

# Computer Forensics workshop

Varighed:  
2 dage workshop

Målgruppe:  
Alle med interesse eller ansvar for netværksopkoblede servere. Der forventes kendskab til TCP/IP på brugerniveau.

Formål:  
Skabe en grundig forståelse for Computer Forensics værktøjer samt metoder. Deltagerne bør efterfølgende være istand til at gennemføre enkle til videregående undersøgelser af egne systemer.

Indhold:

Deltagerne vil lære metoder og værktøjer til struktureret analyse af hackede systemer, herunder udtrækning af slettede filer fra harddisk images.

Efter deltagelse er deltagerne istand til at bringe et kompromitteret system tilbage til et konsistent system der kan stoles på ved brug af anerkendte metoder (best-practice) ved et minimum af omkostninger i form af tid, penge og andre ressourcer.

På workshoppen vil vi gennemgå teknikkerne bagved computer forensics og metoderne til struktureret analyse af data fra harddiske og netværk. Workshop arbejdsformen betyder at vi udfører angreb mod sårbare systemer i praksis med de tilgængelige værktøjer og platforme - på samme måde som en hacker ville gøre det.

På workshoppen tages udgangspunkt i tilgængelige open source værktøjer som [sleuthkit](#), Autopsy og foremost.

Værktøjerne afvikles primært på UNIX men kendskab til UNIX er ikke en nødvendighed. Eksemplerne der gennemgås er både fra UNIX og Windows.