Sysmon Registry Serialization Format

r Value 0 L6]	Header Value 1 [UINT16]	Rule Group Count [UINT32]	Rule Group Begin Offset [UINT32]	Minor Schema Version Major Schema Version [UINT16]
Event Ty	ype Value [INT32]	On Match Value [INT32]	Next Event Type Offset [INT32]	Rule Count [INT32]
Rule Type [INT32]		Filter [INT32]	Next Rule Offset [INT32]	Rule Text Length [INT32]
	Rule Text <variable length<="" td=""><td>UTF-16LE encoded text with 0x0000 termination ></td><td></td><td></td></variable>	UTF-16LE encoded text with 0x0000 termination >		
Rule	· Type [INT32]	Filter [INT32]	Next Rule Offset [INT32]	Rule Text Length [INT32]
	Rule Text <variable length<="" th=""><th>UTF-16LE encoded text with 0x0000 termination ></th><th></th><th></th></variable>	UTF-16LE encoded text with 0x0000 termination >		
	Rule Text <variable length<="" th=""><th>UTF-16LE encoded text with 0x0000 termination ></th><th></th><th></th></variable>	UTF-16LE encoded text with 0x0000 termination >		
Event Ty	Rule Text <variable [int32]<="" length="" td="" value="" ype=""><td>On Match Value [INT32]</td><td>Next Event Type Offset [INT32]</td><td>Rule Count [INT32]</td></variable>	On Match Value [INT32]	Next Event Type Offset [INT32]	Rule Count [INT32]
			Next Event Type Offset [INT32] Next Rule Offset [INT32]	Rule Count [INT32] Rule Text Length [INT32]
	ype Value [INT32]	On Match Value [INT32]		
Rule	ype Value [INT32]	On Match Value [INT32] Filter [INT32]		