



# EP2780 Digital forensik och incidenthantering 7,5 hp

Digital forensics and incident response

## Fastställande

Kursplanen gäller från och med HT 2025 enligt grundutbildningsansvarigs beslut: HS-2025-0428. Beslutsdatum: 2025-03-14

## Betygsskala

A, B, C, D, E, FX, F

## Utbildningsnivå

Avancerad nivå

## Huvudområden

Datalogi och datateknik

## Särskild behörighet

Kunskaper i cybersäkerhet, 6 hp, motsvarande slutförd kurs DD2391/DD2395/IK2206/IV1013.

## Undervisningsspråk

Undervisningsspråk anges i kurstillfällesinformationen i kurs- och programkatalogen.

# Lärandemål

Efter godkänd kurs ska studenten kunna

- beskriva centrala begrepp, modeller och metoder inom digital forensik och incidenthantering
- beskriva skillnader och likheter mellan en forensisk situation och en incidenthanterings-situation
- tillämpa kända metoder för datainsamling och analys i givna situationer
- planera och genomföra datainsamling och dataanalys inför en forensisk analys eller incidentanalys
- presentera och förklara slutsatser från en forensisk analys och en incidentanalys samt föreslå framtida åtgärder
- förklara hur pass säkra slutsatser som kan dras i en forensisk analys
- förklara hur man skiljer mellan digital forensik och incidenthantering
- kritiskt granska och källkritiskt bedöma en forensisk rapport och en incidenthanteringsrapport.

# Kursinnehåll

Kursen ger studenten både praktiska och teoretiska kunskaper om tekniker, metoder, modeller, lagar/regler som gäller vid utredning av digitala brott eller incidenter.

Kursen behandlar bland annat följande:

- Forensikens historia
- Digital forensik och digitala bevis
- Den forensiska/incidenthanterande utredande processen
- Lagstiftning och internationella samarbeten inom digital forensik
- Standarder inom området och kraven på en organisation som arbetar med digital forensik eller incidenthantering
- Datorforensik
- Forensik för inbyggda system och mobila enheter
- Nätverksforensik

# Examination

- LAB1 - Laborationer, 2,0 hp, betygsskala: P, F
- QUI1 - Skriftliga quiz, 5,5 hp, betygsskala: A, B, C, D, E, FX, F

Examinator beslutar, baserat på rekommendation från KTH:s handläggare av stöd till studenter med funktionsnedsättning, om eventuell anpassad examination för studenter med dokumenterad, varaktig funktionsnedsättning.

Examinator får medge annan examinationsform vid omexamination av enstaka studenter.

När kurs inte längre ges har student möjlighet att examineras under ytterligare två läsår.

## Etiskt förhållningssätt

- Vid grupparbete har alla i gruppen ansvar för gruppens arbete.
- Vid examination ska varje student ärligt redovisa hjälp som erhållits och källor som använts.
- Vid muntlig examination ska varje student kunna redogöra för hela uppgiften och hela lösningen.