T-110.6220 Course Intro

Antti Tikkanen

F-Secure

Reverse Engineering Malware

```
.text:00401250  E8 BB DA 0E 00 89 44 24  04 A1 2C A3 57 00 8B 40  F++.ëD$í,úW.ï@
.text:00401260  10 89 04 24 E8 27 D5 0E  00 8B 15 2C A3 57 00 E9  ë$F'+.ï§,úW.T
.text:00401270  4B FF FF FF 8D B6 00 00  00 00 8D BF 00 00 00 00  K   ì¦....ì+....
.text:00401280  55 89 E5 83 EC 08 C7 04  24 01 00 00 00 FF 15 18  Uësâ8¦$... §
.text:00401290  A3 57 00 E8 B8 FE FF FF  90 8D B4 26 00 00 00 00  úW.F+¦  Éì¦&....
.text:004012A0  55 89 E5 83 EC 08 C7 04  24 02 00 00 00 FF 15 18  Uësâ8¦$... §
.text:004012B0  A3 57 00 E8 98 FE FF FF  90 8D B4 26 00 00 00 00  úW.Fÿ¦  Éì¦&....
.text:004012C0  55 8B 0D 54 A3 57 00 89  E5 5D FF E1 8D 74 26 00  UïTúW.ës] ßìt&.
.text:004012D0  55 8B 0D 34 A3 57 00 89  E5 5D FF E1 90 90 90 90  Uï4úW.ës] ßÉÉÉÉ
.text:004012E0  83 EC 7C B8 70 B5 4E 00  89 44 24 34 B8 74 30 4F  â8|+p¦N.ëD$4+t0O
.text:004012F0  00 89 44 24 38 8D 44 24  60 89 44 24 3C B8 90 13  .ëD$8ìD$`ëD$<+É
.text:00401300  40 00 89 44 24 40 8D 44  24 1C 89 7C 24 74 89 5C  @.ëD$@ìD$ë|$të\
.text:00401310  24 6C 89 74 24 70 89 6C  24 78 89 64 24 44 89 04  $lët$pël$xëd$Dë
.text:00401320  24 E8 3A BE 0E 00 8B BC  24 80 00 00 00 85 FF 0F  $F:+.ï+$Ç...à ¤
.text:00401330  84 8B 00 00 00 C7 04 24  10 20 57 00 8B 94 24 80  äï...¦$ W.ïö$Ç
.text:00401340  00 00 00 8D 44 24 50 89  44 24 04 BE 88 E1 56 00  ...ìD$PëD$+êßV.
.text:00401350  31 DB 89 74 24 50 B9 01  00 00 00 89 54 24 54 89  1¦ët$P¦...ëT$Të
.text:00401360  5C 24 58 89 4C 24 20 E8  D4 59 00 00 89 44 24 04  \$XëL$ F+Y..ëD$
.text:00401370  C7 04 24 10 20 57 00 E8  B4 5A 00 00 85 C0 74 2E  ¦$ W.F¦Z..à+t.
.text:00401380  8B 40 08 BA E8 EC 56 00  89 54 24 50 EB 34 66 90  ï@¦F8V.ëT$Pd4fÉ
.text:00401390  B8 E8 EC 56 00 89 44 24  50 8B 44 24 24 89 04 24  +F8V.ëD$PïD$$ë$
.text:004013A0  B8 FF FF FF FF 89 44 24  20 E8 72 C4 0E 00 B8 E8  +    ëD$ Fr-.+F
.text:004013B0  EC 56 00 89 44 24 50 89  F6 8D BC 27 00 00 00 00  8V.ëD$Pë÷ì+'....
.text:004013C0  31 C0 89 44 24 18 8D 44  24 1C 89 04 24 E8 6E BE  1+ëD$ìD$ë$Fn+
.text:004013D0  0E 00 8B 44 24 18 8B 5C  24 6C 8B 74 24 70 8B 7C  .ïD$ï\$lït$pï|
.text:004013E0  24 74 8B 6C 24 78 83 C4  7C C3 8D B6 00 00 00 00  $tïl$xâ-|+ì¦....
```

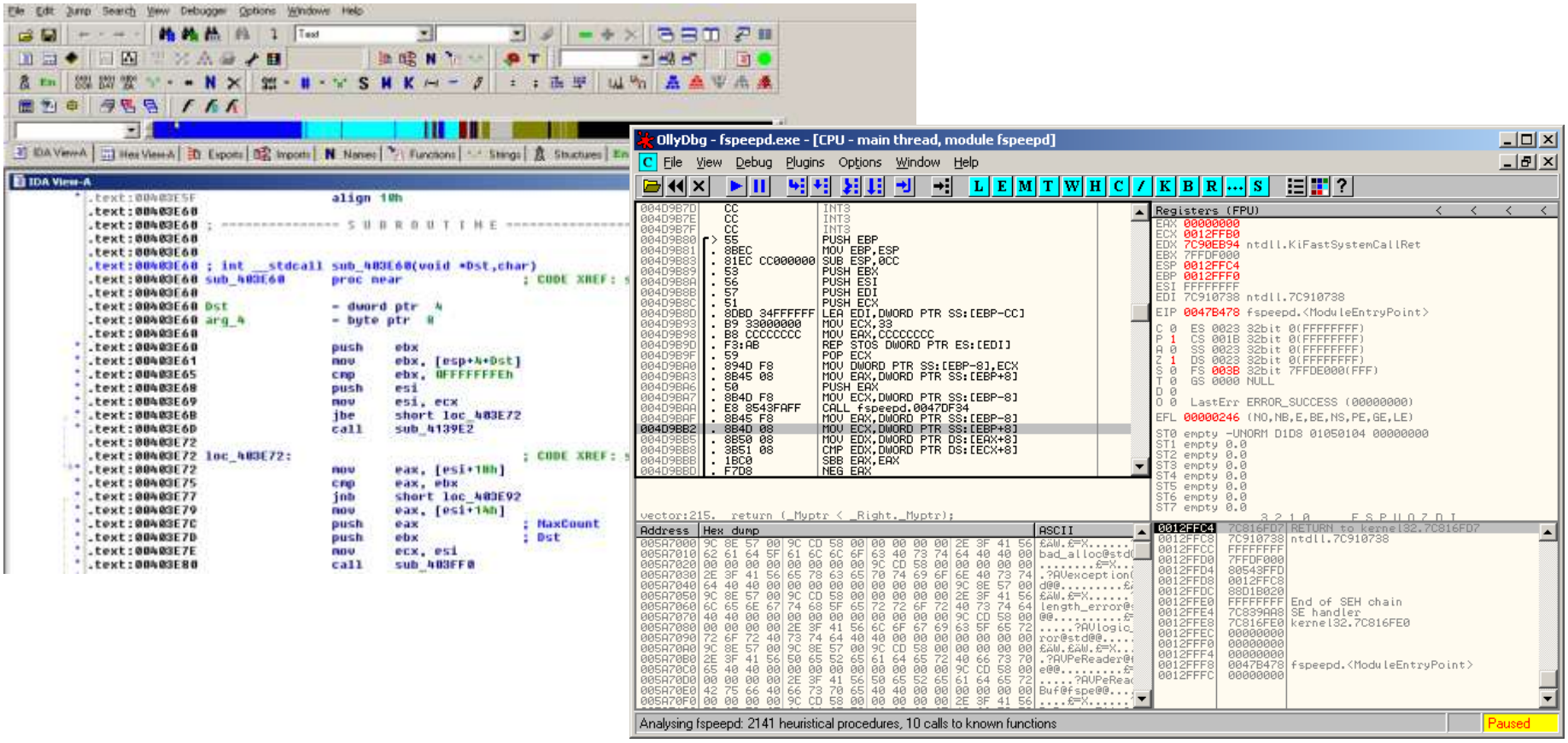
Course Staff

- Staff
  - Main lecturer: Antti Tikkanen
  - Course assistant: Päivi Tynninen
- Visiting lecturers from F-Secure
  - Mikko Hyppönen
  - Paolo Palumbo (static analysis, interpreted languages)
  - Jarkko Turkulainen (obfuscation, dynamic analysis)
  - Karmina Aquino (interpreted languages)
  - Christine Bejerasco (web threats)
  - Broderick Aquilino (Mac)
  - Jarno Niemelä (corporate espionage)
- No visiting hours, only by appointment

Lectures

Date	Topic
21.1.2015	Course Intro + Threats Today
28.1.2015	Static Analysis I
4.2.2015	Static Analysis II
11.2.2015	Dynamic Analysis
25.2.2015	Windows for Reverse Engineers
4.3.2015	Binary Obfuscation and Protection
11.3.2015	Malware Analysis Automation
18.3.2015	Analyzing Interpreted Languages The Malicious Web
25.3.2015	Mac Malware Analysis Industrial Espionage
1.4.2015	Course Project Instructions

Homework



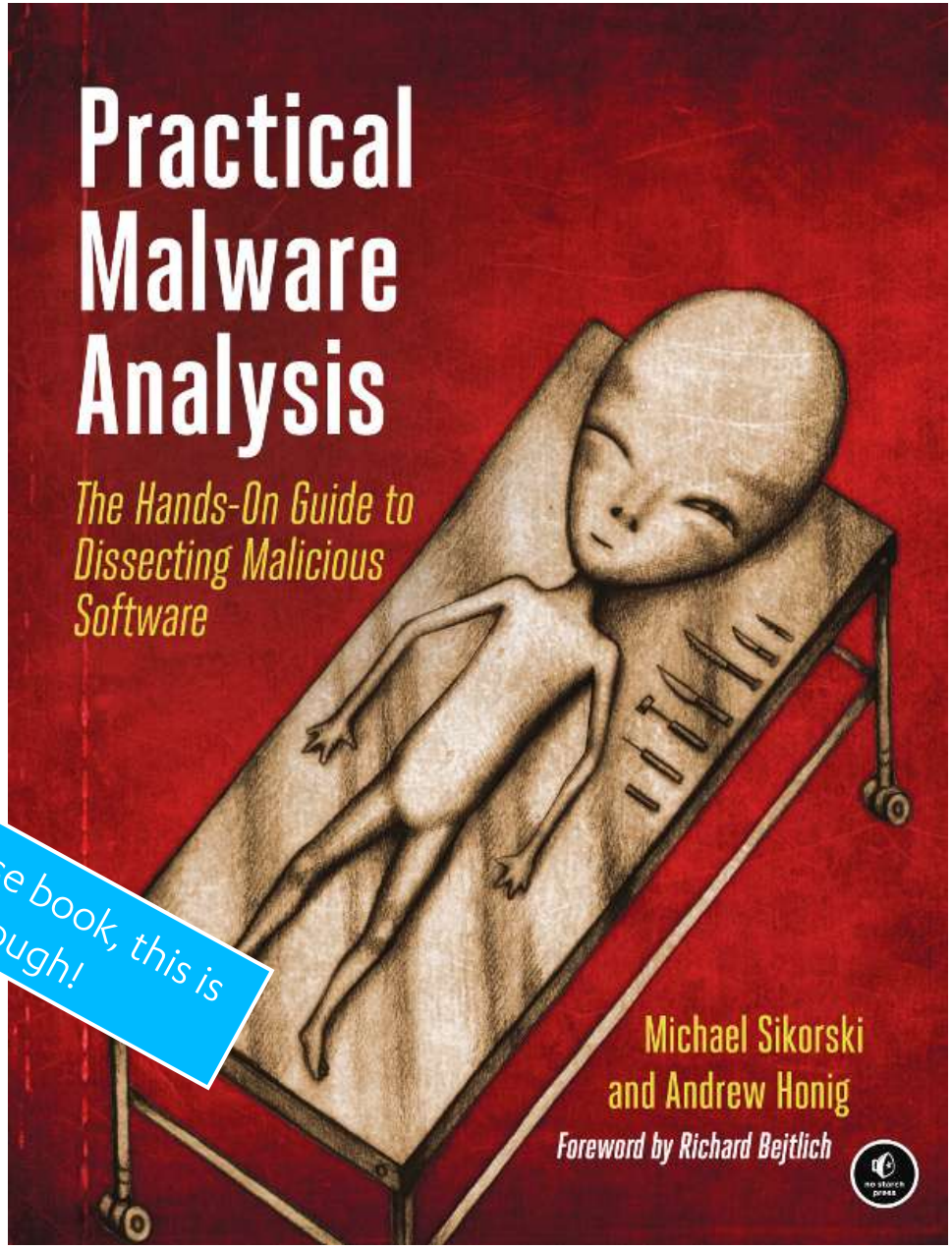
F-Secure

Final Project

- At the end of the course we'll have a mandatory final project
- Course Project 2015: multistage reverse engineering challenge
  - Again, individual work: share ideas, write your own answers
- Deliverables
  - Written report about your solutions
  - Possible source code, IDA databases, …

Grading

- Lectures are not mandatory but very much recommended
- Tool trainings are not mandatory but very much recommended
- Homework
  - 3 rounds, each 20 % of your course grade
- Final project
  - 40 % of your course grade



No official course book, this is a good option though!

F-Secure

Sign up now!

- We can take only up to 35 students
- Sign up in Noppa (don't ask me how..)
- Course **signup will close before next week's lecture**