Sysmon

Tasks

1. Sysmon Basics

   Research and understand Sysmon for Linux. What is it, and what functionalities does it offer?

   What is Sysmon for Linux?

Sysmon for Linux is a system monitoring tool that provides detailed information about system activity. It is part of the Sysinternals Suite but adapted for the Linux environment. Sysmon captures various events related to process creation, network connections, file modifications, and more, making it a valuable tool for security monitoring and incident response.

Functionalities Offered by Sysmon for Linux

- **Process Creation**: Logs detailed information about process creation, including the command line, user, and hash of the executable.
- **Network Connections**: Captures details about network connections, including source and destination IP addresses and ports.
- **File Creation and Modification**: Monitors file system events, allowing users to track file changes and identify unauthorized access.
- **Driver Loading**: Logs events related to the loading of kernel modules.
- **User Activity Monitoring**: Provides insights into user actions and sessions.

- How does it differ from the traditional Windows Sysmon tool?

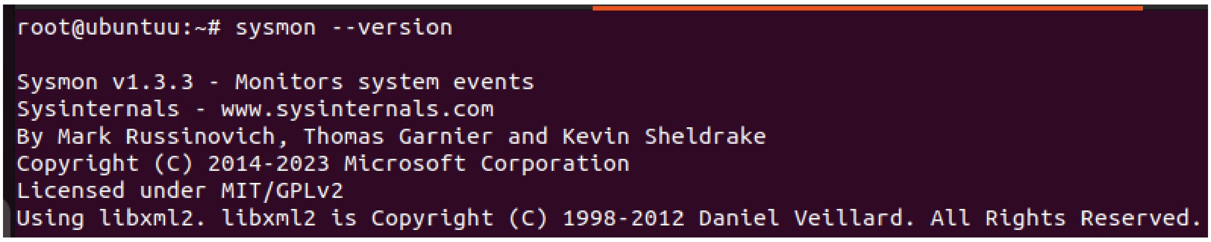
  Operating Environment: The most obvious difference is the operating system—Sysmon for Linux is tailored for Unix-like environments, while the traditional Sysmon is designed for Windows.

  Event Types: Some event types and functionalities differ due to the underlying architecture of the operating systems. For instance, Windows Sysmon can capture WMI events and DNS queries, which are not applicable in Linux.

  Configuration Syntax: The configuration file formats and syntax differ between the two versions.

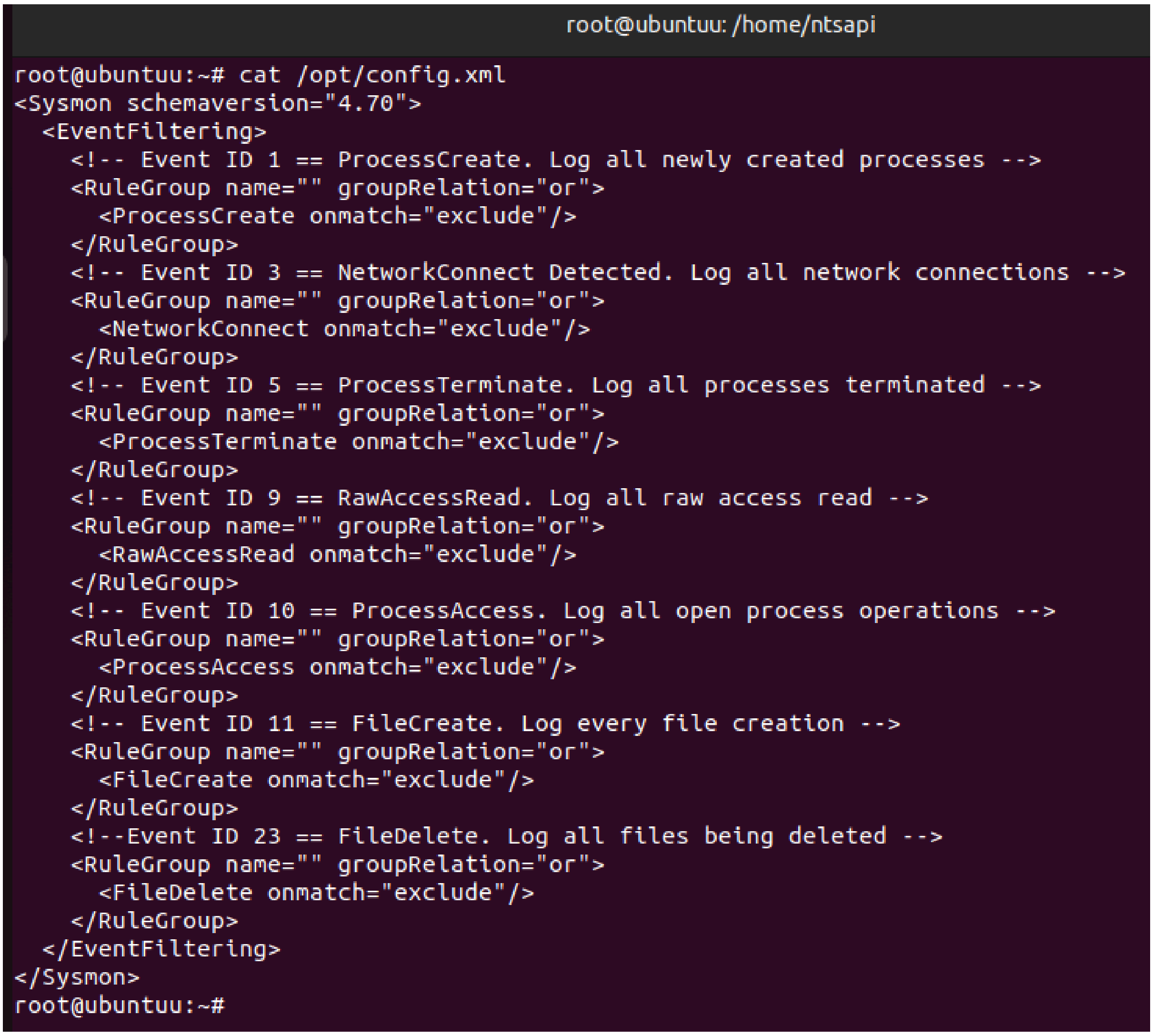
- Install and configure Sysmon for Linux on a test machine.

  Source: Demos/sysmonforlinux at main · OpenSecureCo/Demos (github.com)



```
root@ubuntuu:~# sysmon --version

Sysmon v1.3.3 - Monitors system events
Sysinternals - www.sysinternals.com
By Mark Russinovich, Thomas Garnier and Kevin Sheldrake
Copyright (C) 2014-2023 Microsoft Corporation
Licensed under MIT/GPLv2
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
```

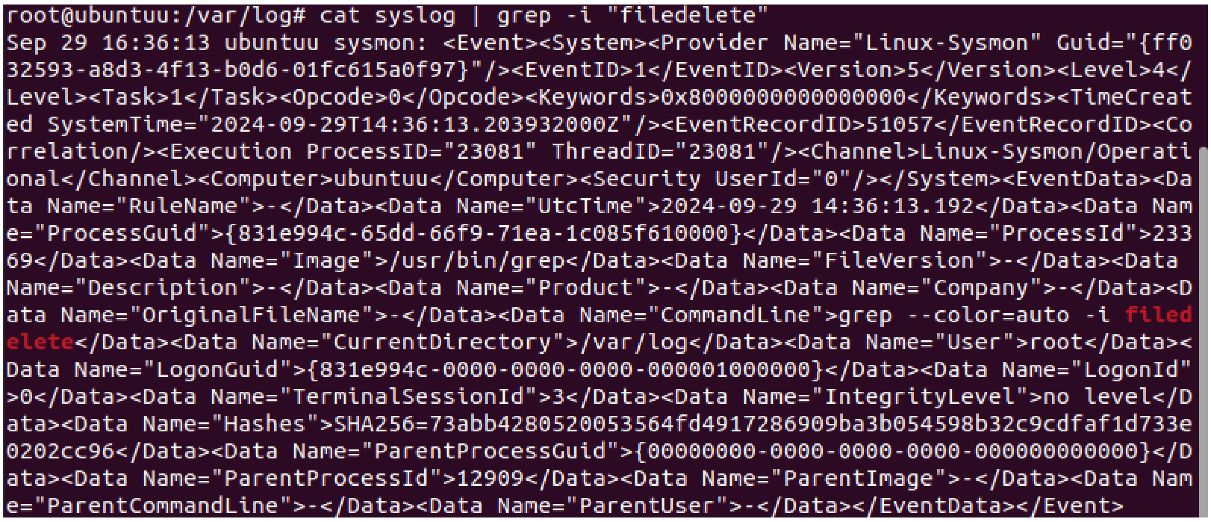


```
root@ubuntuu:~# cat /opt/config.xml
<Sysmon schemaversion="4.70">
  <EventFiltering>
    <!-- Event ID 1 == ProcessCreate. Log all newly created processes -->
    <RuleGroup name="" groupRelation="or">
      <ProcessCreate onmatch="exclude"/>
    </RuleGroup>
    <!-- Event ID 3 == NetworkConnect Detected. Log all network connections -->
    <RuleGroup name="" groupRelation="or">
      <NetworkConnect onmatch="exclude"/>
    </RuleGroup>
    <!-- Event ID 5 == ProcessTerminate. Log all processes terminated -->
    <RuleGroup name="" groupRelation="or">
      <ProcessTerminate onmatch="exclude"/>
    </RuleGroup>
    <!-- Event ID 9 == RawAccessRead. Log all raw access read -->
    <RuleGroup name="" groupRelation="or">
      <RawAccessRead onmatch="exclude"/>
    </RuleGroup>
    <!-- Event ID 10 == ProcessAccess. Log all open process operations -->
    <RuleGroup name="" groupRelation="or">
      <ProcessAccess onmatch="exclude"/>
    </RuleGroup>
    <!-- Event ID 11 == FileCreate. Log every file creation -->
    <RuleGroup name="" groupRelation="or">
      <FileCreate onmatch="exclude"/>
    </RuleGroup>
    <!--Event ID 23 == FileDelete. Log all files being deleted -->
    <RuleGroup name="" groupRelation="or">
      <FileDelete onmatch="exclude"/>
    </RuleGroup>
  </EventFiltering>
</Sysmon>
root@ubuntuu:~#
```

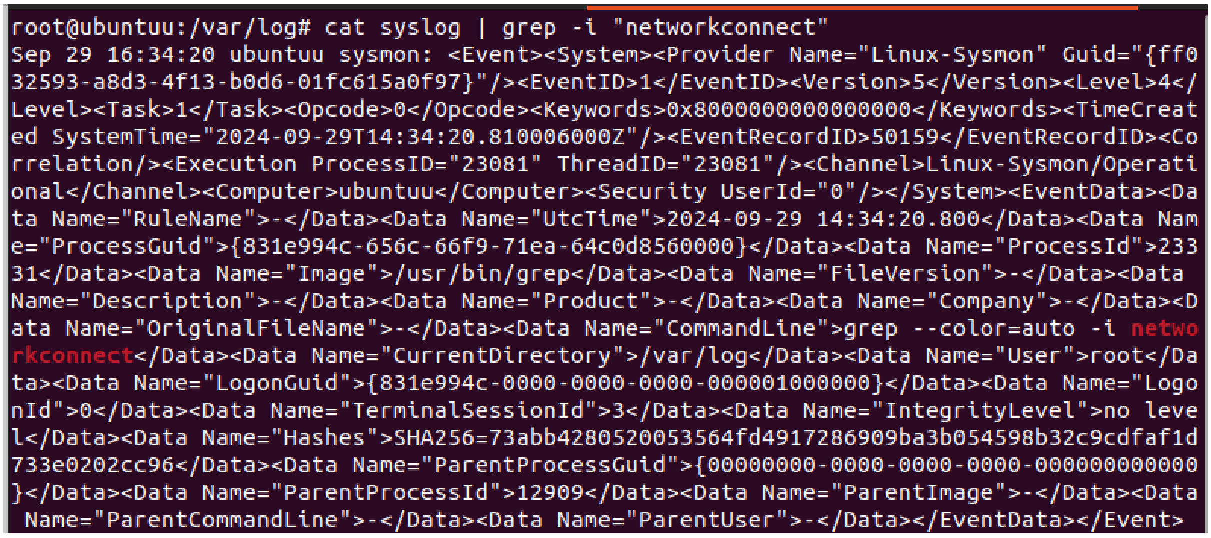
- Experiment with basic configuration options.
- Explore the Sysmon for Linux user interface
- Familiarize yourself with the information Sysmon captures.

2. Monitoring System Activity

- Simulate common system activities: Create, modify, and delete files, Start and stop processes, Establish network connections.

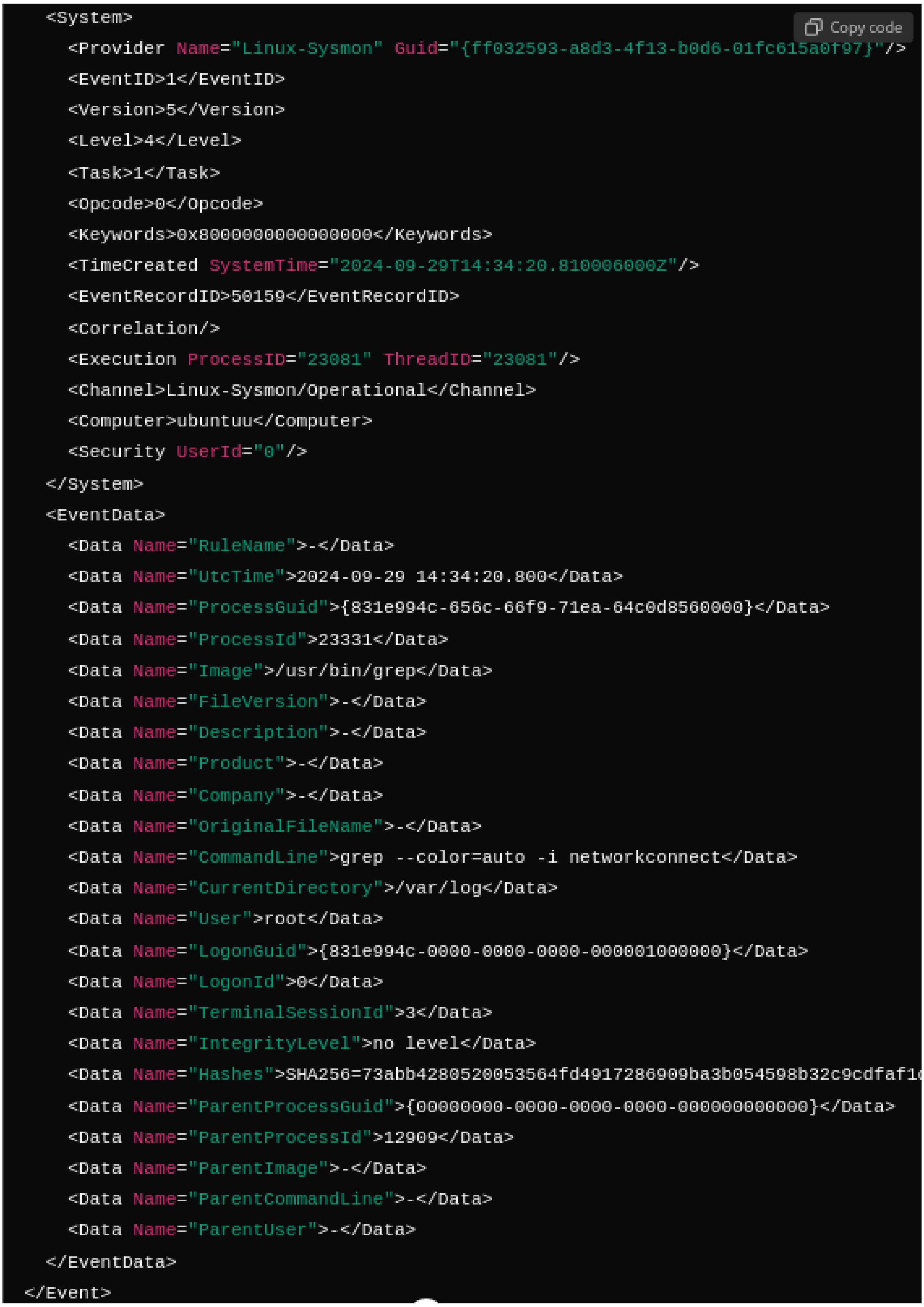


```
root@ubuntuu:/var/log# cat syslog | grep -i "filedelete"
Sep 29 16:36:13 ubuntuu sysmon: <Event><System><Provider Name="Linux-Sysmon" Guid="{ff0
32593-a8d3-4f13-b0d6-01fc615a0f97}"/><EventID>1</EventID><Version>5</Version><Level>4</
Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreat
ed SystemTime="2024-09-29T14:36:13.203932000Z"/><EventRecordID>51057</EventRecordID><Co
rrelation/><Execution ProcessID="23081" ThreadID="23081"/><Channel>Linux-Sysmon/Operati
onal</Channel><Computer>ubuntuu</Computer><Security UserId="0"/></System><EventData><Da
ta Name="RuleName">-</Data><Data Name="UtcTime">2024-09-29 14:36:13.192</Data><Data Nam
e="ProcessGuid">{831e994c-65dd-66f9-71ea-1c085f610000}</Data><Data Name="ProcessId">233
69</Data><Data Name="Image">/usr/bin/grep</Data><Data Name="FileVersion">-</Data><Data 
Name="Description">-</Data><Data Name="Product">-</Data><Data Name="Company">-</Data><D
ata Name="OriginalFileName">-</Data><Data Name="CommandLine">grep --color=auto -i filed
elete</Data><Data Name="CurrentDirectory">/var/log</Data><Data Name="User">root</Data><
Data Name="LogonGuid">{831e994c-0000-0000-0000-000001000000}</Data><Data Name="LogonId"
>0</Data><Data Name="TerminalSessionId">3</Data><Data Name="IntegrityLevel">no level</D
ata><Data Name="Hashes">SHA256=73abb4280520053564fd4917286909ba3b054598b32c9cdfaf1d733e
0202cc96</Data><Data Name="ParentProcessGuid">{00000000-0000-0000-0000-000000000000}</D
ata><Data Name="ParentProcessId">12909</Data><Data Name="ParentImage">-</Data><Data Nam
e="ParentCommandLine">-</Data><Data Name="ParentUser">-</Data></EventData></Event>
```



```
root@ubuntuu:/var/log# cat syslog | grep -i "networkconnect"
Sep 29 16:34:20 ubuntuu sysmon: <Event><System><Provider Name="Linux-Sysmon" Guid="{ff0
32593-a8d3-4f13-b0d6-01fc615a0f97}"/><EventID>1</EventID><Version>5</Version><Level>4</
Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreat
ed SystemTime="2024-09-29T14:34:20.810006000Z"/><EventRecordID>50159</EventRecordID><Co
rrelation/><Execution ProcessID="23081" ThreadID="23081"/><Channel>Linux-Sysmon/Operati
onal</Channel><Computer>ubuntuu</Computer><Security UserId="0"/></System><EventData><Da
ta Name="RuleName">-</Data><Data Name="UtcTime">2024-09-29 14:34:20.800</Data><Data Nam
e="ProcessGuid">{831e994c-656c-66f9-71ea-64c0d8560000}</Data><Data Name="ProcessId">233
31</Data><Data Name="Image">/usr/bin/grep</Data><Data Name="FileVersion">-</Data><Data 
Name="Description">-</Data><Data Name="Product">-</Data><Data Name="Company">-</Data><D
ata Name="OriginalFileName">-</Data><Data Name="CommandLine">grep --color=auto -i netwo
rkconnect</Data><Data Name="CurrentDirectory">/var/log</Data><Data Name="User">root</Da
ta><Data Name="LogonGuid">{831e994c-0000-0000-0000-000001000000}</Data><Data Name="Logo
nId">0</Data><Data Name="TerminalSessionId">3</Data><Data Name="IntegrityLevel">no leve
l</Data><Data Name="Hashes">SHA256=73abb4280520053564fd4917286909ba3b054598b32c9cdfaf1d
733e0202cc96</Data><Data Name="ParentProcessGuid">{00000000-0000-0000-0000-000000000000
}</Data><Data Name="ParentProcessId">12909</Data><Data Name="ParentImage">-</Data><Data
 Name="ParentCommandLine">-</Data><Data Name="ParentUser">-</Data></EventData></Event>
```

- Analyze the generated Sysmon logs. Can you identify the events corresponding to your simulated activities?



```
  <System>
    <Provider Name="Linux-Sysmon" Guid="{ff032593-a8d3-4f13-b0d6-01fc615a0f97}"/>
    <EventID>1</EventID>
    <Version>5</Version>
    <Level>4</Level>
    <Task>1</Task>
    <Opcode>0</Opcode>
    <Keywords>0x8000000000000000</Keywords>
    <TimeCreated SystemTime="2024-09-29T14:34:20.810006000Z"/>
    <EventRecordID>50159</EventRecordID>
    <Correlation/>
    <Execution ProcessID="23081" ThreadID="23081"/>
    <Channel>Linux-Sysmon/Operational</Channel>
    <Computer>ubuntuu</Computer>
    <Security UserId="0"/>
  </System>
  <EventData>
    <Data Name="RuleName">-</Data>
    <Data Name="UtcTime">2024-09-29 14:34:20.800</Data>
    <Data Name="ProcessGuid">{831e994c-656c-66f9-71ea-64c0d8560000}</Data>
    <Data Name="ProcessId">23331</Data>
    <Data Name="Image">/usr/bin/grep</Data>
    <Data Name="FileVersion">-</Data>
    <Data Name="Description">-</Data>
    <Data Name="Product">-</Data>
    <Data Name="Company">-</Data>
    <Data Name="OriginalFileName">-</Data>
    <Data Name="CommandLine">grep --color=auto -i networkconnect</Data>
    <Data Name="CurrentDirectory">/var/log</Data>
    <Data Name="User">root</Data>
    <Data Name="LogonGuid">{831e994c-0000-0000-0000-000001000000}</Data>
    <Data Name="LogonId">0</Data>
    <Data Name="TerminalSessionId">3</Data>
    <Data Name="IntegrityLevel">no level</Data>
    <Data Name="Hashes">SHA256=73abb4280520053564fd4917286909ba3b054598b32c9cdfaf1
    <Data Name="ParentProcessGuid">{00000000-0000-0000-0000-000000000000}</Data>
    <Data Name="ParentProcessId">12909</Data>
    <Data Name="ParentImage">-</Data>
    <Data Name="ParentCommandLine">-</Data>
    <Data Name="ParentUser">-</Data>
  </EventData>
</Event>
```

- Explore specific log entries and understand the captured details.