Some of the many Windows Event IDs and Windows Vista Event IDs recognized by EventLog Analyzer are listed below:

Windows Event ID	Windows Vista Event ID	Event Type	Description
512, 513, 514, 515, 516, 518, 519, 520	4608, 4609, 4610, 4611, 4612, 4614, 4615, 4616	System Events	Identifies local system processes such as system startup and shutdown and changes to the system time
517	4612	Audit Logs Cleared	Identifies all the audit logs clearing events
528, 540	4624	Successful User Logons	Identifies all the user logon events
529, 530, 531, 532, 533, 534, 535, 536, 537, 539	4625	Logon Failures	Identifies all the failed user logon events
538	4634	Successful User Logoff	Identifies all the user logoff events
560, 563, 565, 566	4656, 4658, 4659, 4660, 4661, 4662, 4663, 4664, 5147	Object Access	Identifies when a given object (File, Directory, etc.) is accessed, the type of access (e.g. read, write, delete) and whether or not access was successful/failed, and who performed the action
612	4719	Audit Policy Changes	Identifies all the changes done in the audit policy
624, 625, 626, 627, 628, 629, 630, 642, 644	4720, 4722, 4723, 4724, 4725, 4726, 4738, 4740	User Account Changes	Identifies all the changes done on an user account like user account creation,deletion, password change, etc.
(631 to 641) and (643, 645 to 666)	4727 to 4737, 4739 to 4762	User Group Changes	Identifies all the changes done on an user group such as adding or removing a global or local group, adding or removing members from a global or local group, etc.
672, 680	4768, 4776	Successful User Account Validation	Identifies successful user account logon events, which are generated when a domain user account is authenticated on a domain controller
675, 681	4771, 4777	Failed User Account Validation	Identifies unsuccessful user account logon events, which are generated when a domain user account is authenticated on a domain controller
682, 683	4778, 4779	Host Session Status	Identifies the session re-connection or disconnection

EventLog Analyzer also supports logs received from other syslog supported systems & devices.

Using EventLog Analyzer you can archive or store these Windows event logs, and also generate event log reports in real-time. You get instant access to wide variety of reports for events generated across hosts, users, processes, and host groups. You can also obtain pre-defined compliance reports to meet HIPAA, GLBA, PCI, and Sarbanes-Oxley audit requirements.