HÖGSKOLAN
I SKÖVDE

**KURSPLAN**

# IT-forensik inom incidenthantering A1F

## 7,5 högskolepoäng

**Kurskod:** IT771A
**Revisionsnummer:** 6
**Gäller från:** 2025-01-01
**Beslutad av:** Utbildningskommittén för informationsteknologi
**Beslutsdatum:** 2024-08-16

## 1. Allmänt om kursen

Kursen ges av Högskolan i Skövde och benämns IT-forensik inom incidenthantering A1F (Digital Forensics for Incident Response A1F). Omfattningen är 7,5 högskolepoäng (hp). Kursen är på avancerad nivå och har fördjupningsnivå A1F.

Kursen ingår i huvudområdet informationsteknologi. Kursens utbildningsområde är teknik.

## 2. Behörighetskrav

Kursen har följande behörighetskrav: godkänd IT760A Säker nätverksdrift A1N (eller motsvarande kunskaper).

## 3. Innehåll

Kursen ger studenten fördjupade kunskaper i processer och tekniker för hur en identifierad incident ska hanteras. Studenten får kunskaper om metoder och teori för incidenthantering och fördjupade teoretiska och praktiska kunskaper inom analys av skadlig kod. Studenten kommer även att fördjupa sig inom och diskutera aktuella forskningsinriktningar inom området.

## 4. Mål

Efter avslutad kurs ska studenten kunna:

- redogöra för hur forensiska metoder används inom incidenthantering,
- redogöra för och förklara skadlig kod på en fördjupad teknisk nivå,
- tillämpa forensiska verktyg i syfte att detektera och analysera skadlig kod,
- analysera och problematisera innehållet i forskningsartiklar inom området, samt
- på ett självständigt sätt kritiskt granska och muntligt presentera material från forskning inom intrångsdetektering.

## 5. Examination

Kursen bedöms med betygen A (Utmärkt), B (Mycket bra), C (Bra), D (Tillfredställande), E (Tillräcklig) eller F (Underkänd).

Kursen har följande examinationsmoment:

- **Seminarieuppgifter**
  5 hp, betyg: A/B/C/D/E/F (bestämmer betyg på hel kurs)
- **Laboration**
  2,5 hp, betyg: G/U

Studenter med varaktig funktionsnedsättning som har fått beslut om riktat pedagogiskt stöd kan erbjudas anpassad examination.

## 6. Undervisningsformer och undervisningsspråk

Undervisningen består av seminarier/gruppdiskussioner, föreläsningar och handledning.

Undervisningen bedrivs på engelska.

## 7. Kurslitteratur och övriga läromedel

Kävrestad, J., Birath, M., Clarke, N. (2024). *Fundamentals of digital forensics: A guide to theory, research and applications* (3rd ed.). Springer. ISBN 9783031536489. DOI: 10.1007/978-3-031-53649-6

## 8. Studentinflytande

Studentinflytande i kursen säkerställs genom kursvärdering. Studenterna informeras om resultatet av kursvärderingen och eventuella åtgärder som genomförts eller planeras, grundat på kursvärderingen.

## 9. Övrigt

På Högskolan i Skövdes webbplats finns ytterligare information om kursen samt nationella och lokala styrdokument för högskoleutbildning.