

near Report

Case Overview

Hello world

Case Acquisition

ahjgsd

Case Findings

hagjdfuqh

Case Conclusion

jaghdf

Artifacts

process_list:

comment: asd
name: Idle
physical_offset: 44446144
pid: 0
object_id: 16
active_threads: 0
marked: disabled
ppid: 0

comment: asdg
name: spoolsv.exe
physical_offset: 2108208736
pid: 1128
object_id: 18
active_threads: 0
marked: disabled
ppid: 440

service_list:

registry_list:

kernel_list:

network_list:

