Introduction

DT2016, Undersökning av mobila och inbyggda system

Logistics

- Teachers:
  - Hans Jones
    - hjo@du.se
    - Tel: 023 77 88 35, 070 699 77 80
  - Mevludin (a.k.a Dino) Memedi
    - mmi@du.se
    - 023 77 88 52, 073 720 41 48

Learning outcomes

- Develop simple solutions to problems in assembly language
- Develop scripts and software via different interfaces (APIs) for forensic extraction of data in mobile and embedded systems
- Implement solutions that carve and extract evidence from storage media
- Analyse SMS and database structures from a forensic perspective
- Explain how a GIS functions and analyse different positioning technologies as cell ID and GPS
- Describe how the mobile data system functions (devices, protocols and infrastructure)
- Manage GIS, map-based APIs and Web technologies

Content

Kalender/kurs vecka	Kursavsnitt som kommer att behandlas under föreläsningar	Kapitel i kursboken att läsa på egen hand. Streamad lektion	Lärare	Projektarbete och laborationer
46 (1)	Course intro and planning What is an embedded system? Assembly basics	**Books, slides and other reference material:** Assembly papers and basics Assembly Language for x86 Processors, 6th edition **Stream:** Course intro – the 3 first lectures about assemblely	hjo,prb,mmi	Lab 1. Assembly basics
47 (2)	Assembly cont.	**Books, slides and other reference material:** as first week **Stream:** The 3 last lectures about assemblely	hjo,prb,mmi	Lab 2. Assembly basics cont.
48 (3)	Cell Phone, PDA/smart phone and SIM Card Forensics Mobile memory dumps, MSAB and MPE+	**Books, slides and other reference material:** Relevant chapters from the course books. OH and other reference material **Stream:** Small Scale Digital Forensics and tools. Hexdump tools and analysis. SMS and flash memory	hjo,mmi	Lab 3. MPE+ lab Evaluate forensic tools for mobile phones. SIM/PIM and memory dump analysis etc.
49 (4)	Flash memories (MTD) on phones SMS low level (U)ICC – SIM cards http://en.wikipedia.org/wiki/UICC	**Books, slides and other reference material:** As w48 **Stream:** Fash memory and SIM. SIM, GSM security and lab 5 intro	hjo,mmi	Lab 4. Carve for SMS in memory dumps with Python. MSAB and Cellbrite hex-viewers

Content (2)

50 (5)	Android technology and forensics, content providers, SQLite, etc. Android security	**Books, slides and other reference material:** As w48 **Stream:** Android forensics part 1. Android forensics part 2, lab5 and examination	hjo,mmi	Lab 5. Android technology and forensic methods. Find evidence in Android devices. viaExtract CE virtual
51 (6)	Position technologies, projection reference systems GIS, spatial databases. Track and trace, Google Earth and .kml files etc.	**Books, slides and other reference material:** As w48, HTML basics PHP basics Google static API Google Maps, SQL and spatial data, various GIS tools **Stream:** GIS and location part 1. GIS and location part 2 and lab 6 review	hjo,mmi	Lab 6. GIS - track and trace lab Simple map web service with PHP and Google static API Map display of Cell-id in a C# program Visualize an unknown track file on a map
52 (7)	Cellular infrastructure and Cell Phone Systems. GSM, (W)CDMA, LTE, RFID, NFC (Near Field Communication), Bluetooth Cell phone security Malware, Flexispy etc.	**Books, slides and other reference material:** As w48 **Stream:** Radios and infrastructure part 1 and lab 4 help. Radios and infrastructure part 2 and mobile security	hjo,mmi	Own work with labs
1 (8)		**Books, slides and other reference material:** As w48 **Stream:** N/A	hjo,mmi	Written examination 3,5 hp See project suggestions
2 (9)	Own work			
3 (10)	Own work		hjo,mmi	Last week to send in labs to get grade 5. Written examination hand-in

Class organization

- 1 “review” session per week (Mondays)
  - summary of the material
  - Updates/changes from last year
  - Questions and answers
  - lab discussion, and others
- You are expected to watch corresponding recorded lectures before each review session (check the table at studiehandledning_v14-1.html)
- 2 lab sessions per week
- 1 extra session that can be utilized as a lab session

Assessments

- 6 labs assessed as Pass or Fail
  - Deadlines: check the dates in hand-in folders
- Written project work graded as U, G and VG
  - Individual project on a forensic investigation
  - Critical review of a published scientific paper

Assignment – reviewing a paper on embedded forensics

- The objective is to find (optional), read and review a scientific paper on the field of digital forensics of embedded systems.
- The assignment will consists of a report (max 2 pages) and an oral presentation
  - you will be asked to shortly present your findings during a seminar session via Adobe Connect. Each student will have 10 minutes for presentation and 2-3 minutes for questions and answers. Active participation of other students is recommended.

Assignment – reviewing a paper on embedded forensics (2)

- The report must include the following:
  - Summary: summarize the paper shortly and precisely **in your own words** for an audience of your classmates. This shows your understanding of the paper.
  - Discussion: point out the strengths and limitations of the knowledge and methods of the presented research.
  - Conclusions: discuss the broader implications of the paper to the field of digital forensics (give the big picture in a critical manner). In addition, you should discuss new approaches that you think should have taken place in order to improve the research.
- Assessments – report and oral presentation (Pass/Fail)

Papers

- There is a collection of papers selected for you that you can choose from and review. You can also find a paper by your own given the fact that it is relevant to the topic of the assignment. These kinds of papers need to be approved by teachers before you start to review them.
- The selected papers focus on challenges, techniques and methods in embedded forensics. Different topics are covered including embedded systems like payment cards, CCTV systems, DVR systems, Smart TVs, game consoles and general mobile forensics, among others.

List of selected papers

- J. Grover (2013). Android forensics: automated data collection and reporting from a mobile device. *Digital Investigation,* 10, S12-S20.
- K. Barmpatsalou, et al. (2013). A critical review of 7 years of Mobile Device Forensics. *Digital Investigation,* 10, 323-349.
- C. Anglano (2014). Forensic analysis of WhatsApp Messenger on Android smartphones. *Digital Investigation,* 11, 201-213.

List of selected papers (2)

- C. Ntantogian et al. (2014). Evaluating the privacy of Android mobile applications under forensic analysis. *Computers & Security,* 42, 66-76.
- K. Xynos et al. (2010). Xbox 360: A digital forensic investigation of the hard disk drive. *Digital Investigation,* 6, 104-111.
- M. Kaart and S. Laraghy (2014). Android forensics: interpretation of timestamps. *Digital Investigation,* 11, 234-248.

List of selected papers (3)

- A. Mylonas et al. (2013). Smartphone sensor data as a digital evidence. *Computers & Security,* 38, 51-75.
- I. Sutherland et al. (2014). Forensic analysis of smart TV: A current issue and call to arms. *Digital Investigation,* 11, 175-178.
- J. Park and S. Lee (2014). Data fragment forensics for embedded DVR systems. *Digital Investigation,* 11, 187-200.

List of papers (4)

- L. Tobin et al. (2014). Reverse engineering a CCTV system, a case study. *Digital Investigation,* 11, 179-186.
- T. Souvignet et al. (2014). Payment card forensic analysis: From concepts to desktop and mobile analysis tools. *Digital Investigation,* 11, 143-153.

Finding a paper by yourself

- Majority of publishers require subscription for their journals
- However, there are other open-access publishers too
- For the publishers which require subscription you need to use the library (bibliotek) as a proxy and authenticate with your university's account credentials (demonstration)

Some other journals to consider

- Security and Communication Networks (http://onlinelibrary.wiley.com/journal/10.1002/%28ISSN%291939-0122)
- IEEE Transactions on Information Forensics and Security (http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=10206)
- International Journal of Digital Crime and Forensics (http://www.igi-global.com/journal/international-journal-digital-crime-forensics/1112)
- Journal of Forensic Sciences (http://onlinelibrary.wiley.com/journal/10.1111/%28ISSN%291556-4029)