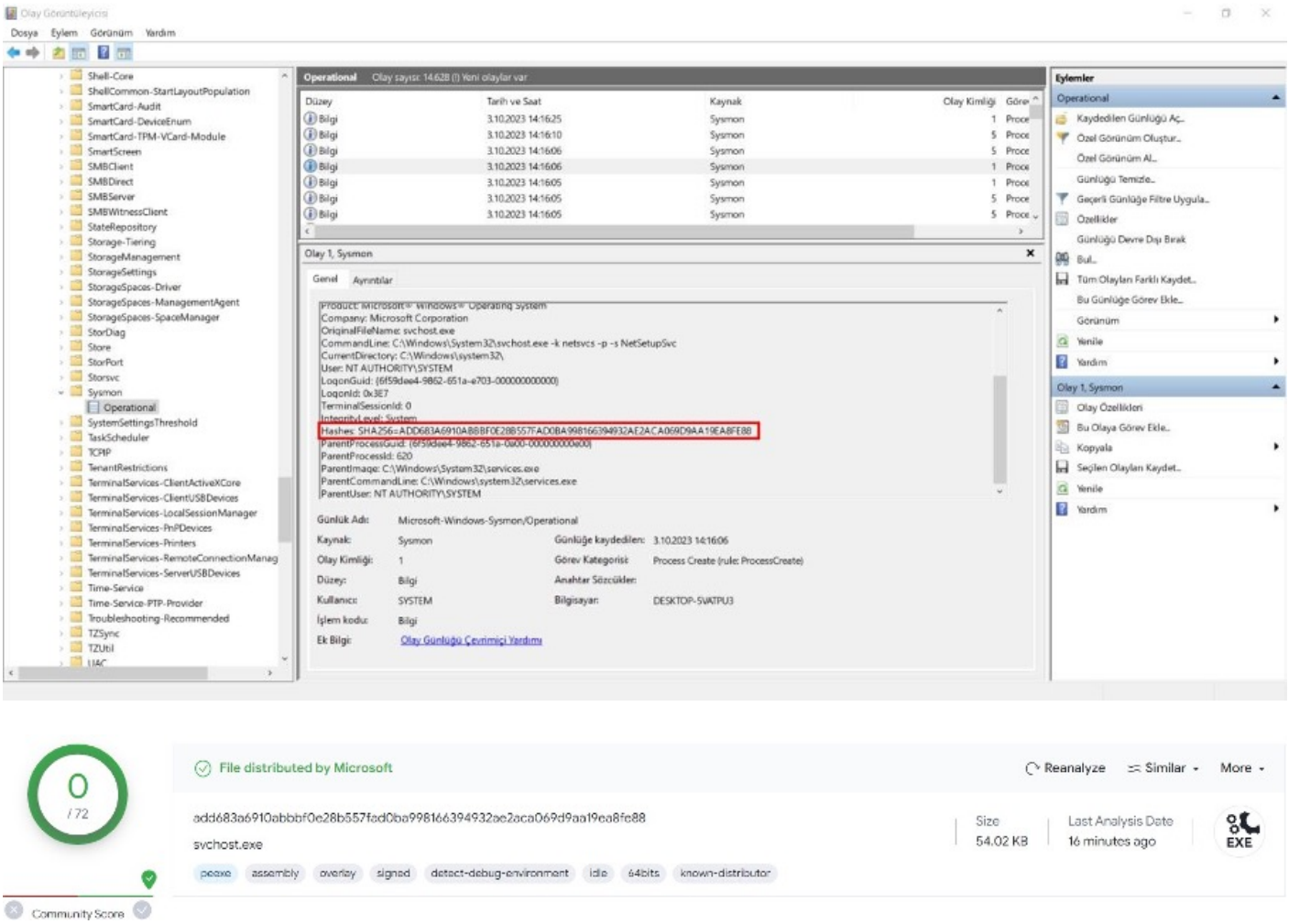
Sysmon’da Olayları HASH Değerlerine Göre İnceleme ve Yorumlama

Olay kayıtları alındığında bir çok işleme ait hash bilgiside alınır. Bir işlemin şüpheli olup olmadığı bu hashler yardımıyla anlaşılabilir. Herhangi bir olaya tıklandığında hash bilgisi virustotal tarzı hizmetler yardımıyla şüpheli olup olmadığı anlaşılabilir.



Virustotal ile incelenen bu olayın normal bir durum olduğu bu şekilde anlaşılabilir.

Revision #2
Created 27 January 2024 16:04:19 by Ertan Sözer
Updated 27 January 2024 16:05:17 by Ertan Sözer