CyBOK

Memory analysis workshop

Joakim Kävrestad
University of Skövde
joakim.kavrestad@his.se

Agenda

CyBOK

- Intro to theory
  - Incident handling
  - Data in memory
  - Malware structures
  - Memory analysis with Volatility
- Lab-time
  - Set up the environment
  - Quick start
  - Do it yourself
- Reflection

Workshop compendium

- Section 1: Theoretical concepts
  - Doodling pages
  - Reflection pages
  - We use a method called 1-2-4-all for reflections
- Section 2: Hands-on lab (Only digital)
  - Install guide
  - Get started
  - Mini-challange
- Section 3: Summary of central concepts (only digital)
  - Selected topics of Cyber Security Body of Knowledge version 1.1 (CyBok) knowledge areas “Forensics”, “Security Operations & Incident Management”, and “Malware and Attack Technologies”
- Section 4: Reflect and feedback

Thank you for listening!

Get in touch:

Connect on Linkedin:
Joakim Kävrsetad
Follow our research group on LinkedIn:
https://www.linkedin.com/company/pics-skovde/