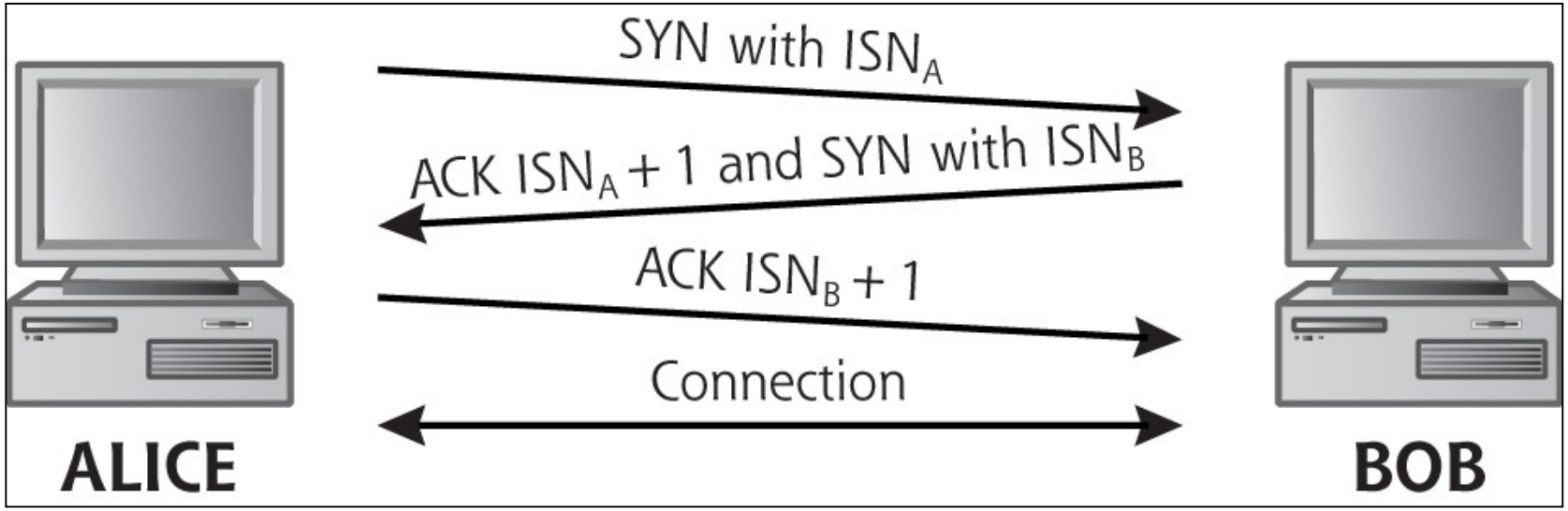


- TCP har 3 tillstånd
  - Anslutning etablering
  - Data sändning
  - Anslutning terminering

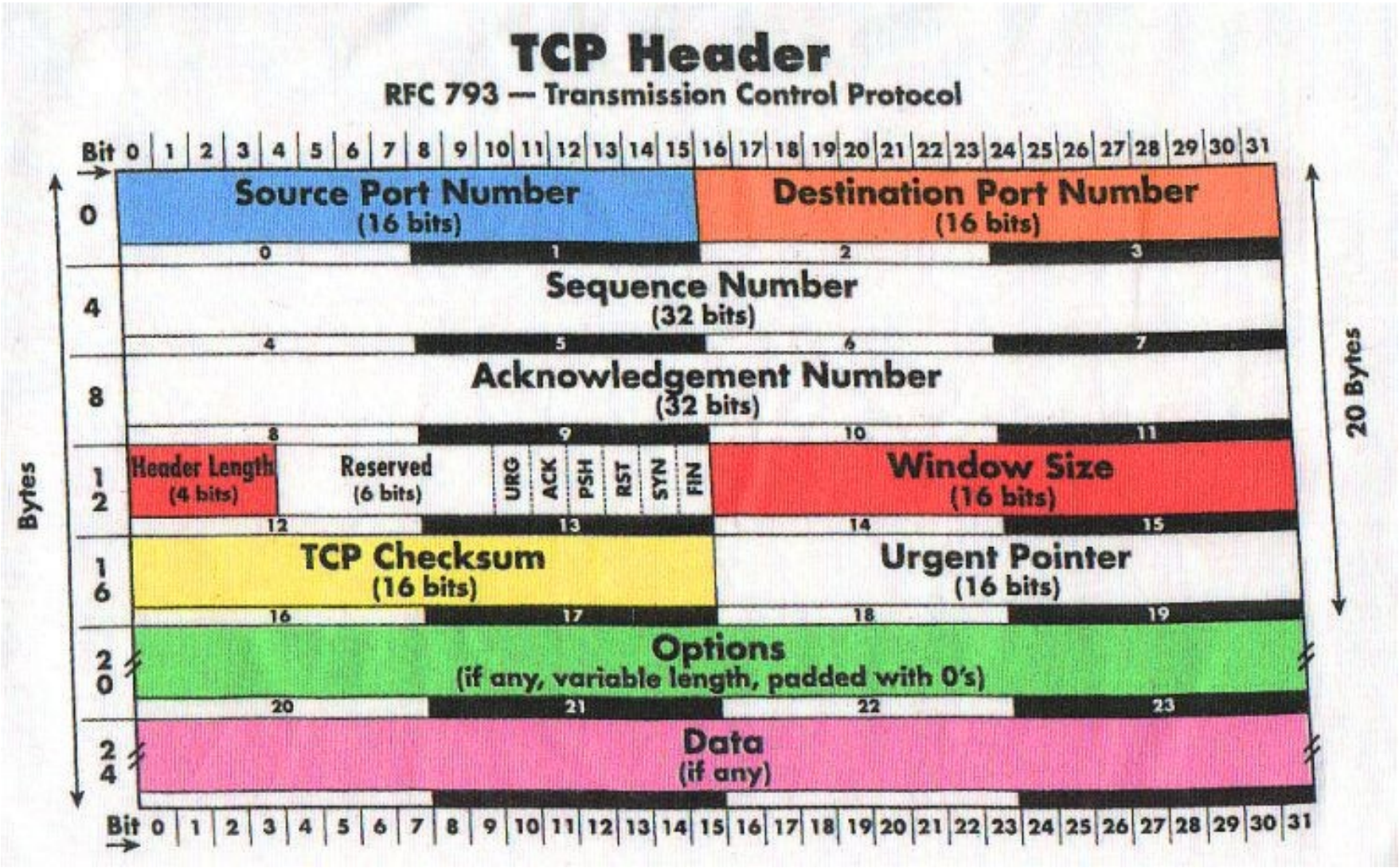
TCP – 3 way handshake

- A TCP connection use the 3-way handshake
  - SYN = Syncronize the sequence number
  - ISN = Initial Sequence Number or Sequence Number
  - ACK = Acknowledgement number
- When both client and server received ACK we have a connection
- Other flags (control bits) to note in a connection
- RST = Reset the connection
- FIN = Finish the connection





TCP Header and Data



Internet Protocol (IP)

- IP header is added to front of TCP/UDP/ICMP packet

Vers	Hlen	Service Type	Total Length	
Identification			Flags	Fragment Offset
Time to Live		Protocol	Header Checksum	
Source IP Address				
Destination IP Address				
IP Options (if any)				Padding
Data				
...				

- ICMP transmit command and control information
- ICMP uses the same header format as IP
- Ping and traceroute uses ICMP
- Note, ICMP (and IP) does not use any port number

http://en.wikipedia.org/wiki/IPv4

Wireshark 1

ftp_capture.pcap [Wireshark 1.6.6 (SVN Rev 41803 from /trunk-1.6)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: ip. Expression... Clear Apply

ip.addr
ip.checksum
ip.checksum_bad
ip.checksum_good
ip.dsfield
ip.dsfield.dscp
ip.dsfield.ecn
ip.dst
ip.dst_host

Enter a display filter, or choose one of your recently used filters. The background color of this field is changed by a continuous syntax check (green is valid, red is invalid, yellow may have unexpected results).

No.					
33					ss-lm > ftp [ACK] Seq=31 Ack=152 Win=17
49					50,6,225
50					Request: PORT 10,1,1,50,6,225
51				84	Response: 200 PORT command successful.
52				84	[TCP Retransmission] Response: 200 PORT command successful.
53				54	spss-lm > ftp [ACK] Seq=53 Ack=182 Win=17339 Len=0
54				60	Request: LIST
55				60	spss-lm > ftp [ACK] Seq=53 Ack=182 Win=17339 Len=0
56				60	[TCP Retransmission] Request: LIST
57				107	Response: 150 Opening ASCII mode data connection for /bin/ls
58				107	[TCP Retransmission] Response: 150 Opening ASCII mode data c
59	8.734520	10.1.1.50	10.1.1.15	TCP	54 spss-lm > ftp [ACK] Seq=59 Ack=235 Win=17286 Len=0
60	8.735264	10.1.1.15	10.1.1.50	TCP	62 ftp-data > cft-0 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_P
61	8.735315	10.1.1.50	10.1.1.15	TCP	62 cft-0 > ftp-data [SYN, ACK] Seq=0 Ack=1 Win=17520 Len=0 MSS=
62	8.738621	10.1.1.15	10.1.1.50	TCP	62 ftp-data > cft-0 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_P

```
Frame 33: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Agere_52:6b:2c (00:02:2d:52:6b:2c), Dst: LinksysG_ac:88:a3 (00:06:25:ac:88:a3)
Internet Protocol Version 4, Src: 10.1.1.50 (10.1.1.50), Dst: 10.1.1.15 (10.1.1.15)
Transmission Control Protocol, Src Port: spss-lm (1759), Dst Port: ftp (21), Seq: 31, Ack: 152, Len: 0
```

```
0000  00 06 25 ac 88 a3 00 02  2d 52 6b 2c 08 00 45 00   ..%..... -Rk,..E.
0010  00 28 7d 2c 40 00 80 06  67 61 0a 01 01 32 0a 01   .(},@... ga...2..
0020  01 0f 06 df 00 15 26 eb  67 43 f2 65 b0 b5 50 10   ......&. gC.e..P.
0030  43 d9 1d 7b 00 00 38 af  bb fc 41 6e               C..{..8. ..An
```

Invalid filter: "ip." is neither a field nor a prot... | Packets: 564 Displayed: 511 Marked: 0 Load time: 0:00.016 | Profile: Default

Wireshark 2

Mark a TCP packet
Analyze > Follow TCP Stream

Follow TCP Stream

Stream Content

```
220 kabar Microsoft FTP Service (Version 5.0).
USER anonymous
331 Anonymous access allowed, send identity (e-mail name) as
PASS ie@user
230 Anonymous user logged in.
PORT 10,1,1,50,6,225
200 PORT command successful.
LIST
150 Opening ASCII mode data connection for /bin/ls.
226 Transfer complete.
PORT 10,1,1,50,6,226
200 PORT command successful.
NLST
150 Opening ASCII mode data connection for file list.
226 Transfer complete.
TYPE I
200 Type set to I.
PORT 10,1,1,50,6,227
200 PORT command successful.
STOR openports.exe
150 Opening BINARY mode data connection for openports.exe.
226 Transfer complete.
PORT 10,1,1,50,6,228
200 PORT command successful.
STOR rifiuti.txt
150 Opening BINARY mode data connection for rifiuti.txt.
226 Transfer complete.
PORT 10,1,1,50,6,229
200 PORT command successful.
STOR stats.log
150 Opening BINARY mode data connection for stats.log.
226 Transfer complete.
QUIT
221
```

Entire conversation (950 bytes)

Find | Save As | Print | ASCII | EBCDIC | Hex Dump | C Arrays | Raw

Help | Filter Out This Stream | Close

Wireshark: Protocol Hierarchy Statistics

Display filter: none

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100,00 %	176	100,00 %	28043	0,004	0	0	0,000
Ethernet	100,00 %	176	100,00 %	28043	0,004	0	0	0,000
Internet Protocol Version 4	97,16 %	171	99,06 %	27779	0,004	0	0	0,000
User Datagram Protocol	11,93 %	21	12,28 %	3443	0,000	0	0	0,000
Hypertext Transfer Protocol	6,82 %	12	7,47 %	2094	0,000	12	2094	0,000
Domain Name Service	1,14 %	2	0,90 %	251	0,000	2	251	0,000
NetBIOS Name Service	3,98 %	7	3,92 %	1098	0,000	7	1098	0,000
Internet Control Message Protocol	6,82 %	12	8,67 %	2430	0,000	12	2430	0,000
Transmission Control Protocol	78,41 %	138	78,12 %	21906	0,003	124	16396	0,002
Hypertext Transfer Protocol	7,95 %	14	19,65 %	5510	0,001	8	3596	0,001
Media Type	1,70 %	3	1,69 %	474	0,000	3	474	0,000
Line-based text data	1,70 %	3	5,13 %	1440	0,000	3	1440	0,000
Address Resolution Protocol	2,84 %	5	0,94 %	264	0,000	5	264	0,000

Help | Close

Statistics > Protocol Hierarchy

How to read and examine logs?

- We can usually open the log as a text file, but not convenient in general (due to the information size)
- We can write our own code to examine – Perl and Python are the common languages used for this
  - Advantages: flexible, answer your needs (if you got the skills)
- We can use dedicated software specialized in log analysis
- Logs are the collection of basic events
  - One basic event is often not really important but several events can lead to interesting conclusions
  - Sometimes it is the only reliable source of information left
- Cross-analyze log files may be useful
- Statistical analysis is also important
- The analysis and understanding is often not obvious
- We have to re-build the puzzle!

Common Log Format

- The Common Log Format is a standardized text file format used by web servers which may be analyzed by a variety of analysis programs, example:
- **Apache access.log**
- Each line in a file stored in the Common Log Format has the following **syntax:** host ident auth-user date request status bytes

```
127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700] "GET /apache_pb.gif HTTP/1.0" 200 2326
```

- A "-" in a field indicates missing data
- **127.0.0.1** is the IP address of the client (remote host) which made the request to the server
- **-** RFC 1413 identity of the client, more info: http://tools.ietf.org/html/rfc1413
- **frank** is the user id of the person requesting the document
- **[10/Oct/2000:13:55:36 -0700]** is the date, time, and time zone when the server finished processing the request
- **"GET /apache_pb.gif HTTP/1.0"** is the request line from the client. The method GET, /apache_pb.gif the resource requested, and HTTP/1.0 the HTTP protocol
- **200** is the HTTP status code returned to the client. 2xx is a successful response, 3xx a redirection, 4xx a client error and 5xx a server error
- **2326** is the size of the object returned to the client, measured in bytes

Combined Log Format

- Another commonly used format string is called the Combined Log Format
- This format is exactly the same as the Common Log Format, with the addition of two more fields
  - **Referer** (html page where apache_pb.gif originated) and **User-agent** (the client)

```
127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700] "GET /apache_pb.gif HTTP/1.0" 200 2326
"http://www.example.com/start.html" "Mozilla/4.08 [en] (Win98; I ;Nav)"
```

- **Apache error.log format**

```
[Wed Oct 11 14:32:52 2000] [error] [client 127.0.0.1] client denied by server configuration:
/export/home/live/ap/htdocs/test
```

- The first item in the log entry is the **date and time** of the message
- The second item lists the severity of the error being reported depending on the configured **LogLevel**
- The third item gives the **IP address of the client** that generated the error
- Beyond that is the **message** itself, a very wide variety of different messages can appear
- In this case a client was denied to access /export/home/live/ap/htdocs/test

LogLevels

Level	Description
Emerg	Emergencies - system is unusable
alert	Action must be taken immediately
Crit	Critical Conditions
Error	Error conditions
Warn	Warning conditions
Notice	Normal but significant condition
Info	Informational
Debug	Debug-level messages

Windows XP IIS Logs

- Microsoft web server is called Internet Information Services (IIS)
- Detailed logging is enabled by default
- Most common and default format is W3C Extended Log File Format
- Log timestamps are GMT
- Default location: %SystemRoot%\System32\Logfiles\W3SVC1\
- Log per day in format exyymmdd.log, where yy=year, mm=month and dd=day
- Example of IIS Log Entry

```
#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2006-10-06 00:13:38
#Fields: date time c-ip cs-username s-sitename s-computername s-ip s-port cs-method cs-uri-stem
cs-uri-query sc-status sc-bytes cs-bytes time-taken cs-version cs-host cs(User-Agent) cs(Referer)

2006-10-06 00:13:38 70.55.118.27 - W3SVC1 LINUXBOX 128.175.24.251 80 GET /headers.htm
- 200 22938 287 672 HTTP/1.1 128.175.24.251 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1)
http://www.google.ca/search?hl=en&q=email+headers+readers&meta=
```

Windows Vista/7 IIS 7.5 Logs

Internet Information Services (IIS) Manager

NB-HJO ▸ Sites ▸ Default Web Site ▸

File View Help

Connections

- NB-HJO (DU\hjo)
  - Application Poo
  - Sites
    - ARQ
    - Default Web

Logging

Use this feature to configure how IIS logs requests on the Web server.

One log file per:

Site

Log File

Format:

W3C

Select Fields

Directory:

%SystemDrive%\inetpub\logs\LogFiles

Encoding:

UTF-8

Log File Rollover

Select the method that IIS uses to create a new log file.

- Schedule:

Daily

- Maximum file size (in bytes):
- Do not create new log files

Use local time for file naming and rollover

Features View | Content View

Configuration: 'localhost' applicationHost.config , <location path="Default Web Site">

W3C Logging Fields

- [x] Date (date)
- [x] Time (time)
- [x] Client IP Address (c-ip)
- [x] User Name (cs-username)
- [ ] Service Name (s-sitename)
- [ ] Server Name (s-computername)
- [x] Server IP Address (s-ip)
- [x] Server Port (s-port)
- [x] Method (cs-method)
- [x] URI Stem (cs-uri-stem)
- [x] URI Query (cs-uri-query)
- [x] Protocol Status (sc-status)
- [x] Protocol Substatus (sc-substatus)
- [x] Win32 Status (sc-win32-status)
- [ ] Bytes Sent (sc-bytes)
- [ ] Bytes Received (cs-bytes)
- [x] Time Taken (time-taken)
- [ ] Protocol Version (cs-version)
- [ ] Host (cs-host)
- [x] User Agent (cs(User-Agent))
- [ ] Cookie (cs(Cookie))
- [ ] Referer (cs(Referer))

OK | Cancel

W3SVC1

and

W3SVC2

u_ex... files

Windows XP FTP Logs

- Microsoft FTP Server
- Detailed logging enabled by default
- Most common and default format is W3C Extended Log File Format
- Log timestamps are GMT
- Default location: %SystemRoot%\System32\Logfiles\MSFTPSVC1\
- Log per day in format exyymmdd.log, where yy=year, mm=month and dd=day
- Example of FTP Log Entry

```
#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2006-10-22 00:05:51
#Fields: date time c-ip cs-username s-sitename s-computername s-ip cs-method cs-uri-stem sc-status sc-bytes
cs-bytes  time-taken cs-host
2006-10-22 16:23:11 172.18.24.252 salestaff MSFTPSVC1 intranetweb 172.19.90.111 21 [32]USER salestaff 331 0 0 0 -
2006-10-22 16:23:11 172.18.24.252 salestaff MSFTPSVC1 intranetweb 172.19.90.111 21 [32]PASS - 230 0 0 31 -
2006-10-22 16:23:21 172.18.24.252 salestaff MSFTPSVC1 intranetweb 172.19.90.111 21 [32]sent
/Confidential_Password_List.xls 226 13824 0 0 -
2006-10-22 16:23:28 172.18.24.252 salestaff MSFTPSVC1 intranetweb 172.19.90.111 21 [32]QUIT - 226 0 0 0 -
```

Microsoft DHCP Server Logs

- Dynamic Host Configuration Protocol (DHCP) service in which IP address assigned dynamically upon request by host
- Microsoft servers provide this services
- IP address loaned for a short period and thus which machine had which IP address is based on particular point in time
- Logs record host to which IP was assigned
- Time is local system time zone!
- Default location for log is: %SystemRoot%\System32\DHCP\
- Logs stored in one file per day basis
- Format of log file name is: DhcpSrvLog-XXX.log, where XXX=three letters of day of week, i.e. DhcpSrvLog-Sat.log
- Therefore, only 1 full week stored!

DHCP Log example

```
Microsoft DHCP Service Activity Log

Event ID Meaning
00 The log was started.
01 The log was stopped.
02 The log was temporarily paused due to low disk space.
10 A new IP address was leased to a client.
11 A lease was renewed by a client.
12 A lease was released by a client.
13 An IP address was found to be in use on the network.
14 A lease request could not be satisfied because the scope's
   address pool was exhausted.
15 A lease was denied.
16 A lease was deleted.
17 A lease was expired.
20 A BOOTP address was leased to a client.
21 A dynamic BOOTP address was leased to a client.
22 A BOOTP request could not be satisfied because the scope's
   address pool for BOOTP was exhausted.
23 A BOOTP IP address was deleted after checking to see it was
   not in use.
24 IP address cleanup operation has began.
25 IP address cleanup statistics.
30 DNS update request to the named DNS server
31 DNS update failed
32 DNS update successful
50+ Codes above 50 are used for Rogue Server Detection information.

ID,Date,Time,Description,IPAddress,HostName,MAC Address
10,10/22/06,06:14:25,Assign,172.18.24.252,WRT300_12.xxx.com,001839AC8765,
```

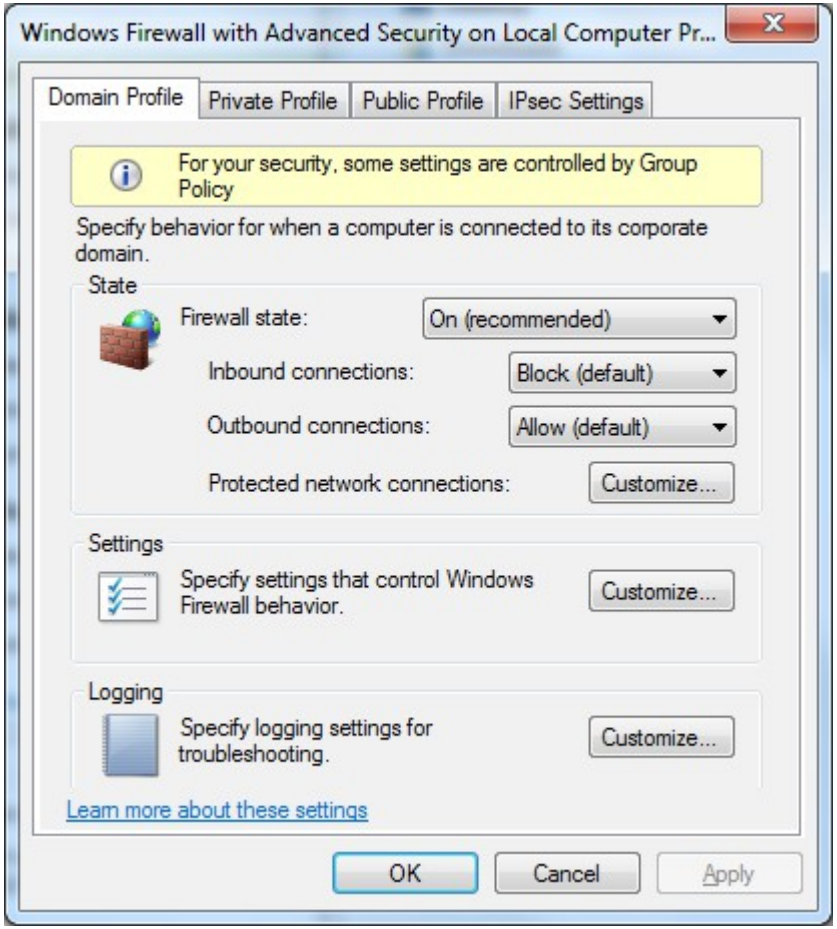
- **Event ID** - see table, **Date**, **Time** (Local system time zone)
- **Description** - action, **IP address** - IP assigned
- **Host name** - to which IP assigned
- **MAC address** - to which IP assigned

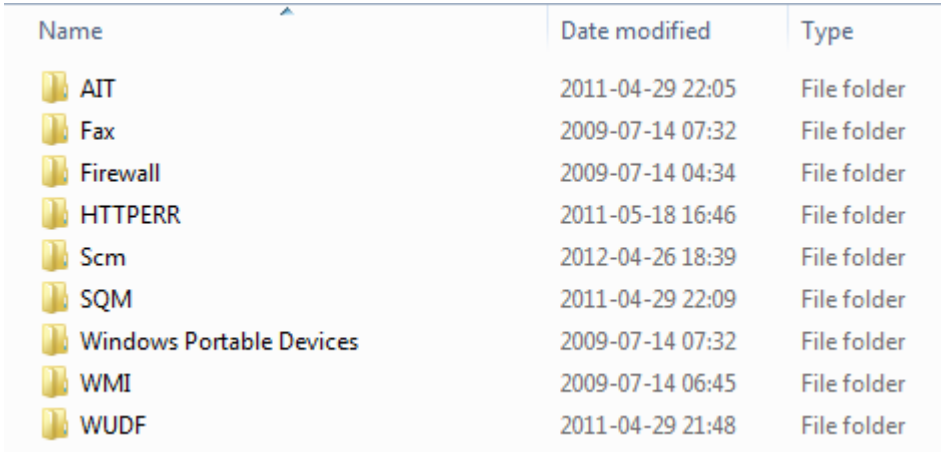
Windows XP Firewall Logs

- Firewall added to XP with SP 2
- Firewall on by default
- Good logging utility, however, it is off by default
- Enabling is buried deep in user interface
  - Don’t expect to find it enabled often, except in domain settings with good administrator!
- Default location of firewall logs is: %SystemRoot%\pfirewall.log
- Always look for it anyway
- Windows Firewall Log Header and data

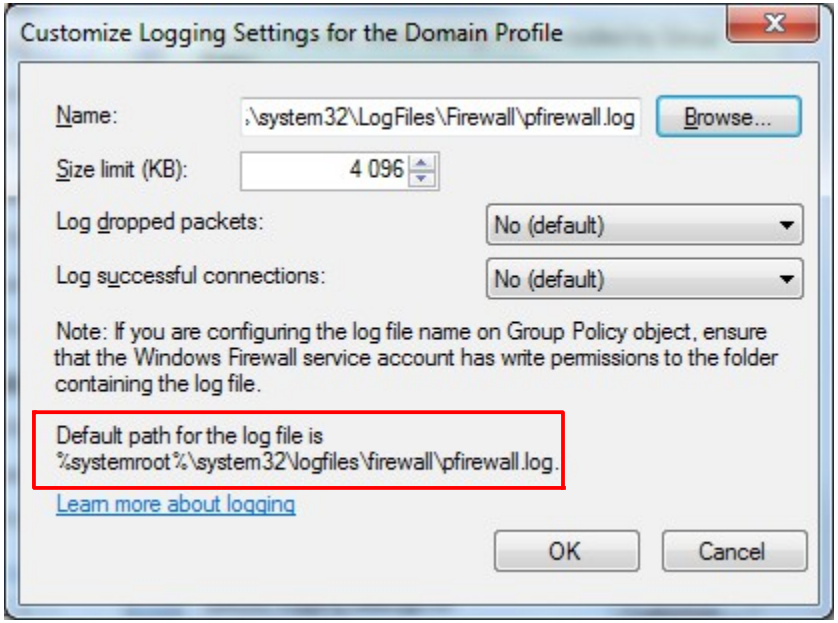
```
#Fields: date time action protocol src-ip dst-ip src-port dst-port
size tcpflags tcpsyn tcpack tcpwin icmptype icmpcode info path

2006-10-29 11:36:19 OPEN TCP 192.168.1.101 128.175.13.63 1124 80 - - - - - - - - - -
2006-10-29 11:36:19 CLOSE TCP 192.168.1.101 128.175.13.63 1123 80 - - - - - - - - - -
2006-10-29 11:36:19 OPEN TCP 192.168.1.101 128.175.13.63 1126 80 - - - - - - - - - -
2006-10-29 11:36:19 OPEN TCP 192.168.1.101 128.175.13.63 1123 80 - - - - - - - - - -
2006-10-29 11:36:19 OPEN UDP 192.168.1.101 68.87.64.146 1025 53 - - - - - - - - - -
2006-10-29 11:36:19 OPEN TCP 192.168.1.101 64.233.169.104 1125 80 - - - - - - - - - -
```

Windows Vista/7 Firewall Logs





Name	Date modified	Type
AIT	2011-04-29 22:05	File folder
Fax	2009-07-14 07:32	File folder
Firewall	2009-07-14 04:34	File folder
HTTPERR	2011-05-18 16:46	File folder
Scm	2012-04-26 18:39	File folder
SQM	2011-04-29 22:09	File folder
Windows Portable Devices	2009-07-14 07:32	File folder
WMI	2009-07-14 06:45	File folder
WUDF	2011-04-29 21:48	File folder



Microsoft Port Reporter

- Port Reporter is a logging service which runs on Microsoft Windows 2000, XP, Server 2003 and newer...?
- Useful for troubleshooting, security, application profiling, application development, and so on...
- Port Reporter logs
  - Ports that are used and the time they are used
  - Processes that use the ports
  - Whether a process is a service
  - All the modules that each process has loaded
  - The user account that each process runs under
- Also logs TCP/IP port usage data and port changes
  - Increase or decrease in connections, port state changes etc.
- Port Reporter comes from MS PortrQry used in local mode
  - Similar to netstat.exe -ano

Port Reporter Service Log files

- The service creates 3 log files with a name which uses date and time in 24-hour format (the *) when the file was created
  - PR-INITIAL-*.log
    - Contains data about the ports, processes and modules running on system when the service started up
  - PR-PORTS-*.log
    - Contains summary data about TCP and UDP port activity on computer listed using comma-separated value (.csv) format:
      - date, time, protocol, local port, local IP address, remote port, remote IP address, PID, module, user context
  - PR-PIDS-*.log
    - Contains detailed information about ports, processes, related modules and user account process uses to run
    - Each line in PR-PORTS log has a corresponding entry in the PR-PIDS log
- In summary the 3 log files provide
  - Snapshot of port usage when service starts
  - Summary data on ongoing port usage
  - Detail data on ongoing port usage

Microsoft Port Reporter Parser

- Helps reviewing log data and apply filters and criterias to identify interesting ports, processes, modules and IP addresses etc.

Port Reporter Parser - File Open: C:\WINDOWS\system32\Logfiles\PortReporter\PR-PORTS-011-04-22-0-0-0.log

File Edit Tools Help

Total records: 1580 Criteria has not been applied to this data

Date	Time	Protocol	Local Port	Local IP	Remote Port	Remote IP	Remote Name	PID	Module	Account
11/04/22	00:00:08	TCP	3058	127.0.0.1	22350	127.0.0.1		1760	adNetworkLicenseS	<NT AUTHORITY\SYSTEM>
11/04/22	00:00:08	TCP	22350	127.0.0.1	3058	127.0.0.1		1316	CodeMeter.exe	<NT AUTHORITY\SYSTEM>
11/04/22	00:00:47	TCP	3060	130.243.36.216	80	74.125.39.102		3648	firefox.exe	<DU\hjo>
11/04/22	00:00:48	TCP	3061	130.243.36.216	80	74.125.39.138		3648	firefox.exe	<DU\hjo>
11/04/22	00:02:24	TCP	3063	127.0.0.1	22350	127.0.0.1		1760	adNetworkLicenseS	<NT AUTHORITY\SYSTEM>
11/04/22	00:02:24	TCP	22350	127.0.0.1	3063	127.0.0.1		1316	CodeMeter.exe	<NT AUTHORITY\SYSTEM>
11/04/22	00:02:36	TCP	3065	130.243.36.216	445	130.243.57.20		4	System	
11/04/22	00:04:39	TCP	3069	127.0.0.1	22350	127.0.0.1		1760	adNetworkLicenseS	<NT AUTHORITY\SYSTEM>
11/04/22	00:04:39	TCP	22350	127.0.0.1	3069	127.0.0.1		1316	CodeMeter.exe	<NT AUTHORITY\SYSTEM>
11/04/22	00:05:42	TCP	3072	130.243.36.216	135	130.243.57.20		568	lsass.exe	<NT AUTHORITY\SYSTEM>
11/04/22	00:05:42	TCP	3073	130.243.36.216	1026	130.243.57.20		568	lsass.exe	<NT AUTHORITY\SYSTEM>
11/04/22	00:05:42	TCP	3074	130.243.36.216	135	130.243.57.117		568	lsass.exe	<NT AUTHORITY\SYSTEM>
11/04/22	00:05:42	TCP	3075	130.243.36.216	49159	130.243.57.117		568	lsass.exe	<NT AUTHORITY\SYSTEM>
11/04/22	00:05:42	TCP	3076	130.243.36.216	389	130.243.57.20		0	System Idle	
11/04/22	00:05:42	TCP	3077	130.243.36.216	389	130.243.57.20		0	System Idle	
11/04/22	00:05:42	TCP	3078	130.243.36.216	445	130.243.57.20		4	System	
11/04/22	00:05:42	TCP	3080	130.243.36.216	445	130.243.57.118		4	System	
11/04/22	00:06:55	TCP	3085	127.0.0.1	22350	127.0.0.1		1760	adNetworkLicenseS	<NT AUTHORITY\SYSTEM>
11/04/22	00:06:55	TCP	22350	127.0.0.1	3085	127.0.0.1		1316	CodeMeter.exe	<NT AUTHORITY\SYSTEM>
11/04/22	00:09:10	TCP	3088	127.0.0.1	22350	127.0.0.1		1760	adNetworkLicenseS	<NT AUTHORITY\SYSTEM>
11/04/22	00:09:10	TCP	22350	127.0.0.1	3088	127.0.0.1		1316	CodeMeter.exe	<NT AUTHORITY\SYSTEM>
11/04/22	00:11:27	TCP	3092	127.0.0.1	22350	127.0.0.1		1760	adNetworkLicenseS	<NT AUTHORITY\SYSTEM>
11/04/22	00:11:27	TCP	22350	127.0.0.1	3092	127.0.0.1		1316	CodeMeter.exe	<NT AUTHORITY\SYSTEM>
11/04/22	00:13:42	TCP	3096	127.0.0.1	22350	127.0.0.1		1760	adNetworkLicenseS	<NT AUTHORITY\SYSTEM>
11/04/22	00:13:42	TCP	22350	127.0.0.1	3096	127.0.0.1		1316	CodeMeter.exe	<NT AUTHORITY\SYSTEM>
11/04/22	00:14:37	TCP	3098	130.243.36.216	443	63.245.209.92		3648	firefox.exe	<DU\hjo>
11/04/22	00:14:37	TCP	3099	130.243.36.216	443	63.245.209.92		3648	firefox.exe	<DU\hjo>

Sawmill

FTP - Overview

127.0.0.1:8988/?dp=reports&p=ftp&wbsi=93737464000

Freja och Embla - | iGoogle | Synonymer.se - Lexi... | Språkrådet - Lexin | xda-developers | Android Developers | Metasploit Unleashe... | Other bookmarks

SAWMILL

Reports of profile FTP | View Config | Admin | Logout {hjo} | Help | About

Date Picker | Filters | Printer Friendly | Miscellaneous

- Calendar
- Overview
- Date and time
- Actions
- Protocols
- Source IPs
- Destination IPs
- Source ports
- Destination ports
- Tcp flags
- TCP SYNs
- TCP ACKs
- TCP windows
- ICMP types
- ICMP codes
- Infos
- Paths
- Sessions
- Single-page Summary
- Log detail

Overview

23/Sep/2003 - 06/Mar/2007, 1261 days *(entire date range)*

	All days	Average per day
Packets	70,068	55
Size	2.18 M	1.77 K
Unique source IPs	222	0
Sessions	0	0
Session events	0	0
Session users	0	0
Session begin	-	-
Session end	-	-
Session duration	00:00:00	00:00:00

Admin - Profiles

127.0.0.1:8988/?dp=index

Freja och Embla - | iGoogle | Synonymer.se - Lexi... | Other bookmarks

SAWMILL

Change Trial Mode | Logout {hjo} | Support | Help | About

Profiles | Scheduler | Preferences | Licensing | Import | My Account

Create New Profile

FTP	View Reports	View Config	
www	View Reports	View Config	

Splunk 1

Splunk Manager - Splunk...

hjo-pclap:8000/en-US/manager/launcher/adddata?breadcrumbs=Home|%2Fapp%2Flauncher%2Fhome

Freja och Embla - | iGoogle | Synonymer.se - Lexi... | Språkrådet - Lexin | xda-developers | Android Developers | Metasploit Unleashe... | Other bookmarks

« Back to Home

Logged in as admin | Alerts | Jobs | Logout

splunk> Home » Add Data

Help

Get your data into Splunk from this machine or any other machine in your network

To get started, choose your data type from this list, OR choose a collection method from the second list below.

- A file or directory of files
- Syslog
- Windows event logs
- Windows Registry
- Windows performance metrics
- Unix/Linux logs and metrics
- File integrity monitoring
- Configuration files
- OPSEC LEA
- Cisco device logs
- IIS logs
- Apache logs
- WebSphere logs, metrics and other data
- **Any other data...**

Choose how you want Splunk to consume your data.

- From files and directories
- From a TCP port
- From a UDP port
- Run and collect the output of a script
- Collect Windows performance data from a remote machine (WMI)
- Collect Windows registry data
- Collect Windows performance data
- Collect Windows event logs locally
- Collect Windows event logs from other machines
- Monitor an Active Directory schema

Is your data on another machine, besides this Splunk server? Install Splunk's universal forwarder on that machine and tell it to send the data to this Splunk server.

Back

Splunk 2

Search - Search - Splunk ...

hjo-pclap:8000/en-US/app/search/flashtimeline?auto_pause=true&q=search%20source%3D"C%3A%5C%5Chj

Freja och Embla - | iGoogle | Synonymer.se - Lexi... | Språkrådet - Lexin | xda-developers | Android Developers | Other bookmarks

splunk> Search

Logged in as admin | App | Manager | Alerts | Jobs | Logout

Summary | Search | Status | Views | Searches & Reports | Help | About

Search | Actions

source="C:\\hjo\\cases\\logparser-scripts\\samples\\pfirewall.log.old"

All time

6 matching events

Create alert | Add to dashboard | Save search | Build report

Timeline: zoom in | zoom out | select all | Scale: linear | log | 1 bar = 1 month

4 events during March 2007

18 fields | Pick fields

On Field discovery

Selected fields (3)

host (1)

source (1)

sourcetype (1)

Other interesting fields (6)

index (1)

linecount (n) (2)

punct (1)

splunk_server (1)

timeendpos (n) (1)

timestartpos (n) (1)

All 18 Fields

Options... | Results per page 10

1 3/6/07 5:59:19.000 PM

```
2007-03-06 17:59:19 CLOSE TCP 192.168.1.6 192.168.1.1 4595 2869 - - - - - - - - -
2007-03-06 17:59:19 OPEN TCP 192.168.1.6 192.168.1.1 4597 2869 - - - - - - - - -
2007-03-06 17:59:19 OPEN-INBOUND TCP 192.168.1.1 192.168.1.6 1764 2869 - - - - - - - -
-
2007-03-06 17:59:19 CLOSE TCP 192.168.1.6 192.168.1.1 4598 2869 - - - - - - - - -
2007-03-06 17:59:19 OPEN-INBOUND TCP 192.168.1.1 192.168.1.6 1765 2869 - - - - - - - -
-
2007-03-06 17:59:19 OPEN TCP 192.168.1.6 192.168.1.1 4601 2869 - - - - - - - - -
2007-03-06 17:59:19 CLOSE TCP 192.168.1.6 192.168.1.1 4601 2869 - - - - - - - - -
2007-03-06 17:59:19 CLOSE TCP 192.168.1.6 192.168.1.1 4604 2869 - - - - - - - - -
2007-03-06 17:59:29 OPEN-INBOUND TCP 192.168.1.1 192.168.1.6 1766 2869 - - - - - - - -
-
2007-03-06 17:59:30 CLOSE TCP 192.168.1.6 207.68.178.239 4550 80 - - - - - - - - -
```

Show all 300 lines

host=HJO-PCLAP | sourcetype=backup_file | source=C:\hjo\cases\logparser-scripts\samples\pfirewall.log.old

2 3/5/07 1:07:20.000 PM

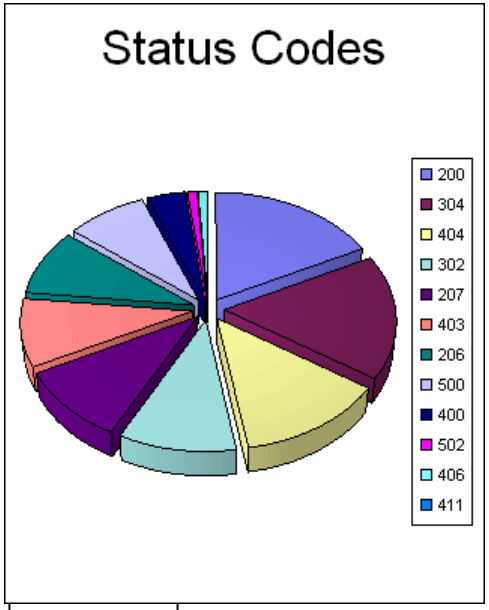
```
2007-03-05 13:07:20 OPEN TCP 192.168.1.6 151.193.163.8 3793 443 - - - - - - - - -
2007-03-05 13:07:21 CLOSE TCP 192.168.1.6 151.193.163.8 3805 443 - - - - - - - - -
```

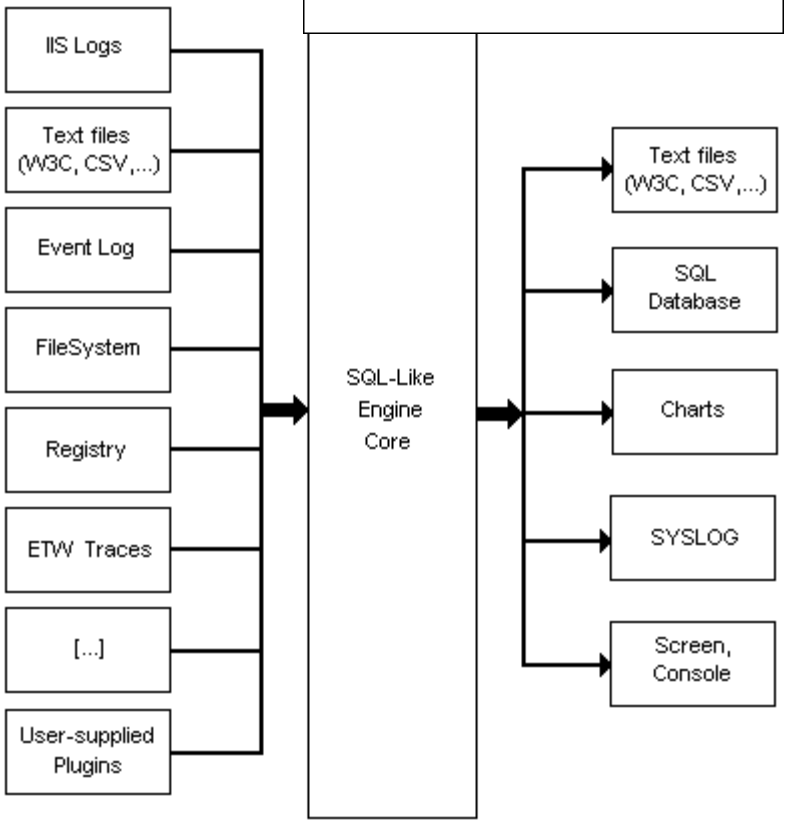
MicroSoft Log Parser (free)

- As an application developer you often need to write some logs for your application
  - There is many logging framework to choose among: Log4net, Log4j, Microsoft Logging Application Block, etc.
  - But when it come to read those logs, search for data, create reports, extract statistics or perform some alert/action on them, things become harder
- Log Parser performs SQL queries against a variety of log files and other system data sources
  - You can query any log and data sources (database, event log, IIS logs, file system, registry, etc.) with a complex SQL query!
  - On the down side, using it from the command line become quickly unpractical as you need to type your SQL query in a DOS prompt
    - logparser -i:EVT "SELECT TOP 20 * FROM Security WHERE EventID=5032 ORDER BY TimeGenerated DESC" -o DATAGRID
    - logparser -i:W3C -o:DATAGRID ”SELECT RowNumber, date, time, action, protocol, src-ip, dst-ip, src-port, dst-port FROM c:\pfirewall.log WHERE dst-port IN (80; 443) ORDER BY RowNumber”

Log Parser Architecture

- Swiss Army knife for processing Windows logs of all types (and others). The world is your database with Log Parser!
- **Input Formats** are generic *record providers*
  - Input Formats can be thought of as SQL tables containing the data you want to process
  - Manage .evtx (Vista/7) event logs as well
- A **SQL-Like Engine Core** processes the records generated by an Input Format
  - SQL language (SELECT, WHERE, GROUP BY, HAVING, ORDER BY etc.)
  - Aggregate functions (SUM, COUNT, AVG, MAX, MIN etc.)
  - A rich set of functions (e.g. SUBSTR, CASE, REVERSEDNS, etc.)
- **Output Formats** are generic *consumers of records*
  - They can be thought of as SQL tables that receive the results of the data processing
  - BSD syslog protocol, RFC 3164





Log Parser Lizard

http://www.lizard-labs.net/log_parser_lizard.aspx

Log Parser Lizard

Home | Query | Tools

Save Query | Save to File | Input Log Format | Query Properties | Run Query | Display Grid | Display Chart | Advanced Grid | Edit Mode | Chart Type | Swap chart rows and columns | Swap grid rows and columns | Compress NULL values

Query | View

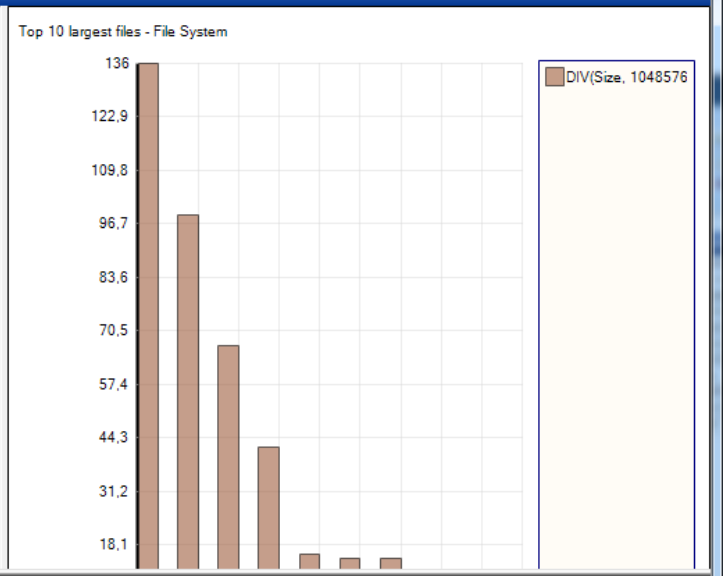
File System

- Top 10 largest files
- Top 20 largest files that have not...
- The top 10 largest duplicate files

IIS Logs | Event Logs | Active Directory | Log4Net | File System | T-SQL

Top 10 largest files - File System

EXTRACT_PATH(Path)	EXTRACT_FILENAME(Path)	DIV(Size, 1048576)
d:\apps	OOo_3.3.0_Win_x86_install_en-US.exe	136
d:\apps	eclipse-java-helios-SR2-win32-x86_64.zip	99
d:\apps	jdk-6u25-windows-x64.exe	67
d:\apps	ActivePython-2.7.1.4-win64-x64.msi	42
d:\apps	jre-6u25-windows-x64.exe	16
d:\apps	thebat_pro_4-2-36-4.rar	15
d:\apps\ida-pro	idafree50.exe	15
d:\apps	KillDiskSuiteFree-Setup.exe	11
d:\apps	FoxitReader431_enu_Setup.exe	7
d:\apps\cutepdf	converter.exe	5



Query

```
SELECT TOP 10 EXTRACT_PATH(Path), EXTRACT_FILENAME(Path), DIV(Size, 1048576)
FROM d:\apps\*.* ORDER BY DIV(Size, 1048576) DESC
```

Input records: 0, Output records: 0, Rows in table: 10

File System

www.lizard-labs.net

SQALP (Simple Query Analyzer for Log Parser)

Visual LogParser - Serialcoder.net

File Edit Query View Tools Windows Help

EVT

Untitled 1* | Untitled 2* | Untitled 3* | Untitled 4*

```
SELECT RecordNumber, TimeGenerated, Message
FROM Application
WHERE EventID=8194 AND SourceName='VSS'
order by RecordNumber desc
```

batch file alternative (%filename% in sql)

echo off
cls
logparser.exe -i:W3C file:WinFW.sql?filename=C:\pfirewall.log -o:DATAGRID

Examples

EVT Input Format Examples

Logons

Create an XML report file containing logon account names and dates from the Security Event Log:

```
LogParser "SELECT TimeGenerated AS
LogonDate, EXTRACT_TOKEN(Strings, 0, '|')
AS Account INTO Report.xml FROM Security
WHERE EventID NOT IN (541;542;543) AND
```

FROM entry | Fields | Parameters | Examples

Results

RecordNumber	TimeGenerated	Message
16489	2009-05-08 13:15:32	Volume Shadow Copy Service error: Unexpected error querying for the IVssWriterCallback interface. hr = 0x80...
15886	2009-05-05 17:13:24	Volume Shadow Copy Service error: Unexpected error querying for the IVssWriterCallback interface. hr = 0x80...
15816	2009-05-05 16:23:41	Volume Shadow Copy Service error: Unexpected error querying for the IVssWriterCallback interface. hr = 0x80...
15708	2009-05-05 10:28:17	Volume Shadow Copy Service error: Unexpected error querying for the IVssWriterCallback interface. hr = 0x80...
15705	2009-05-05 10:26:53	Volume Shadow Copy Service error: Unexpected error querying for the IVssWriterCallback interface. hr = 0x80...
14829	2009-04-16 09:42:28	Volume Shadow Copy Service error: Unexpected error querying for the IVssWriterCallback interface. hr = 0x80...
14737	2009-04-15 20:05:55	Volume Shadow Copy Service error: Unexpected error querying for the IVssWriterCallback interface. hr = 0x80...
14734	2009-04-15 20:05:19	Volume Shadow Copy Service error: Unexpected error querying for the IVssWriterCallback interface. hr = 0x80...
14594	2009-04-13 02:07:46	Volume Shadow Copy Service error: Unexpected error querying for the IVssWriterCallback interface. hr = 0x80...
14590	2009-04-12 23:45:07	Volume Shadow Copy Service error: Unexpected error querying for the IVssWriterCallback interface. hr = 0x80...
14587	2009-04-12 23:43:30	Volume Shadow Copy Service error: Unexpected error querying for the IVssWriterCallback interface. hr = 0x80...
14004	2009-03-31 02:07:05	Volume Shadow Copy Service error: Unexpected error querying for the IVssWriterCallback interface. hr = 0x80...
13928	2009-03-29 13:34:42	Volume Shadow Copy Service error: Unexpected error querying for the IVssWriterCallback interface. hr = 0x80...
13904	2009-03-28 13:11:06	Volume Shadow Copy Service error: Unexpected error querying for the IVssWriterCallback interface. hr = 0x80...
13901	2009-03-28 13:08:54	Volume Shadow Copy Service error: Unexpected error querying for the IVssWriterCallback interface. hr = 0x80...

Results | Messages

Query batch completed.

DATAGRID

EVT parameters

Misc	
binaryFormat	HEX
direction	FW
formatMessage	True
formatMsg	True
fullEventCode	False
fullText	True
iCheckpoint	
msgErrorMode	MSG
resolveSIDs	False
stringsSep	|

binaryFormat
Format of the binary Data field

MicroSoft Log Parser, events etc.

- Log Parser download
  - http://www.microsoft.com/technet/scriptcenter/tools/logparser/default.mspx
- Visual Log Parser GUI (SQALP)

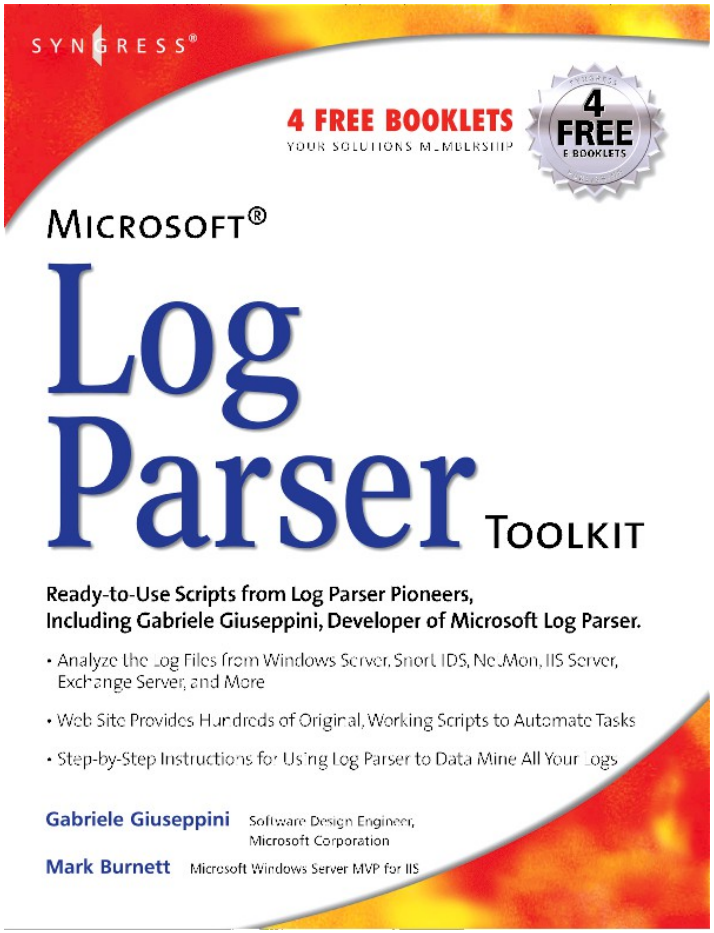
http://en.serialcoder.net/logiciels/visual-logparser.aspx

- Log Parser Help File
  - Very good resource!
- Book with loads of scripts and queries

http://www.elsevierdirect.com/companion.jsp?ISBN=9781932266528

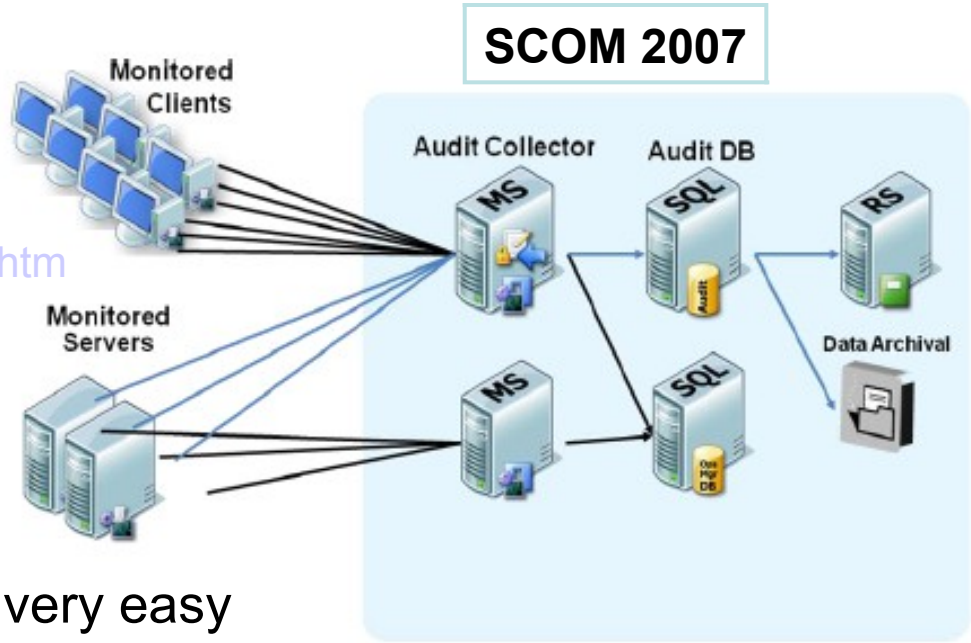
- Microsoft log events
  - http://eventlogs.blogspot.com
  - http://eventid.net (what does it mean?)
- Forensic Log Parsing with Microsoft's Log Parser
  - http://www.securityfocus.com/infocus/1712

"Mastering Windows Network Forensics and Investigation" have a good tutorial as well!



Microsoft System Center Operations Manager 2007 R2 and Syslog (RFC 3164) alternatives

- Microsoft System Center Operations Manager är ett händelse- och prestandaövervakningsverktyg som innehåller en mängd funktioner för att reducera den tid det tar att konfigurera ett system eller en tillämpning
- Course and other white papers
  - http://www.microsoft.com/systemcenter/operationsmanager/en/us/default.aspx
- End-to-End Service Monitoring
- Client Monitoring
- Audit Collection

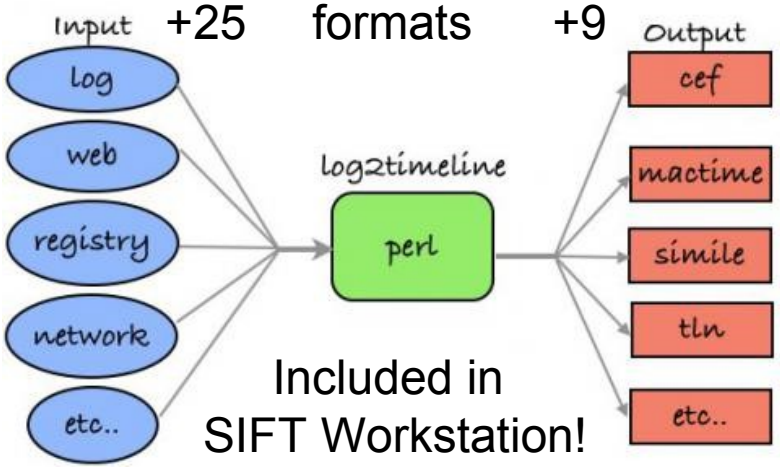


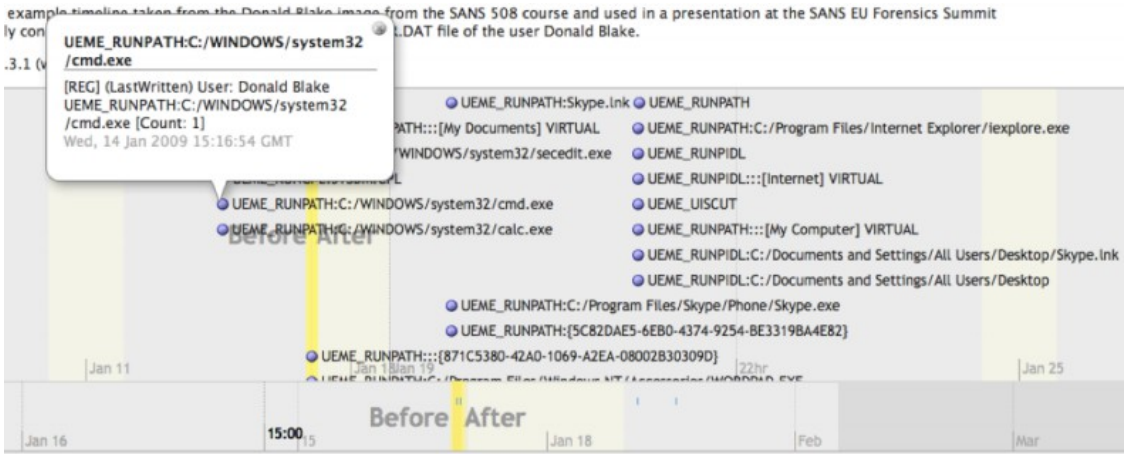
- Syslog - GNU/Linux setup
  - http://www.aboutdebian.com/syslog.htm
- Other (Windows) Syslog servers
  - http://en.wikipedia.org/wiki/Syslog
- Convert Windows log to Syslog
  - http://www.syslogserver.com
- Setting up Syslog to redirect logging to separate log server is very easy

Log2timeline - http://log2timeline.net/

- A framework for automatic creation of a super timeline. The main purpose is to provide a single tool to parse various log files and artifacts found on suspect systems (and supporting systems, such as network equipment) and produce a timeline that can be analysed by forensic investigators/analysts
- The tool is written in Perl for Linux but has been tested using Mac OS X (10.5.7+ and 10.6.+). Parts of it should work natively in Windows as well (with ActiveState Perl installed)
- "Mastering the Super Timeline With log2timeline" can be downloaded here
  - http://www.sans.org/reading_room/whitepapers/logging/mastering-super-timeline-log2timeline_33438

SIMILE: http://www.simile-widgets.org/timeline/





Common Linux log file names and usage

- Most of the logs are located in /var/log or /var/log/<foldername>/*
- Usually in ASCII format – any text editor/script will do it
- Examples of logs, there may be some distribution name differences
  - /var/log/auth.log: Authenication logs
  - /var/log/cron.log: Crond logs (cron job)
  - /var/log/kern.log: Kernel logs
  - /var/log/message: General message and system related stuff
  - /var/log/boot.log : System boot log
  - /var/log/mail/*: Mail server logs (more files inside this directory)
  - /var/log/apache/*: Apache access and error logs directory
  - /var/log/samba/*: SMB server logs
  - /var/log/utmp or /var/log/wtmp : Login records file
- utmp, wtmp and lastlog (who, last, lastb, lastlog, w, etc.)
  - Are binary files (utmp structure), lastlog may be distribution specific
- logrotate /etc/logrotate.conf
  - Rotate, compress (and mail logs), run as a daily cron job

utmp.h structure (Ubuntu 9.04)

```
struct utmp {
        short   ut_type;            /* Type of record */
        pid_t   ut_pid;             /* PID of login process */
        char    ut_line[UT_LINESIZE]; /* Device name of tty - "/dev/" */
        char    ut_id[4];           /* Terminal name suffix, or inittab(5) ID */
        char    ut_user[UT_NAMESIZE]; /* Username */
        char    ut_host[UT_HOSTSIZE]; /* Hostname for remote login, or kernel version for run-level messages */
        struct  exit_status ut_exit;  /* Exit status of a process marked as DEAD_PROCESS;
                        not used by Linux init(8) */
        /* The ut_session and ut_tv fields must be the same size when compiled 32- and 64-bit.
          This allows data files and shared memory to be shared between 32- and 64-bit applications. */
      #if __WORDSIZE == 64 && defined __WORDSIZE_COMPAT32
        int32_t ut_session;         /* Session ID (getsid(2)), used for windowing */
        struct {
            int32_t tv_sec;         /* Seconds */
            int32_t tv_usec;        /* Microseconds */
        } ut_tv;                    /* Time entry was made */
      #else
         long   ut_session;         /* Session ID */
         struct timeval ut_tv;      /* Time entry was made */
      #endif
        int32_t ut_addr_v6[4];      /* Internet address of remote host; IPv4 address uses just ut_addr_v6[0] */
        char __unused[20];          /* Reserved for future use */
      };
```