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

comment: temp  
 name: SearchIndexer.  
 physical\_offset: 2133860448  
 pid: 1792  
 object\_id: 42  
 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

### registry\_list

comment: temp  
 name: HKEY\_LOCAL\_MACHINE  
 physical\_offset: 142495760  
 marked: disabled  
 object\_id: 3  
 file\_path: /SystemRoot/System32/Config/SAM

### kernel\_list

comment: tcp  
 name: monitor.sys  
 physical\_offset: 94305536  
 marked: disabled  
 object\_id: 124  
 file\_path: /SystemRoot/system32/DRIVERS/monitor.sys

### network\_list

comment: udp  
 physical\_offset: 2107902624  
 object\_id: 608  
 marked: disabled  
 protocol\_version: UDPv6  
 local\_address: 0:0:0:0:0:1  
 port: 61588

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