Introduction

DT2016, Undersökning av mobila och inbyggda system
Logistics

• Teachers:
  – Hans Jones
    • [hjo@du.se](mailto:hjo@du.se)
    • Tel: 023 77 88 35, 070 699 77 80
  – Mevludin (a.k.a Dino) Memedi
    • [mmi@du.se](mailto: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
<table>
<thead>
<tr>
<th>Kalender/kursvecka</th>
<th>Kursavsnitt som kommer att behandlas under föreläsningar</th>
<th>Kapitel i kursboken att läsa på egen hand. Streamad lektion</th>
<th>Lärare</th>
<th>Projektarbete och laborationer</th>
</tr>
</thead>
<tbody>
<tr>
<td>46 (1)</td>
<td>Course intro and planning</td>
<td>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 assembly</td>
<td>hjo, prb, mmi</td>
<td>Lab 1. Assembly basics</td>
</tr>
<tr>
<td></td>
<td>What is an embedded system?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Assembly basics</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Stream: The 3 last lectures about assembly</td>
<td></td>
<td></td>
</tr>
<tr>
<td>48 (3)</td>
<td>Cell Phone, PDA/smart phone and SIM Card Forensics</td>
<td>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</td>
<td>hjo, mmi</td>
<td>Lab 3. MPE+ lab Evaluate forensic tools for mobile phones. SIM/PIM and memory dump analysis etc.</td>
</tr>
<tr>
<td></td>
<td>Mobile memory dumps, MSAB and MPE+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>49 (4)</td>
<td>Flash memories (MTD) on phones</td>
<td>Books, slides and other reference material: As w48</td>
<td>hjo, mmi</td>
<td>Lab 4. Carve for SMS in memory dumps with Python. MSAB and Cellbrite hex-viewers</td>
</tr>
<tr>
<td></td>
<td>SMS low level</td>
<td>Stream: Flash memory and SIM, SIM, GSM security and lab 5 intro</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(U)ICC – SIM cards</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Week</td>
<td>Topic</td>
<td>Reference Material</td>
<td>Stream</td>
<td>Lab</td>
</tr>
<tr>
<td>------</td>
<td>----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>-------------------------------------------</td>
<td>-----</td>
</tr>
<tr>
<td>50</td>
<td>Android technology and forensics, content providers, SQLite, etc.</td>
<td>Books, slides and other reference material: As w48</td>
<td>Stream: Android forensics part 1.</td>
<td>hjo</td>
</tr>
<tr>
<td></td>
<td>Android security</td>
<td></td>
<td>Android forensics part 2, lab 5 and</td>
<td>mmi</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>examination</td>
<td></td>
</tr>
<tr>
<td>51</td>
<td>Position technologies, projection reference systems</td>
<td>Books, slides and other reference material: As w48, HTML basics</td>
<td>Stream: GIS and location part 1.</td>
<td>hjo</td>
</tr>
<tr>
<td></td>
<td>GIS, spatial databases.</td>
<td>PHP basics</td>
<td>GIS and location part 2 and lab 6 review</td>
<td>mmi</td>
</tr>
<tr>
<td></td>
<td>Track and trace, Google Earth and .xml files etc.</td>
<td>Google static API</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Google Maps, SQL and spatial data, various GIS tools</td>
<td></td>
<td></td>
</tr>
<tr>
<td>52</td>
<td>Cellular infrastructure and Cell Phone Systems.</td>
<td>Books, slides and other reference material: As w48</td>
<td>Stream: Radios and infrastructure part 1</td>
<td>hjo</td>
</tr>
<tr>
<td></td>
<td>GSM, (W)CDMA, LTE, RFID, NFC (Near Field Communication), Bluetooth</td>
<td></td>
<td>and lab 4 help. Radios and infrastructure</td>
<td>mmi</td>
</tr>
<tr>
<td></td>
<td>Cell phone security</td>
<td></td>
<td>part 2 and mobile security</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Malware, Flexispy etc.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>Books, slides and other reference material: As w48</td>
<td>Stream: N/A</td>
<td>hjo</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>mmi</td>
</tr>
<tr>
<td>2</td>
<td>Own work</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Own work</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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 consist 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

List of selected papers (2)


List of selected papers (3)


List of papers (4)

• L. Tobin et al. (2014). Reverse engineering a CCTV system, a case study. Digital Investigation, 11, 179-186.

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)

  (http://www.igi-global.com/journal/international-journal-digital-crime-forensics/1112)

– Journal of Forensic Sciences
  (http://onlinelibrary.wiley.com/journal/10.1111/%28ISSN%29291556-4029)