



# Logs and Event Analysis

## MODULE 11

## Contents

11.1 Learning Objectives .....	3
11.2 Introduction.....	3
11.3 Windows registry .....	4
11.3.1 Registry and forensics.....	5
11.3.1.1 System information.....	5
11.4 Windows event log file .....	7
11.4.1 Windows Event Log File Format.....	7
11.4.2 Reading from Windows event log file .....	9
11.4.3 Using Microsoft log parser .....	10
11.4.4 Understanding Windows user account management logs .....	11
11.4.5 Understanding Windows file and other object Access sets .....	12
11.4.6 Auditing policy change .....	12
11.5 Windows password storage.....	12
11.5.1 SAM.....	12
11.5.1.1 Removing LM hash.....	13
11.5.1.2 Related attacks .....	13
11.5.2 AD.....	13
11.6 Summary .....	14
11.7 Check Your Progress .....	14
11.8 Further Readings.....	15
<b>References, Article Source &amp; Contributors.....</b>	<b>15</b>

# Logs and Event Analysis

---

## 11.1 Learning Objectives

---

After going through this unit, you will be able to:

- Fetch registry and various keys in registry related to event logs.
- Explain the event log file structure.
- Retrieve event information from log files correlate its use while doing forensic investigation.
- Correlate user account policies, audit policies and mechanisms of changing audit policy while doing forensic investigation.
- Use various tools used for log and event analysis.

---

## 11.2 Introduction

---

In this chapter we will discuss two very important aspects of windows and other systems which plays very vital role in forensics. They are: Event logs and Password cracking. In computer log management and intelligence, log analysis (or system and network log analysis) is an art and science seeking to make sense out of computer-generated records (also called log or audit trail records). The process of creating such records is called data logging. Typical reasons why people perform log analysis are:

- Compliance with security policies
- Compliance with audit or regulation
- System troubleshooting
- Forensics (during investigations or in response to subpoena)
- Security incident response

The Security Log, in Microsoft Windows, is a log that contains records of login/logout activity or other security-related events specified by the system's audit policy. Auditing allows administrators to configure Windows to record operating system activity in the Security Log. Event logging provides system administrators with information useful for diagnostics and auditing. The different classes of events that will be logged, as well as what details will appear in the event messages, are often considered early in the development cycle. Many event logging technologies allow or even require each class of event to be assigned a unique "code", which is used by the event logging software or a separate viewer (e.g., Event Viewer) to format and output a human-readable message. This facilitates localization and allows system administrators to more easily obtain information on problems that occur.

Windows registry is also a very important source to maintain and manage logs. As well registry also has variety of controls/keys where general records pertaining events etc. are maintained which can be very vital during digital forensics.

In cryptanalysis and computer security, password cracking is the process of recovering passwords from data that have been stored in or transmitted by a computer system. The purpose of password cracking might be to help a user recover a forgotten password (installing an entirely new password is less of a security risk, but it involves System Administration privileges), to gain unauthorized access to a system, or as a preventive measure by System Administrators to check for easily crack-able passwords. On a file-by-file basis, password cracking is utilized to gain access to digital evidence for which a judge has allowed access but the particular file's access is restricted.


---

### 11.3 Windows registry

---

Windows registry keeps most of the information pertaining policies, status etc. in form of keys, sub keys and values. Windows registry can be worked upon by administrator through application like 'regedit'. Windows can also be supplied with a command like tool like 'reg' to help users work on registry. Registry contains hives under which sub keys are present. These hives play important role in the overall functioning of the system.

**VIDEO LECTURE**



This lecture is adopted from <https://youtu.be/tBwAHqqPoQY> available under Creative Commons Attribution license (reuse allowed)

### 11.3.1 Registry and forensics

An investigator can acquire quite a good deal of information by studying and analysing registry. Many tools like ProDiscover, ProScript can be very handy to get a good deal of analysis of registry entries. Registry entries can be used to acquire and analyse many important information necessary for forensics analysis. These information use system, time zone, shares, audit policy, wireless SSIDS, auto start locations, user login, activities, USB removable devices, trusted devices, cache, cookie and history etc.

#### 11.3.1.1 System information

Basic information of system can be acquired for registry. Certain system information and its registry key are listed below:

*Table 1: Various important log attributes and respective registry keys.*

<b>System Information</b>	<b>Key</b>
<b>Computer Name</b>	SYSTEM\CurrentControlSet\Control\ComputerName\ActiveComputerName
<b>Time of last shutdown</b>	SYSTEM\ControlSet00x\Control\Windows
<b>Product name ,build, version</b>	SOFTWARE\Microsoft\Windows NT\CurrentVersion
<b>Time zone settings</b>	SYSTEM\CurrentControlSet\Control\TimeZoneInformation
<b>User created shares</b>	SYSTEM\CurrentControlSet\Services\lanmanserver\Shares
<b>Audit policy</b>	\SECURITY\Policy\PolAdtEv
<b>Wireless SSIDs</b>	SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces\{GUID}
<b>USB devices connected</b>	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Enum\USBSTOR
<b>last time</b>	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses
<b>Mounted Devices</b>	HKEY_LOCAL_MACHINE\System\MountedDevices
<b>User</b>	SAM\SAM\Domains\Account\Users\{RID}
<b>information stored in the user's</b>	Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{GUID}\Count
<b>most recently used</b>	\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
<b>most recently used</b>	\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
<b>Search Assistant MRU Lists</b>	Software\Microsoft\Search Assistant\ACMrU
<b>Internet downloads directory</b>	Computer\HKEY_CURRENT_USER\Software\Microsof
<b>Restore points</b>	HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\SystemRestore

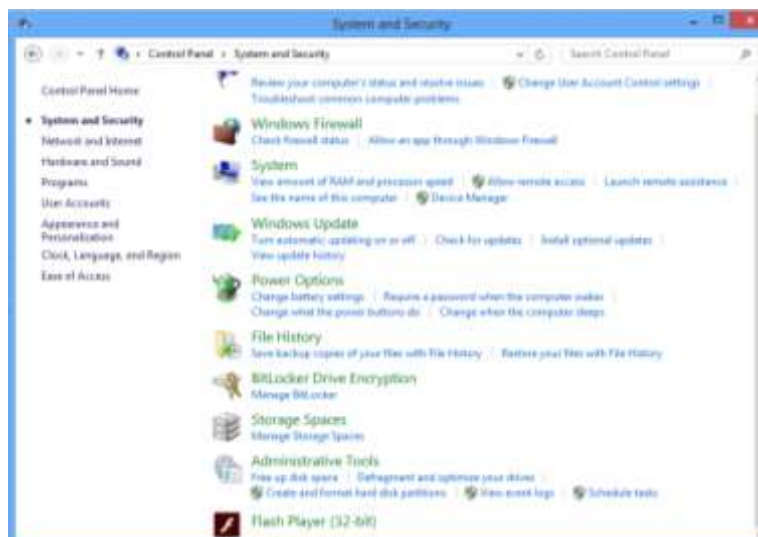
Table 1 list out few important keys and their paths. This information acquired using these keys has to be recorded using Encase and can lead to many conclusions while putting up the case.

Computers' here is the name that the user gives to its computer. The name of computer generally is made once in the lifetime usage of the system and hence it can be used to trace various activities on network and internet carried by the user. Time of last shutdown is the time at which the system was completely shut down.

This information can lead us to know the status of the user and time stamps of various files and can co-relate to give an idea of the mental status of the suspect. Sometime user themselves create shared folders and applications for others to use over local network or internet (remote desktops). This information can be traced out to find and analyse what kind of things or information the user was trying to share and thus stamps of the shared files/folders can also be analysed. Audit policy information can be very useful as it can let us know about what types of information/events an investigator should look for in the event log. Service set identifications (SSIDs) maintained by Windows can be useful in situations where unauthorised access is need to be investigated and IP addresses needs to be traced. Artefacts of a USB devices connected to computer are also registered via PnP (plug and play) manager. The sub key formed for every USB device under the key path in table 1 is of the form *Disk &Ven\_###&Prod\_###&Rev###*. This and other information can be used to trace and collect vital evidences pertaining to a case. Similar is the case with mounted devices information under registry. Many applications maintain MRU lists i.e. they keep a list of recently used files or opened/created files. Also search assistant MRU lists are also maintained by search applicants. MRU lists of connected systems etc. are also maintained. This information can of genuine help to understand victim's state of mind or condition just before the crime. System restore points can be studied to understand how and when the user created back-ups. Restore points can be used to understand long back status of the user work. Events are any occurrences or triggering of an activity. The operating system logs some of these occurrences or events. However, the key PolAdEvt in registry can be used to set audit configuration in order to log events based on user requirements. Other key available for logging events is:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\<Event Log>

One can view events logs from the control panel also (see *Figure 1, Figure 2* and *Figure 3*).



*Figure 1: System and Security in control panel*

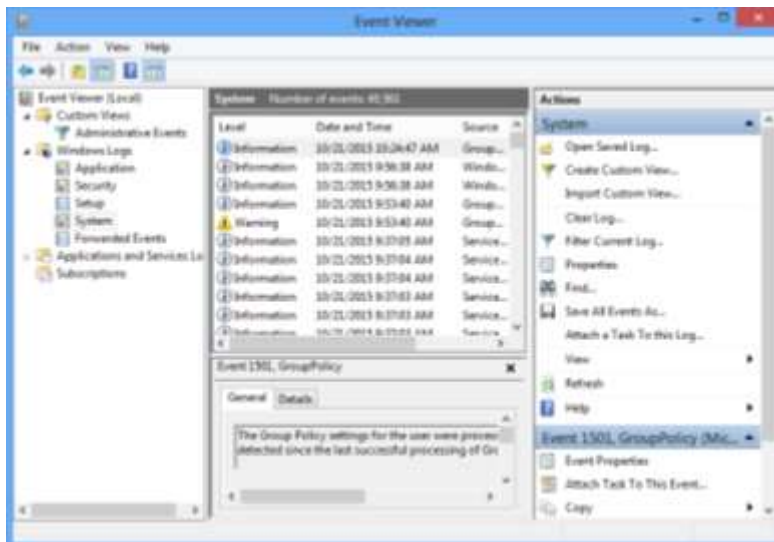


Figure 2: Event Viewer.

---

## 11.4 Windows event log file

---

In windows event logs are stored in binary format. Event logs are stored in form of headers and set of records. The event logs are in form of headers and set of records. The event logs are in form of pipe or buffer where event addition can lead to several of older events out of the file.

---

### 11.4.1 Windows Event Log File Format

---

Each log file consists of a Header record (given as ELF\_LOGFILE\_HEADER structure) and the Body. The body again consists of Event records, the Cursor record and unused space. The body could form a ring buffer, where the cursor record will mark the border between the oldest and the newest event record. Unused space could be empty, slack and padding

Windows Event Log (EVT)– ForensicsWiki,

[www.forensicswiki.org/wiki/Windows\\_Event\\_Log\\_\(EVT\)](http://www.forensicswiki.org/wiki/Windows_Event_Log_(EVT))

The Windows XML Event Log (EVTX) format was introduced in Windows Vista as a replacement for the Windows Event Log (EVT) format.

Whenever an event has to be written/created/updated ELF\_LOGFILE\_HEADER and the ELF\_EOF\_RECORD structures are written in the event log.

Whenever an application needs to log (or is set in registry to log an event) it calls ReportEvent function which adds an EVENTLOGRECORD structure taking the parameters from the system (see figure 3).

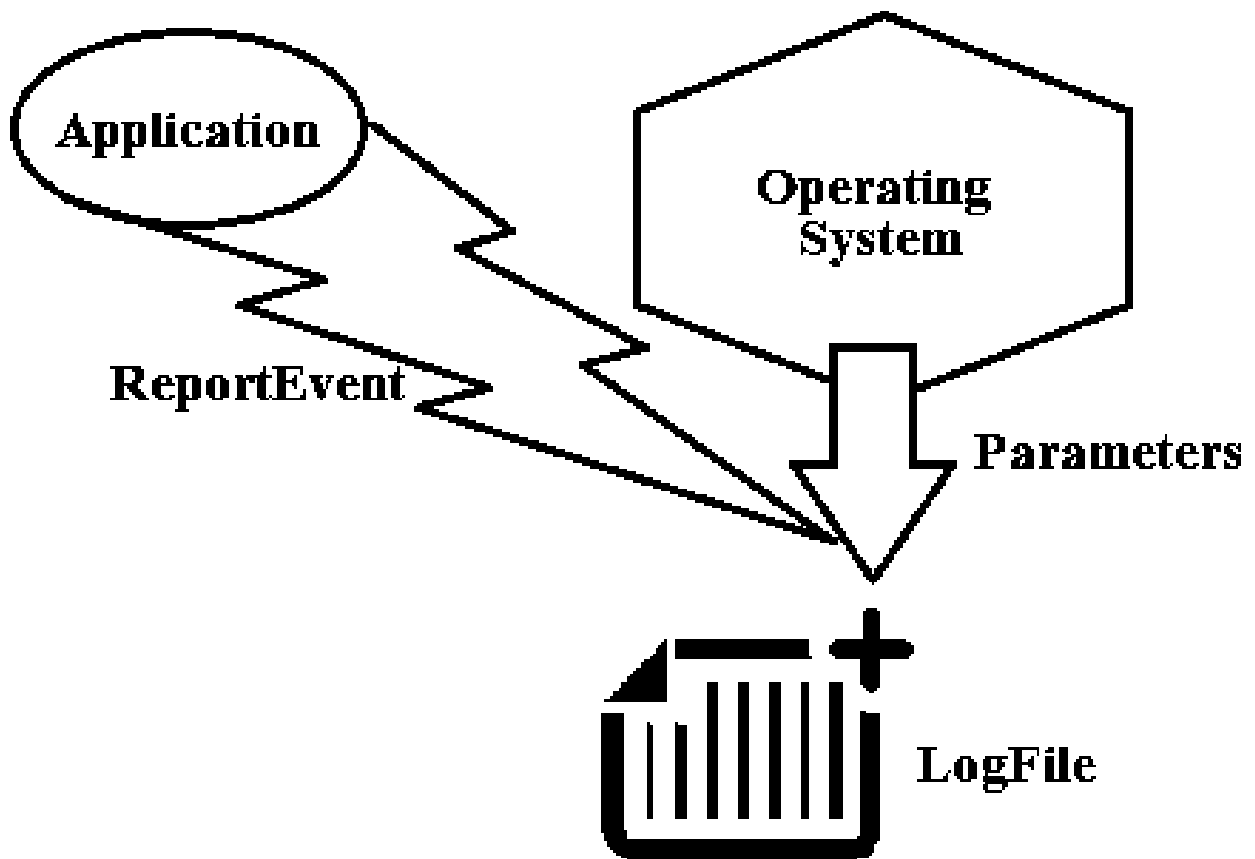


Figure 3: Event logs and reporting in windows

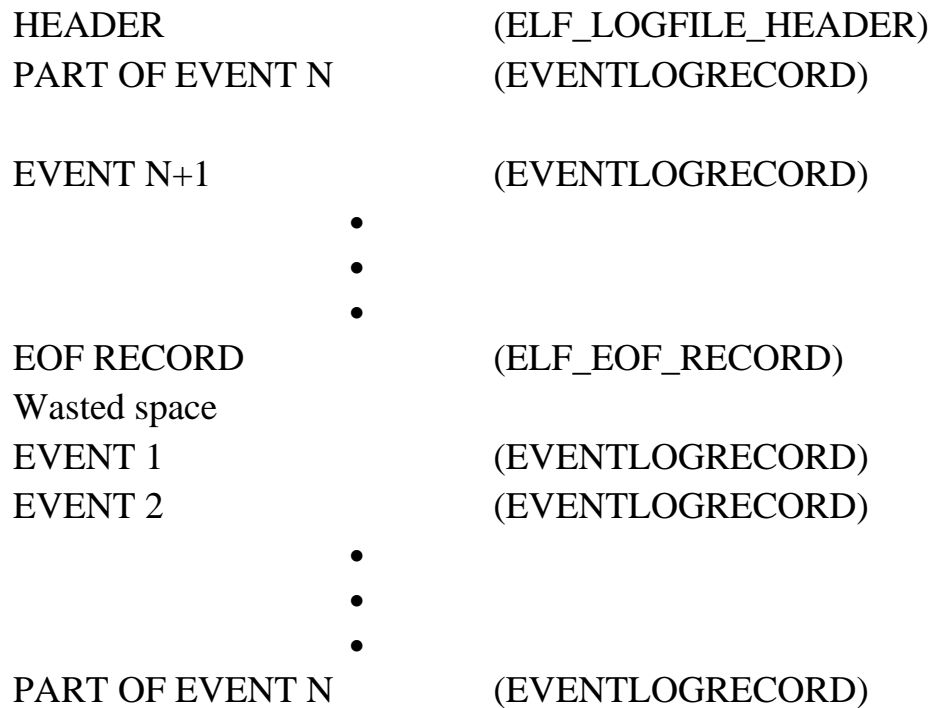
The event records are organized in either non-wrapping or wrapping way. The non-wrapping is a simple one where records are added between header and EOF record structures.

*Non-wrapping:*

HEADER	(ELF_LOGFILE_HEADER)
EVENT 1	(EVENTLOGRECORD)
	•
	•
	•
EVENT 2	(EVENTLOGRECORD)
EOF RECORD	(ELF_EOF_RECORD)



### Wrapping:



The Wrapping mode uses circular way of adding new records. In this an old record is overwritten as new records come in.

---

### 11.4.2 Reading from Windows event log file

---

On Windows the event logs can be managed with "Event Viewer" (eventvwr.msc) or "Windows Events Command Line Utility" (wevtutil.exe). Event Viewer can represent the EVTXML (XML format) files in both "general view" (or formatted view) and "details view" (which has both a "friendly view" and "XML view"). Note that the formatted view can hide significant event data that is stored in the event record and can be seen in the detailed view.

An event viewer application like Windows Event Viewer or log parser uses the OpenEventLog function to open the event log for an event source. Then the viewer application uses the ReadEventLog function to read event records from the log. The following diagram illustrates this process (see figure 4).

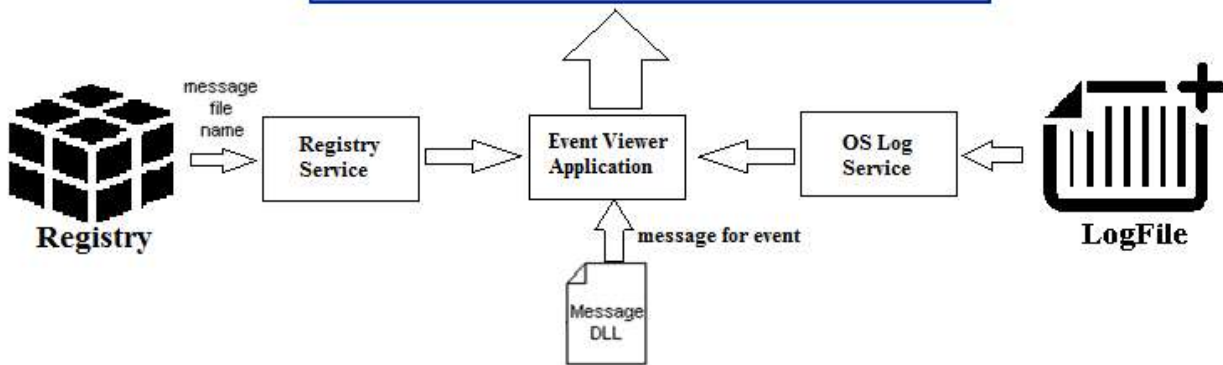
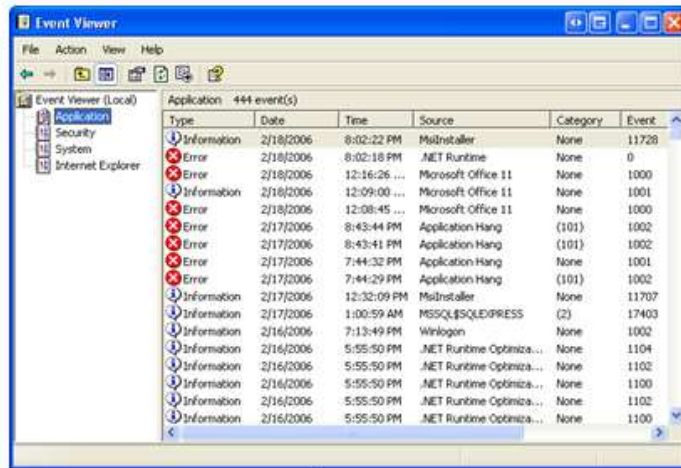


Figure 4: Process of viewing Event logs in windows.

### 11.4.3 Using Microsoft log parser

Logparser is a flexible command line utility that was initially written by Gabriele Giuseppini, a Microsoft employee, to automate tests for IIS logging. It was intended for use with the Windows operating system, and was included with the IIS 6.0 Resource Kit Tools. The default behavior of logparser works like a "data processing pipeline", by taking an SQL expression on the command line, and outputting the lines containing matches for the SQL expression.

Microsoft describes Logparser as a powerful, versatile tool that provides universal query access to text-based data such as log files, XML files and CSV files, as well as key data sources on the Windows operating system such as the Event Log, the Registry, the file system, and Active Directory. The results of the input query can be custom-formatted in text based output, or they can be persisted to more specialty targets like SQL, SYSLOG, or a chart.

#### Common usage:

```
$ logparser <options> <SQL expression>
```

**Example:** Selecting date, time and client username accessing ASPX-files, taken from all .log-files in the current directory.

```
$ logparser -i:IISW3C -q "SELECT date, time, cs-username FROM *.log WHERE cs-uri-stem LIKE '%.aspx' ORDER BY date, time;"
```

```

C:\Program Files\Log Parser 2.2>logparser /h
Microsoft (R) Log Parser Version 2.2.10
Copyright (C) 2004 Microsoft Corporation. All rights reserved.

Usage:   LogParser [-i:<input_format>] [-o:<output_format>] [<SQL query>] [-f:<query_filename>] [-p:<param_value1>...<param_valueN>]
         [-<input_format_options>] [-<output_format_options>]
         [-qI:ON|OFF] [-e:<max_errors>] [-iwl:ON|OFF]
         [-statsI:ON|OFF] [-saveDefaults] [-queryInfo]

LogParser -c -i:<input_format> -o:<output_format> <from_entity>
         <into_entity> [-<where_clause>] [-<input_format_options>]
         [-<output_format_options>] [-multiSiteI:ON|OFF]
         [-qI:ON|OFF] [-e:<max_errors>] [-iwl:ON|OFF]
         [-statsI:ON|OFF] [-queryInfo]

-i:<input_format>      : one of IISW3C, NCSA, IIS, IISODBC, BIN, IISMSID,
                     HTTPERR, URLSCAN, CSU, TSU, W3C, XML, EUT, ETW,
                     NETMON, REG, ADS, TEXTLINE, TEXTWORD, PS, COM (if
                     omitted, will guess from the FROM clause)
-o:<output_format>    : one of CSU, TSU, XML, DATAGRID, CHART, SYSLOG,
                     NEUROVIEW, NAT, W3C, IIS, SQL, TPL, NULL (if omitted,
                     will guess from the INTO clause)
-qI:ON|OFF           : quiet mode; default is OFF
-e:<max_errors>       : max # of parse errors before aborting; default is -1
                     (<ignore all>)
-iwl:ON|OFF          : ignore warnings; default is OFF
-statsI:ON|OFF       : display statistics after executing query; default is
                     ON
-c                   : use built-in conversion query
-multiSiteI:ON|OFF  : send BIN conversion output to multiple files
                     depending on the SiteID value; default is OFF
-saveDefaults        : save specified options as default values
-restoreDefaults     : restore factory defaults
-queryInfo           : display query processing information (does not
                     execute the query)

Examples:
LogParser "SELECT date, REVERSEDNS(c-ip) AS Client, COUNT(*) FROM file.log
          WHERE sc-status<200 GROUP BY date, Client" -e10
LogParser file:noQuery.sql?input=C:\temp\ex*.log?output=results.csv
LogParser -c -i:BIN -o:W3C file1.log file2.log "ComputerName IS NOT NULL"

Help:
-h GRAMMAR           : SQL Language Grammar
-h FUNCTIONS I <function> I : Functions Syntax
-h EXAMPLES          : Example queries and commands
-h -i:<input_format>  : Help on <input_format>
-h -o:<output_format> : Help on <output_format>
-h -c                : Conversion help

C:\Program Files\Log Parser 2.2>logparser "select count(distinct c-ip) from ex07
COUNT(DISTINCT c-ip)
2177

Statistics:
Elements processed: 6384
Elements output:   1
Execution time:    0.03 seconds

C:\Program Files\Log Parser 2.2>

```

Figure 5: LogParser.

#### 11.4.4 Understanding Windows user account management logs

Audit policies in windows can be edited using local group policy editor (see figure 2). Windows user account management security policy setting informs the operating system to logs when the following user account management tasks are performed:

- On creation, changing, deletion, renaming, disabling, enabling, locking out, or unlocking of an user account.
- On user account password change.
- On adding of Security identifier (SID) history to an user account.
- The restore mode password for Directory Services is set.
- Permissions on accounts are modified. Etc.

This policy setting is very useful for investigators in tracking events that involve getting sense of user accounts.

To view complete list of events in user account management please visit Microsoft site: <https://technet.microsoft.com/en-us/library/dn319091.aspx>.

---

### **11.4.5 Understanding Windows file and other object Access sets**

---

Objects on internet or computer can be tracked using object access policy setting in audit events. If appropriate object access auditing subcategories (like file operations, Registry etc.) is enabled one can audit attempts to access a file, directory, registry key, or any other object (see figure 2). Many other subcategories are Audit Application Generated, Audit Certification Services, Audit Detailed File Share, Audit File Share, Audit File System, Audit Filtering Platform Connection, Audit Kernel Object, Audit Other Object Access Events, Audit Registry, Audit Security Account Management etc.

---

### **11.4.6 Auditing policy change**

---

We can track the audit policy changes even. a local system or network Policy Change can be tracked using audit policy change events. Policies are mostly centrally created by admin or privileged users, thus, any changes or attempts to change these policies can be an important aspect of security management as well as while gathering investigative information. Few subcategories in this are: Audit Policy Change, Audit Authentication Policy Change, Audit Authorization Policy Change, Audit Filtering Platform Policy Change, Audit MPSSVC Rule-Level Policy Change, Audit Other Policy Change Events.

---

## **11.5 Windows password storage**

---

User and passwords in a window system are stored in either of two places:

- a) SAM(Security Account Manager)
- b) AD(Activity directory)

---

### **11.5.1 SAM**

---

The Security Account Manager (SAM) is a database file in Windows XP, Windows Vista and Windows 7 that stores users' passwords. It can be used to authenticate local and remote users. Beginning with Windows 2000 SP4, Active Directory is used to authenticate remote users. SAM uses cryptographic measures to prevent forbidden users to gain access to the system.

The user passwords are stored in a hashed format in a registry hive either as a LM hash or as a NTLM hash. This file can be found in %SystemRoot%/system32/config/SAM and is mounted on HKLM/SAM.

In an attempt to improve the security of the SAM database against offline software cracking, Microsoft introduced the SYSKEY function in Windows NT 4.0. When SYSKEY is enabled, the on-disk copy of the SAM file is partially encrypted, so that the password hash values for all local accounts stored in the SAM are encrypted with a key (usually also referred to as the "SYSKEY"). It can be enabled by running the syskey program. Since a hash function is one-way, this provides some measure of security for the storage of the passwords.

In the case of online attacks, it is not possible to simply copy the SAM file to another location. The SAM file cannot be moved or copied while Windows is running, since the Windows kernel

obtains and keeps an exclusive filesystem lock on the SAM file, and will not release that lock until the operating system has shut down or a "Blue Screen of Death" exception has been thrown. However, the in-memory copy of the contents of the SAM can be dumped using various techniques (including pwdump), making the password hashes available for offline brute-force attack.

---

#### **11.5.1.1 Removing LM hash**

---

Most versions of Windows can be configured to disable the creation and storage of valid LM hashes when the user changes their password. This is the default setting in Windows Vista, but was disabled by default in previous versions of Windows. Note: enabling this setting does not immediately clear the LM hash values from the SAM, but rather enables an additional check during password change operations that will instead store a "dummy" value in the location in the SAM database where the LM hash is otherwise stored. (This dummy value has no relationship to the user's password - it is the same value used for all user accounts.)

---

#### **11.5.1.2 Related attacks**

---

In Windows NT 3.51, NT 4.0 and 2000, an attack was devised to bypass the local authentication system. If the SAM file is deleted from the hard drive (e.g. mounting the Windows OS volume into an alternate operating system), the attacker could log in as any account with no password. This flaw was corrected with Windows XP, which shows an error message and shuts down the computer. However, there exist software utilities which, by the aforementioned methodology of using either an emulated virtual drive, or boot disk (usually Unix/Linux) based environment to mount the local drive housing the active NTFS partition, and using programmed software routines and function calls from within assigned memory stacks to isolate the SAM file from the Windows NT system installation directory structure (default: %SystemRoot%/system32/config/SAM) and, depending on the particular software utility being used, removes the password hashes stored for user accounts in their entirety, or in some cases, modify the user account passwords directly from this environment.

This software has both a highly pragmatic and beneficial use as a password clearing or account recovering utility for individuals who have lost or forgotten their windows account passwords, as well as a possible use as a malicious software security bypassing utility. Essentially granting a user with enough ability, experience, and familiarity with both the cracking utility software and the security routines of the Windows NT kernel (as well as offline and immediate local access to the target computer) the capability to entirely bypass/remove the windows account passwords from a potential target computer. Only recently, Microsoft released a utility called LockSmith, which is part of MSDart. MSDart is not freely available to end-users, however.

---

### **11.5.2 AD**

---

Active Directory (AD) is a directory service that Microsoft developed for Windows domain networks and is included in most Windows Server operating systems as a set of processes and services.

An AD domain controller authenticates and authorizes all users and computers in a Windows domain type network—assigning and enforcing security policies for all computers and installing or updating software. For example, when a user logs into a computer that is part of a Windows domain, Active Directory checks the submitted password and determines whether the user is a system administrator or normal user.

Active Directory makes use of Lightweight Directory Access Protocol (LDAP) versions 2 and 3, Microsoft's version of Kerberos, and DNS.

As a directory service, an Active Directory instance consists of a database and corresponding executable code responsible for servicing requests and maintaining the database. The executable part, known as Directory System Agent, is a collection of Windows services and processes that run on Windows 2000 and later. Objects in Active Directory databases can be accessed via LDAP, ADSI (a component object model interface), messaging API and Security Accounts Manager services.

---

## 11.6 Summary

---

1. Event logs and Password cracking plays very important role in digital forensics.
2. Event logging provides system administrators with information useful for diagnostics and auditing. Windows registry is also a very important source to maintain and manage logs.
3. Password cracking is utilized to gain access to digital evidence for which a judge has allowed access but the particular file's access is restricted.
4. Registry entries can be used to acquire and analyze much important information like system, time zone, shares, audit policy, wireless SSIDS, auto start locations, user login, activities, USB removable devices, trusted devices, cache, cookie and history etc.
5. User and passwords in a window system are stored in either Security Account Manager or Activity directory.
6. The most important methods of password cracking are brute force method, dictionary searches, syllable attack, rule based attack, hybrid attack, password guessing, rainbow attack.
7. There are several tools /software available to assist passwords recovery or cracking. Few examples are windows key generator, CMOSPwd, ERD commander.

---

## 11.7 Check Your Progress

---

1. Fill in the blanks.

- a) \_\_\_\_\_ and \_\_\_\_\_ can be very handy to get a good deal of analysis of registry entries.
- b) When an application calls the \_\_\_\_\_ function to write an entry to the event log, the system passes the parameters to the \_\_\_\_\_.
- c) An event viewer application uses the \_\_\_\_\_ function to open the event log for an event source.
- d) SAM Stands for \_\_\_\_\_.

- e) the \_\_\_\_\_ subcategory needs to be enabled to audit file operations and the \_\_\_\_\_ subcategory needs to be enabled to audit registry accesses

2. State True or False

- a) In windows event logs are stored in binary format.
- b) Policy Change audit events do not allow you to track changes to important security policies on a local system or network.
- c) The Security Account Manager (SAM) is a database file in Windows.
- d) Office Password Recovery Toolbox is software which stores lost password to any Microsoft Office document effectively.
- e) Non-wrapping can occur when the event log is created or when the event log is cleared.

11.8 Answers to Check Your Progress

1. Fill in the blanks.

- a) ProDiscover, ProScript
- b) ReportEvent, event-logging service
- c) OpenEventLog
- d) Security Account Manager.
- e) File System, Registry

2. State True or False

- a) True
- b) False
- c) True
- d) False
- e) True

---

## 11.8 Further Readings

---

- 1. Linda Volonino, Reynaldo Anzaldua; Computer Forensics For Dummies, Wiley Publishing, Inc.
- 2. Investigating Hard Disks, File and Operating Systems: EC-Council | Press
- 3. Windows Event Log (EVT) – ForensicsWiki, [www.forensicswiki.org/wiki/Windows\\_Event\\_Log\\_\(EVT\)](http://www.forensicswiki.org/wiki/Windows_Event_Log_(EVT))
- 4. Audit User Account Management - TechNet – Microsoft, [https://technet.microsoft.com/en-us/library/dd772693\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/dd772693(v=ws.10).aspx)
- 5. Event Log File Format (Windows) - MSDN – Microsoft, [https://msdn.microsoft.com/en-us/library/windows/desktop/bb309026\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/bb309026(v=vs.85).aspx)
- 6. Policy Change - TechNet – Microsoft, [https://technet.microsoft.com/en-us/library/dd772669\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/dd772669(v=ws.10).aspx)
- 7. Reading from the Event Log (Windows) - MSDN – Microsoft, [https://msdn.microsoft.com/en-us/library/windows/desktop/aa363675\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/aa363675(v=vs.85).aspx)

## References, Article Source & Contributors

- [1] Active Directory - Wikipedia, the free encyclopedia, [https://en.wikipedia.org/wiki/Active\\_Directory](https://en.wikipedia.org/wiki/Active_Directory)
- [2] CMOSPwd, <https://packages.gentoo.org/packages/app-forensics/cmospwd>
- [3] Dictionary attack - Wikipedia, the free encyclopedia, [https://en.wikipedia.org/wiki/Dictionary\\_attack](https://en.wikipedia.org/wiki/Dictionary_attack)
- [4] Event logging – Wikipedia, [https://en.wikipedia.org/wiki/Event\\_logging](https://en.wikipedia.org/wiki/Event_logging)
- [5] Log analysis - Wikipedia, the free encyclopedia, [https://en.wikipedia.org/wiki/Log\\_analysis](https://en.wikipedia.org/wiki/Log_analysis) \
- [6] logparser - Wikipedia, the free encyclopedia, <https://en.wikipedia.org/wiki/Logparser>
- [7] Microsoft Desktop Optimization Pack - Wikipedia, , [https://en.m.wikipedia.org/.../Microsoft\\_Diagnostics\\_and\\_Recovery\\_Tool](https://en.m.wikipedia.org/.../Microsoft_Diagnostics_and_Recovery_Tool)
- [8] Passware kit, [http://azizalstsetia.blogspot.in/2011/04/passware-kit-forensic-103-full-version\\_7549.html](http://azizalstsetia.blogspot.in/2011/04/passware-kit-forensic-103-full-version_7549.html)
- [9] Password cracking - Wikipedia, the free encyclopedia, [https://en.wikipedia.org/wiki/Password\\_cracking](https://en.wikipedia.org/wiki/Password_cracking).
- [10] Rainbow table - Wikipedia, the free encyclopedia, [https://en.wikipedia.org/wiki/Rainbow\\_table](https://en.wikipedia.org/wiki/Rainbow_table)
- [11] Recover lost MS Office Password, [recoverlostofficepassword.wikidot.com](http://recoverlostofficepassword.wikidot.com)
- [12] Security Account Manager - Wikipedia, the free encyclopedia, [https://en.wikipedia.org/wiki/Security\\_Account\\_Manager](https://en.wikipedia.org/wiki/Security_Account_Manager)
- [13] Windows XML Event Log, (EVTX), [http://www.forensicwiki.org/wiki/Windows\\_XML\\_Event\\_Log\\_\(EVTX\)](http://www.forensicwiki.org/wiki/Windows_XML_Event_Log_(EVTX))



## **EXPERT PANEL**



**Dr. Jeetendra Pande, Associate Professor- Computer Science, School of  
Computer Science & IT, Uttarakhand Open University, Haldwani**



**Dr. Ajay Prasad, Sr. Associate Professor, University of Petroleum and  
Energy Studies, Dehradun**



**Dr. Akashdeep Bharadwaj, Professor, University of Petroleum and Energy  
Studies, Dehradun**



**Mr. Sridhar Chandramohan Iyer, Assistant Professor- Universal College of  
Engineering, Kaman, Vasai, University of Mumbai**



**Mr. Rishikesh Ojha, Digital Forensics and eDiscovery Expert**



**Ms. Priyanka Tewari, IT Consultant**



**Mr. Ketan Joglekar, Assistant Professor, GJ College, Maharashtra**



**Dr. Ashutosh Kumar Bhatt, Associate Professor, Uttarakhand Open University, Haldwani**



**Dr. Sangram Panigrahi, Assistant Professor, Siksha 'O' Anusandhan, Bhubaneswar**



This MOOC has been prepared with the support of



© Commonwealth Educational Media Centre for Asia , 2021. Available in Creative Commons Attribution-ShareAlike 4.0 International license to copy, remix and redistribute with attribution to the original source (copyright holder), and the derivative is also shared with similar license.