Capturing Volatile and Protected Data Using FTK Imager



Phil Chapman
SENIOR INSTRUCTOR

@PhilChap777

Overview



Capture Volatile Data from a Live Machine

- Points to consider
- Order of volatility
- Risk

Capturing RAM

Capturing Registry Files

Capturing Volatile Data from a Live Machine



Order of Volatility

System Caches

RAM

Network-based resources (Cloud)

Non-Volatile

- System settings
- Registry
- External Storage
- Internal Storage



Work to a Plan

Avoid uncertainty and doubt

Record your actions

Be aware of the risk

- Use write-blocker

Check your results

Record/Hash your results

Capturing RAM from a Live Machine

Demo



Conduct a RAM Capture using FTK Imager

Include Pagefile

Check results

Capturing Windows Registry with FTK Imager

Demo



Conduct a Protected Files Capture using FTK Imager

Check results