Forensics II

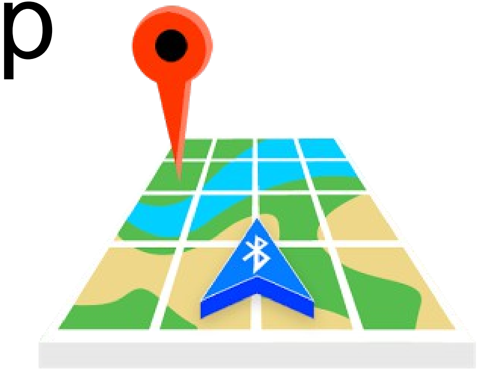
Android reverse engineering

Logs [repetition]

Android reverse enginering tools

- dex2jar
  - A group of tools to work with android .dex and java .class files in combination with for example Java Decompiler
  - https://code.google.com/p/dex2jar/
- smali/baksmali
  - An assembler/disassembler for the dex format used by dalvik, Android's Java VM implementation
  - https://code.google.com/p/smali/
- android-apktool
  - A tool for reverse engineering 3rd party, closed, binary Android apps
  - It can decode resources to nearly original form and rebuild them after making some modifications (smali/baksmali integration)
  - It makes possible to **debug smali code** step by step via DDMS (wiki)
  - https://code.google.com/p/android-apktool/
- apk-signer
  - https://code.google.com/p/apk-signer/

Reversing an Android app



- Task – get rid of the lockout time nag in the Android Bluetooth GPS output program
  - http://www.meowsbox.com/btgps/index.html
- Tools
  - Apktool, dex2jar, Java Decompiler and jarsigner (Java JDK)
- Get hold of the apk file e.g. /data/app/com.meowsbox.btgps.apk, (can also be in /data/app-private/) from the Android phone or Internet
- Unzip the com.meowsbox.btgps.apk file and grab classes.dex file
  - Run ”d2j-dex2jar classes.dex” which will convert the dex file into a ordinary jar file which can be opened with Java Decompiler
- Run ”apktool d com.meowsbox.btgps.apk” which will decompress it and disassembly the apk file
  - A folder is created with the resources and .smali ”dalvik” code etc.
- Using Java Decompiler try to localize where the time nag is in the java code and find the corresponding code in the smali ”assemblies”

Java vs. dalvik code

I changed the opcode from **if-eqz** to **if-nez** in BluetoothChat.smali

```
public void sendNMEAString(String paramString)
{
  if (this.mChatService.getState() == 3)
  {
    if (!this.isRegistered)
      break label44;
    byte[] arrayOfByte1 = paramString.getBytes();
    this.mChatService.write(arrayOfByte1);
    int i = this.limit_nmeaCount + 1;
    this.limit_nmeaCount = i;
  }
  while (true)
  {
    return;
    label44: if (this.limit_nmeaCount < 3000)
    {
      byte[] arrayOfByte2 = paramString.getBytes();
      this.mChatService.write(arrayOfByte2);
      int j = this.limit_nmeaCount + 1;
      this.limit_nmeaCount = j;
      continue;
    }
  TextView localTextView = (TextView)findViewById(2131099664);
  localTextView.setText(
    "***Trial time limit reached: GPS output disabled.");
```

```
.method public sendNMEAString(Ljava/lang/String;)V
    .locals 8
    .parameter "nmeaString"

    .prologue
    const/4 v7, 0x1

    .line 954
    iget-object v4, p0, Lcom/meowsbox/btgps/BluetoothChat;->mChatService:Lcom/meowsbox/btgps/BluetoothChatService;

    invoke-virtual {v4}, Lcom/meowsbox/btgps/BluetoothChatService;->getState()I

    move-result v4

    const/4 v5, 0x3

    if-ne v4, v5, :cond_0

    .line 955
    iget-boolean v4, p0, Lcom/meowsbox/btgps/BluetoothChat;->isRegistered:Z

    if-nez v4, :cond_1

    .line 956
    invoke-virtual {p1}, Ljava/lang/String;->getBytes()[B
```

First if – jump to :cond_0

Second if – jump!

Repackaging and protection

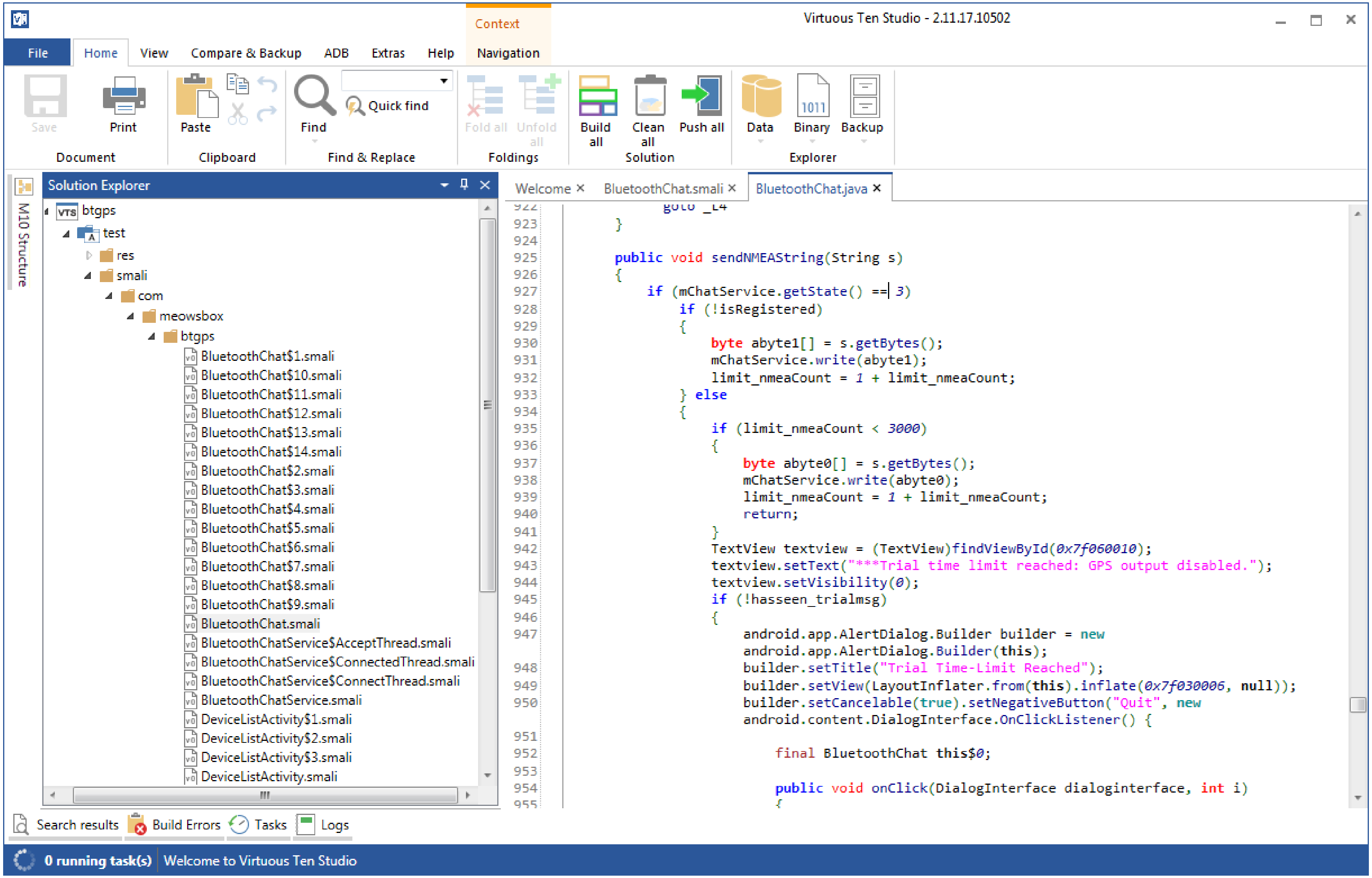
- When the smali code changes are saved run
  - ”apktool b com.meowsbox.btgps com.meowsbox.btgps_new.apk”
- After rebuilding the application it needs to be signed, run
  - "C:\Program Files\Java\jdk1.7.0_XX\bin\jarsigner" -keystore C:\Users\hjo\.android\debug.keystore com.meowsbox.btgps_new.apk androiddebugkey
  - Use the password android
- After this you can install the cracked app with ADB etc.

- To protect your code enable proguard in the project.properties file
  - proguard.config == proguard-project.txt
  - Note that Proguard never runs when you compile ”debug” code!
- To obfuscate your android program (android:debuggable should be off in the AndroidManifest.xml as well) and create ”release” code
  - In eclipse mark your project and select File > Export > Android > Export Android Application which will compile and align your code
  - Then follow the wizard and point out your debug keystore (as above) or your registred developer keystore and enter the password

Virtuous Ten Studio

- Fully featured IDE (free, small time nag)
- Seamless integration of useful external tools
  - ApkTool, Smali/Baksmali, ADB, Zipalign, Sign, dex2jar
  - Winmerge, Remote Theme Injector (RTI) and many more
- Work with your apks just like having real java code
- Edit smali code like never before
  - Syntax highlighting, Live syntax error checking
  - Jumping to smali references (method calls, fields, classes, gotos), Help files on almost every smali command and topic
- Enhanced XML workflow
- Unpack and repack boot images
  - Edit any content of your boot.img (no need of Linux)
- Direct communication with the Android device
- Tutorials
  - http://www.virtuous-ten-studio.com/

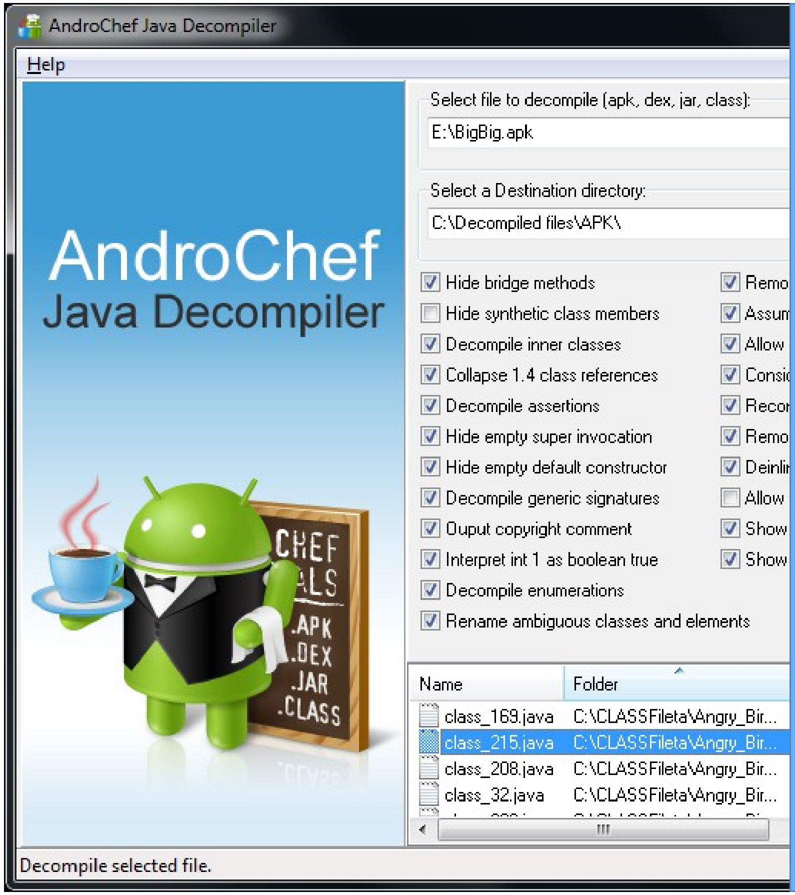
Virtuous Ten Studio (VTS)



```
        goto _L4
    }

    public void sendNMEAString(String s)
    {
        if (mChatService.getState() == 3)
            if (!isRegistered)
            {
                byte abyte1[] = s.getBytes();
                mChatService.write(abyte1);
                limit_nmeaCount = 1 + limit_nmeaCount;
            } else
            {
                if (limit_nmeaCount < 3000)
                {
                    byte abyte0[] = s.getBytes();
                    mChatService.write(abyte0);
                    limit_nmeaCount = 1 + limit_nmeaCount;
                    return;
                }
                TextView textview = (TextView)findViewById(0x7f060010);
                textview.setText("***Trial time limit reached: GPS output disabled.");
                textview.setVisibility(0);
                if (!hasseen_trialmsg)
                {
                    android.app.AlertDialog.Builder builder = new
                    android.app.AlertDialog.Builder(this);
                    builder.setTitle("Trial Time-Limit Reached");
                    builder.setView(LayoutInflater.from(this).inflate(0x7f030006, null));
                    builder.setCancelable(true).setNegativeButton("Quit", new
                    android.content.DialogInterface.OnClickListener() {

                        final BluetoothChat this$0;

                        public void onClick(DialogInterface dialoginterface, int i)
                        {
```

AndroChef Java Decompiler

- AndroChef Java Decompiler builds upon DJ Java Decompiler at: http://www.neshkov.com/
- AndroChef: http://www.neshkov.com/ac_decompiler.html



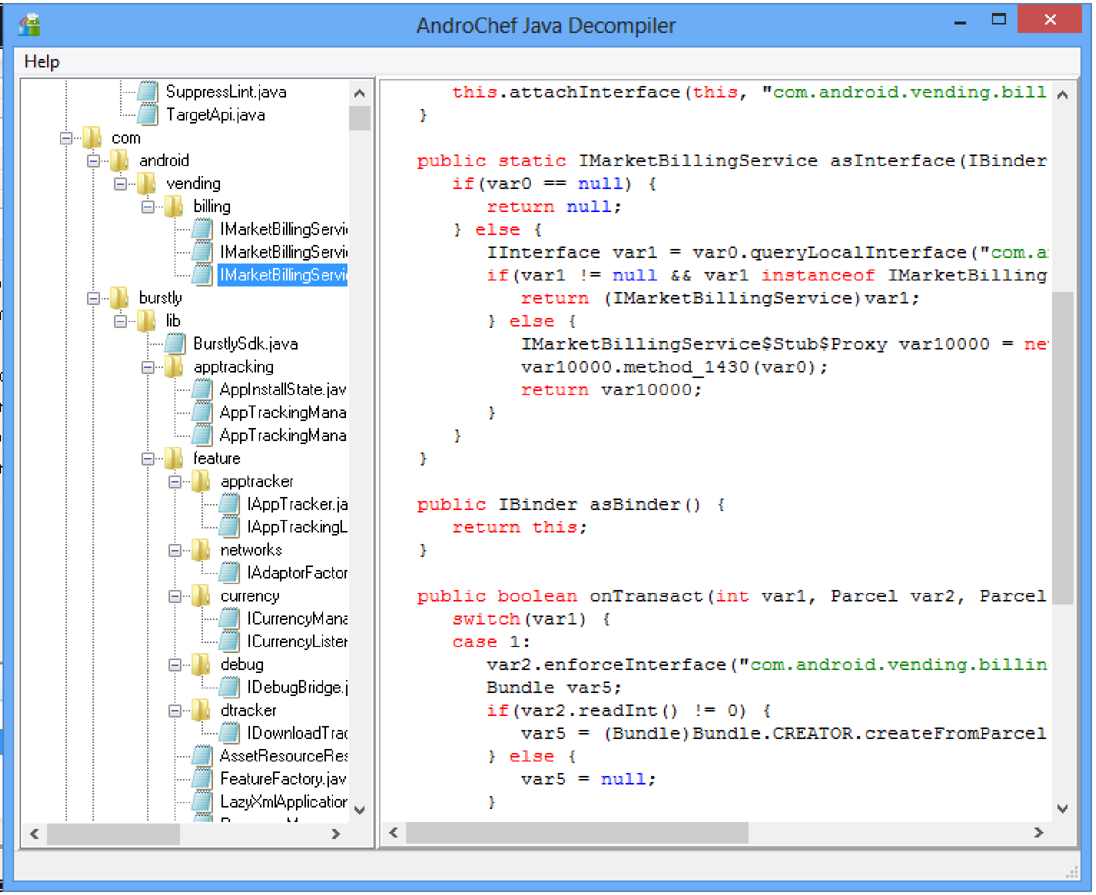
Select file to decompile (apk, dex, jar, class):
E:\BigBig.apk

Select a Destination directory:
C:\Decompiled files\APK\

☑ Hide bridge methods ☑ Remo
☐ Hide synthetic class members ☑ Assum
☑ Decompile inner classes ☑ Allow
☑ Collapse 1.4 class references ☑ Consi
☑ Decompile assertions ☑ Recor
☑ Hide empty super invocation ☑ Remo
☑ Hide empty default constructor ☑ Deinli
☑ Decompile generic signatures ☐ Allow
☑ Ouput copyright comment ☑ Show
☑ Interpret int 1 as boolean true ☑ Show
☑ Decompile enumerations
☑ Rename ambiguous classes and elements

Name	Folder
class_169.java	C:\CLASSFileta\Angry_Bir...
class_215.java	C:\CLASSFileta\Angry_Bir...
class_208.java	C:\CLASSFileta\Angry_Bir...
class_32.java	C:\CLASSFileta\Angry_Bir...

Decompile selected file.

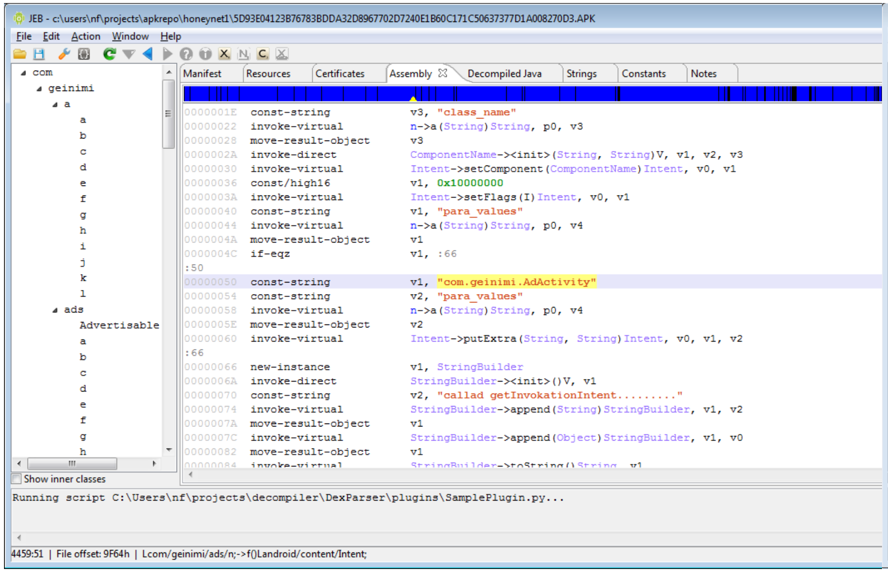


```
         this.attachInterface(this, "com.android.vending.bill
      }

      public static IMarketBillingService asInterface(IBinder
         if(var0 == null) {
            return null;
         } else {
            IInterface var1 = var0.queryLocalInterface("com.a
            if(var1 != null && var1 instanceof IMarketBilling
               return (IMarketBillingService)var1;
            } else {
               IMarketBillingService$Stub$Proxy var10000 = ne
               var10000.method_1430(var0);
               return var10000;
            }
         }
      }

      public IBinder asBinder() {
         return this;
      }

      public boolean onTransact(int var1, Parcel var2, Parcel
         switch(var1) {
         case 1:
            var2.enforceInterface("com.android.vending.billin
            Bundle var5;
            if(var2.readInt() != 0) {
               var5 = (Bundle)Bundle.CREATOR.createFromParcel
            } else {
               var5 = null;
            }
```

JEB - The Interactive Android Decompiler

- Full-fledged Dalvik decompiler. At its core, JEB's unique feature is its ability to directly decompile Dalvik bytecode to Java source code
- Interactivity. Analysts need flexible tools, especially when they deal with obfuscated or protected pieces of code
- Full APK view. Take advantage of the full APK view, including decompressed manifest, resources, certificates, strings, constants, etc.
- API for Automation. Use JEB's Application Programming Interface (API) to write Python scripts and plugins, and automate your analysis needs.
- Track your progress. Save your analysis to binary files, track progress through JEB's revision history mechanism
- Technical support and Multi-platform
- http://www.android-decompiler.com/

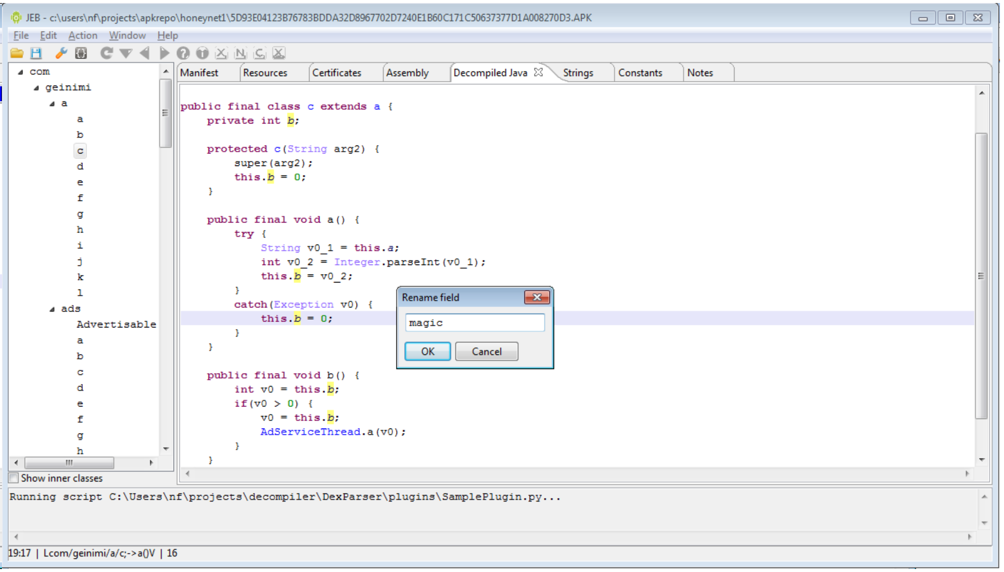
JEB Decompiler



```
0000001E  const-string          v3, "class_name"
00000022  invoke-virtual        n->a(String)String, p0, v3
00000028  move-result-object    v3
0000002A  invoke-direct         ComponentName-><init>(String, String)V, v1, v2, v3
00000030  invoke-virtual        Intent->setComponent(ComponentName)Intent, v0, v1
00000036  const/high16          v1, 0x10000000
0000003A  invoke-virtual        Intent->setFlags(I)Intent, v0, v1
00000040  const-string          v1, "para_values"
00000044  invoke-virtual        n->a(String)String, p0, v4
0000004A  move-result-object    v1
0000004C  if-eqz                v1, :66
:50
00000050  const-string          v1, "com.geinimi.AdActivity"
00000054  const-string          v2, "para_values"
00000058  invoke-virtual        n->a(String)String, p0, v4
0000005E  move-result-object    v2
00000060  invoke-virtual        Intent->putExtra(String, String)Intent, v0, v1, v2
:66
00000066  new-instance          v1, StringBuilder
0000006A  invoke-direct         StringBuilder-><init>()V, v1
00000070  const-string          v2, "callad getInvokationIntent........."
00000074  invoke-virtual        StringBuilder->append(String)StringBuilder, v1, v2
0000007A  move-result-object    v1
0000007C  invoke-virtual        StringBuilder->append(Object)StringBuilder, v1, v0
00000082  move-result-object    v1
00000084  invoke-virtual        StringBuilder->toString()String, v1
```

```
Running script C:\Users\nf\projects\decompiler\DexParser\plugins\SamplePlugin.py...
```

4459:51 | File offset: 9F64h | Lcom/geinimi/ads/n;->f()Landroid/content/Intent;



```
public final class c extends a {
    private int b;

    protected c(String arg2) {
        super(arg2);
        this.b = 0;
    }

    public final void a() {
        try {
            String v0_1 = this.a;
            int v0_2 = Integer.parseInt(v0_1);
            this.b = v0_2;
        }
        catch(Exception v0) {
            this.b = 0;
        }
    }

    public final void b() {
        int v0 = this.b;
        if(v0 > 0) {
            v0 = this.b;
            AdServiceThread.a(v0);
        }
    }
```

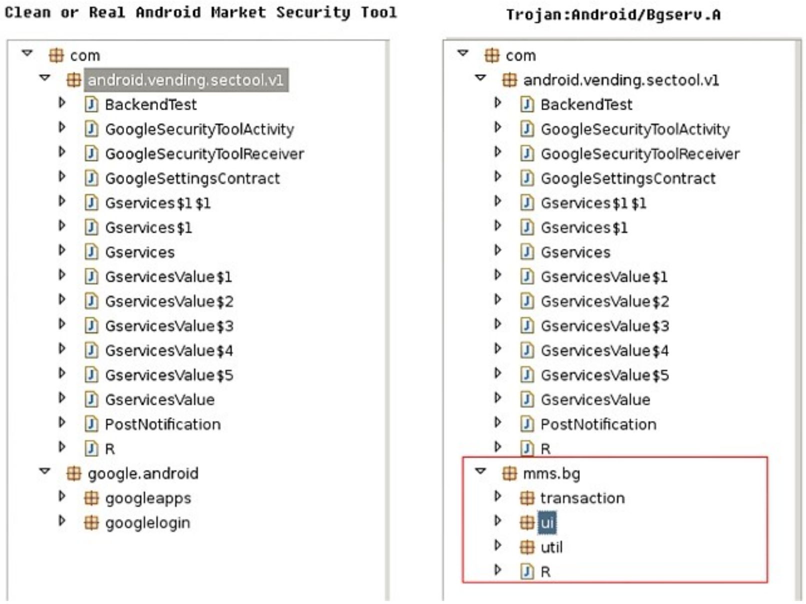
Rename field: magic

```
Running script C:\Users\nf\projects\decompiler\DexParser\plugins\SamplePlugin.py...
```

19:17 | Lcom/geinimi/a/c;->a()V | 16

Some Android Trojans analysis

- Geinimi Trojan Technical Analysis
  - Read, collect, send and delete SMS messages
  - Pull all contact information and send it to a remote server (number, name, the time they were last contacted)
  - Place a phone call
  - Silently download files
  - Launch a web browser with a specific URL
  - http://blog.mylookout.com/2011/01/geinimi-trojan-technical-analysis/
- Android Bgserv
  - Google released a security solution to deal with the Trojan:Android/DroidDream.A
  - http://www.f-secure.com/weblog/archives/00002116.html
- An app may contain an exploit which root your phone silently
  - Rageagainstthecage - CVE-2010-EASY Android local root exploit (C) 2010 by 743C
  - Patched/closed in 2.2.2 and later
- Solutions?
  - AV and firewall tools?

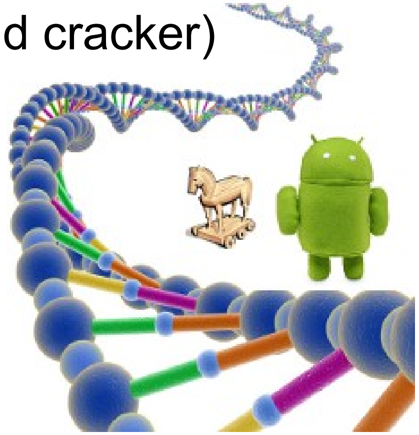


```
Clean or Real Android Market Security Tool
com
  android.vending.sectool.v1
    BackendTest
    GoogleSecurityToolActivity
    GoogleSecurityToolReceiver
    GoogleSettingsContract
    Gservices$1$1
    Gservices$1
    Gservices
    GservicesValue$1
    GservicesValue$2
    GservicesValue$3
    GservicesValue$4
    GservicesValue$5
    GservicesValue
    PostNotification
    R
  google.android
    googleapps
    googlelogin
```

```
Trojan:Android/Bgserv.A
com
  android.vending.sectool.v1
    BackendTest
    GoogleSecurityToolActivity
    GoogleSecurityToolReceiver
    GoogleSettingsContract
    Gservices$1$1
    Gservices$1
    Gservices
    GservicesValue$1
    GservicesValue$2
    GservicesValue$3
    GservicesValue$4
    GservicesValue$5
    GservicesValue
    PostNotification
    R
  mms.bg
    transaction
    ui
    util
    R
```

Android reversing resources

- Androguard Reverse Engineering
  - Malware and goodware analysis of Android applications
  - Wiki page have a open source database of Android Malwares
  - https://code.google.com/p/androguard/
- Virtual Machine for Android Reverse Engineering
  - https://redmine.honeynet.org/projects/are
- XDA developers
  - Android Development and Hacking > Android Software Development
- Android cracking
  - Got many nice crackmes and tutorials (Way of the android cracker)
  - http://androidcracking.blogspot.se/
- Google for “Android malware reversing”
  - http://www.android-x86.org/ (run apk in full speed)
  - http://www.malgenomeproject.org/

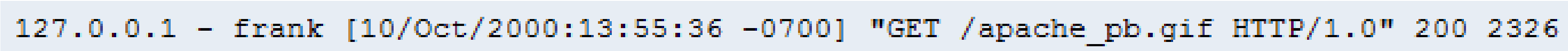


How to read and examine logs?

- 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

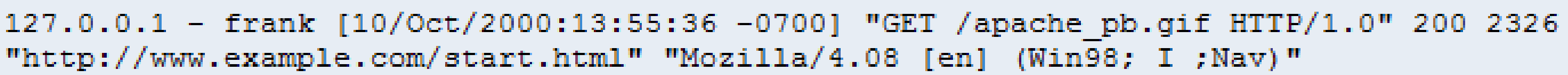


```
127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700] "GET /apache_pb.gif HTTP/1.0" 200 2326
```

- 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

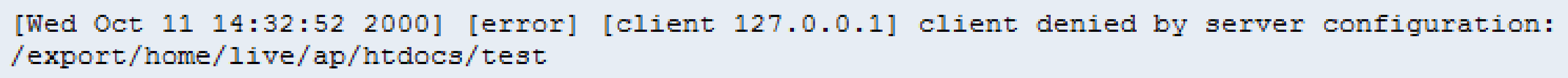
Combined Log Format

- 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)"
```

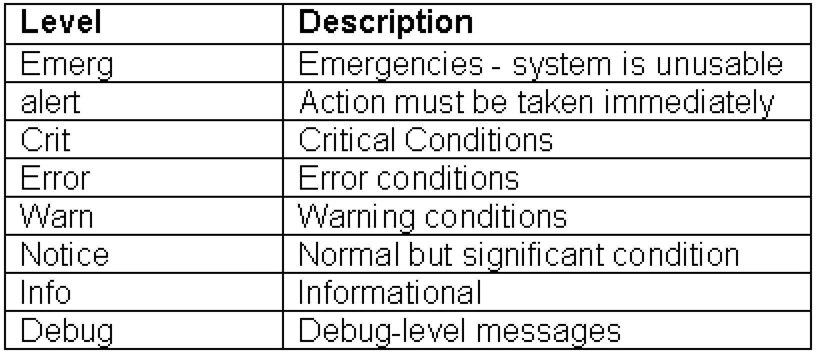
- **Apache error.log format**



```
[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

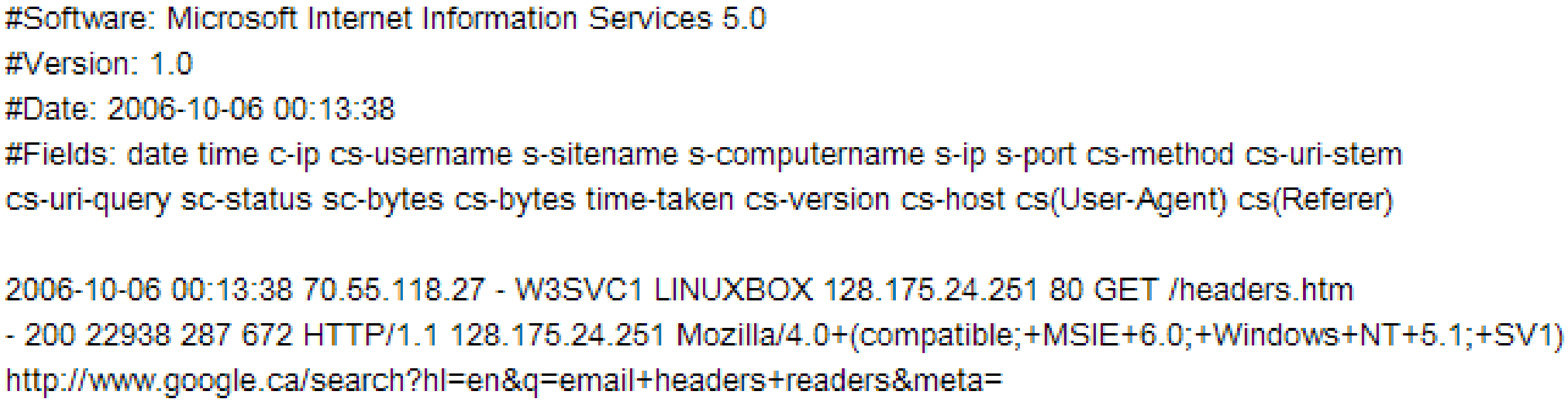
LogLevels



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

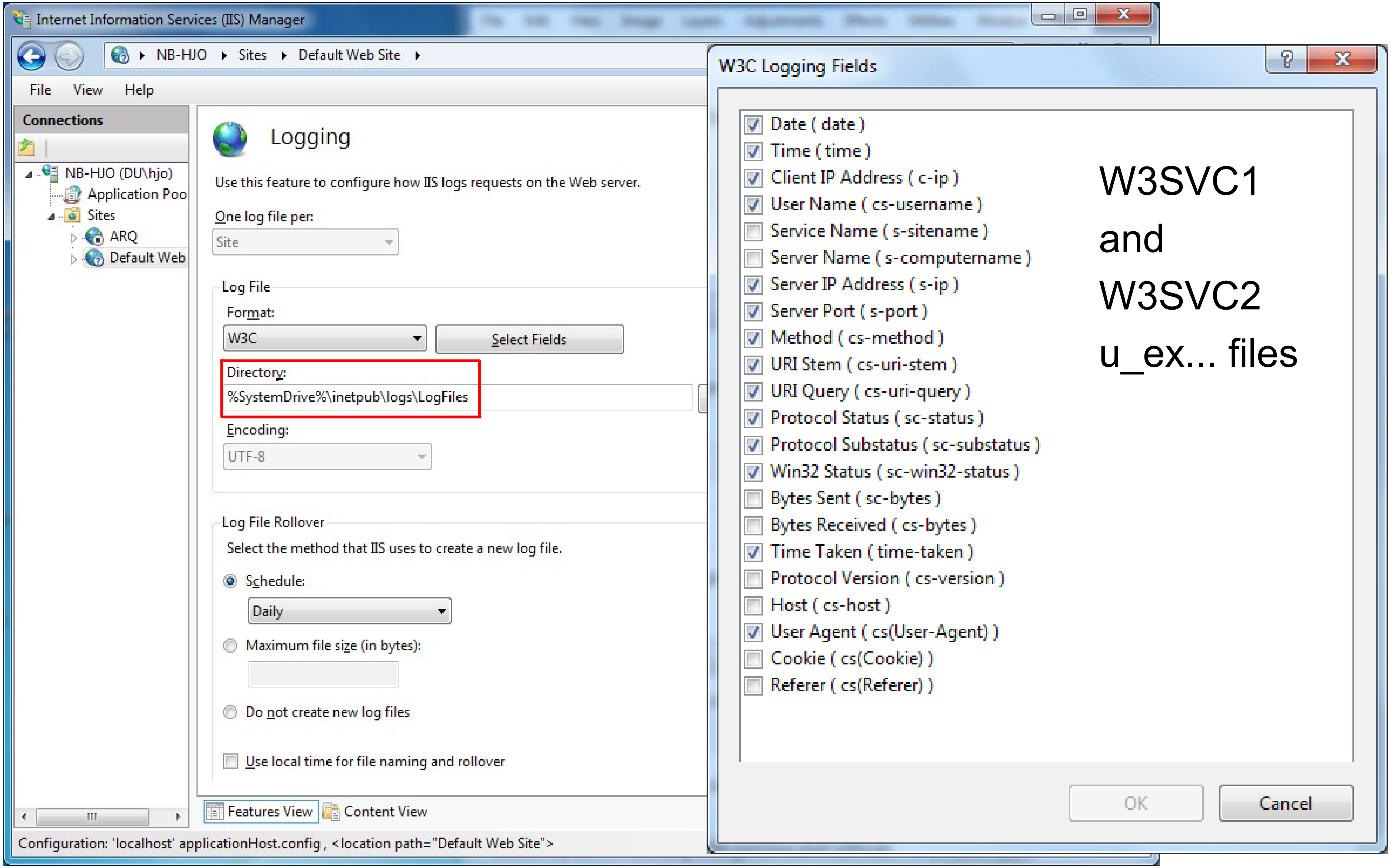
Windows XP IIS Logs

- 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



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

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

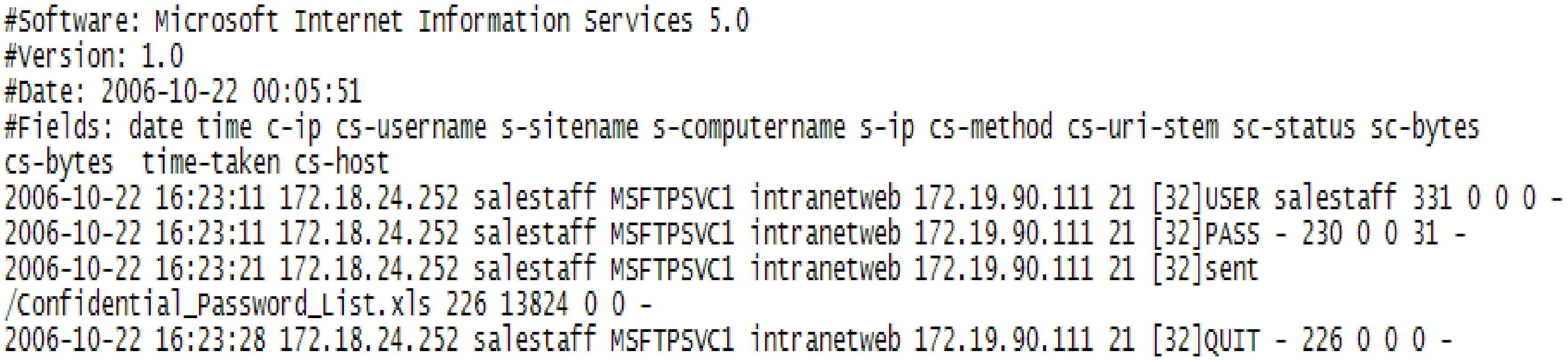
W3C Logging Fields

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

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

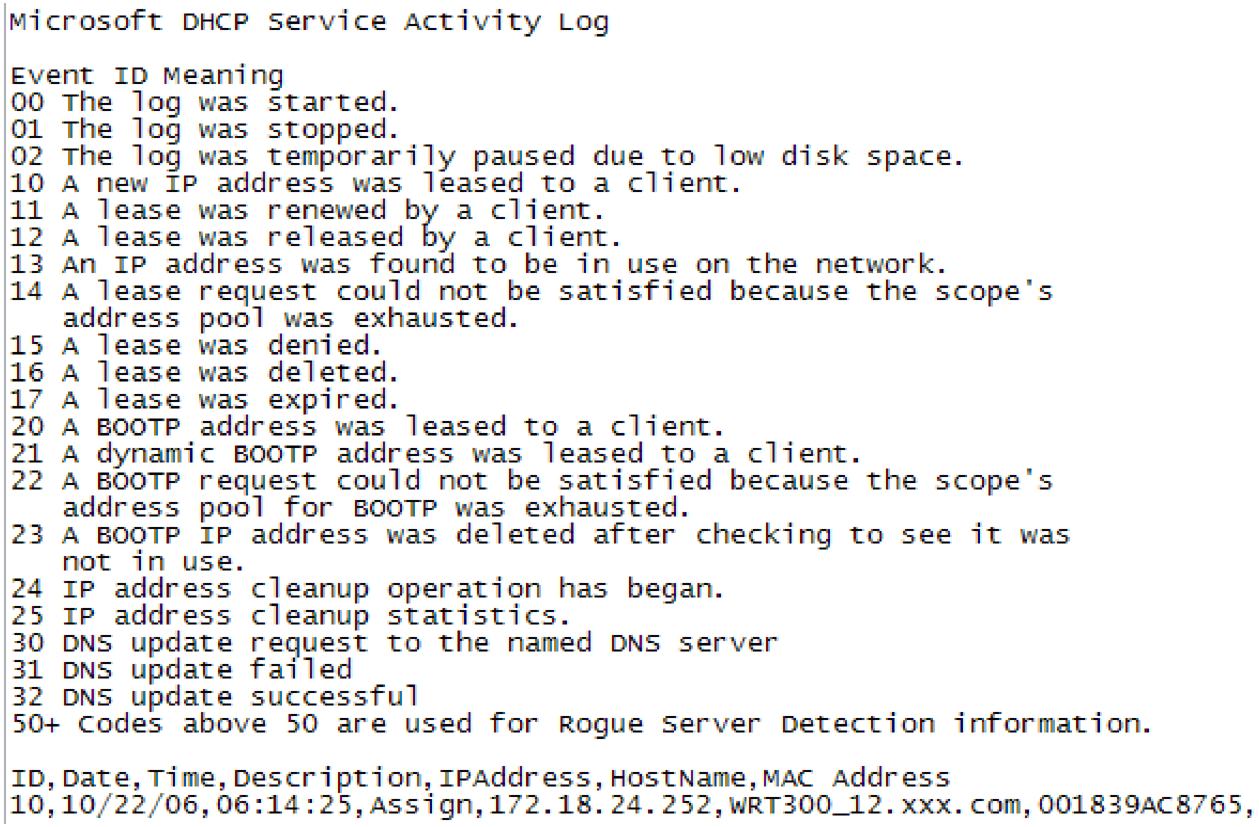


```
#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2006-10-22 00:05:51
#Fields: date time c-ip cs-username s-sitename s-computername s-ip cs-method cs-uri-stem sc-status sc-bytes
cs-bytes  time-taken cs-host
2006-10-22 16:23:11 172.18.24.252 salestaff MSFTPSVC1 intranetweb 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

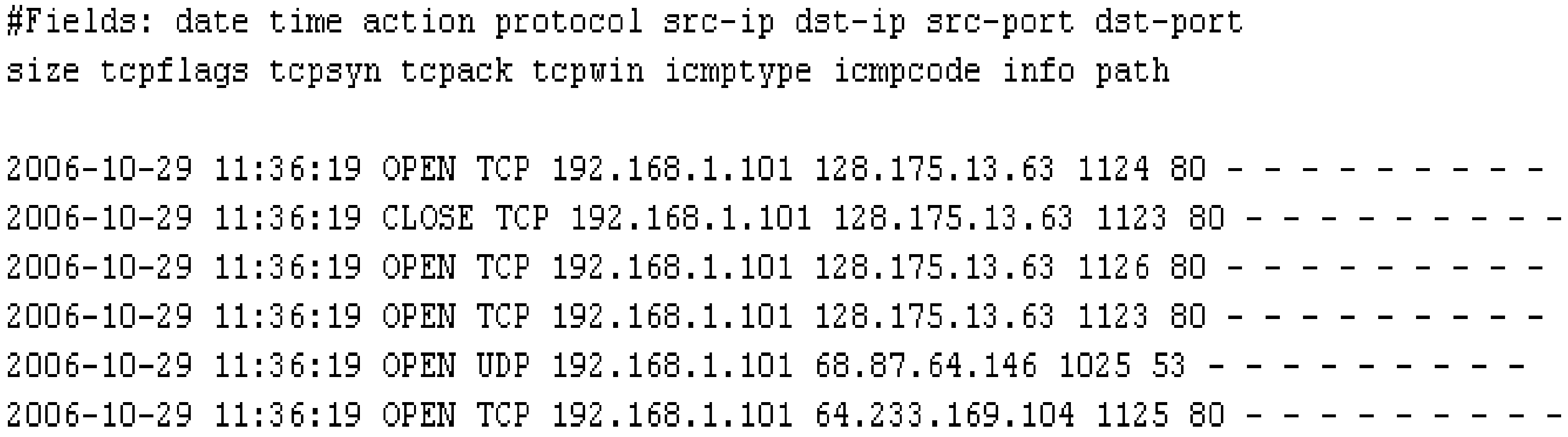


```
Microsoft DHCP Service Activity Log

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

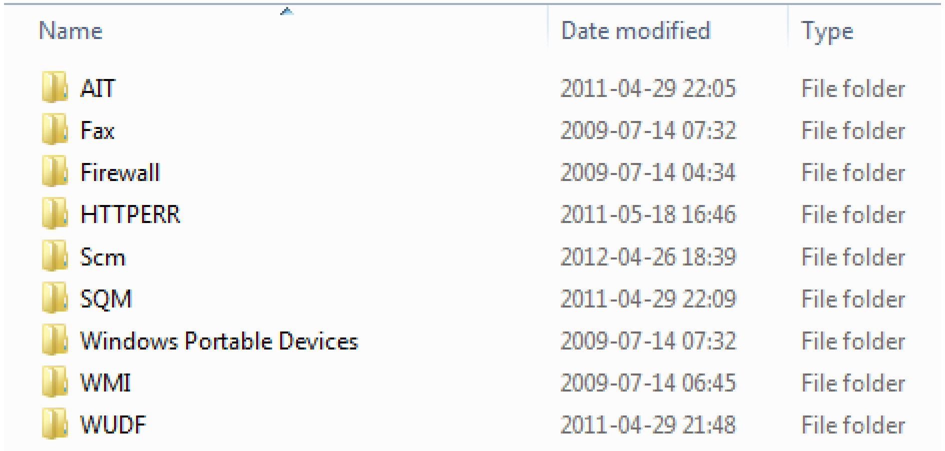
Windows XP Firewall Logs

- 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

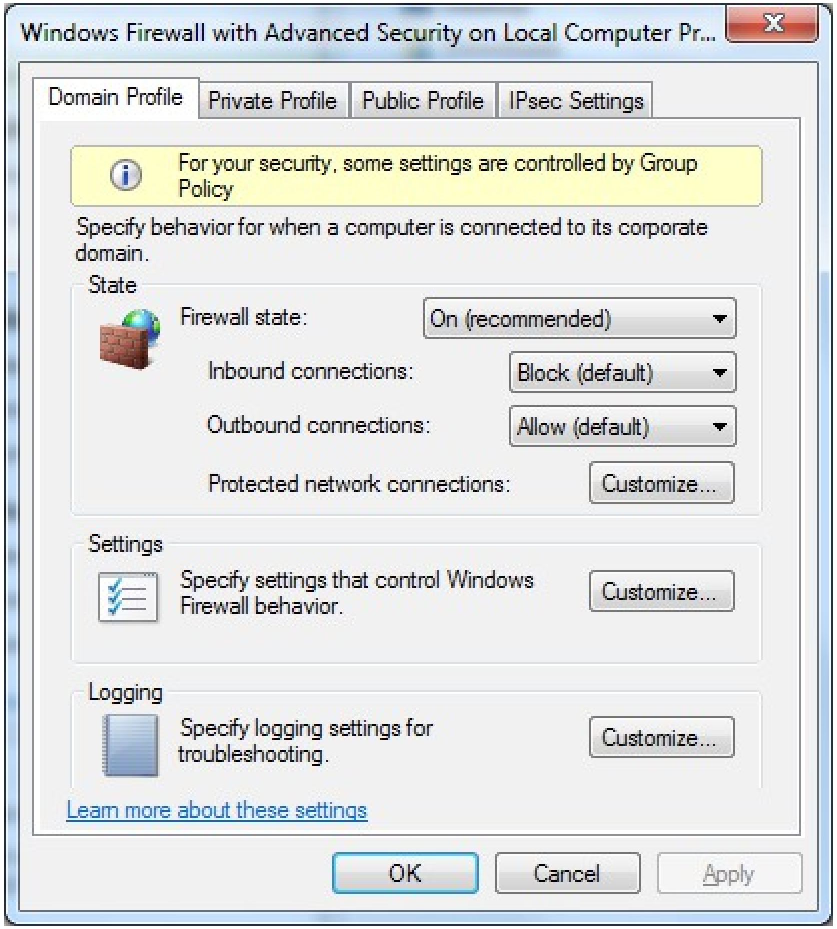


```
#Fields: date time action protocol src-ip dst-ip src-port dst-port
size tcpflags tcpsyn tcpack tcpwin icmptype icmpcode info path

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



Windows Firewall with Advanced Security on Local Computer Pr...

For your security, some settings are controlled by Group Policy

Specify behavior for when a computer is connected to its corporate domain.

State

Firewall state: On (recommended)

Inbound connections: Block (default)

Outbound connections: Allow (default)

Protected network connections:

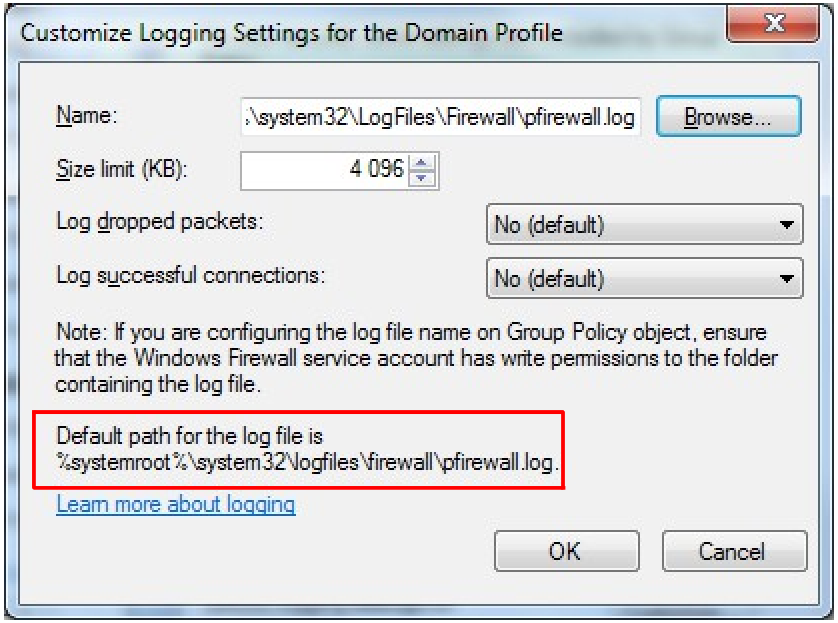
Settings

Specify settings that control Windows Firewall behavior.

Logging

Specify logging settings for troubleshooting.

Learn more about these settings



Customize Logging Settings for the Domain Profile

Name: .\system32\LogFiles\Firewall\pfirewall.log

Size limit (KB): 4 096

Log dropped packets: No (default)

Log successful connections: No (default)

Note: If you are configuring the log file name on Group Policy object, ensure that the Windows Firewall service account has write permissions to the folder containing the log file.

Default path for the log file is %systemroot%\system32\logfiles\firewall\pfirewall.log.

Learn more about logging

Microsoft Port Reporter

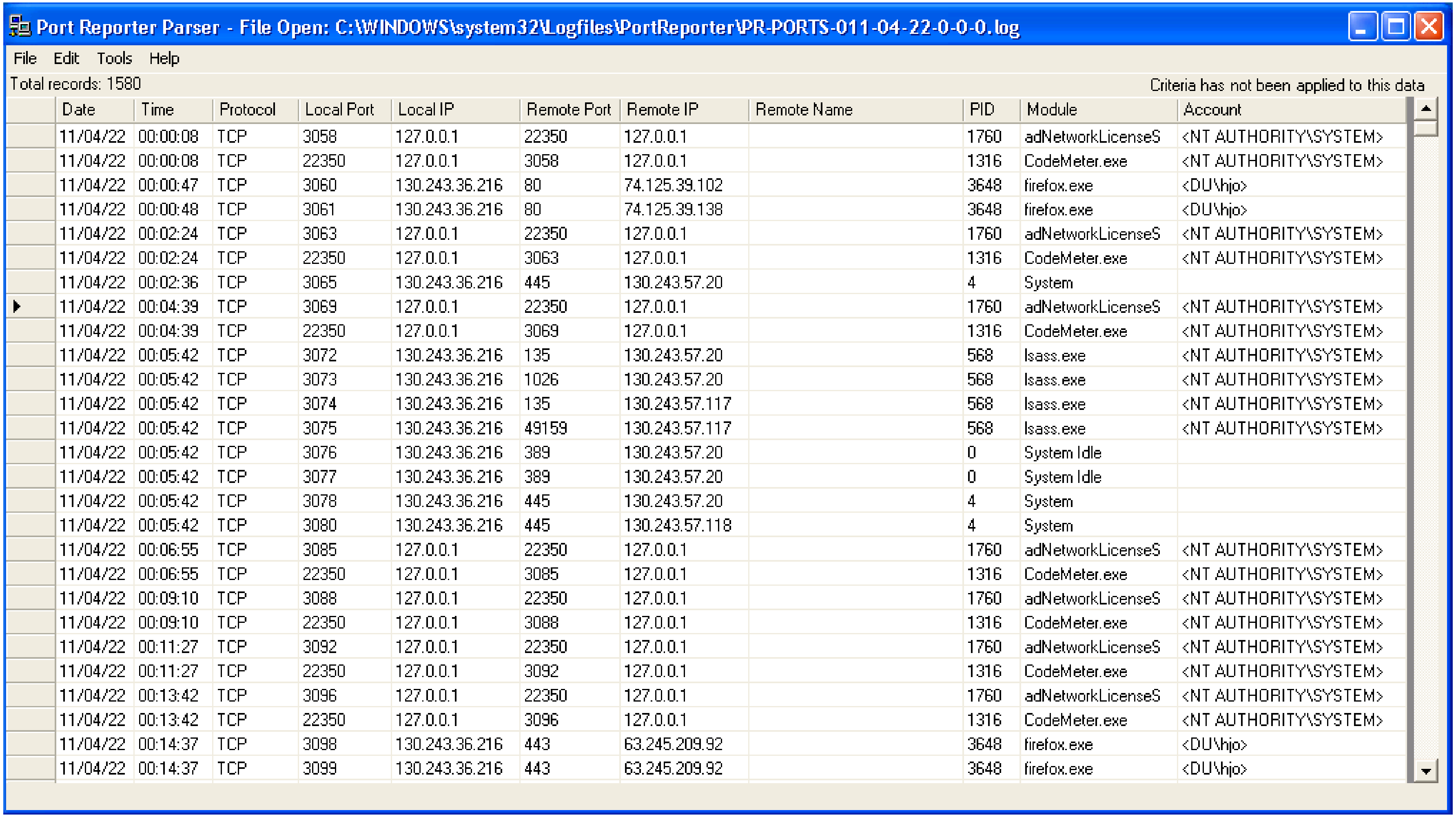
- Port Reporter is a logging service which runs on Microsoft Windows 2000, XP, Server 2003 and newer...?
- Useful for troubleshooting, security, application profiling, application development, and so on...
- Port Reporter logs
  - Ports that are used and the time they are used
  - Processes that use 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.



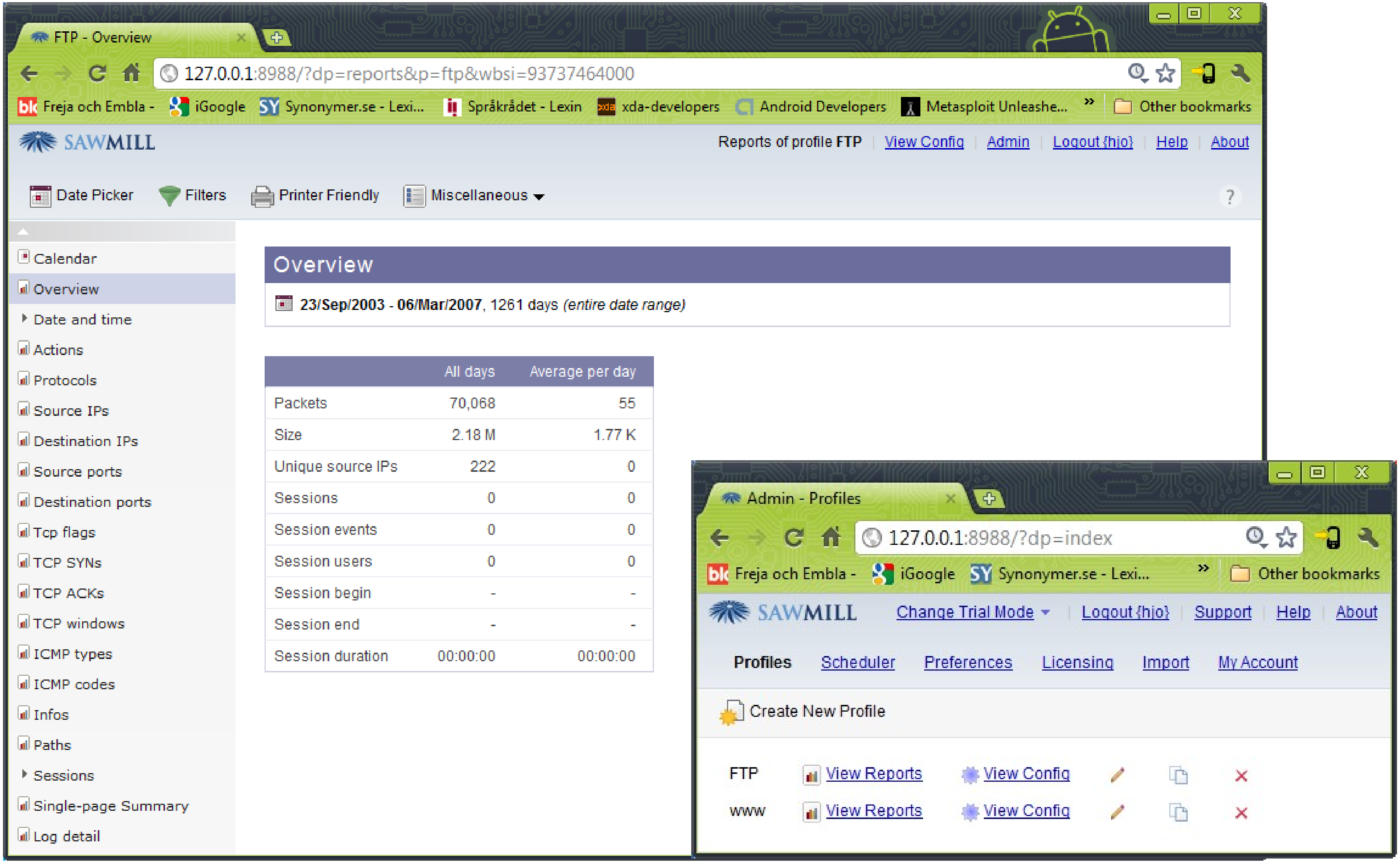
Port Reporter Parser - File Open: C:\WINDOWS\system32\Logfiles\PortReporter\PR-PORTS-011-04-22-0-0-0.log

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



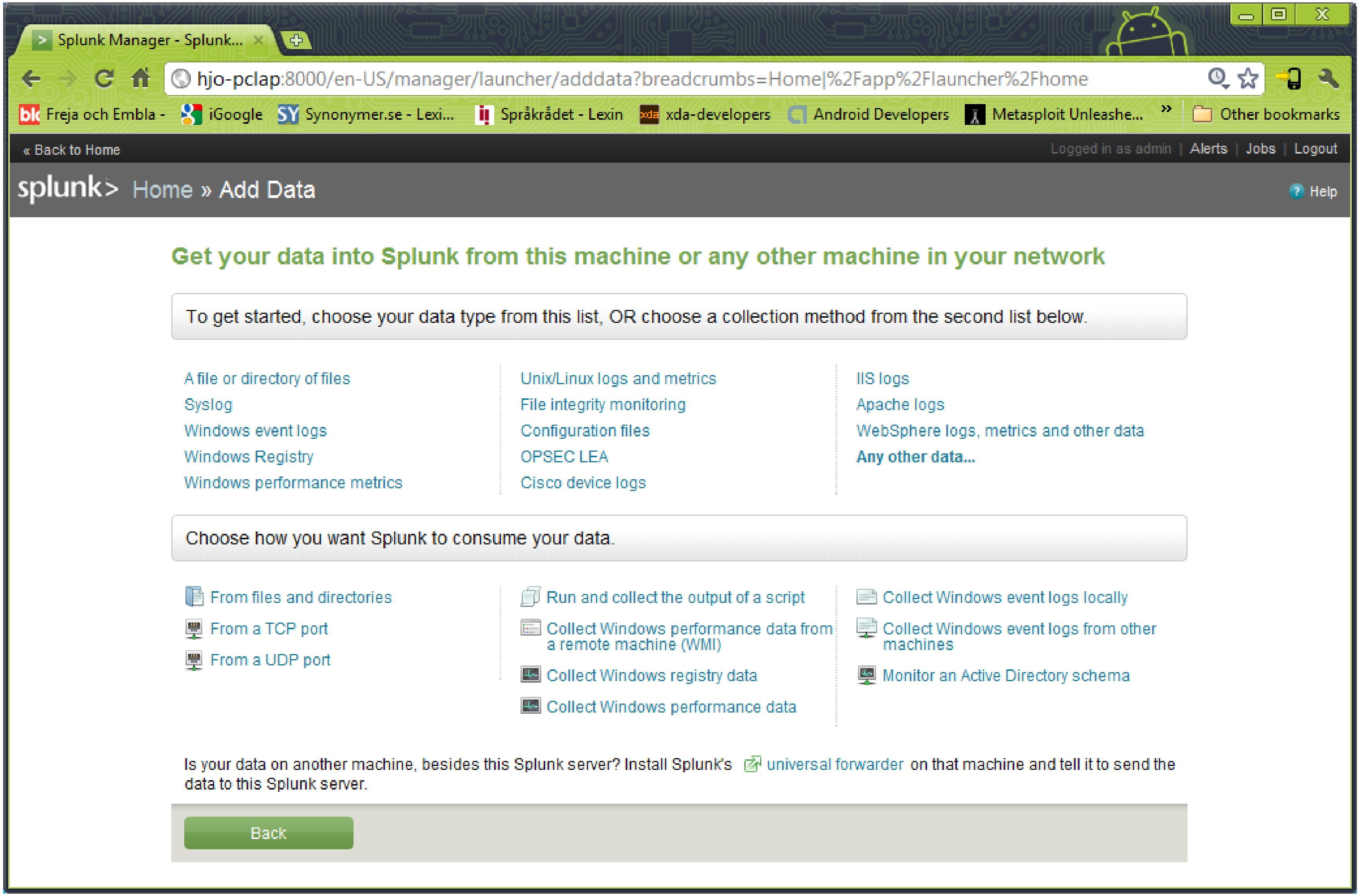
Overview

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

FTP	View Reports	View Config	✎	⧉	✕
www	View Reports	View Config	✎	⧉	✕

Splunk 1



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.

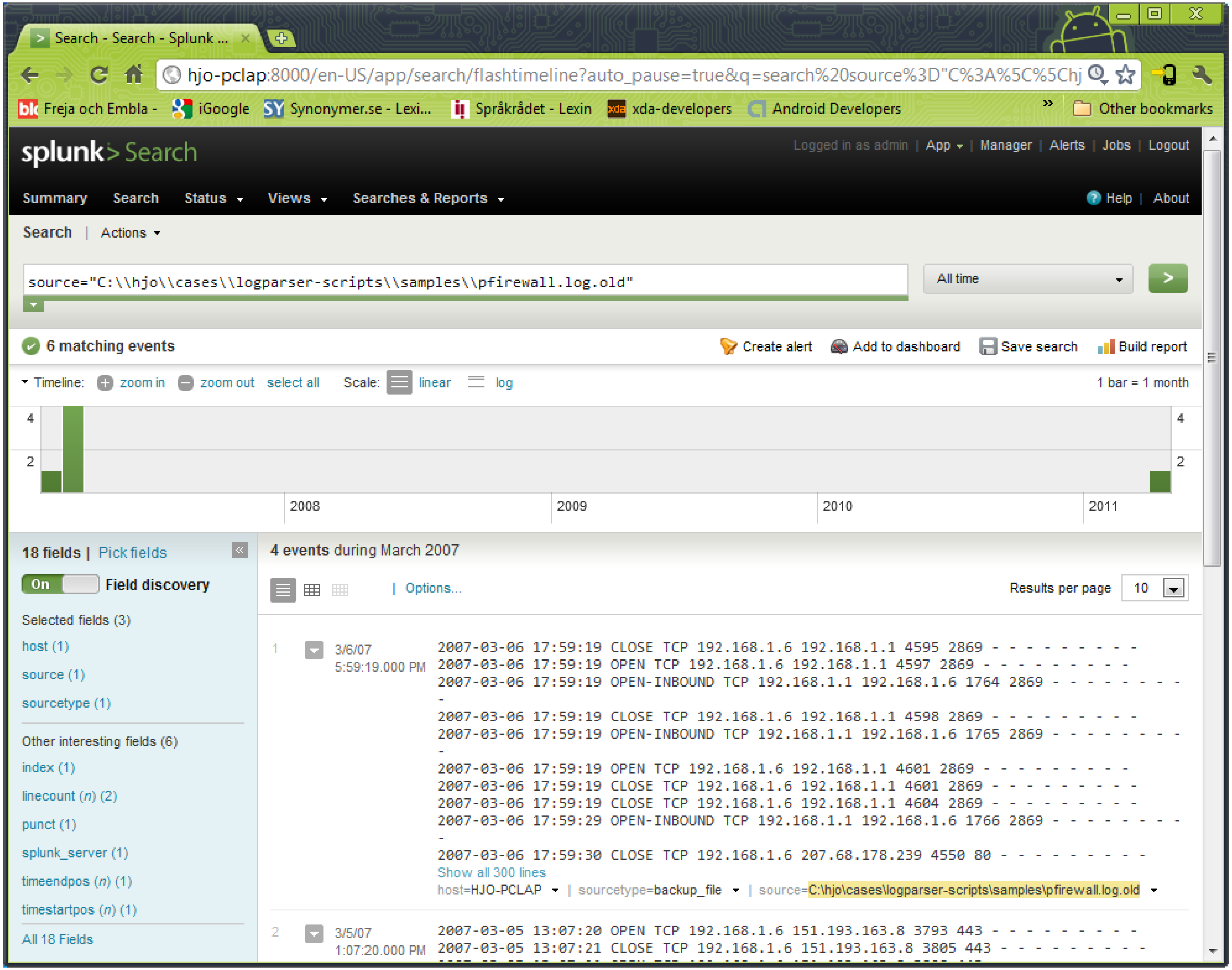
- A file or directory of files
- Syslog
- Windows event logs
- Windows Registry
- Windows performance metrics
- Unix/Linux logs and metrics
- File integrity monitoring
- Configuration files
- OPSEC LEA
- Cisco device logs
- IIS logs
- Apache logs
- WebSphere logs, metrics and other data
- **Any other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

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
All time
>
Create alert | Add to dashboard | Save search | Build report
Timeline: zoom in | zoom out | select all
Scale: linear | log
1 bar = 1 month
4
2
2008
2009
2010
2011
Pick fields
On
Options...

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

6 matching events

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

4 events during March 2007

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

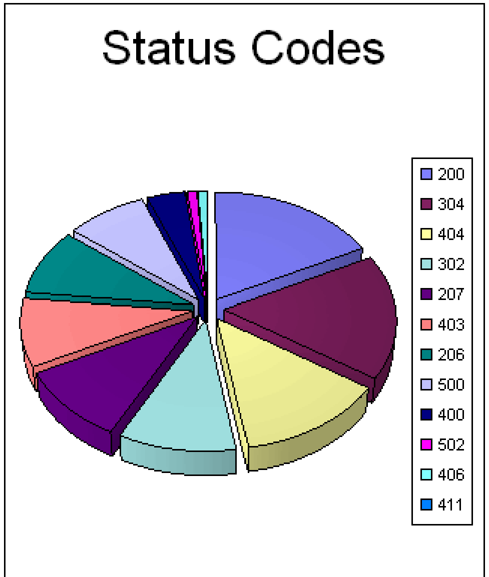
```
2007-03-05 13:07:20 OPEN TCP 192.168.1.6 151.193.163.8 3793 443 - - - - - - - - -
2007-03-05 13:07:21 CLOSE TCP 192.168.1.6 151.193.163.8 3805 443 - - - - - - - - -
```

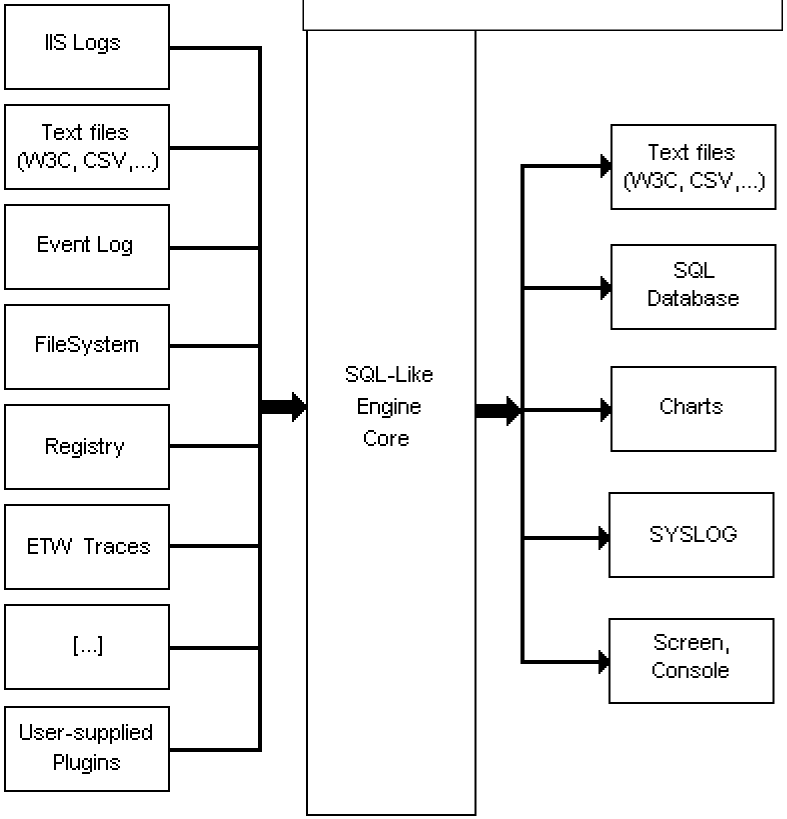
MicroSoft Log Parser (free)

- 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


Status Codes


IIS Logs

Text files (W3C, CSV,...)

Event Log

FileSystem

Registry

ETW Traces

[...]

User-supplied Plugins

SQL-Like Engine Core

Text files (W3C, CSV,...)

SQL Database

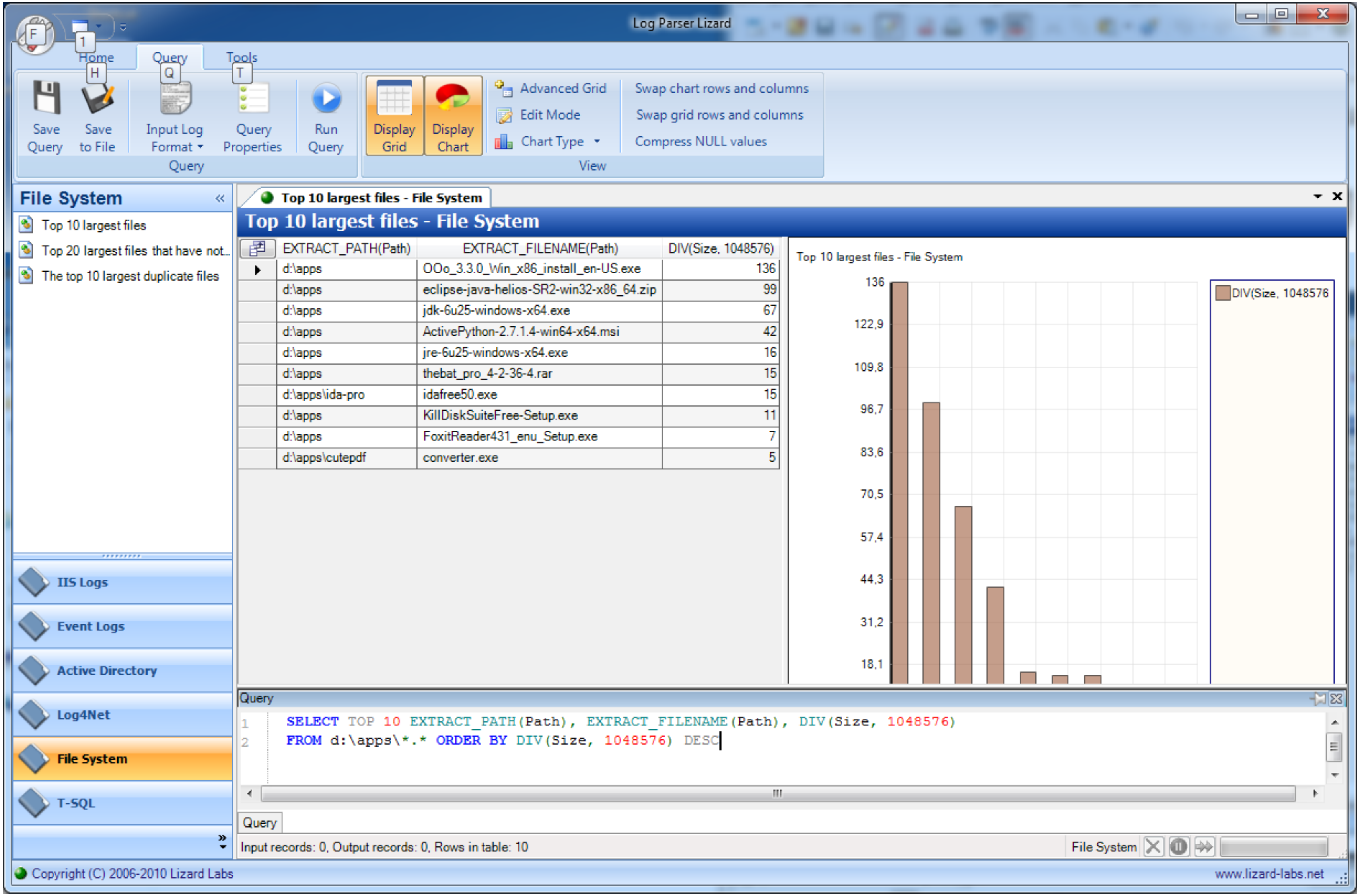
Charts

SYSLOG

Screen, Console

Log Parser Lizard

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

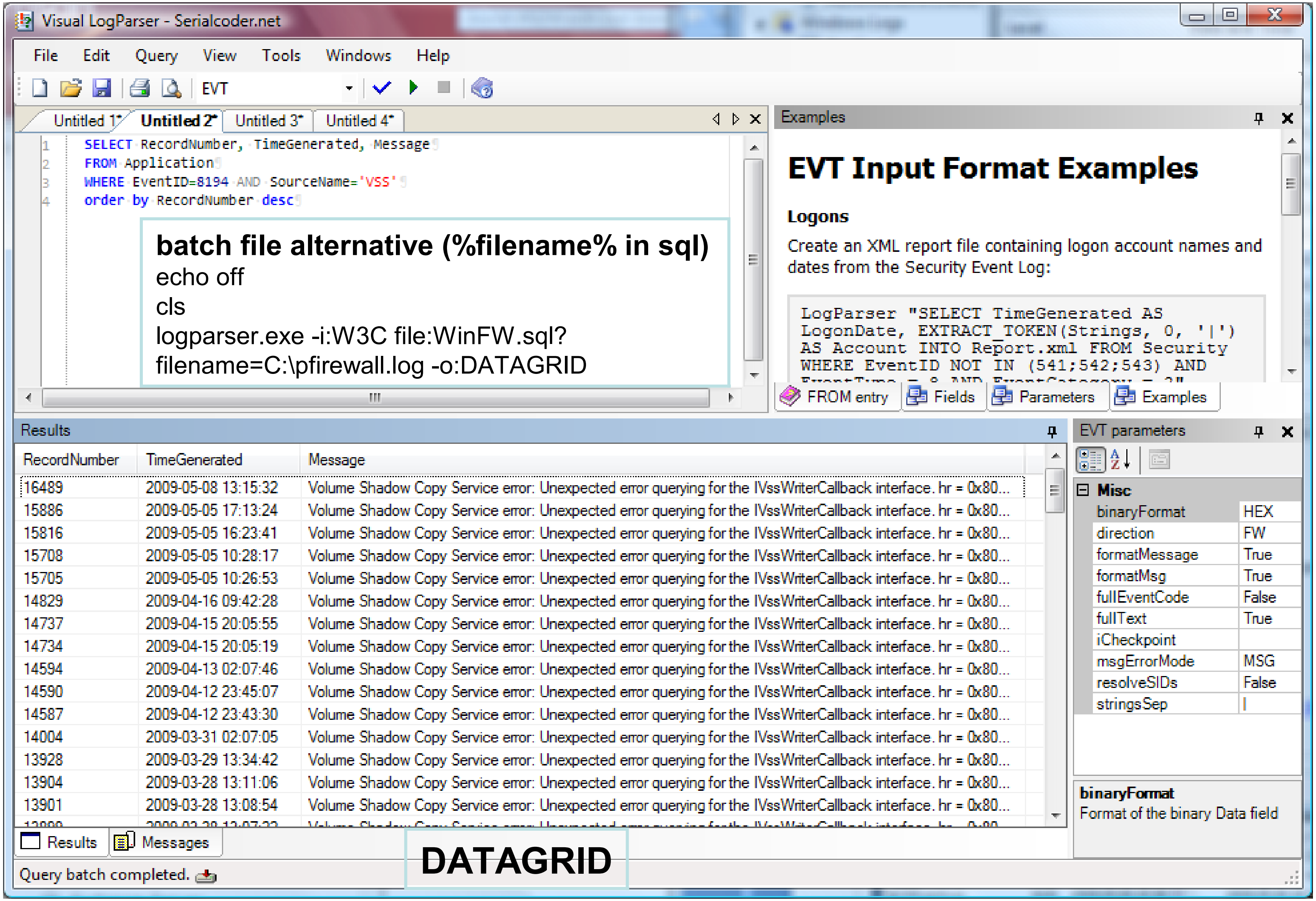


EXTRACT_PATH(Path)	EXTRACT_FILENAME(Path)	DIV(Size, 1048576)
d:\apps	OOo_3.3.0_Win_x86_install_en-US.exe	136
d:\apps	eclipse-java-helios-SR2-win32-x86_64.zip	99
d:\apps	jdk-6u25-windows-x64.exe	67
d:\apps	ActivePython-2.7.1.4-win64-x64.msi	42
d:\apps	jre-6u25-windows-x64.exe	16
d:\apps	thebat_pro_4-2-36-4.rar	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

```
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

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*
Examples
FROM entry Fields Parameters Examples
Results
EVT parameters
Results Messages

```
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
```

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
```

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...

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

Query batch completed.

DATAGRID

MicroSoft Log Parser, events etc.

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

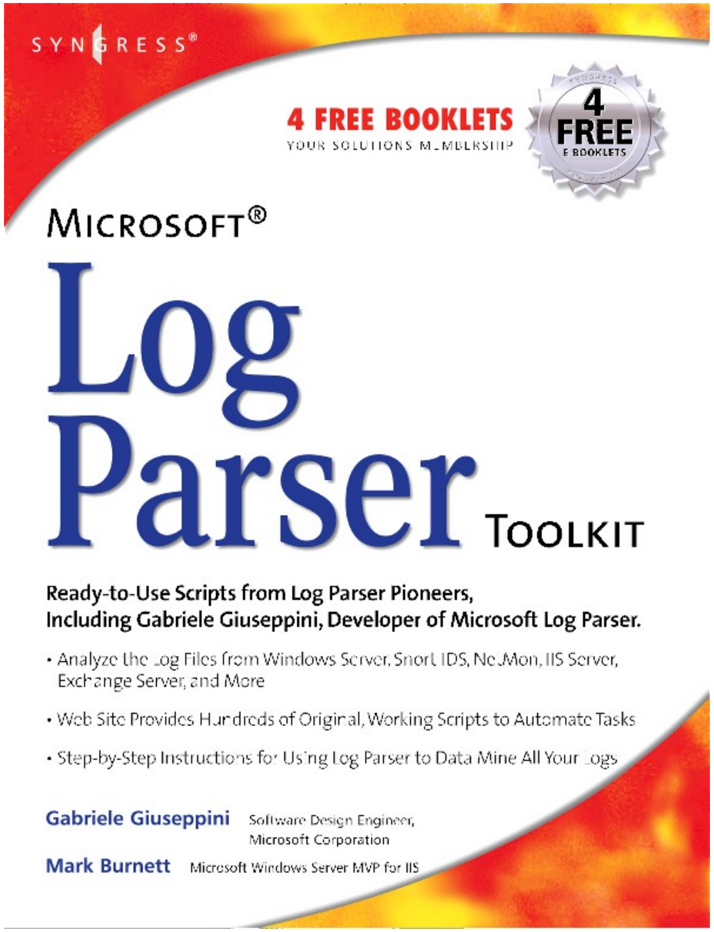
http://en.serialcoder.net/logiciels/visual-logparser.aspx

- 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!


SYNGRESS®
4 FREE BOOKLETS
YOUR SOLUTIONS MEMBERSHIP
4 FREE E BOOKLETS
MICROSOFT®
Log Parser TOOLKIT
Ready-to-Use Scripts from Log Parser Pioneers, Including Gabriele Giuseppini, Developer of Microsoft Log Parser.
• Analyze the Log Files from Windows Server, Snort IDS, NetMon, IIS Server, Exchange Server, and More
• Web Site Provides Hundreds of Original, Working Scripts to Automate Tasks
• Step-by-Step Instructions for Using Log Parser to Data Mine All Your Logs
Gabriele Giuseppini Software Design Engineer, Microsoft Corporation
Mark Burnett Microsoft Windows Server MVP for IIS