Introduktion

Välkommen till kursen DT1035

Kriminalteknisk (forensisk) Datavetenskap 1

Lärare:

Hans Jones hjo@du.se

Hans Edy Mårtensson hem@du.se

Kriminalteknisk Datavetenskap 1 - kursinnehåll

- Incidents and IR (Incident Response)
- Perform an investigation
- Live response or IR
- Hårddiskar och partitioner, SSD
- Disk images, tools and analysis
- Crypto (and hashes)
- File systems and hiding information
- FTK, PRTK and RV
- Binary files, network captures, text logs and analysis

Kriminalteknisk Datavetenskap 1 - kursinnehåll

- E-mail and internet investigations
- Windows forensics - registry
- Linux forensics
- Advanced forensics, anti-forensics
- Case studies and investigation (the book)

- Praktiskt
  - Inlämningar i kursens moment - fronter i en packad fil
  - VPN - DU Wiki = http://wiki.du.se
  - Verktyg, labbmaterial etc. servershare = \\lagring\student\digitalbrott

Kursens upplägg

- Kursens verksamhet
  - Streamade föreläsningar från tidigare år
  - Ett Adobe Connect (samtal.du.se) möte per vecka där nyheter och kursuppdateringar samt veckans laboration introduceras
  - Ett par kortare Adobe Connect möten per vecka (laboration) där frågor besvaras
- Kursens mål mm.
  - Se kursplanen i Fronter
- Examination
  - Se betygskriterier dokument i Fronter > Kursmaterial > Examination

Kursens moment

- Översikt
  - 5 laborationer, en hemuppgift samt ett grupparbete projekt som avslutas i domstol (”mock trail”) (värderat till 5 hp)
  - Praktisk och teoretisk tentamen (värderat till 2,5 hp)
- Hemuppgift under kursen hela längd
  - Lösa forensiskt case med open source och gratisverktyg
    - Beskriva lösningsmetoder och verktyg i en liten rapport
  - Cracka lösenord med fri programvara och prova på krypterad lagring
    - File carving och analys
    - Knäcka TrueCrypt lagringsvolym

Lab 0x1 (Perl) and 0x2 (IR)

- Labb 0x1
  - Hantera Perl i Windows
  - Förstå Perl och skapa eget Perl program
- Labb 0x2
  - Secure a software
  - Live response or Incident Response (IR)
  - Live acquisition

Lab 0x3. Hiding data, time analysis and file systems

- ADS (Alternate Data Streams)
- Steganografi
- Olika former av slack space …
- File mangling och filsignaturer (magic numbers)
- Kombinera filer
- Filers access time
- Hantera Recycle Bin korrekt
- Filsystem
- Anti-forensics verktyg

Lab 0x4. FTK lab on a prepared image

- Förberedd forensisk image från Accessdata
- Walk thru och frågor från AccessData
- Hela sviten av verktyg används
- Accessdata Forensic ToolKit
  - Hittar nålen i höstacken

- Accessdata Password Recovery Toolkit
  - Knäcker lösenordsskyddade filer
- Accessdata Registry Viewer
  - Fiska ut registry nycklar och värden ur registerfiler

Lab 0x5. Registry, text logs and network forensics

- Registry Viewer
- RegRipper
- Log Parser
- Finding data in text based log files
- Finding data in binary files
- WireShark
- NetworkMiner
- Network packet analysis

Projektarbete i samarbete med juridiken?

- Ej spikat ännu… (stående rad...)
- Bilda grupper på ca: 3-4 personer
- Samarbete med IT-juridik kursen
- Images för undersökning – jaktbrott eller försvinnande
- Avslutas med att gruppen ger en presentation av utfört arbete
- Gruppen opponerar på en annan grupp under ”mock trail”?

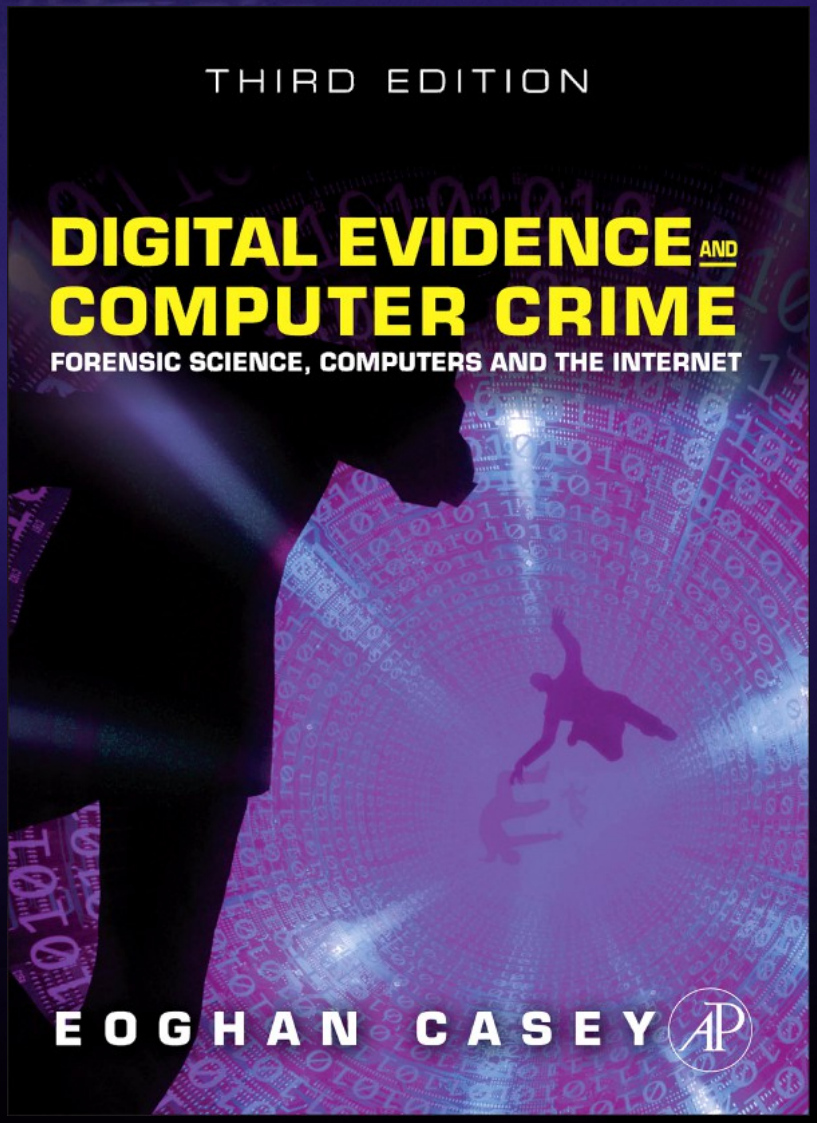
Praktisk och teoretisk tentamen

- Ca: 4h total tid
- Forensiska uppgifter delges och du ska praktiskt utföra det som krävs under tidspress
  - Bevis image och frågor delas ut
  - Dina skills som professionell forensics utredare kommer att mätas!
  - Betyg beror på vad man klarat av utföra med godkänt resultat
- Teoretiska kryssfrågor i Fronter
  - Ett antal frågor att besvara (ca 55 st.)
  - Tiden börjar gå från att du öppnar frågorna
  - 1 h maximal öppetid

Preliminärt schema

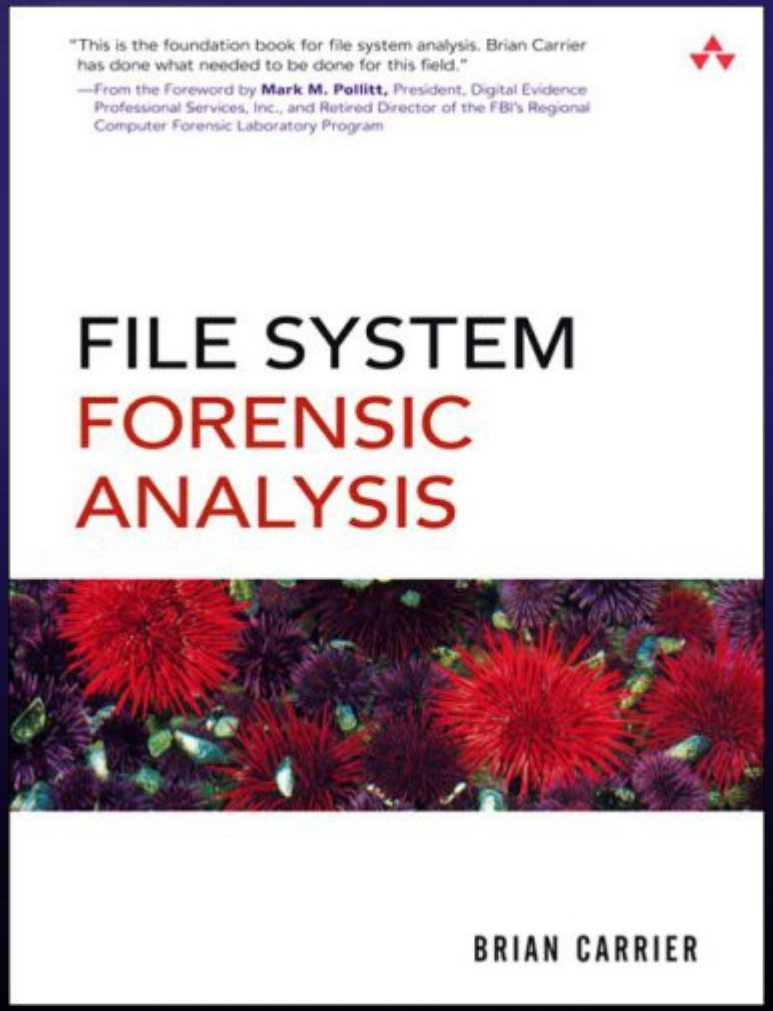
- Ca: 16 föreläsningar
  - Plus en gästföreläsning
- Planeringsförslag för att vara i ”fas”
  - Se studiehandledning i fronter
  - Studiehandledningen är ”work in progress” eftersom ändringar kan ske i kursen
  - Projektet som utförs tillsammans med juridiken påbörjas i kursvecka 7 (v20)
  - Projektet redovisas i kursvecka 9 (v22) eller 10 (v23)
  - Praktiska tentan genomförs sista kursveckan 10 (v23)

Literature 1



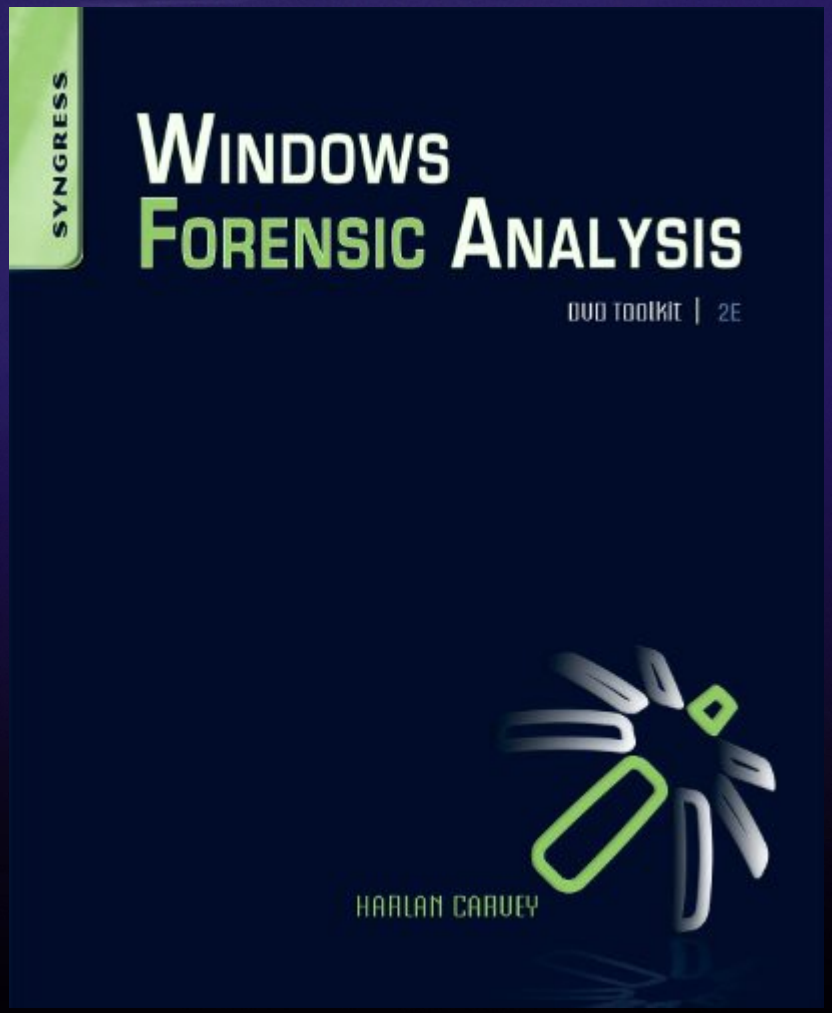
- ISBN-13: 978-0123742681
- Kursen berör mest part 2, part 4 och part 5
- http://www.disclosedigital.com

Literature 2



- ISBN-10: 0321268172
- Kursen berör mest part 1, part 2 och part 3
- http://www.digital-evidence.org

Literature 3



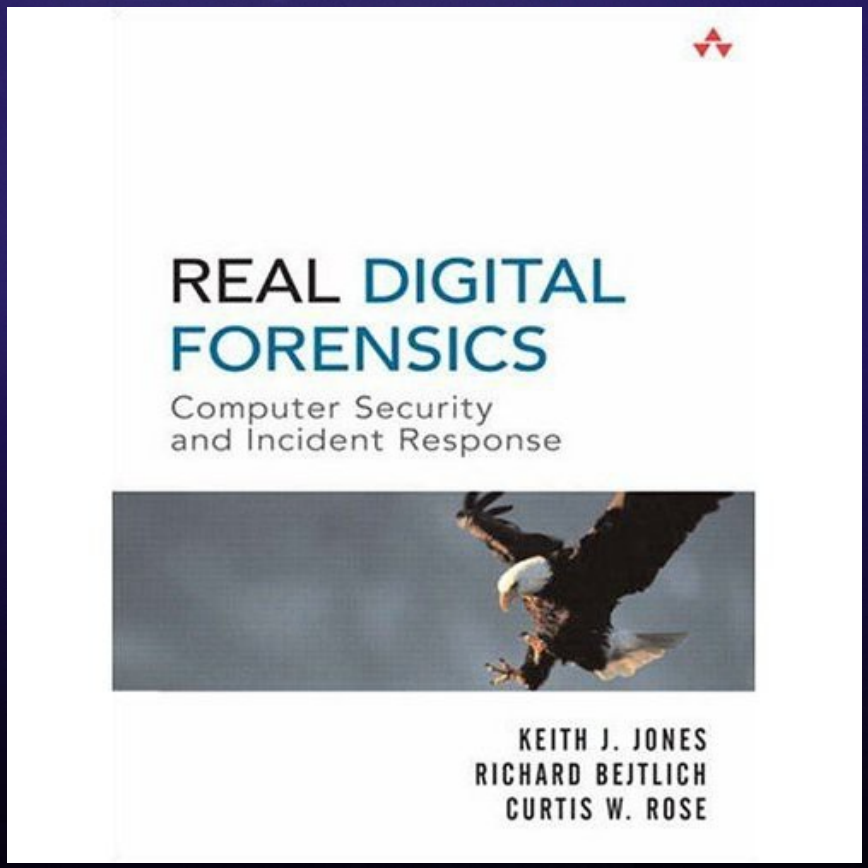
- WFA = Windows Forensic Analysis
- 2 and 3 edition (2012 – deals with Windows 7)

ISBN-13: 978-1597494229

ISBN-13: 978-1597497275

- http://windowsir.blogspot.com/

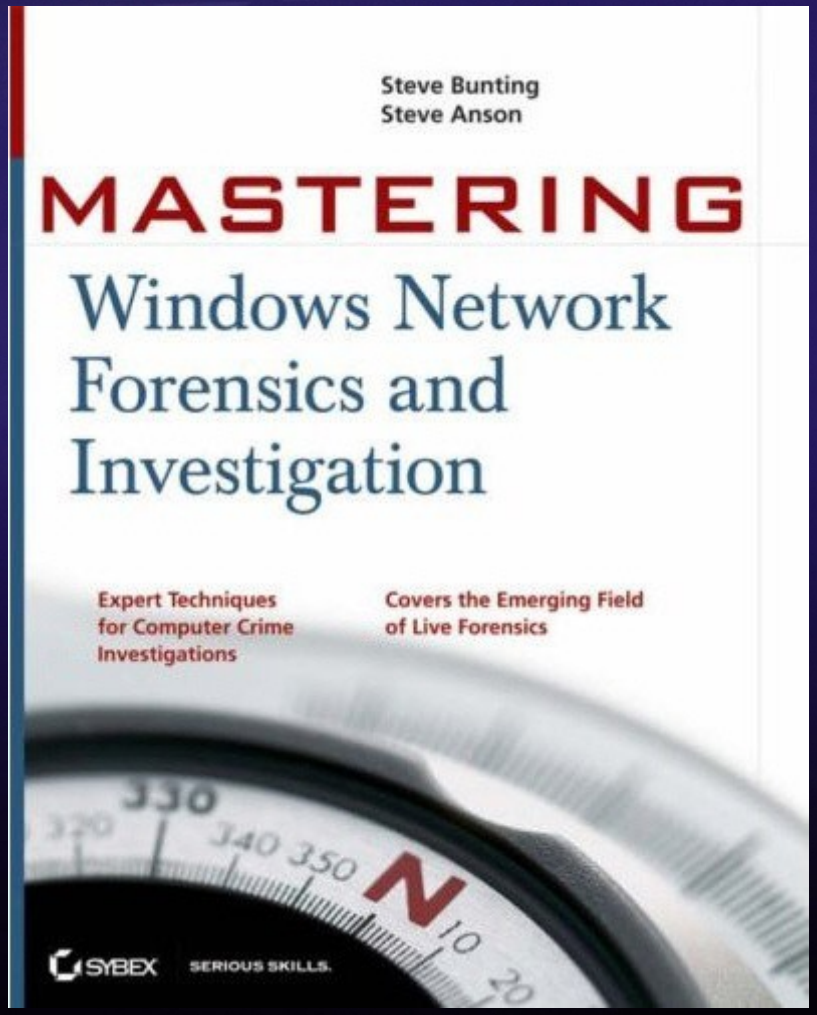
Literature 4



- RDF = Real Digital Forensics
- ISBN-10: 0321240693

http://www.informit.com/store/product.aspx?isbn=0321240693

Literature 5



ISBN-13: 978-0470097625

http://www.sybex.com/WileyCDA/SybexTitle/Mastering-Windows-Network-Forensics-and-Investigation.productCd-0470097620,navId-290591.html

E-material mm.

- http://www.e-evidence.info
- http://users.du.se/~hjo/cs/
- Se mer länkar i fronter, bloggar etc.
- Verktyg, dokumentation och träningsmaterial etc. finns i server-sharet
  - \\lagring\student\digitalbrott
- Forensic Wiki
  - http://www.forensicswiki.org
- DU Wiki - http://wiki.du.se/
- …
- Frågor?