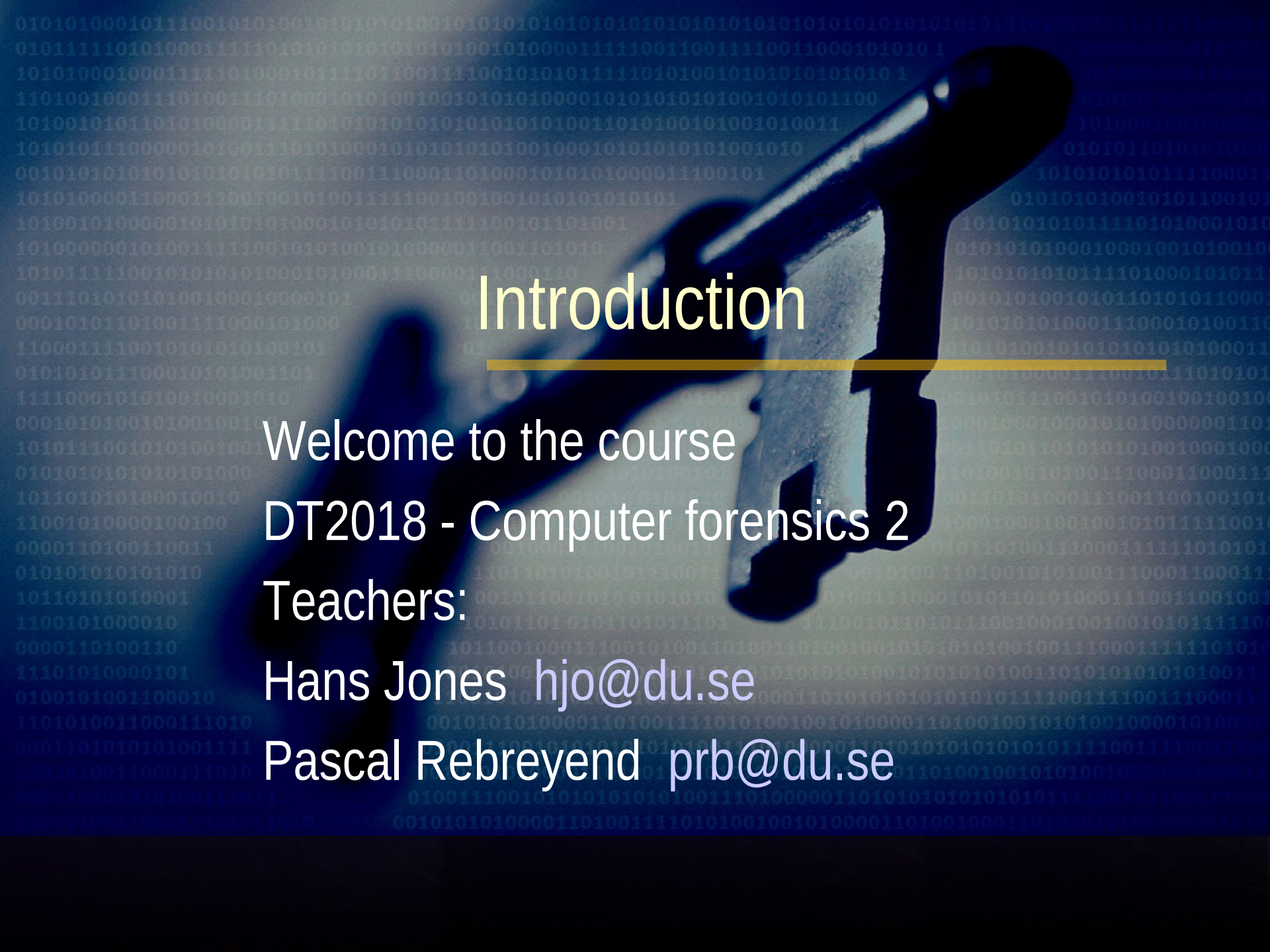


Introduction

Welcome to the course

DT2018 - Computer forensics 2

Teachers:

Hans Jones hjo@du.se

Pascal Rebreyend prb@du.se

Planning, goals and examination

- Planning = studiehandledning
- Goals and exam = betygskriteria document in fronter
- Points and other info = course plan link in fronter
- Examination seminar of project work (connect or physically)
  - A verbal presentation of the project work
  - Critical opposition other students report (report handed in ”in time”)
  - Verbal presentation is marked by students and teachers
  - Finished or ”almost finished” labs are required in order to be allowed to be examined
- Project work (or a home work combination 1a, 1b, 2a, 2b)
  - Week 8 - 10 in course (work however start week 2 or 3 in course)
  - Researching a subject with presentation and a written report

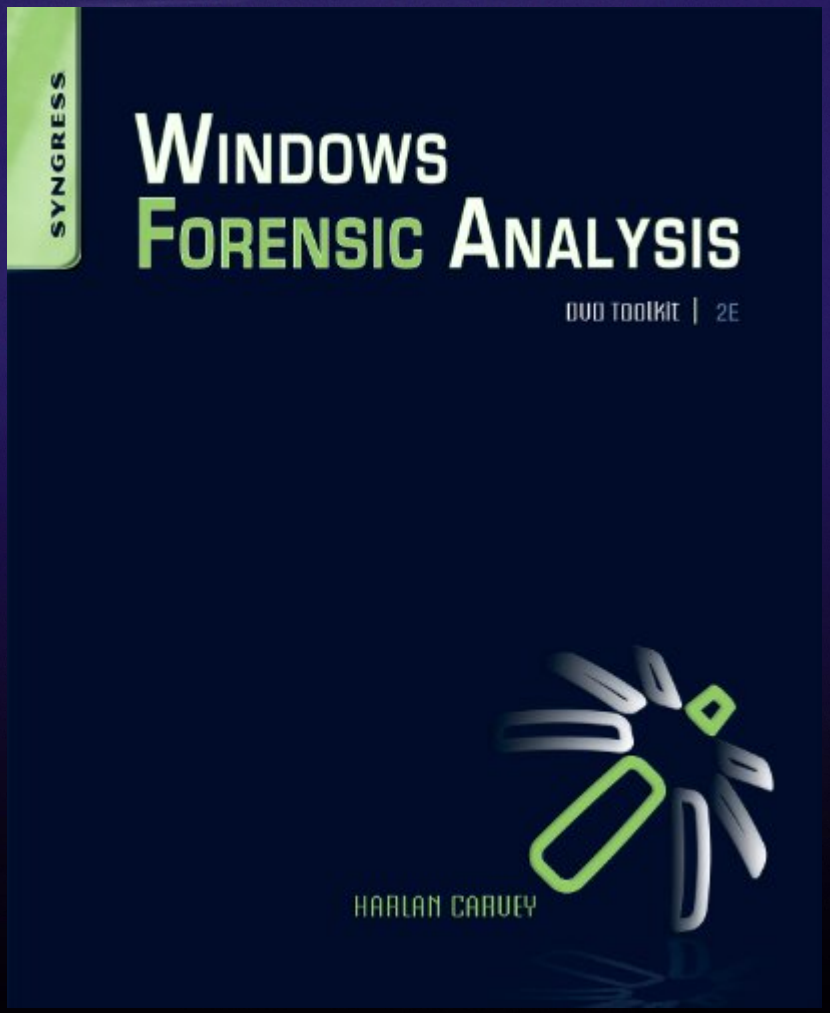
Report writing

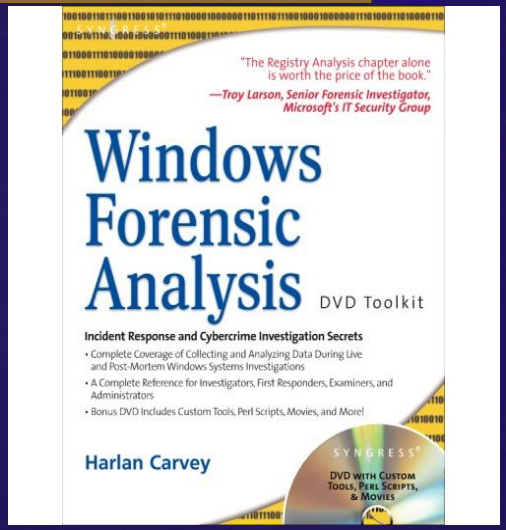
- The report should be organized as follows:
  - **Introduction** - introduce the topic and relate it to previous work (see next slide). The final paragraph of this section should contain objectives of the paper or identified research questions.
  - **Methods** – present the methodology and approach that you have undertaken to complete the task(s).
  - **Results** – present the results with text. You can also refer to figures and tables.
  - **Discussion and conclusions** – speculate on your findings by connecting them to the research field that is Digital Forensics. Refer to appropriate scientific works.

Opposition and finding scientific papers

- The opposition report should be organized as follows:
  - Summary of the work
  - Discussion and conclusions – your reflection on the author's (your peer's) work
- As it was stated above, you need to review scientific literature. For this reason, you can use the library (biblioteket) as a proxy to access journals which Högksolan Dalarna pays yearly subscription for students and staff
- For DT2016 (Embedded Forensics) we explained ways for doing this. Please watch: https://connect1.du.se/p13pkzwq7eg/ starting from the minute 24 for more details

Literature 1

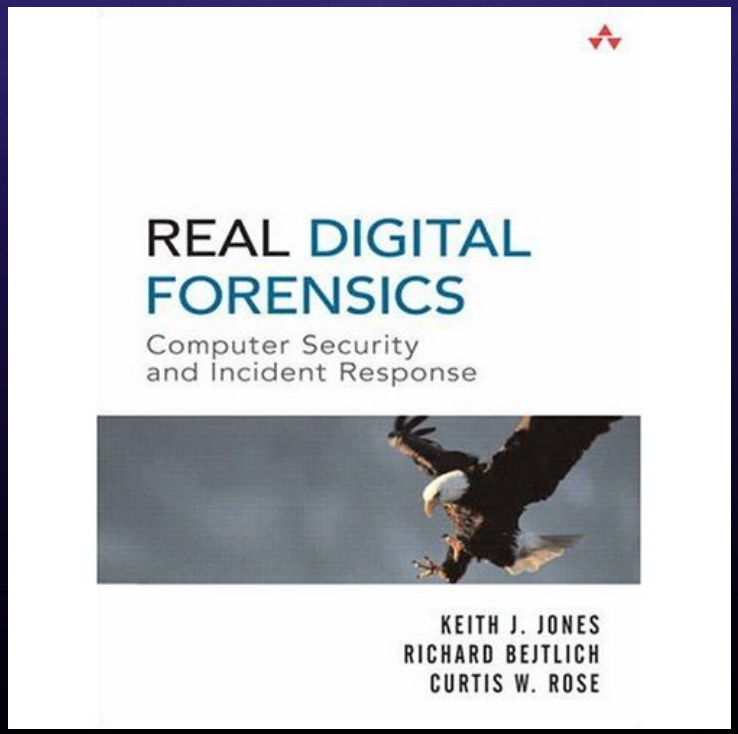


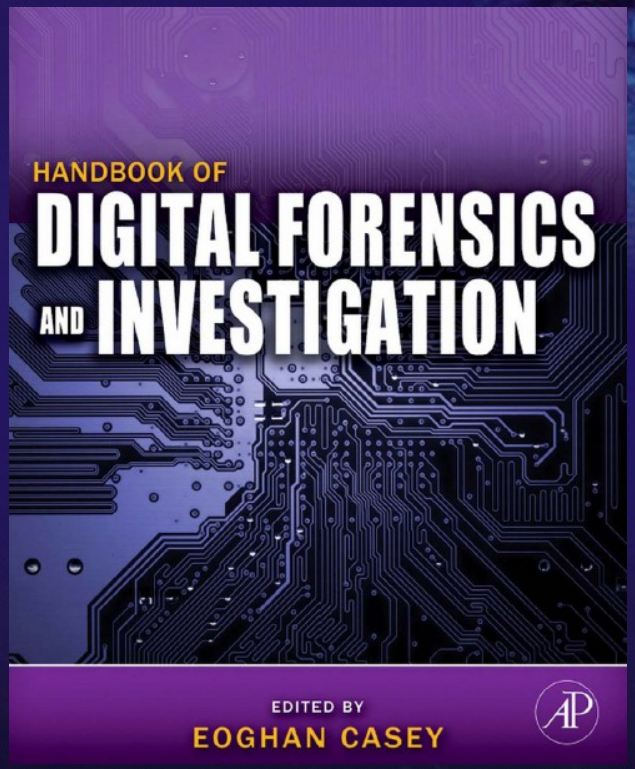


- WFA = Windows Forensic Analysis 2 editon
- ISBN-10: 1597494224
- http://windowsir.blogspot.com/

Literature 2

- RDF = Real Digital Forensics
- ISBN-10: 0321240693
- http://www.informit.com/store/product.aspx?isbn=0321240693



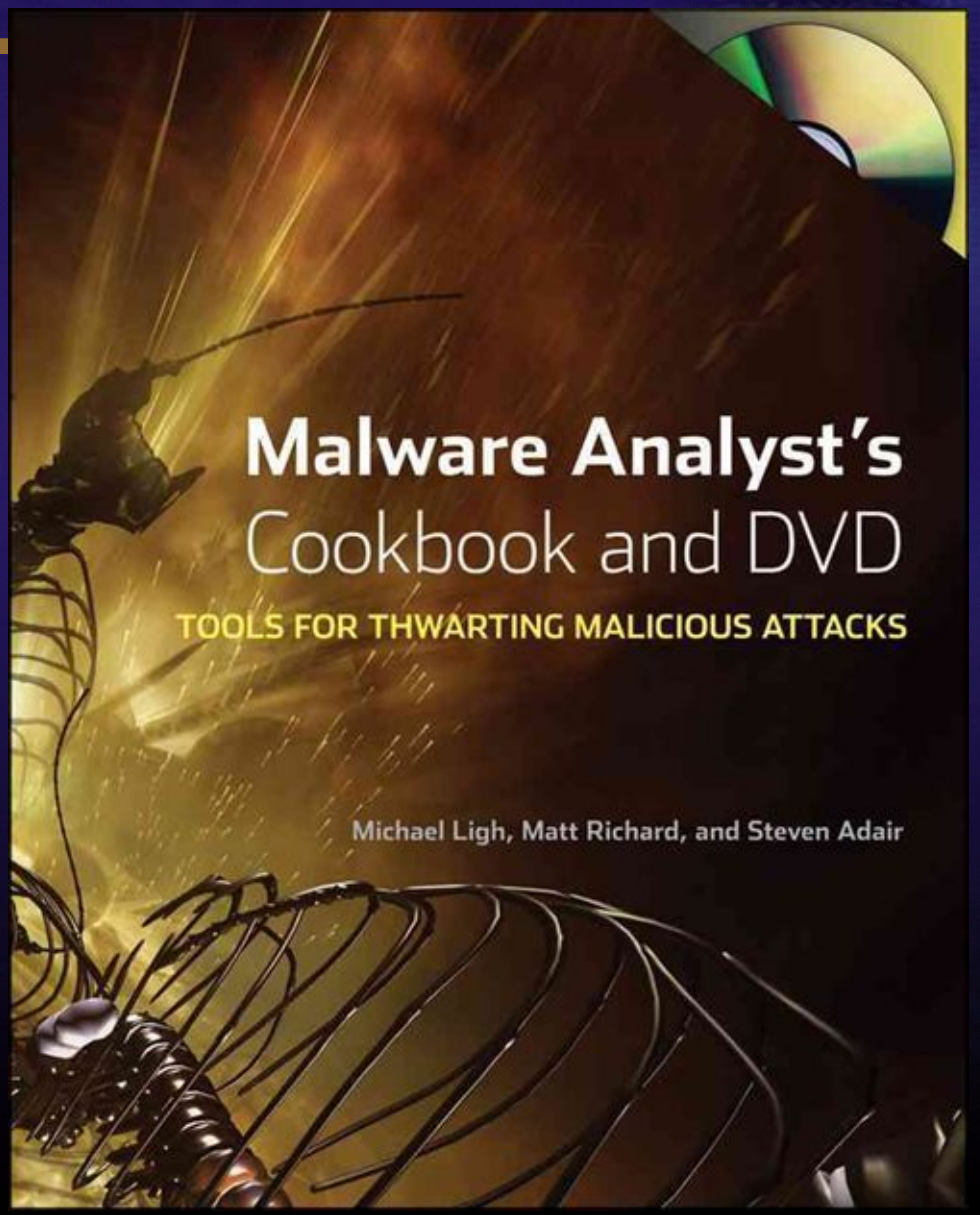


- Handbook of Digital Forensics and investigation
- ISBN-10: 0123742674

http://www.elsevierdirect.com/product.jsp?isbn=9780123742674

Literature 3

- Boken har ett stort antal verktyg på en DVD (vilken kan laddas ner) som är mycket intressanta!
- Jag har lagt DVDn på [server]\malware\malwarecookbook.com
- Password “infected”
- På internet
- http://www.malwarecookbook.com/
- Full pott på Amazon, läs recensionerna för att veta mer
- Helt enkelt bästa boken i ämnet!

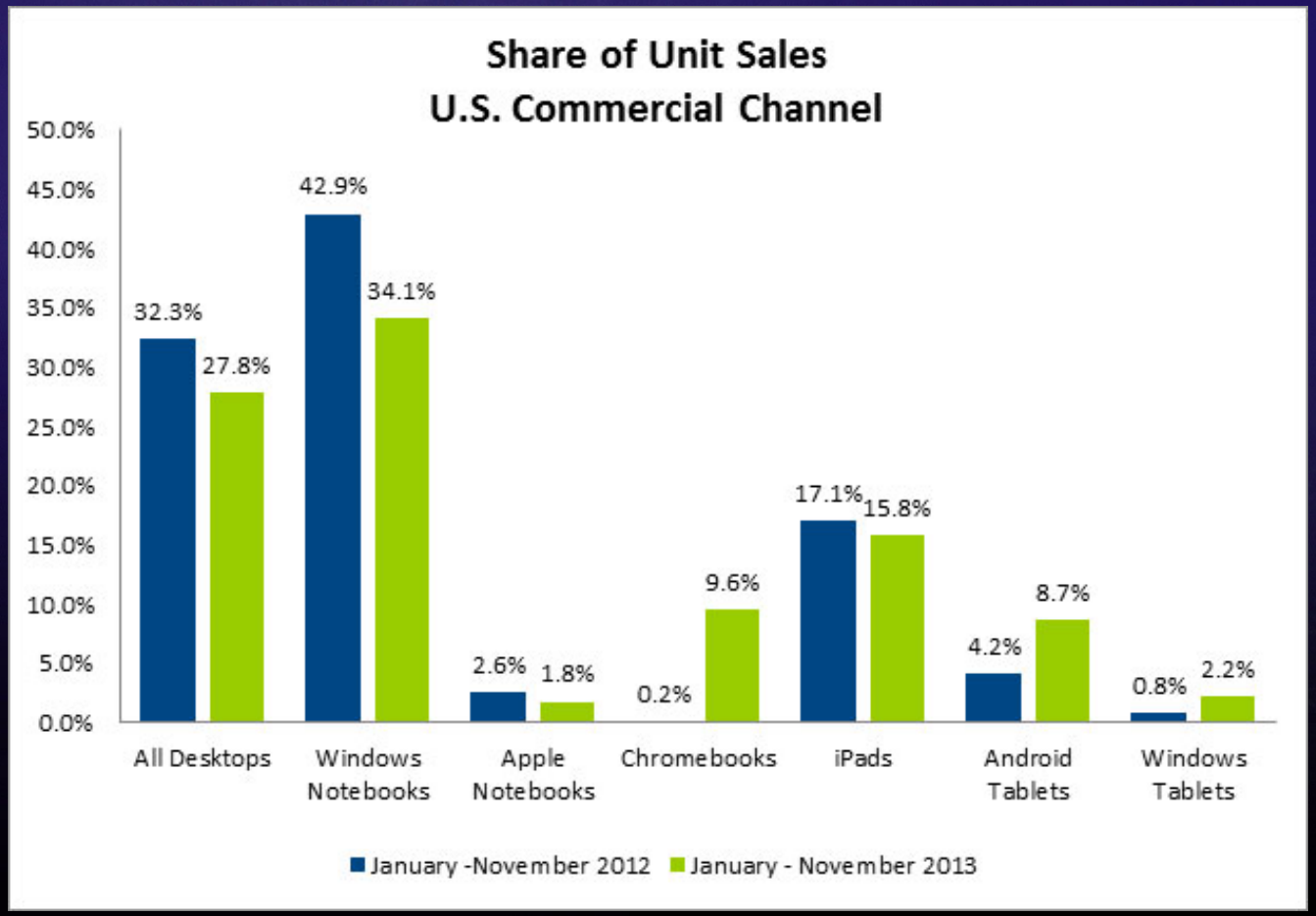


Literature 4 and your responsibility

- Various readings on your own
  - Python/Perl, OS, tools, APIs, guidelines, research, blogs, subjects, etc.
  - http://users.du.se/~hjo/cs/dt2018/readings/
- Gaining knowledge – your own work and responsibility!
- Trained to give explanations in complex topics
  - Verbal and written
  - A big part of the forensic work is about this
- Critically review others work

Forensic project considerations

- Market trends – wearables, virtual assistants, ...
- Smart watches, smart home appliances, …



Forensic project I

- Your own forensic work or existing home work
  - Example: Kevin Lund, MacOSX forensics – see the dt2018/project folder
  - Perform ”home work”: Hex challenge (1a or 1b) and Crypto challenge (2a or 2b) and present your solution
- Project exemples
  - Forensics on OS as Mac OS X ***, Windows 10, Chrome OS, etc.
  - Examine free/open source forensic tools or them vs. other commercial tools
  - Deep dive into memory analysis, executable analysis, Windows registry analysis or other analysis chapter from the books
  - Examine forensic file analysis (carving/memory dump) tools. Check with forensic wiki or the DFRWS 2012/2013 challenges which dealt with data block classification
  - DFRWS 2014 challenge – Mobile Malware Analysis (DFRWS 2015?)
  - Encase vs. FTK (we have the newest release of FTK)
  - MPE+ vs. Cellbrite (I have a Cellbrite dongle I can lend to you)
  - GPGPU – parallel programming and crypto - **CrypTool**

Forensic project II

- Social media forensics
- Malware analysis with the help of the malware analysis book (RCE etc.)
- Prepare a forensic image with hard to find evidence
- Cloud computing and forensics – Google Takeout etc.
- Virtualization and forensics – what if the criminal runs everything in an virtual environment? What can bee seen in the host OS?
- Hur bevisa att ett rootkit (ej) existerat på datorn? (Ch7 - WFA)
- File systems advanced: after ext4 comes Btrfs, ZFS etc.
- Välja ett arbete som man kan fortsätta senare med som examensarbete eller utöka någon av laborationerna
- Obfuscation and anti-debugging technologies - RCE
- Bleeding edge uppslag från forensic blogg eller eget förslag...?
- Mobile and embedded forensics subject such as Windows phone, wearables or other new stuff

AccessData Certified Examiner - ACE

- Student offer from HDA!
- Free (no prerequisites) multiple choice online exam of Knowledge Based and Practical Based elements
- The FTK suite of tools is required (FTK *, RV, PRTK)
- In preparation for the process
  - ACE Study Guide
  - ACE Preparation Videos
- If you get ACE a maintenance exam will be needed after 1 year
  - After this the maintenance exam will be held every second year
- More info
  - http://accessdata.com/training/certifications
  - [server]\forensics\AccessData Certified Examiner ACE

ACCESSDATA CERTIFIED EXAMINER

Hans Jones

This credential shall be valid for a period of two years from the date shown or the anniversary date, whichever is later.

February 27, 2015

AccessData

UR-fc1p7132e98qw32-3413871

Powered by: SYNTRICATE

Mark A. Stringer
ACE Program Manager

E-material etc.

- Links, check fronter and books etc.
  - http://www.forensicswiki.org
  - Forensic blogs
- Tools, papers etc.
  - \\projects\digitalbrott
  - http://users.du.se/~hjo/cs/
  - DU Library - http://du.se/biblioteket/
- Earlier books in the program and other stuff
  - http://www.forensicfocus.com/
- …