Memory Analysis

Incident Response Team pulls the memory from the suspect system and reviews it for possible malicious activity.

TOOLS

Volatility, to review the memory
Velociraptor, to dump the memory

https://www.velocidex.com/

https://www.volatilityfoundation.org/

CDV2_0421

Backdoors™ & Breaches

PROCEDURES

Created by: BLACK HILLS | Information Security