

Kickstart: Introduction to Incident Response elective course

This material is prepared for use in *Introduction to Incident Response elective course* and was prepared by Henrik Kramselund, xhek@kea.dk. It contains the very basic information to get started!

These course and exercises are expected to be performed in a training setting with network connected systems. The exercises use a number of tools which can be copied and reused after training. A lot is described about setting up your workstation in the Github repositories.

To get kickstarted in this course:

- ☐ Make sure you can login to Fronter <https://kea-fronter.itslearning.com/>
Electronic version of this document will be uploaded here!
- ☐ Lecture plan for this course will be in Fronter
(Source is also in Git <https://github.com/kramse/kea-it-sikkerhed>)
- ☐ Bookmark the main Github page: <https://github.com/kramse/>
Note: there are two pinned repositories `security-courses` and `kramse-labs`
- ☐ Slides and exercises booklet – PDF will be in Fronter
Source is in Github – feel free to clone or download single files
<https://github.com/kramse/security-courses/tree/master/courses/incident-response/intro-to-incident-response>
- ☐ We will use virtual machines in teams of two persons, so check BIOS settings
– make sure CPU settings have virtualisation turned ON
- ☐ Select and install virtualisation software
- ☐ Read about setup of exercise systems here
<https://github.com/kramse/kramse-labs>
- ☐ Get the book *Intelligence-Driven Incident Response* (IDIR)
Scott Roberts. Rebekah Brown, ISBN: 9781491934944
- ☐ Get the book *Forensic Discovery* (FD), Dan Farmer and Wietse Venema! Either on paper or PDF
You can download for free:
<http://fish2.com/security/>

I hope we will have a fun and enjoyable time in this course.

Kickstart: Introduction to Incident Response elective course

Best regards

Henrik Kramselund, he/him