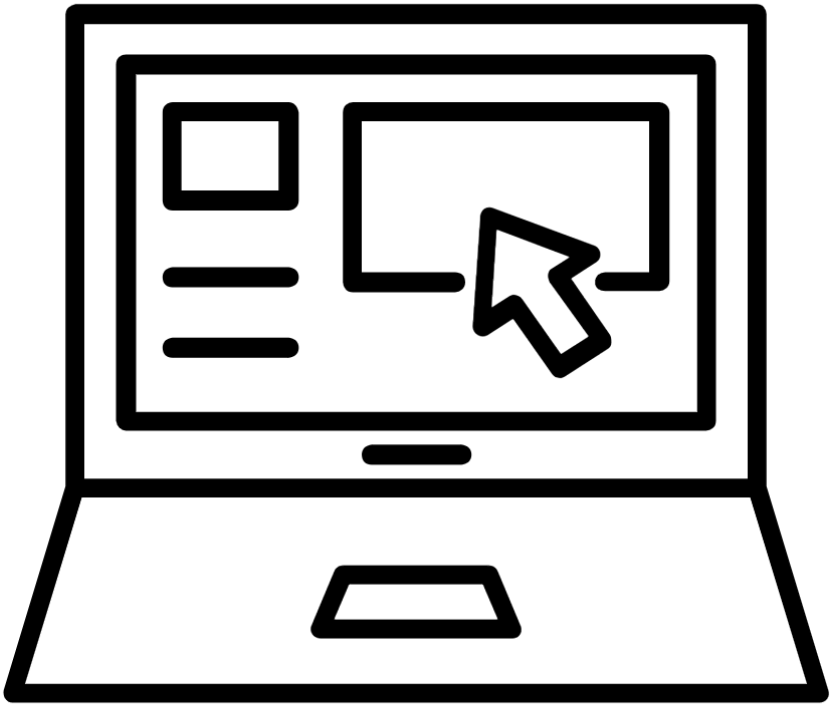
Udstyrskrav



XLEB@kea.dk

1. Krav til Hardware

For at kunne deltage i kurset, så kan det min anbefaling arbejdet med emnet sker på en stand alone maskine. Der arbejdes med malware som kan inficere systemet, selv om man tager sine forholdsregler.

Den computer man anvender skal kunne køre virtualiseringssoftware, hvilket stiller krav til hvad hardware man har med.

Minimumskrav
I5 processor eller tilsvarende
16 gb ram
250 gb eller mere harddisk og en SSD
(Vi kommer til at anvende forensics software, som kræver en hurtig harddisk.)

Kan man finde en computer med ovenstående specifikationer, eller derover, vil tingene køre bedre og mere "smertefrit".

Vi sigter i undervisningen efter at kunne køre 2 virtuelle systemer, foruden det installerede operativsystem. Kan man ikke dette, vil der være en mindre funktionalitet som går tabt. Eksemplet på hvordan det ser ud vises på tavlen. Der kommer også en vejledninge i opsætning på dette, således at kursisten kan arbejde videre på eks. en stationær computer andetsteds.

Du skal have USB stick på minimum 16 gb og gerne et par stykker. Det bedste er hvis man har USB 3.0, da andre mindre versioner kan give udfordringer en gang i mellem.
Dette er til dataindsamling og vi skal bruge en bootable USB stick med Caine Linux eller Paladin Linux (kræver registrering og evt donering)

2. Software som skal downloades

Det software vi kommer til at anvende på kurset vil være open source og gratis tilgængeligt. Så vil nogle af mine eksempler anvende VMware, da der er nogle ting som er lidt bedre at anvende her. Som eks. netværksopsætningen.

Inden kursusdagen så kan du sagtens forberede hentning af noget software.

Forensics Software:
FTK_Imager (gratis og kræver registrering) =
https://accessdata.com/products-services/forensic-toolkit-ftk/ftkimager
Autopsy (gratis) = https://www.autopsy.com/
Caine linux (gratis) = https://www.caine-live.net/
Rufus (gratis) = https://rufus.ie/

XLEB@kea.dk

Dumpit (gratis) = https://github.com/thimbleweed/All-In-USB/tree/master/utilities/DumpIt
magnet axiom ram capture (gratis og kræver registrering) =
https://www.magnetforensics.com/resources/magnet-ram-capture/

Virtualiserings Software
Virtualbox (gratis) = https://www.virtualbox.org/

Images til virtuelle maskiner
Windows 7 og 10 (gratis / 90 dages prøve licens for VMware og Virtualbox) =
https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/
Remnux Linux (gratis) = https://remnux.org/

Log analyse
Splunk (gratis og kræver registrering) = https://www.splunk.com/
Netmon freemium (gratis og kræver registrering) =
https://logrhythm.com/products/logrhythm-netmon-freemium/

Backup Image software (Ikke noget krav, nice to have)
Hvis noget skulle gå galt, er det en god ide, at have løbende backups af dine data. Det vil gøre en reetablering lettere

Der er flere muligheder. Jeg anvende terabyte for windows, som koster lidt, men er det hele værd. Link = https://www.terabyteunlimited.com/image-for-windows.htm

3. Registreringer

Det er en god ide, at have en alternativ e-mail til at registrere software med. Så man ikke anvender sin arbejds e-mail.

Vi kommer til at anvende software som kræver registrering, som eks. Splunk, FTK imager, VMware og Paladin

4. Netværk

På skolen bliver der opstillet et trådløst netværk som kursisterne kan anvende til at gå på, når der anvendes malware.

Det netværk jeg tager med er 2 nedenstående muligheder (**Det er absolut ikke noget krav,** da jeg stiller udstyr op til formålet)

https://www.gl-inet.com/products/gl-ar150/

https://www.gl-inet.com/products/gl-ar750s/

XLEB@kea.dk

(Til oplysning, så kan begge routere kan købes på amazon.co.uk hvis man skulle have lyst til dette.)

Begge routere kan koble på et eksisterende netværk og derfra lave en indkapsling af netværket vi arbejder på. Vi kobler på en VPN uden for skolens netværk. På den måde minimere vi risikoen for at inficere vores eget netværk.

Skulle ovenstående give anledning til spørgsmål, skal i være velkommen til at kontakte nedenstående e-mail

XLEB@kea.dk