EventID 1 Process Create	
UtcTime	Time in UTC when event was created
ProcessGuid	Process Guid of the process that got spawned/created (child)
ProcessId	Process ID used by the OS to identify the created process (child)
Image	File path of the process being spawned/created. Considered also the child or source process
FileVersion	Version of the image associated with the main process (child)
Description	Description of the image associated with the main process (child)
Product	Product name the image associated with the main process (child) belongs to
OriginalFileName	OriginalFileName from the PE header, added on compilation
Company	Company name the image associated with the main process (child) belongs to
CommandLine	Arguments which were passed to the executable associated with the main process
CurrentDirectory	The path without the name of the image associated with the process
User	Name of the account who created the process (child) . It usually contains domain name and user name
LogonGuid	Logon GUID of the user who created the new process. Value that can help you correlate this event with others that contain the same Logon GUID
LogonId	Login ID of the user who created the new process. Value that can help you correlate this event with others that contain the same Logon ID
TerminalSessionId	ID of the session the user belongs to
IntegrityLevel	Integrity label assigned to a process
Hashes	Full hash of the file with the algorithms in the HashType field
ParentProcessGuid	ProcessGUID of the process that spawned/created the main process (child)
ParentProcessId	Process ID of the process that spawned/created the main process (child)
ParentImage	File path that spawned/created the main process
ParentCommandLine	Arguments which were passed to the executable associated with the parent process

EventID 2 File creation time changed	
UtcTime	Time in UTC when event was created
ProcessGuid	Process Guid of the process that changed the file creation time
ProcessId	Process ID used by the OS to identify the process changing the file creation time
Image	File path of the process that changed the file creation time
TargetFilename	Full path name of the file
CreationUtcTime	New creation time of the file
PreviousCreationUtcTime	Previous creation time of the file

EventID 3 Network connection	
UtcTime	Time in UTC when event was created
ProcessGuid	Process Guid of the process that made the network connection
ProcessId	Process ID used by the OS to identify the process that made the network connection
Image	File path of the process that made the network connection
User	Name of the account who made the network connection
Protocol	Protocol being used for the network connection
Initiated	Indicated process initiated TCP connection
SourceIsIpv6	Is the source IP an Ipv6
SourceIp	source IP address that made the network connection
SourceHostname	DNS name of the host that made the network connection
SourcePort	source port number
SourcePortName	name of the source port being used
DestinationIsIpv6	is the destination IP an Ipv6
DestinationIp	IP address destination
DestinationHostname	DNS name of the host that is contacted
DestinationPort	destination port number
DestinationPortName	name of the destination port

EventID 4 Sysmon service state changed	
UtcTime	Time in UTC when event was created
State	Sysmon service state
Version	Sysmon binary version
SchemaVersion	Sysmon config schema version

EventID 5 Process terminated	
UtcTime	Time in UTC when event was created
ProcessGuid	Process Guid of the process that terminated
ProcessId	Process ID used by the OS to identify the process that terminated
Image	File path of the executable of the process that terminated

EventID 6 Kernel driver loaded	
UtcTime	Time in UTC when event was created
ImageLoaded	File path of the driver loaded
Hashes	Hashes captured by Sysmon driver
Signed	Is the driver loaded signed
Signature	Signer name of the driver
SignatureStatus	Status of the signature

EventID 7 Image loaded	
UtcTime	Time in UTC when event was created
ProcessGuid	Process Guid of the process that loaded the image
ProcessId	Process ID used by the OS to identify the process that loaded the image
Image	File path of the process that loaded the image
ImageLoaded	Path of the image loaded
FileVersion	Version of the image loaded
Description	Description of the image loaded
Product	Product name the image loaded belongs to
Company	Company name the image loaded belongs to
OriginalFileName	OriginalFileName from the PE header, added on compilation
Hashes	Full hash of the file with the algorithms in the HashType field
Signed	State whether the image loaded is signed
Signature	The signer name
SignatureStatus	status of the signature

EventID 8 Remote thread	
UtcTime	Time in UTC when event was created
SourceProcessGuid	Process Guid of the source process that created a thread in another process
SourceProcessId	Process ID used by the OS to identify the source process that created a thread in another process
SourceImage	File path of the source process that created a thread in another process
TargetProcessGuid	Process Guid of the target process
TargetProcessId	Process ID used by the OS to identify the target process
TargetImage	File path of the target process
NewThreadId	Id of the new thread created in the target process
StartAddress	New thread start address
StartModule	Start module determined from thread start address mapping to PEB loaded module list
StartFunction	Start function is reported if exact match to function in image export tables

EventID 9 Raw access read	
UtcTime	Time in UTC when event was created
ProcessGuid	Process Guid of the process that conducted reading operations from the drive
ProcessId	Process ID used by the OS to identify the process that conducted reading operations from the drive
Image	File path of the process that conducted reading operations from the drive
Device	Target device

EventID 10 Process Access	
UtcTime	Time in UTC when event was created
SourceProcessGUID	Process Guid of the source process that opened another process. It is derived from a truncated part of the machine GUID, the process start-time and the process token ID.
SourceProcessId	Process ID used by the OS to identify the source process that opened another process. Derived partially from the EPROCESS kernel structure
SourceThreadId	ID of the specific thread inside of the source process that opened another process
SourceImage	File path of the source process that created a thread in another process
TargetProcessGUID	Process Guid of the target process
TargetProcessId	Process ID used by the OS to identify the target process
TargetImage	File path of the executable of the target process
GrantedAccess	The access flags (bitmask) associated with the process rights requested for the target process
CallTrace	Stack trace of where open process is called. Included is the DLL and the relative virtual address of the functions in the call stack right before the open process call

EventID 11 File create	
UtcTime	Time in UTC when event was created
ProcessGuid	Process Guid of the process that created the file
ProcessId	Process ID used by the OS to identify the process that created the file (child)
Image	File path of the process that created the file
TargetFilename	Name of the file that was created
CreationUtcTime	File creation time

EventID 12 Registry event (Object create and delete)	
UtcTime	Time in UTC when event was created
EventType	CreateKey or DeleteKey
ProcessGuid	Process Guid of the process that created or deleted a registry key
ProcessId	Process ID used by the OS to identify the process that created or deleted a registry key
Image	File path of the process that created or deleted a registry key
TargetObject	Complete path of the registry key

EventID 13 Registry event (Value set)	
UtcTime	Time in UTC when event was created
EventType	SetValue
ProcessGuid	Process Guid of the process that modified a registry value
ProcessId	Process ID used by the OS to identify the process that that modified a registry value
Image	File path of the process that that modified a registry value
TargetObject	Complete path of the modified registry key
Details	Details added to the registry key

EventID 14 Registry event (Key and value rename)	
UtcTime	Time in UTC when event was created
EventType	RenameKey
ProcessGuid	Process Guid of the process that renamed a registry value and key
ProcessId	Process ID used by the OS to identify the process that renamed a registry value and key
Image	File path of the process that renamed a registry value and key
TargetObject	Complete path of the renamed registry key
NewName	New name of the registry key

EventID 15 File create stream hash	
UtcTime	Time in UTC when event was created
ProcessGuid	Process Guid of the process that created the named file stream
ProcessId	Process ID used by the OS to identify the process that created the named file stream
Image	File path of the process that created the named file stream
TargetFilename	Name of the file
CreationUtcTime	File download time
Hash	Full hash of the file with the algorithms in the HashType field

EventID 16 Sysmon config state changed	
UtcTime	Time in UTC when event was created
Configuration	File path of the Sysmon config file being updated
ConfigurationFileHash	Hash (SHA1) of the Sysmon config file being updated

EventID 17 Pipe event (Pipe created)	
UtcTime	Time in UTC when event was created
EventType	CreatePipe
ProcessGuid	Process Guid of the process that created the pipe
ProcessId	Process ID used by the OS to identify the process that created the pipe
PipeName	Name of the pipe created
Image	File path of the process that created the pipe

EventID 18 Pipe event (Pipe connected)	
UtcTime	Time in UTC when event was created
EventType	ConnectPipe
ProcessGuid	Process Guid of the process that connected the pipe
ProcessId	Process ID used by the OS to identify the process that connected the pipe
PipeName	Name of the pipe connected
Image	File path of the process that connected the pipe

EventID 19 WMI event (WmiEventFilter activity detected)	
UtcTime	Time in UTC when event was created
EventType	WmiFilterEvent
Operation	wmievent filter operation
User	User that created the WMI filter
EventNamespace	Event namespace of the WMI class
Name	Event namespace of the WMI class
Query	WMI filter query

EventID 20 WMI event (WmiEventConsumer activity detected)	
UtcTime	Time in UTC when event was created
EventType	WmiConsumerEvent
Operation	wmievent consumer
User	user that created the wmi consumer
Name	name of the consumer created
Type	Type of wmi consumer
Destination	command of consumer

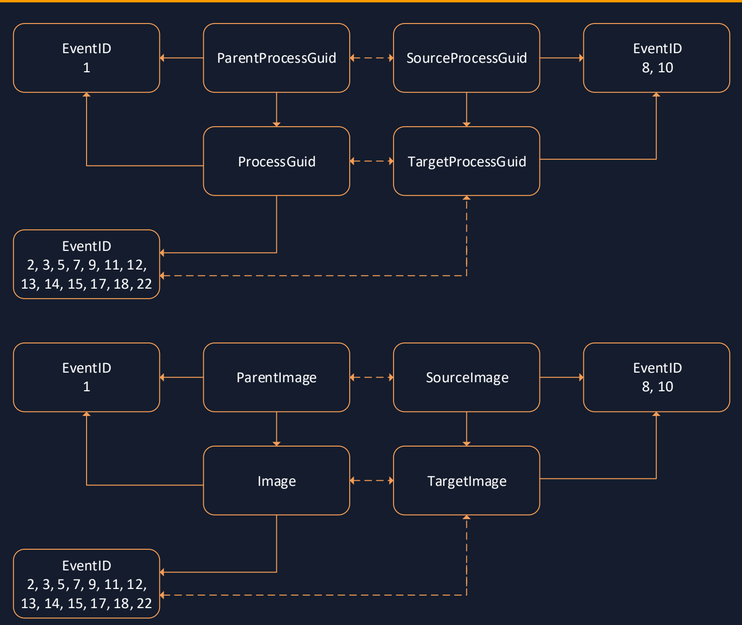
EventID 21 WMI event (WmiEventConsumerToFilter activity detected)	
UtcTime	Time in UTC when event was created
EventType	WmiBindingEvent
Operation	wmievent consumer to filter
User	user that created the wmi filter
Consumer	Consumer created to bind
Filter	Filter created to bind

EventID 22 DNS	
UtcTime	Time in UTC when event was created
ProcessGuid	Process Guid of the process that made the DNS query
ProcessId	Process ID of the process that made the DNS query
QueryName	DNS name that was queries
QueryStatus	Query result status code
QueryResults	Query results
Image	File path of the process that made the DNS query

EventID 255 Sysmon Error	
UtcTime	Time in UTC when event was created
ID	Error code
Description	Error description

Universal for all events	
RuleName	Name of the configured rule

Event relationships



Credits	
Creator	Olaf Hartong (@olafhartong)
Thanks	Mark Russinovich (@markrussinovich), Roberto Rodriguez (@Cyb3rWard0g)
Version	1.1