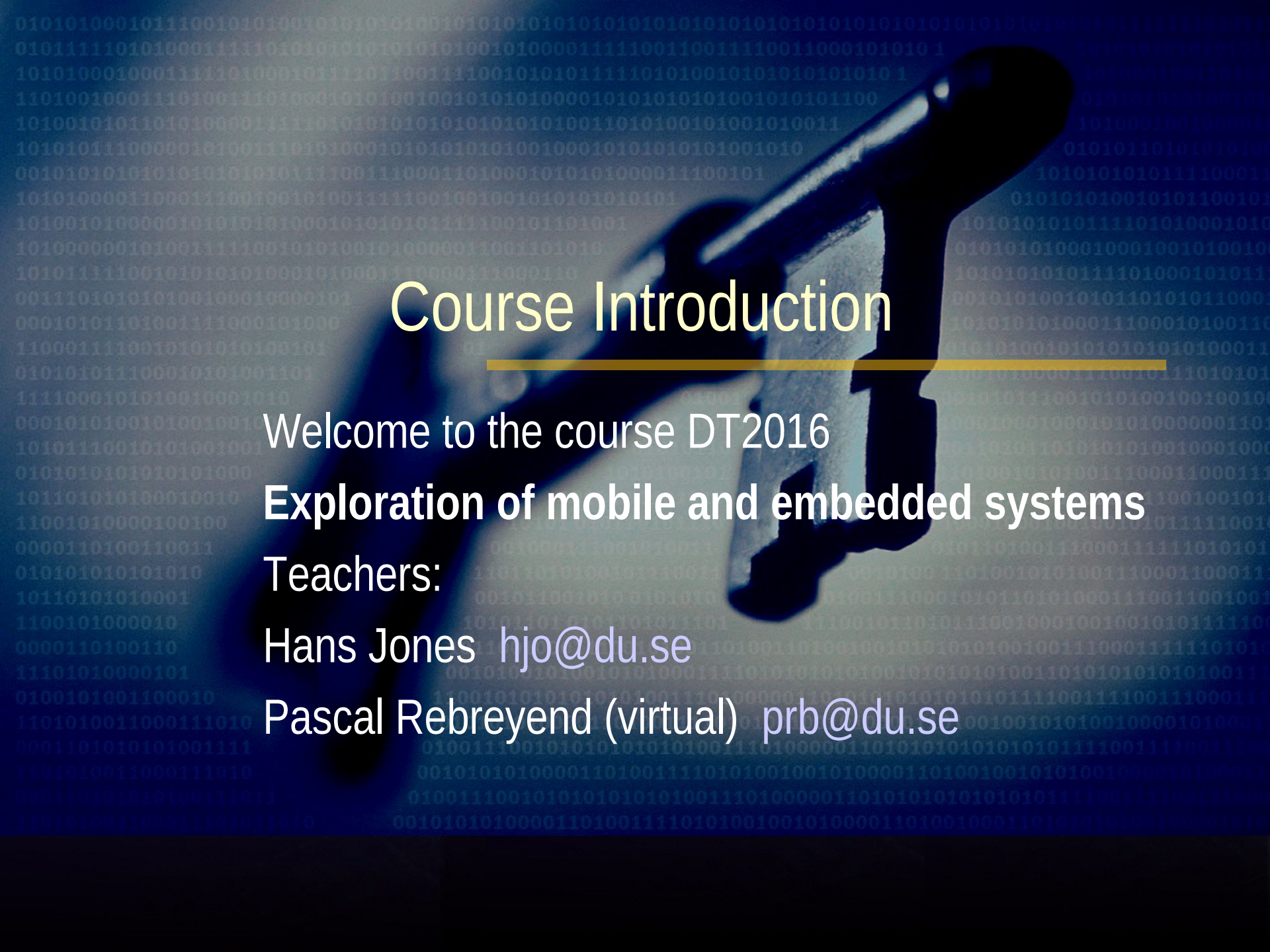


Course Introduction

Welcome to the course DT2016

Exploration of mobile and embedded systems

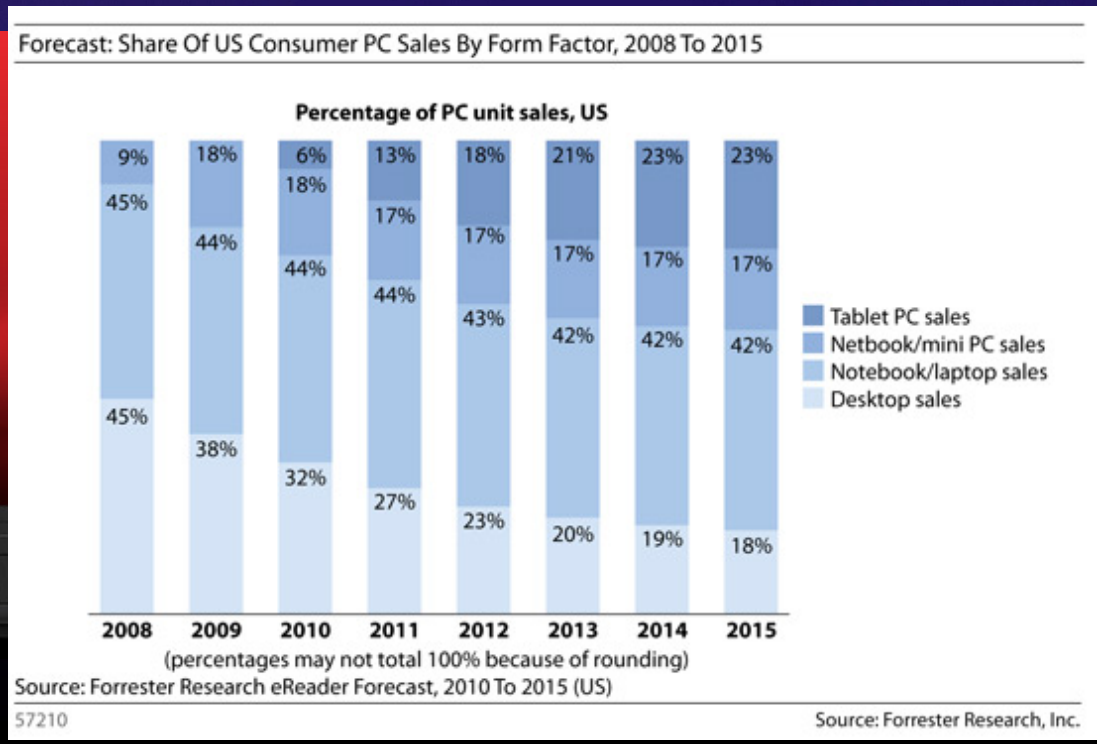
Teachers:

Hans Jones hjo@du.se

Pascal Rebreyend (virtual) prb@du.se

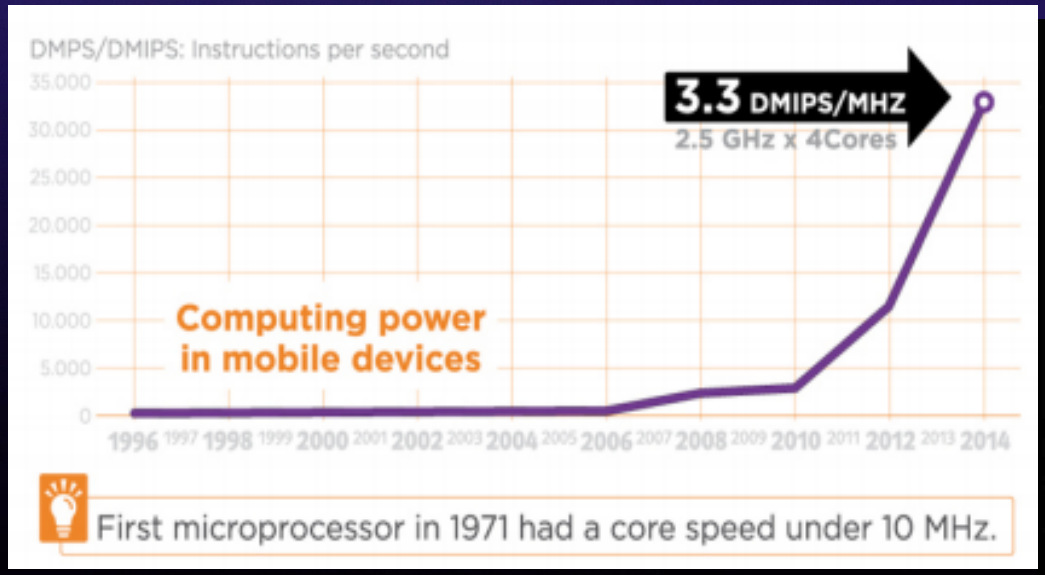
Flight of the desktops – the future is mobile!

- Tablets are more or less a smart phone with a large screen
- x86 CPU:s are declining? – portable needs energy efficiency!
- Systems as Motorola ATRIX and Asus Padfone etc.
- Laptop is a screen and keyboard or just a bigger screen for tablets



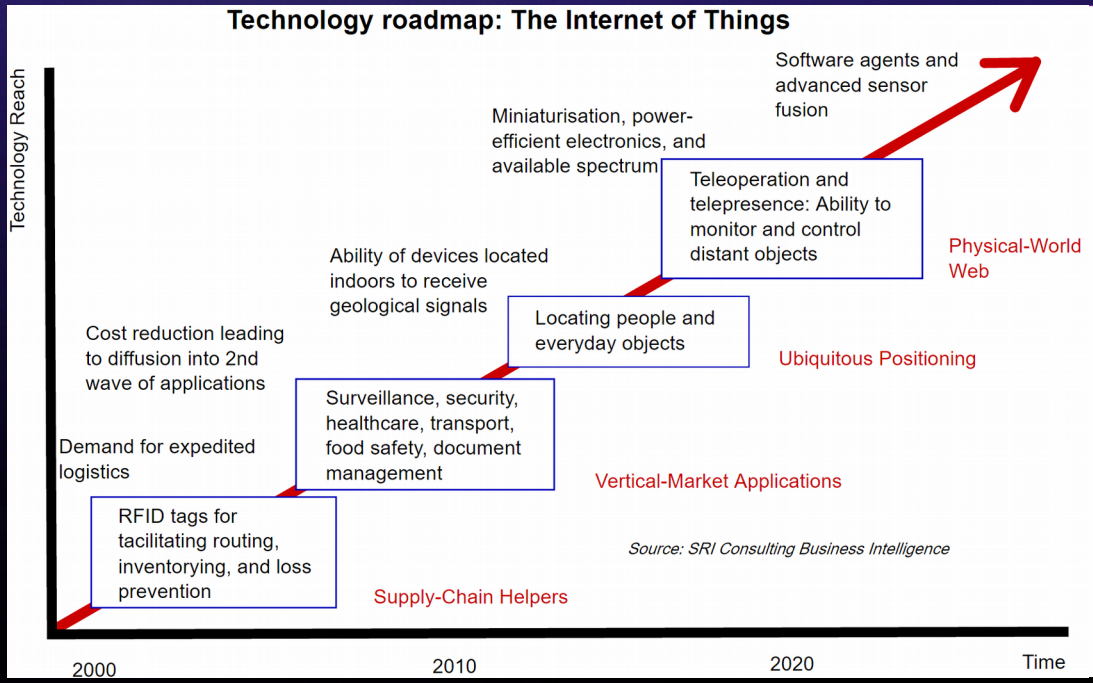
Flight of the desktops – the future is mobile!

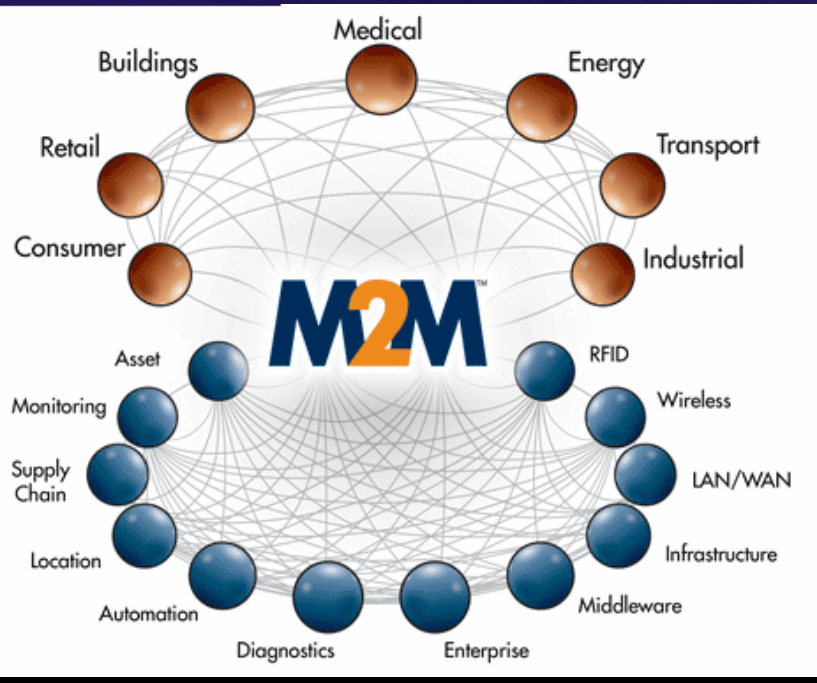
- Last 2-3 years not so much exiting stuff have happened
- Ultrabook spec. 2013, 10/15W - http://en.wikipedia.org/wiki/Ultrabook
- Year 2000 – 1 TeraFlop in computing power needed a super computer with 10 000 CPUs consuming 1 MW
- Year 2015 – 1 TeraFlop need about 10 Watts



M2M the cloud, IoT and IoE

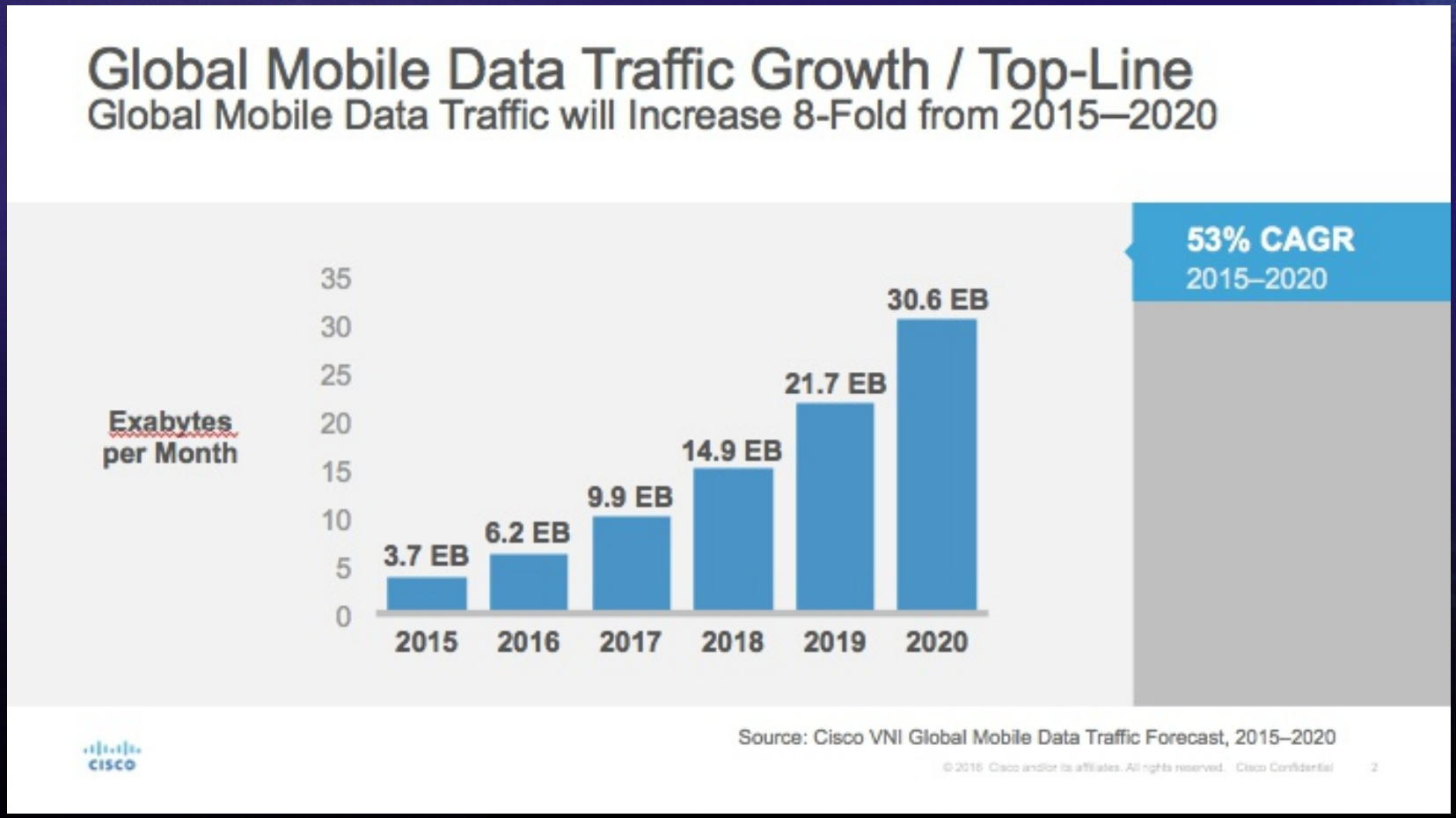
- Machine-to-machine refers to technologies that allow both wireless and wired systems to communicate with other devices of the same ability
- M2M uses sensors/actuators to capture an event which is relayed through a network to a software which translate it into meaningful information
- M2M birthed < IoT (Internet of Things) which birthed < IoE (Internet of Everything)
- https://en.wikipedia.org/wiki/Internet_of_things





Mobile internet traffic will surge in the near future

- Recently mobile traffic accounted just over 50% of the global internet traffic
- By 2017-2018 mobile traffic will account for 75% of the global internet traffic!

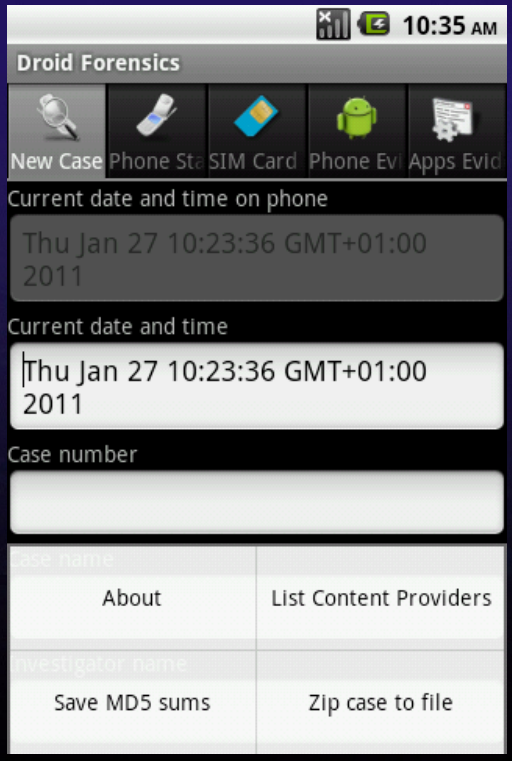


Goals, contents, labs, points and examination

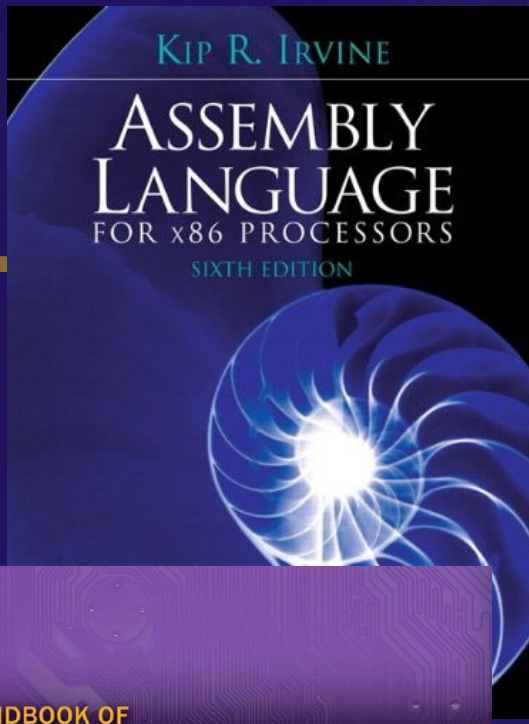
- Fronter > Kursplan
  - http://www.du.se/sv/Utbildning/Kurser-A-O/Kursplan/?kod=DT2016
- Fronter > Kursmaterial > studiehandledning
- Assessment
  - Approved laborations: 4,5 hp
  - Written forensic project report and critical paper review: 3 hp
- Examination
  - Labs
  - Induvidual project work related to the course subject
    - Examples on a later slide, own proposal possible ...
  - Critical review of paper
  - Approved labs in time == higher chance to grade VG

Project examples

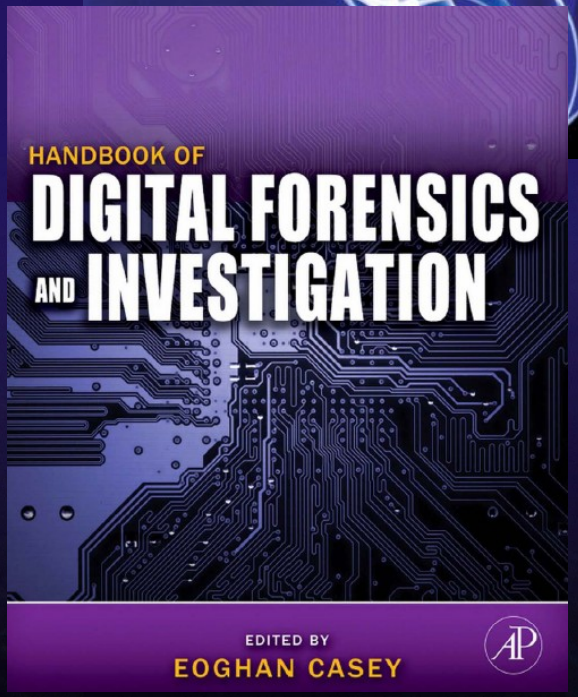
- Make an Android forensic software
  - An app as Droid Forensics or a tool as the DFRWS 2011 challenge
- Examine a flash memory hexdump from a cell phone
  - As the forensics challenge from DFRWS 2010
- Find user generated data (evidence)
- Make your own tools
- Research
- ...
- Written report



Literature 1



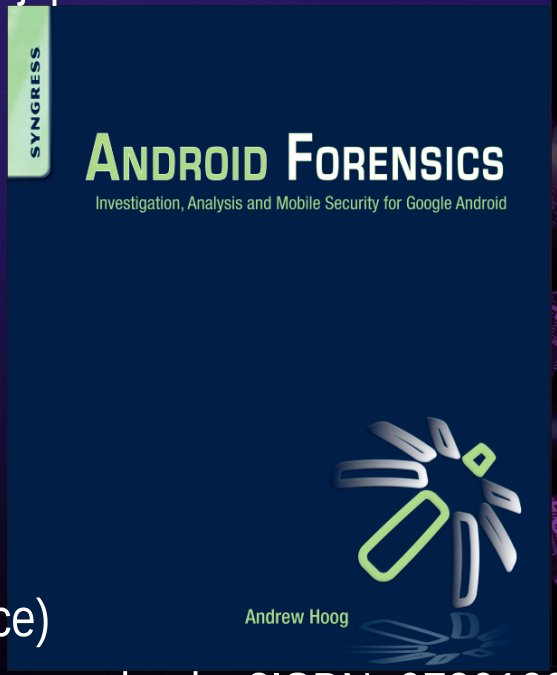
- Assembly Language
  - http://kipirvine.com/asm/
- Handbook of Digital Forensics and Investigation
  - Ch 8 (embedded) and ch 10 (infrastructure)
- Docs on [server]\embedded_forensics\...
  - SIM cards and cellphones
  - Hardware and software
  - Protocols and standards
  - Guidelines and challenges (DFRWS 2010/2011)
  - Tools and infrastructure
  - Blogs, websites, links etc…

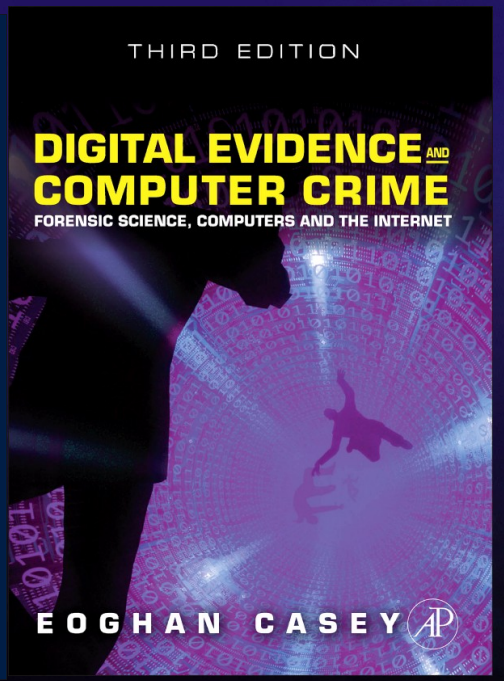


- Subject is very diversified and dynamic, being up to date is a must!

Literature 2

- Android Forensics: Investigation, Analysis and Mobile Security for Google Android (Syngress)
  - Free chapters 3 (ADB) and 6 (forensic tech)
  - http://store.elsevier.com/product.jsp?isbn=9781597496513
  - ISBN-10: 1597496510

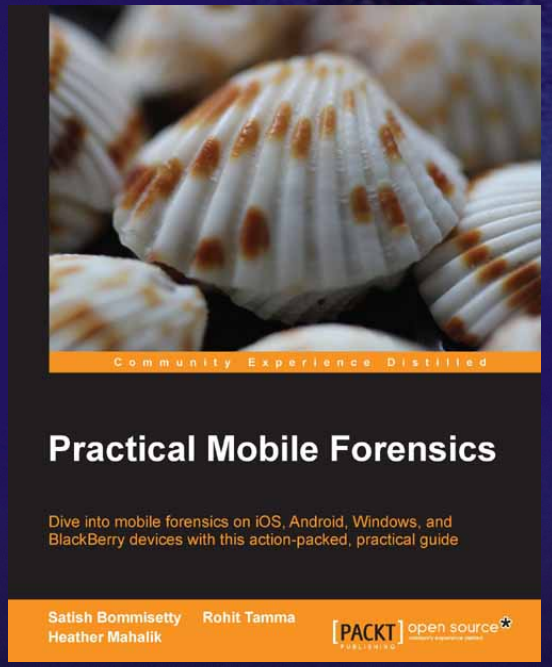




- Digital Evidence and Computer Crime, Third Edition
  - Free chapter 20 (mobile evidence)
  - http://www.elsevierdirect.com/companion.jsp?ISBN=9780123742681

Literature 3 (newer books may exist)

- Practical Mobile Forensics
  - Two first chapters are free - Introduction and iOS internals
  - https://www.packtpub.com/application-development/practical-mobile-forensics
- CyanogenMod Wiki
  - Rooting instructions etc.
  - https://wiki.cyanogenmod.org/w/Main_Page
- XDA-University (XDA-developers)
  - Hacking instructions etc.
  - http://www.xda-developers.com/
  - http://xda-university.com/
- Android Developers
  - http://developer.android.com



Facts and trends (5 years ago)

- Study from Europol and European Commission
  - Over 70% of the solved criminal cases in Europe involved phone forensics
  - In UK / Sweden / Germany / France its over 90%
- Good Reasons Why You Should Focus on Embedded Forensics
  - Small Scale Digital Devices (SSDD) are in the majority
  - On the long term everything is going to be small scale
  - SSDDs have great forensic potential
  - Anti-forensics is more difficult
  - It lags behind other digital forensics fields
  - It's relative easy to get results on Forensic Data Recovery from Flash Memory
  - It's so diverse, it needs more people
  - You like new gadgets ☺

Top 7 ways investigators catch criminals with mobile forensics

- Bypass security codes that locks the phone with special mobile forensic tools (memory dump and enumeration of structures)
- Use safe (cloned) SIM cards designed for forensics (cards that don't connect to network but enable start of the phone)
- Live acquisition (shielded Faraday bag and phone kept turned on)
- Trusted time source stamps (SMS, core network)
- Tracking movements (GPS and core network)
- Recovering deleted data in the phone (memory dump)
- Getting the physical image, usually only logical data is possible (only information that is visible via UI)
- Source:

http://computer-forensics.sans.org/blog/2009/07/01/top-7-ways-investigators-catch-criminals-using-mobile-device-forensics/

E-material etc.

- **In Fronter there may be more up to date info!**
- **Wikis**
  - https://en.wikipedia.org/wiki/Mobile_device_forensics
  - https://github.com/secmobi/wiki.secmobi.com
  - http://www.forensicswiki.org
- DFRWS 2010 and 2011 submissions at: http://www.dfrws.org/2010/ and http://www.dfrws.org/2011
- Tools, papers etc.
  - \\projects\digitalbrott

DFRWS
DIGITAL FORENSIC RESEARCH WORKSHOP

Retired equipment in the course

- MSAB
- MPE+

AccessData