

LOGPARSER ÖRNEKLERİ

Yardım için:

logparser -h -i:<input type>

Örnek: logparser -h -i:FS

logparser -h -i:ADS

logparser -h -i:EVT

```
C:\Program Files (x86)\Log Parser 2.2>logparser -h -i:FS

Input format: FS (FileSystem properties)

Returns properties of files and folders

FROM syntax:

  <filename> [, <filename> ...]

  Comma-separated list of paths (e.g. "C:\*.*, D:\folder\*.*")

Parameters:

  -recurse <level> : Max subdirectory recursion level (0=no
recurse, -1=all levels) [default value=-1]

  -preserveLastAccTime ON|OFF : Preserve files' last access time [default
value=OFF]

  -useLocalTime      ON|OFF : Use local time for dates [default value=ON]

Fields:

  Path (S)                Name (S)                Size (I)
  Attributes (S)          CreationTime (T)       LastAccessTime (T)
  LastWriteTime (T)       FileVersion (S)        ProductVersion (S)
  InternalName (S)       ProductName (S)        CompanyName (S)
  LegalCopyright (S)     LegalTrademarks (S)    PrivateBuild (S)
  SpecialBuild (S)       Comments (S)           FileDescription (S)
  OriginalFilename (S)

Examples:

Print the 10 largest files on the C: drive:

  LogParser "SELECT TOP 10 * FROM C:\*.* ORDER BY Size DESC" -i:FS
```

1) Log Parser Dosya ve Dizin İşlemleri

Örnek1:

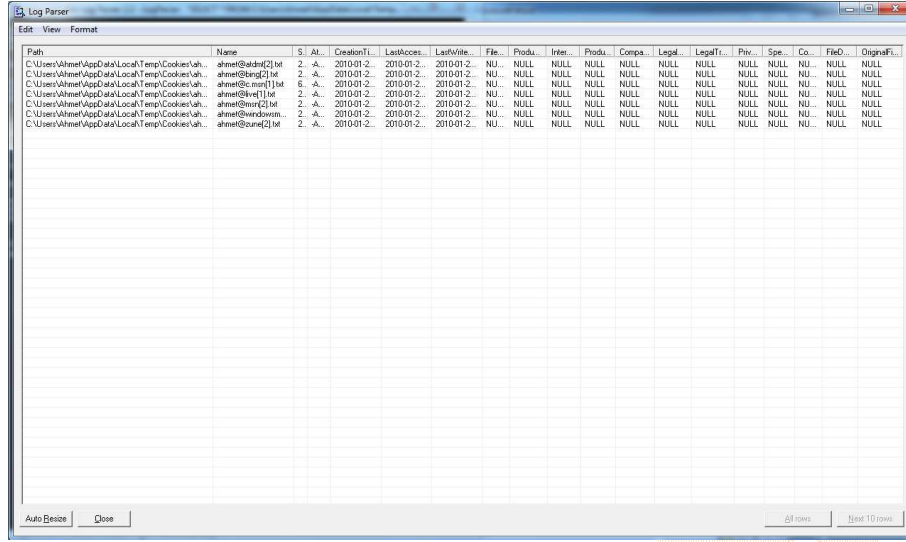
Bir dizindeki toplam dosya sayısı, bu dosyaların büyüklüğü ile ilgili sorgu ve değişik çıktı formatları:

```
LogParser "SELECT count(Size) as [Toplam Dosya Sayisi], sum(Size) as Buyuklugu FROM  
'C:\Users\Ahmet\AppData\Local\Temp\*.*' " -i:FS
```

```
C:\Program Files (x86)\Log Parser 2.2>LogParser "SELECT count(Size) as  
[Toplam  
Dosya Sayisi], sum(Size) as Buyuklugu FROM  
'C:\Users\Ahmet\AppData\Local\Temp\*.  
*' " -i:FS  
Toplam Dosya Sayisi Buyuklugu  
-----  
66                1364289  
  
Statistics:  
-----  
Elements processed: 66  
Elements output:    1  
Execution time:     0.00 seconds
```

Datagrid Formatında görünüm:

```
LogParser "SELECT count(Size) as [Toplam Dosya Sayisi], sum(Size) as Buyuklugu FROM  
'C:\Users\Ahmet\AppData\Local\Temp\*.*' " -i:FS -o:datagrid
```

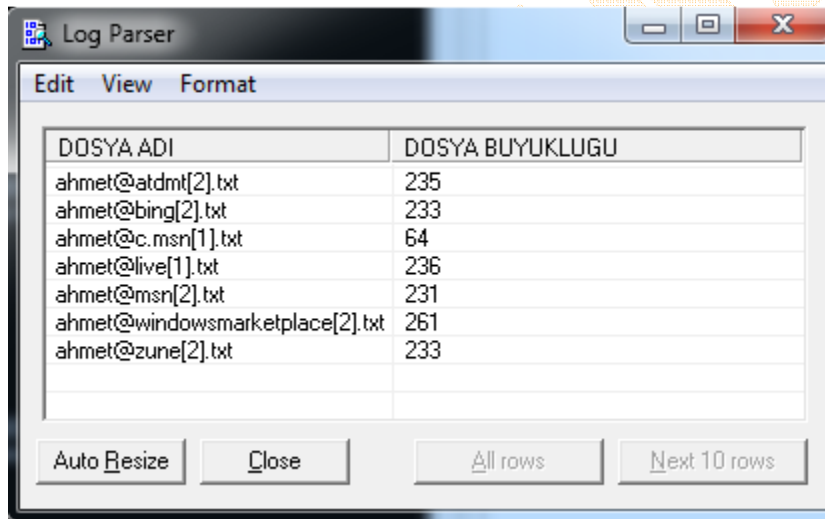



Path	Name	S	At.	CreationT.	LastAccess.	LastWrite.	File...	Probu.	Inter.	Probu.	Comp.	Legd.	LegdF...	Phr.	Spe.	Co.	FileD.	SignaF...
C:\Users\Ahmet\AppData\Local\Temp\Cookies\lah...	ahmet@atdmt[2].txt	2	A.	2010-01-2...	2010-01-2...	2010-01-2...	NU..	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NU..	NULL	NULL
C:\Users\Ahmet\AppData\Local\Temp\Cookies\lah...	ahmet@bing[2].txt	2	A.	2010-01-2...	2010-01-2...	2010-01-2...	NU..	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NU..	NULL	NULL
C:\Users\Ahmet\AppData\Local\Temp\Cookies\lah...	ahmet@c.msn[1].txt	6	A.	2010-01-2...	2010-01-2...	2010-01-2...	NU..	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NU..	NULL	NULL
C:\Users\Ahmet\AppData\Local\Temp\Cookies\lah...	ahmet@live[1].txt	2	A.	2010-01-2...	2010-01-2...	2010-01-2...	NU..	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NU..	NULL	NULL
C:\Users\Ahmet\AppData\Local\Temp\Cookies\lah...	ahmet@msn[2].txt	2	A.	2010-01-2...	2010-01-2...	2010-01-2...	NU..	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NU..	NULL	NULL
C:\Users\Ahmet\AppData\Local\Temp\Cookies\lah...	ahmet@windowsmarketplace[2].txt	2	A.	2010-01-2...	2010-01-2...	2010-01-2...	NU..	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NU..	NULL	NULL
C:\Users\Ahmet\AppData\Local\Temp\Cookies\lah...	ahmet@zune[2].txt	2	A.	2010-01-2...	2010-01-2...	2010-01-2...	NU..	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NU..	NULL	NULL

Örnek4:

A harfi ile başlayanlar ve büyüklükleri:

LogParser "SELECT name as [DOSYA ADI], size as [DOSYA BUYUKLUGU] FROM C:\Users\Ahmet\AppData\Local\Temp*. * where Name like 'A%' " -i:FS -o:datagrid

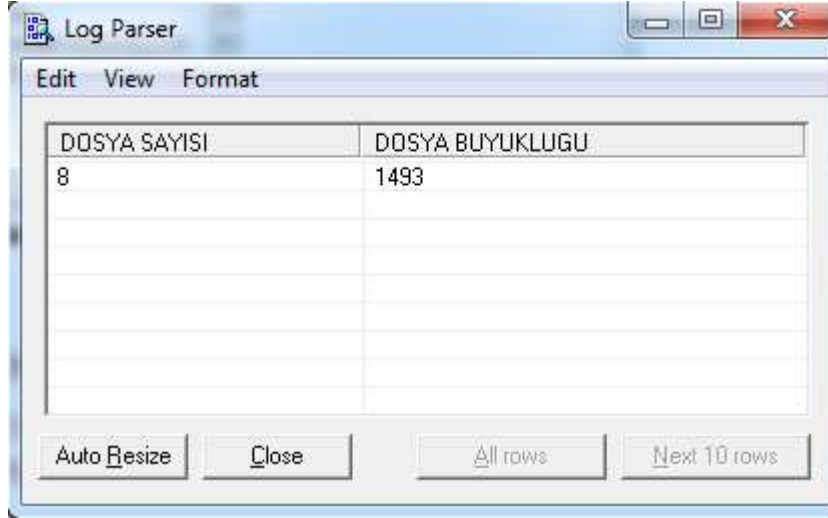


DOSYA ADI	DOSYA BUYUKLUGU
ahmet@atdmt[2].txt	235
ahmet@bing[2].txt	233
ahmet@c.msn[1].txt	64
ahmet@live[1].txt	236
ahmet@msn[2].txt	231
ahmet@windowsmarketplace[2].txt	261
ahmet@zune[2].txt	233

Örnek5:

Dosya Uzantısı ".txt" olanlar ve toplam büyüklüğü:

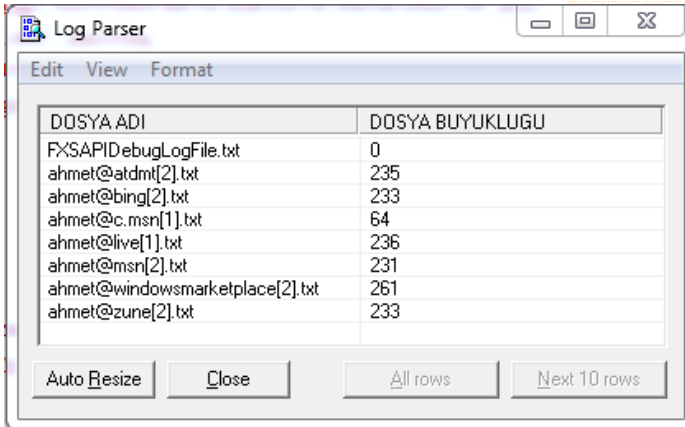
LogParser "SELECT count(Size) as [DOSYA SAYISI], sum(Size) as [DOSYA BUYUKLUGU] FROM 'C:\Users\Ahmet\AppData\Local\Temp*. *' where EXTRACT_EXTENSION(Name) = 'txt' " -i:FS -o:datagrid



DOSYA SAYISI	DOSYA BUYUKLUGU
8	1493

Örnek6:

LogParser "SELECT name as [DOSYA ADI], sum(Size) as [DOSYA BUYUKLUGU] FROM 'C:\Users\Ahmet\AppData\Local\Temp*.*' where EXTRACT_EXTENSION(Name) = 'txt' Group By Name " -i:FS -o:datagrid

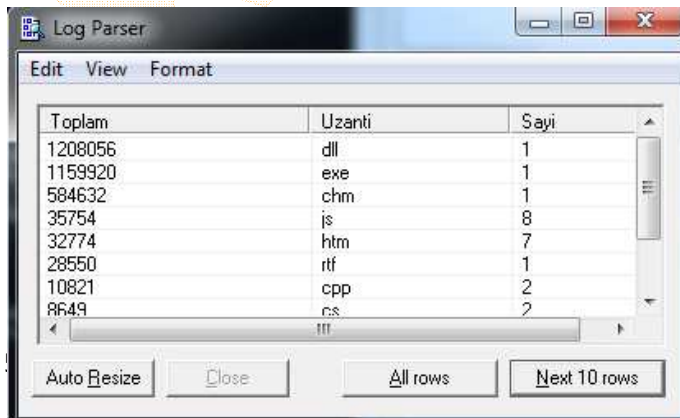


DOSYA ADI	DOSYA BUYUKLUGU
FXSAPIDebugLogFile.txt	0
ahmet@atdm[2].txt	235
ahmet@bing[2].txt	233
ahmet@c.msrl[1].txt	64
ahmet@live[1].txt	236
ahmet@msrl[2].txt	231
ahmet@windowsmarketplace[2].txt	261
ahmet@zune[2].txt	233

'C:\Users\Ahmet\AppData\Local\Temp\' dizinindeki adı ve uzantısı ne olursa olsun her şeyi, "Name" alanının değerlerini "DOSYA ADI" alanında, "Size" alanın toplamlarını "DOSYA BUYUKLUGU" alanında, Uzantısı "*.txt" olacak şekilde adına göre grupla ve datagrid formatında çıktı ver.

Örnek7:

LogParser "Select TOP10 sum(size) as Toplam, EXTRACT_EXTENSION(Name) as Uzanti, Count(*) as Sayi from *.* group by Uzanti order by Toplam Desc" -i:FS -o:datagrid

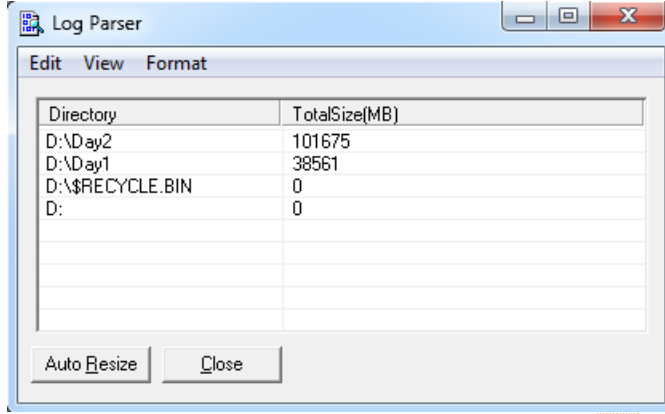


Toplam	Uzanti	Sayi
1208056	dll	1
1159920	exe	1
584632	chm	1
35754	js	8
32774	htm	7
28550	rtf	1
10821	cpp	2
8649	cs	2

Tüm kayıtlardan ilk 10 tanesini al, "size" alanları toplamını "Toplam" alanında göster, Dosya adı uzantılarını "Uzanti" alanında, her bir uzantıdan kaç tane varsa "Sayi" alanında göster, uzantılara göre grupla, boyutlarına göre sırala ve datagrid olarak çıktı ver.

Örnek8:

logparser -recurse:1 -i:fs "select extract_path(path) as Directory, div(sum(size),1048576) as TotalSize(MB) from *.* group by Directory order by TotalSize(MB) DESC" -o:datagrid



Directory	TotalSize(MB)
D:\Day2	101675
D:\Day1	38561
D:\\$RECYCLE.BIN	0
D:	0

Çalıştırıldığı dizindeki tüm dizinleri derinlik 1 olacak şekilde (belirtilmezse alt dizinleri de gösterir) al, dizin adresini (path) "Directory" olarak ata ve göster, boyutlarını 1048576 sayısına bölerek mb cinsine çevir - TotalSize(MB) olarak göster, Directory'e göre gruplandır ve TotalSize(MB)'a göre sırala, DataGrid biçiminde çıktı ver.

Örnek9:

Bir dosyanın md5 algoritmasının bulunması:

LogParser.exe "SELECT Name, HASHMD5_FILE(Path) FROM 'C:\Users\Ahmet\AppData\Local\Temp*.*' where EXTRACT_EXTENSION(Name) = 'txt' " -i:FS

```
D:\>LogParser.exe "SELECT Name, HASHMD5_FILE(Path) FROM
'C:\Users\Ahmet\AppData\Local\Temp\*.*' where EXTRACT_EXTENSION(Name) = 'txt'
" -i:FS
```

Name	HASHMD5_FILE(Path)
FXSAPIDebugLogFile.txt	D41D8CD98F00B204E9800998ECF8427E
ahmet@atdmt[2].txt	DB59582323C36034B13F2EEE71E459E3
ahmet@bing[2].txt	A83A7330BB8A9DB1E3FF87144494C983
ahmet@c.msn[1].txt	6B7FD2EF6FC03B9500F568A9F2ABC1C0
ahmet@live[1].txt	663E21B4C97E797D198B1AEAB4496F73
ahmet@msn[2].txt	7206403BA8C74D916EC5A9D70F9EA058
ahmet@windowsmarketplace[2].txt	C7C046DFBAF44541D8E9EF5945680C55
ahmet@zune[2].txt	D2373BC0C0A4B4A35D7B1874F74CEE44

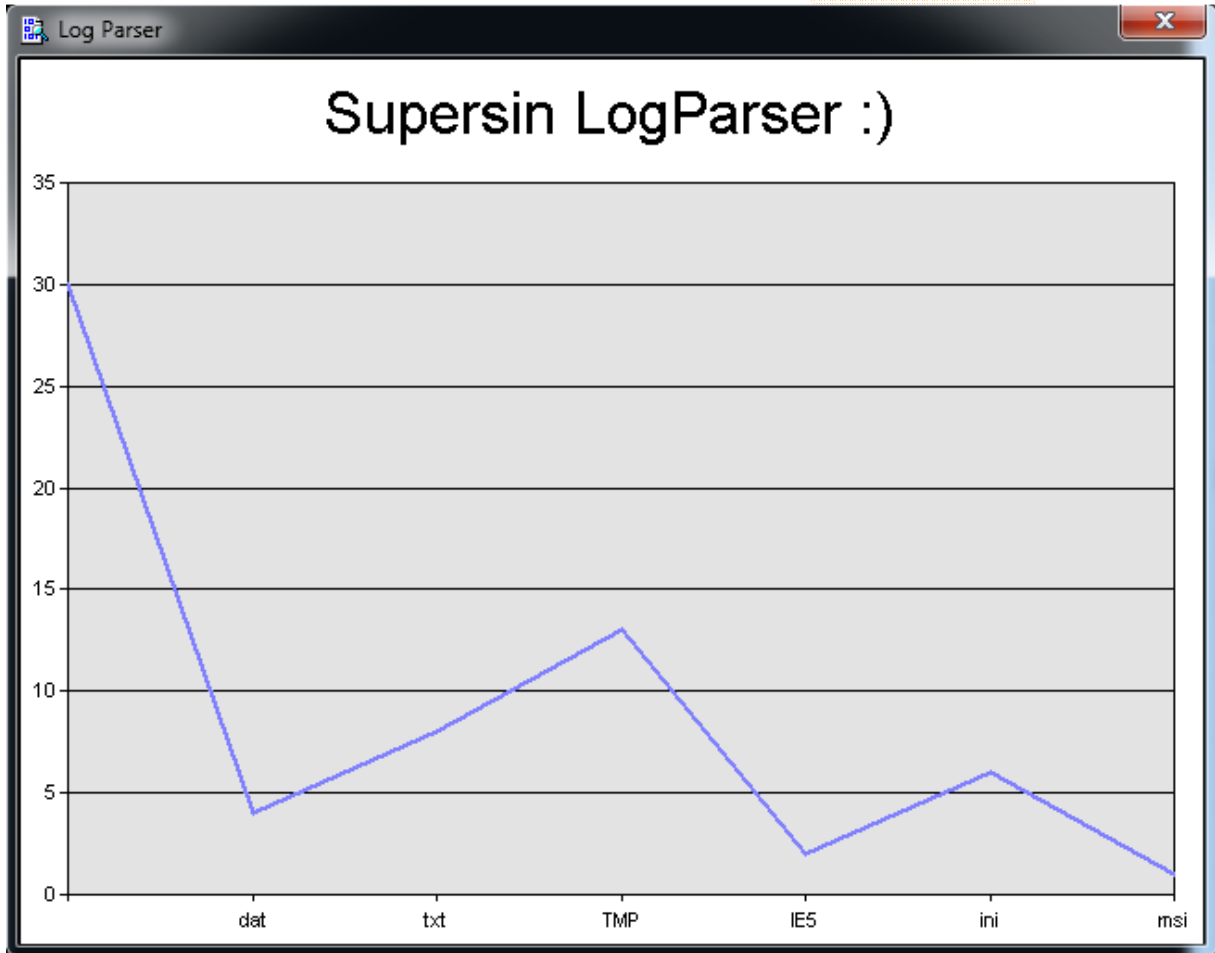
Statistics:

```
Elements processed: 64
Elements output: 8
Execution time: 0.03 seconds
```

Örnek10:

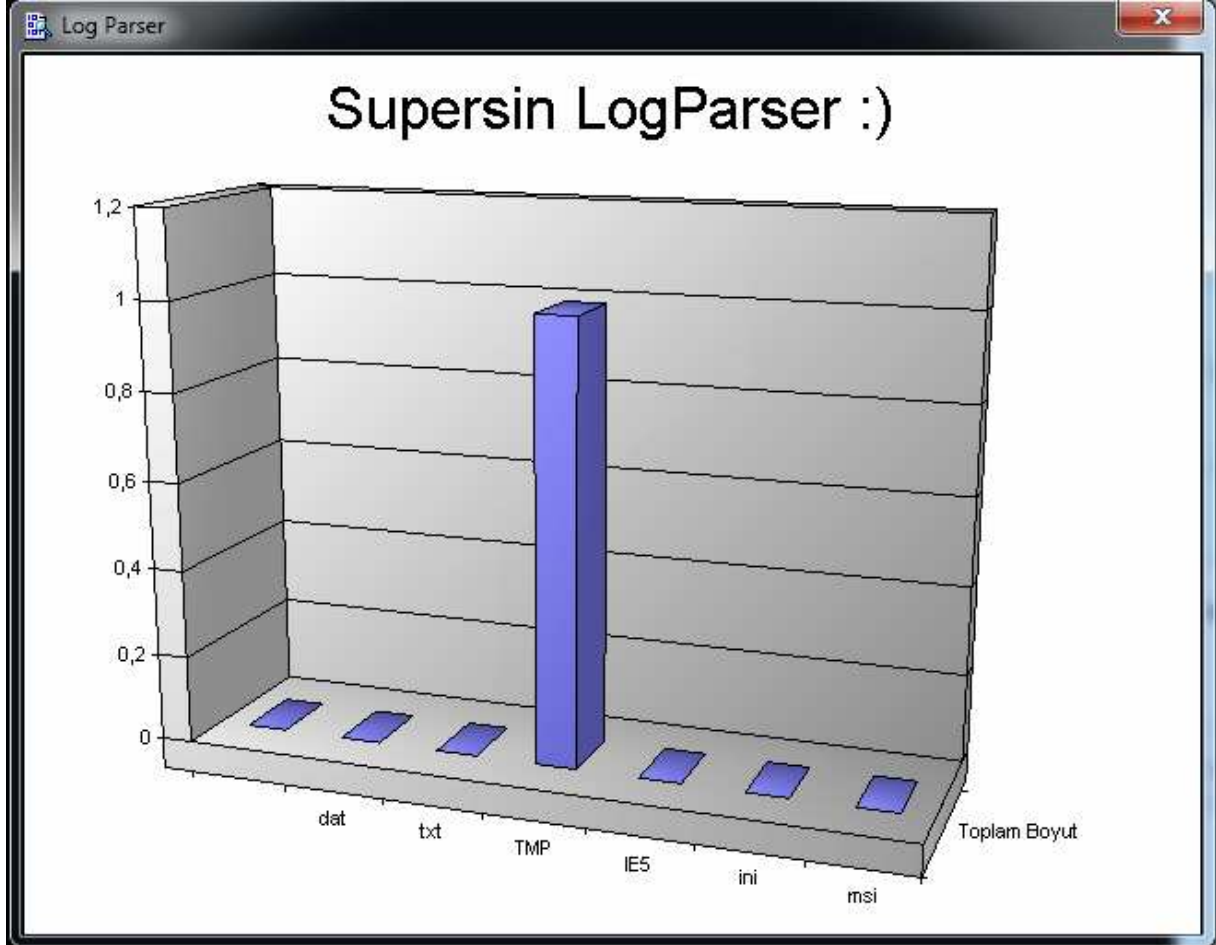
Dosya Tiplerine Gore 'C:\Users\Ahmet\AppData\Local\Temp*.*' Dizinindeki Dosya Sayılarının Grafiksel Çıktısı:

```
LogParser.exe "SELECT EXTRACT_EXTENSION(Name), count(Size) into chart.gif FROM
'C:\Users\Ahmet\AppData\Local\Temp\*.*' group by EXTRACT_EXTENSION(name)" -i:FS -view -charttitle
"Supersin LogParser :)"
```

**Örnek11:**

Buda benzer bir örnek:

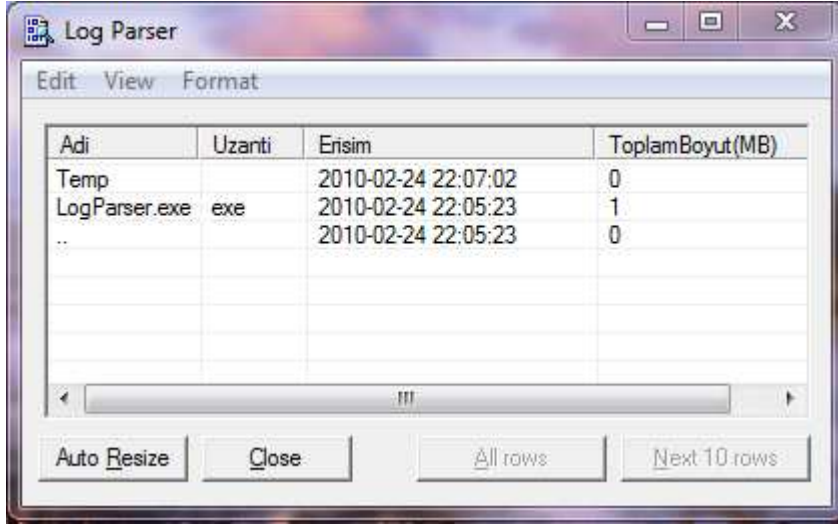
LogParser.exe "SELECT EXTRACT_EXTENSION(Name) as [Dosya Tipi], div(sum(size),1048576) as [Toplam Boyut] into chart.gif FROM 'C:\Users\Ahmet\AppData\Local\Temp*.*' group by EXTRACT_EXTENSION(name)" -i:FS -charttype:Column3D -view -charttitle "Supersin LogParser :)"



Örnek 12:

Dosyaların ilk 3 tanesinin son erişim tarihine göre sıralanması:

```
logparser -recurse:0 "select top 3 name as Adi, EXTRACT_EXTENSION(Name) as Uzanti, LastAccessTime as Erisim, div(sum(size),1048576) as ToplamBoyut(MB) from *.* group by Erisim,Adi,Uzanti order by Erisim desc" -i:FS -o:datagrid
```



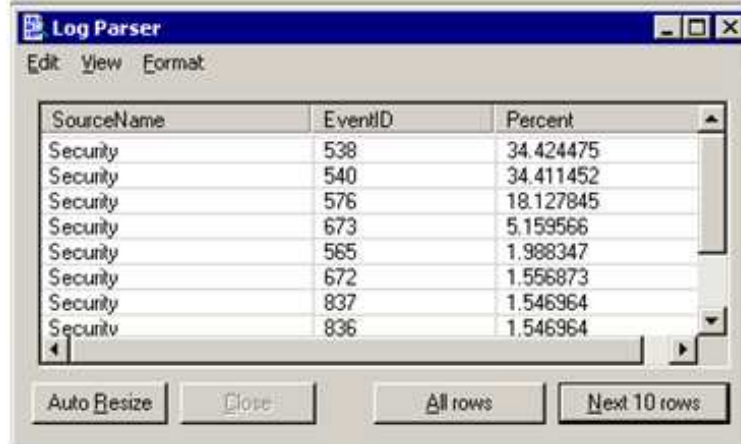
Adi	Uzanti	Erisim	ToplamBoyut(MB)
Temp		2010-02-24 22:07:02	0
LogParser.exe	exe	2010-02-24 22:05:23	1
..		2010-02-24 22:05:23	0

LOGPARSER EVENT LOG OKUMA ÖRNEKLEMELERİ

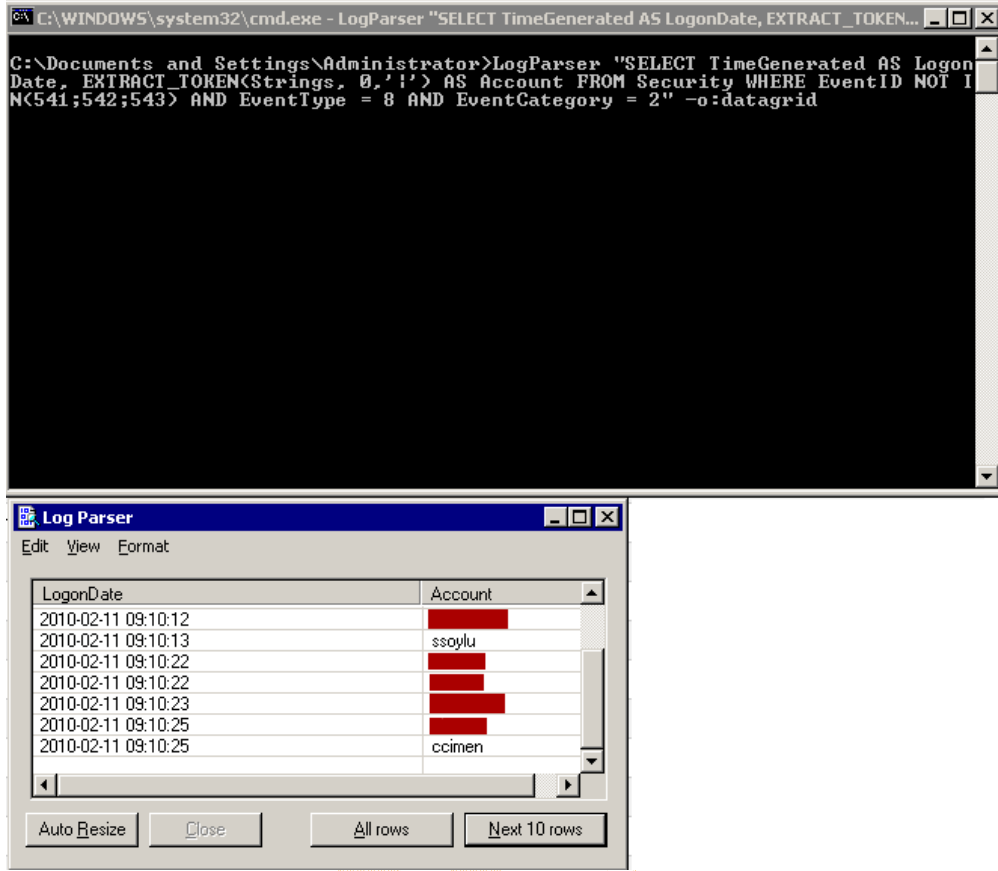
Örnek1:

Security Log'ları yüzdeleri

```
C:\Documents and Settings\Administrator>LogParser "SELECT SourceName, EventID, M
UL<PROPCOUNT(*) ON <SourceName>,100.0) AS Percent FROM Security GROUP BY SourceN
ame, EventID ORDER BY SourceName, Percent DESC" -o:datagrid
```



SourceName	EventID	Percent
Security	538	34.424475
Security	540	34.411452
Security	576	18.127845
Security	673	5.159566
Security	565	1.988347
Security	672	1.556873
Security	837	1.546964
Security	836	1.546964

Örnek 2:**Kimlerin Hangi Saatte Logon Olduğu Bilgisi:**

The screenshot shows a Windows command prompt window with the following command and output:

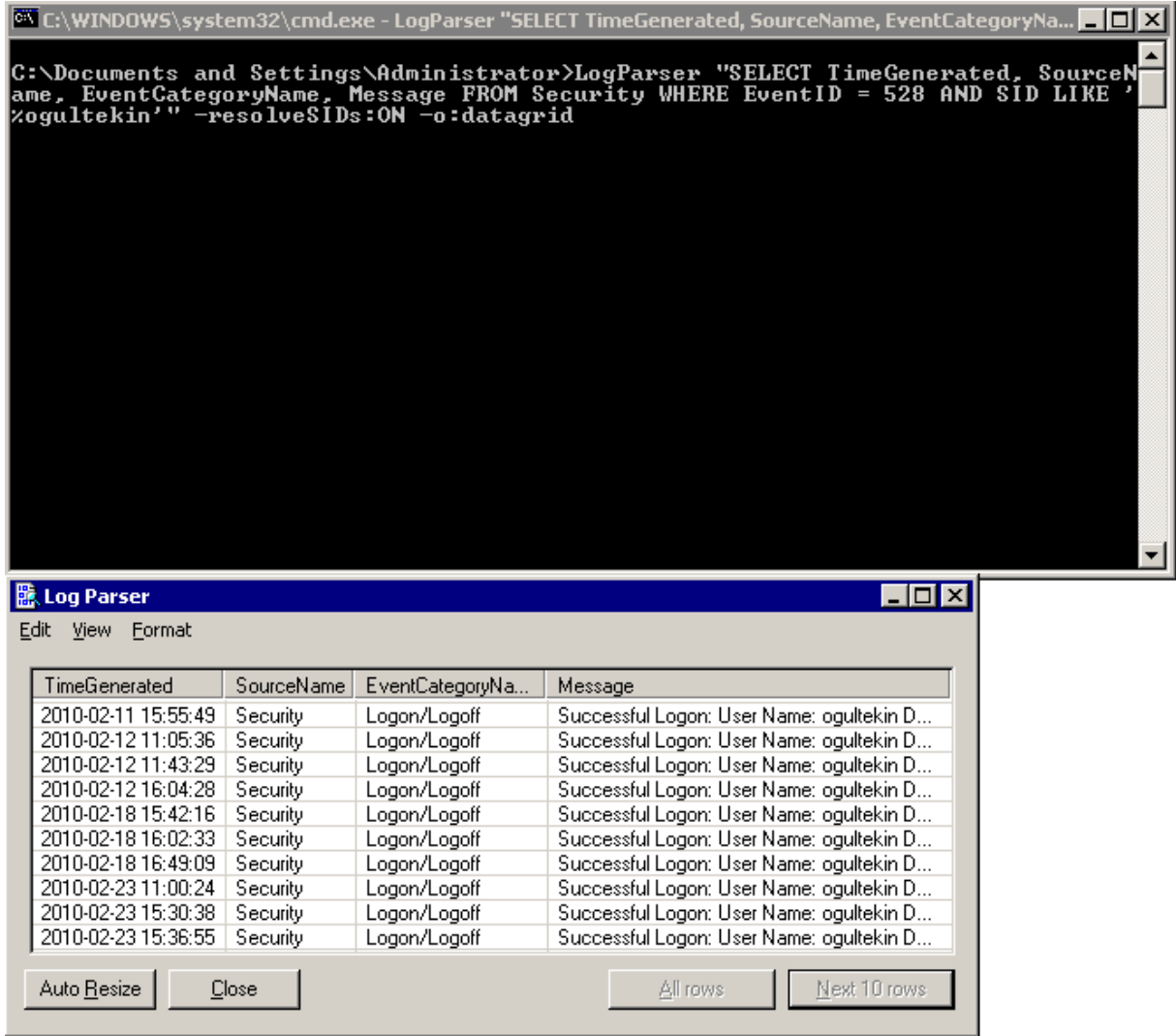
```
C:\WINDOWS\system32\cmd.exe - LogParser "SELECT TimeGenerated AS LogonDate, EXTRACT_TOKEN...  
C:\Documents and Settings\Administrator>LogParser "SELECT TimeGenerated AS LogonDate, EXTRACT_TOKEN(Strings, 0, 'i') AS Account FROM Security WHERE EventID NOT IN (541;542;543) AND EventType = 8 AND EventCategory = 2" -o:datagrid
```

The Log Parser application window displays the following data:

LogonDate	Account
2010-02-11 09:10:12	[REDACTED]
2010-02-11 09:10:13	ssoylu
2010-02-11 09:10:22	[REDACTED]
2010-02-11 09:10:22	[REDACTED]
2010-02-11 09:10:23	[REDACTED]
2010-02-11 09:10:25	[REDACTED]
2010-02-11 09:10:25	ccimen

Örnek3:

Bir kullanıcının ne zaman hangi bilgisayarda nasıl oturum açtığı bilgisi:



```

C:\WINDOWS\system32\cmd.exe - LogParser "SELECT TimeGenerated, SourceName, EventCategoryName, Message FROM Security WHERE EventID = 528 AND SID LIKE 'ogultekin'" -resolveSIDs:ON -o:datagrid
  
```

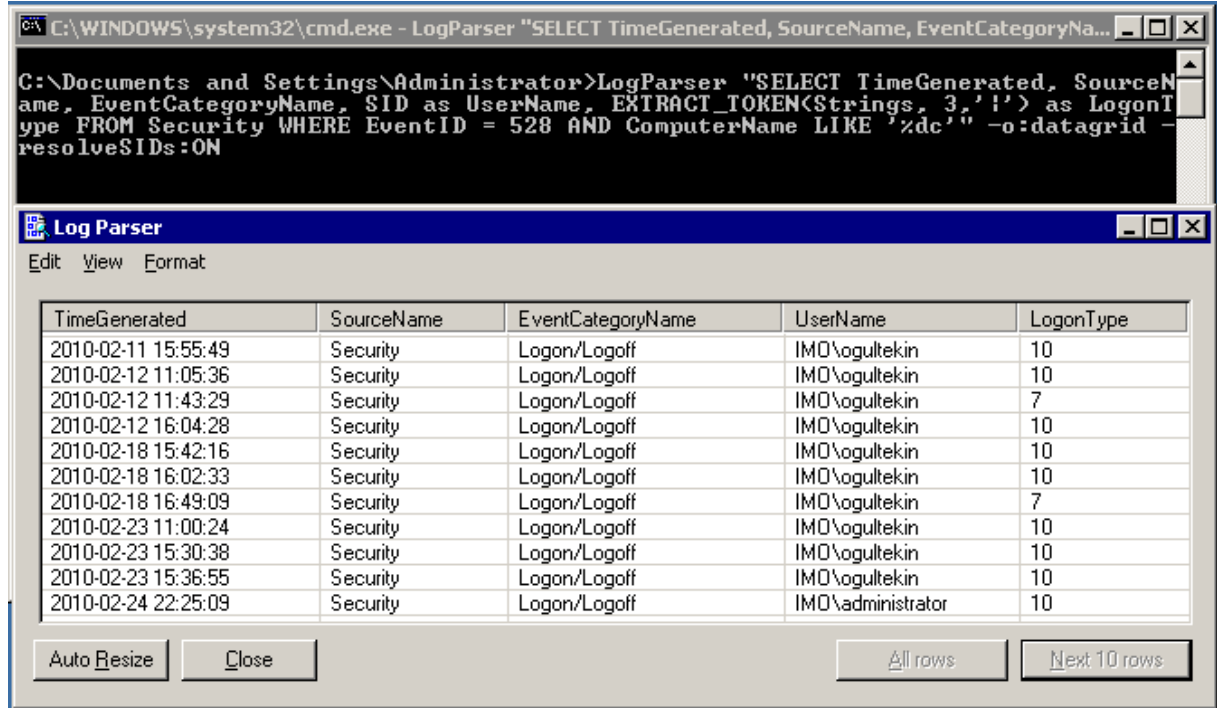
TimeGenerated	SourceName	EventCategoryName	Message
2010-02-11 15:55:49	Security	Logon/Logoff	Successful Logon: User Name: ogultekin D...
2010-02-12 11:05:36	Security	Logon/Logoff	Successful Logon: User Name: ogultekin D...
2010-02-12 11:43:29	Security	Logon/Logoff	Successful Logon: User Name: ogultekin D...
2010-02-12 16:04:28	Security	Logon/Logoff	Successful Logon: User Name: ogultekin D...
2010-02-18 15:42:16	Security	Logon/Logoff	Successful Logon: User Name: ogultekin D...
2010-02-18 16:02:33	Security	Logon/Logoff	Successful Logon: User Name: ogultekin D...
2010-02-18 16:49:09	Security	Logon/Logoff	Successful Logon: User Name: ogultekin D...
2010-02-23 11:00:24	Security	Logon/Logoff	Successful Logon: User Name: ogultekin D...
2010-02-23 15:30:38	Security	Logon/Logoff	Successful Logon: User Name: ogultekin D...
2010-02-23 15:36:55	Security	Logon/Logoff	Successful Logon: User Name: ogultekin D...

Örnek4:**Belirtilen Bilgisayarda Kim, Hangi Zamanda, Nasıl Oturum açmış:**

```

C:\WINDOWS\system32\cmd.exe - LogParser "SELECT TimeGenerated, SourceName, EventCategoryName, Message FROM Security WHERE EventID = 528 AND ComputerName LIKE '%dc%' -o:datagrid
  
```

TimeGenerated	SourceName	EventCategoryName	Message
2010-02-11 15:55:49	Security	Logon/Logoff	Successful Logon: User Name: ogultekin Domain: I...
2010-02-12 11:05:36	Security	Logon/Logoff	Successful Logon: User Name: ogultekin Domain: I...
2010-02-12 11:43:29	Security	Logon/Logoff	Successful Logon: User Name: ogultekin Domain: I...
2010-02-12 16:04:28	Security	Logon/Logoff	Successful Logon: User Name: ogultekin Domain: I...
2010-02-18 15:42:16	Security	Logon/Logoff	Successful Logon: User Name: ogultekin Domain: I...
2010-02-18 16:02:33	Security	Logon/Logoff	Successful Logon: User Name: ogultekin Domain: I...
2010-02-18 16:49:09	Security	Logon/Logoff	Successful Logon: User Name: ogultekin Domain: I...
2010-02-23 11:00:24	Security	Logon/Logoff	Successful Logon: User Name: ogultekin Domain: I...
2010-02-23 15:30:38	Security	Logon/Logoff	Successful Logon: User Name: ogultekin Domain: I...
2010-02-23 15:36:55	Security	Logon/Logoff	Successful Logon: User Name: ogultekin Domain: I...

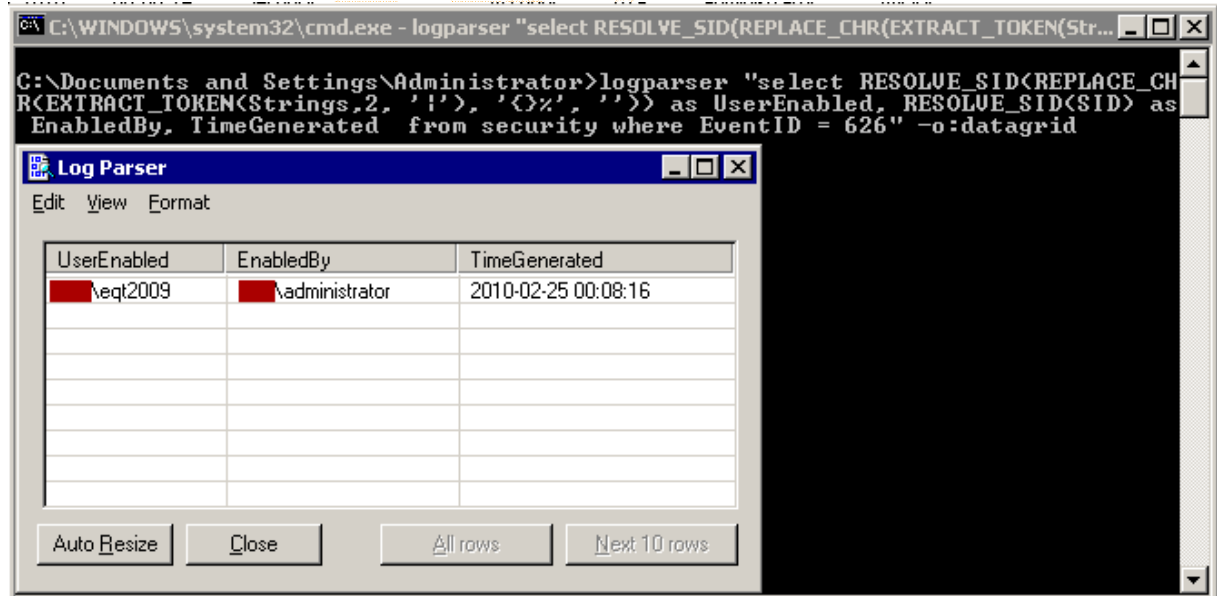
Örnek5:**Belirtilen Bilgisayarda Kim Nasıl Logon Olmuş?**


The screenshot shows a Windows command prompt window with the following command:

```
C:\WINDOWS\system32\cmd.exe - LogParser "SELECT TimeGenerated, SourceName, EventCategoryName, SID as UserName, EXTRACT_TOKEN(Strings, 3, '!') as LogonType FROM Security WHERE EventID = 528 AND ComputerName LIKE '%dc'" -o:datagrid -resolveSIDs:ON
```

Below the command prompt is the Log Parser application window. It displays a table with the following data:

TimeGenerated	SourceName	EventCategoryName	UserName	LogonType
2010-02-11 15:55:49	Security	Logon/Logoff	IMD\vogultekin	10
2010-02-12 11:05:36	Security	Logon/Logoff	IMD\vogultekin	10
2010-02-12 11:43:29	Security	Logon/Logoff	IMD\vogultekin	7
2010-02-12 16:04:28	Security	Logon/Logoff	IMD\vogultekin	10
2010-02-18 15:42:16	Security	Logon/Logoff	IMD\vogultekin	10
2010-02-18 16:02:33	Security	Logon/Logoff	IMD\vogultekin	10
2010-02-18 16:49:09	Security	Logon/Logoff	IMD\vogultekin	7
2010-02-23 11:00:24	Security	Logon/Logoff	IMD\vogultekin	10
2010-02-23 15:30:38	Security	Logon/Logoff	IMD\vogultekin	10
2010-02-23 15:36:55	Security	Logon/Logoff	IMD\vogultekin	10
2010-02-24 22:25:09	Security	Logon/Logoff	IMD\administrator	10

Örnek 6:**Devre dışı bırakılan bir hesabı kim tekrar kullanıma açmış?**


The screenshot shows a Windows command prompt window with the following command:

```
C:\WINDOWS\system32\cmd.exe - logparser "select RESOLVE_SID(REPLACE_CHR(EXTRACT_TOKEN(Strings, 2, '!'), '{ }%', '')) as UserEnabled, RESOLVE_SID(SID) as EnabledBy, TimeGenerated from security where EventID = 626" -o:datagrid
```

Below the command prompt is the Log Parser application window. It displays a table with the following data:

UserEnabled	EnabledBy	TimeGenerated
veqt2009	administrator	2010-02-25 00:08:16

