

# Avancerade Forensiska Verktyg I/III



Mattias Weckstén  
IT-forensik och informationssäkerhet | 20/180 hp



# Kursplan

- Kunskap och förståelse
  - Identiera och utvinna data av olika karaktär
  - Redogöra för hur man kopplar samman datastrukturer på olika nivåer
- Färdighet och förmåga
  - Tillämpa kända metoder för dataanalys på okända fall
  - Planera och genomföra en IT forensisk undersökning
- Sammanställa och presentera analysresultat på ett för ståeligt sätt för en person utan tekniska fackkunskaper
- Kritisera och identiera svagheter i bentriga rapporter och metodbeskrivningar
- Värderingsförmåga och föhållingsätt
  - Visa insikt om de etiska och juridiska aspekterna av utredningsarbete

# Översikt

- Hårdvara
- Filsystem
- First response
- Inhämtning
- Koncept
- Miljön
- Söka och bokmärka
- Filsignatur och hashanalys
- Windowsartifakter
- Avancerad EnCase

# Schema

vecka 3 Ch1 Computer Hardware, Ch3 First Response  
vecka 4 Ch4 Acquiring Digital Evidence, Ch5 EnCase concepts  
vecka 5 Ch6 EnCase environment, Ch2 File Systems  
vecka 6 Ch7 Understanding, searching for and bookmarking  
data  
vecka 7 Ch8 File signature analysis and hash analysis  
vecka 8 Ch9 Windows Operating System Artifacts  
vecka 9 Ch10 Advanced EnCase  
vecka 10 ...

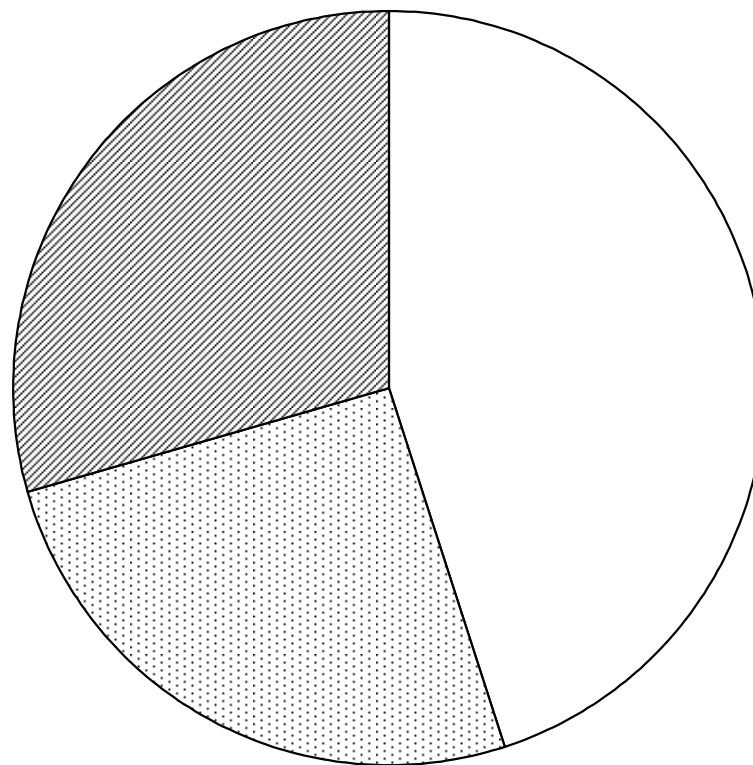
# Skrivna uppgifter

# Laborationer

# Litteratur

# Kursbudget

Timbudget



Föreläsning  Labbar  Administration

# Studieplan

## Studieplan för DT2002

	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	
	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5
11																									
12																	F	F	F	F					
13																			F	F					
14																									
15																	F	F	F	F					
16															L	L	F	F	F	F					
17															L	L	F	F	F	F					
18																	F	F	F	F					
19															L	L	F	F	F	F					
20																	L	L	F	F					
21																									

F = Föreläsning      L = Labb      U = Uppgift A-D      B = Inläsning      T = Tentaprep.

Varje ruta är en timma. Hela kursen är 200 timmar.

# IT-forensik och informationssäkerhet, 120/180 hp

	Termin 1		Termin 2	
År 1	Introduktion till IT-forensik	Kriminologi och IT-relaterad brottslighet	Programmering	Datautvinning från digitala lagringsmedia
	Administration av datorsystem	Administration av operativsystem	Juridik med IT-rätt	Grundläggande websystem
År 2	Termin 3		Termin 4	
	Biometrisk identifiering	Trådlösa nätverk	Avancerade IT-forensiska verktyg I	Utredning av IT-brott eller Examensarbete
	Datornätverk I	Datornätverk II	Nätverkssäkerhet	Riskanalys och IT-säkerhetssystem
År 3	Termin 5		Termin 6	
	Avancerade IT-forensiska verktyg II	Underrättelseverksamhet och spårning på internet	Examensarbete	
	Tillämpad matematik och statistik		Krypteringsmetoder och säkring av datasystem	Valbar kurs