KURSPLAN

Digital undersökningsteknik och digitala bevis

Computer Forensics

6 högskolepoäng (6 credits)

Kurskod: DV1592
Huvudområde: Datavetenskap
Utbildningsområde: Teknik
Utbildningsnivå: Grundnivå
Fördjupning: G1F - Grundnivå, har mindre än 60 hp kurs/er på grundnivå som förkunskapskrav

Ämnesgrupp: Datateknik
Undervisningsspråk: Svenska men undervisning på engelska kan förekomma.
Gäller från: 2019-01-21
Fastställd: 2018-10-01

1. Beslut

Denna kurs är inrättad av dekan 2017-12-20. Kursplanen är fastställd av prefekten vid institutionen för datalogi och datorsystemteknik 2018-10-01 och gäller från 2019-01-21.

2. Förkunskapskrav

För tillträde till kursen krävs genomgången kurs i Nätverkssäkerhet 2, 4 hp eller Tillämpad nätverkssäkerhet 7,5 hp.

3. Syfte och innehåll

3.1 Syfte

Mer och mer information hanteras av IT-system, information som kan vara både känslig och hemlig. Obehöriga användare som gör intrång i IT-system lämnar spår efter sig, oavsett om det är personer, virus eller annan skadlig programvara. För säkerhetsadministratörer och polis är det viktigt att hitta och säkra dessa spår som ett led i bevisföringen och för att i framtiden kunna skydda information. I kursen lär sig studenten vilka spår olika program lämnar efter sig och var någonstans i datorn eller i nätverket dessa spår kan hittas. Studenten lär sig också hur man praktiskt skyddar system för att försvåra eller omöjliggöra att obehöriga kan plocka ut information från en dator.

3.2 Innehåll

Kursen omfattar följande moment:
• Historik och terminologi som ger förståelse för ”Computer Forensics”.
• Genomgång av olika typer av datorsystem/enheter/operativsystem och lagring av användarens filer, information och beteende.
• Teknik och metodik för att säkerställa spår (bevissäkring), både på körande system (”live system”) och avstängda system genom tillverkning av giltiga digitala kopior av system samt nätverkstrafik.
• Analysmetoder för att sammanställa och dokumentera, t.ex. dataintrång.

4. Lärandemål

Följande lärandemål examineras i kursen:

4.1 Kunskap och förståelse

Efter genomförd kurs ska studenten:
• redogöra för problematiken kring återskapande av data i olika operativsystem.
• redogöra i detalj för hur spårning på nätverk fungerar.
• förklara vilka skyddsåtgärder som behöver genomföras på en dator/enhet för att bevara digitala spår.

4.2 Färdighet och förmåga

Efter genomförd kurs ska studenten:
• bevissäkra en enhet genom att tillverka säkra digitala kopior.
• analysera insamlad data och nätverkstrafik samt sammanställa lämpliga och opartiska rapporter för olika typer av uppdragsgivare.

4.3 Värderingsförmåga och förhållningssätt

Efter genomförd kurs ska studenten:

• identifiera och verkställa lämpliga metoder och tekniker för inhämta, utforska, skapa och värdera underlag och digitala bevis.

5. Läraktiviteter

Föreläsningar och laborationer introducerar viktiga begrepp, och förståelse. Laborationer med inkluderade frågor/övningar underlättar för kursdeltagarna att inhämta kunskap. I laborationerna och inlämningsuppgift övas analytiskt tänkande då kursdeltagaren utifrån resultaten ska dra slutsatser för vad de betyder.

6. Bedömning och examination

Examinationsmoment för kursen

Kod	Benämning	Omfattning	Betyg
1905	Laboration	2 hp	GU
1915	Inlämningsuppgift	1 hp	AF
1925	Salstentamen	3 hp	AF

Kursen bedöms med betygen A Utmärkt, B Mycket bra, C Bra, D Tillfredsställande, E Tillräckligt, FX Underkänd, något mer arbete krävs, F Underkänd.

Slutbetyget är ett viktat och avrundat genomsnitt av betygen på de graderade momenten. Om sammanvägt betyg ligger exakt mellan två betygssteg sker avrundning nedåt.

I kurstillfällets kurs-PM framgår i vilka examinationsmoment som kursens lärandemål examineras samt gällande bedömningsgrunder.

7. Kursvärdering

Kursvärdering ska göras i enlighet med BTH:s beslut om frågeställning i kursvärderingar och beslut om process för hantering och uppföljning av kursvärderingar.

8. Begränsningar i examen

Kursen kan ingå i examen men inte tillsammans med annan kurs vars innehåll, helt eller delvis, överensstämmer med innehållet i denna kurs.

9. Kurslitteratur och övriga lärresurser

Digital Archaeology: The Art and Science of Digital Forensics, Michael W. Graves, Addison-Wesley Professional, ISBN: 9780132853774

Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet Författare: Eoghan Casey Förlag: Academic Press Upplaga 3 ISBN13: 9780123742681

Material från institutionen

Online-material

Referenslitteratur
Brott och digitala bevis : en handledning Författare: Stefan Kronqvist Förlag: Norstedts juridik AB Upplaga 3 ISBN13: 9789139016021

10. Övrigt

Denna kurs ersätter kursen DV1513