stark Report

## Case Overview

Hello world

## Case Acquisition

ahjgsd

## Case Findings

hagjdfuqh

## Case Conclusion

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

## Artifacts

### process\_list

comment: asd  
 name: Idle  
 physical\_offset: 44446144  
 pid: 0  
 object\_id: 16  
 active\_threads: 0  
 marked: disabled  
 ppid: 0

comment: Test  
 name: svchost.exe  
 physical\_offset: 2107906864  
 pid: 1156  
 object\_id: 17  
 active\_threads: 0  
 marked: disabled  
 ppid: 440

comment: asdg  
 name: spoolsv.exe  
 physical\_offset: 2108208736  
 pid: 1128  
 object\_id: 18  
 active\_threads: 0  
 marked: disabled  
 ppid: 440

### service\_list

comment: Temp  
 display\_name: Remote Procedure Call (RPC)  
 name: RpcSs  
 physical\_offset: 156575264  
 object\_id: 50  
 start: SERVICE\_AUTO\_START  
 state: SERVICE\_RUNNING  
 marked: disabled  
 type: SERVICE\_WIN32\_SHARE\_PROCESS

comment: Temp  
 display\_name: Offline Files  
 name: CscService  
 physical\_offset: 163008640  
 object\_id: 51  
 start: SERVICE\_AUTO\_START  
 state: SERVICE\_RUNNING  
 marked: disabled  
 type: SERVICE\_WIN32\_SHARE\_PROCESS

### registry\_list

### kernel\_list

comment: Temp  
 name: TSDDD.dll  
 physical\_offset: 94333264  
 marked: disabled  
 object\_id: 126  
 file\_path: /SystemRoot/System32/TSDDD.dll

comment: Temp  
 name: lltdio.sys  
 physical\_offset: 2107855200  
 marked: disabled  
 object\_id: 128  
 file\_path: /SystemRoot/system32/DRIVERS/lltdio.sys

### network\_list

comment: Udp  
 physical\_offset: 2109824704  
 object\_id: 611  
 marked: disabled  
 protocol\_version: UDPv4  
 local\_address: 192.168.253.128  
 port: 1900

comment: Tcp  
 physical\_offset: 2111054464  
 object\_id: 613  
 marked: disabled  
 protocol\_version: TCPv6  
 local\_address: 0:0:0:0:0:0  
 port: 5357