

Kursplan

Kriminalteknisk datavetenskap II 7,5 högskolepoäng, Grundnivå 2

Computer Forensics II 7.5 Credits*, First Cycle Level 2

Lärandemål

Efter avslutad kurs ska den studerande kunna

- använda open source verktyg för forensisk användning på olika plattformar
- utvinna information ur datasystems internminne via RAM-dumpar från olika plattformar
- redogöra för och utvinna information ur Windows registret
- skapa egenutvecklad mjukvara för lösningar på forensiska problem
- genomföra filanalys och reverse engineering av mjukvara
- granska och analysera stora datamängder i syfte att utvinna mönster och bevis
- redogöra för, värdera och bedöma IT-lösningar som brottslingar och brottsbekämpare har till förfogande
- självständigt söka, analysera och presentera den senaste informationen och tekniken inom området

Innehåll

Kursen behandlar initialt hur internminnesanalys via RAM-dumpar ifrån olika plattformar kan genomföras med open source verktyg. Därefter undervisas de studerande i hur Windows registret analyseras detaljerat. Vidare tränas de studerande i analys av binära filer och reverse engineering av mjukvara.

Kursen behandlar olika slags forensiska problem som forensiker kan ställas inför. I detta arbete kan såväl speciella standardverktyg som egenutvecklad mjukvara behöva användas eller utvecklas för att kunna forcera kryptering och tolka olika slags filer och filsystem. I kursen behandlas även användandet av verktyg för att identifiera potentiella bevis med hjälp av elektroniska fotspår och mönsterigenkänning. Detta område inbegriper även loggar, nätverkstrafik och databaser.

Ett individuellt projektarbete där de studerande fördjupar sig i ett forensisk område avslutar kursen. Resultatet redovisas i en skriftlig rapport och muntlig presentation. I samband med detta presenteras även resultatet ifrån en kritisk granskning av en forensisk rapport.

Examinationsformer

Skriftliga laborationsrapporter (4 hp). Ett individuellt projektarbete de studerande fördjupar

sig i ett relevant forensiskt ämne tillsammans med en kritisk granskning vars resultat redovisas i en skriftlig rapport och muntligt i ett seminarie. (3,5 hp).

Arbetsformer

Föreläsningar, laborationer, projektarbete.

Studenten ska förvärva kunskaper och färdigheter främst via självstudier av kursens innehåll.

Betyg

Som betygsskala används U–VG.

Skriftliga laborationsrapporter (U-G).

Förkunskapskrav

Undersökning av mobila och inbyggda system eller motsvarande kunskaper

IT-rätt, grundläggande, Grundnivå 1, 7,5 hp

Grundkurs i IT-kriminologi, Grundnivå 1, 7,5 hp

Övrigt

Kursen kan ges som campuskurs och/eller som distanskurs.

Om kursen ges på distans måste studenten ombesörja för tillgång till en tillräckligt kraftfull dator med aktuell Microsoft Windows OS och internetuppkoppling om minst 2 Mbit/s.

Vidare krävs en webbkamera och ett headset med mikrofon.

Ersätter DT2014.

Ämnestillhörighet:

Datateknik

Ämnesgrupp:

Datateknik

Utbildningsområde:

Tekniska området, 100%

Kursen kan ingå i följande huvudområde(n):

1. Datateknik

Fördjupningsbeteckning för respektive huvudområde:

1. G2F



D.nr: Du Ku 2014/249
Sida 3(3)
DT2018

Fastställt:

Fastställt 2014-06-19

Kursplanen gäller fr.o.m. 2014-08-20