Project suggestions forensic 2

Starts at once and is individual. Subjects are more or less anything with forensics, but must be rather advanced. Time spent on the project should be between 40 - 80 hours. Remember that you may continue with chosen subject for thesis if suitable. **Note! Students doing project work do not need to do the homwork tasks.**

OBS!
Om du inte gör ett projekt så måste du välja hemuppgifter och redovisa din lösning på dessa i stället vid projektredovisningen. Du måste utföra 2 st. en av varje typ, t.ex. 1b och 2b.

IT-architechture, social media, web technologies etc.

- Facebook forensics and other social media goldmines to dig out evidence from
- Anonymous services as TOR, Ipredator, OneSwarm etc.
- Google chrome OS and Web browser
- Cloud computing, Google Wave etc. and forensics
- Big brother watching you technologies – electronic footprints
- Forensics on other/new OS as Mac (done!)
- Windows 7 news as Windows sensor API/event viewer och WBF API (Windows Biometrical Framework) etc.
- Busy Box, Linux router OS etc.
- Virtualization technologies and forensics
- How will SSD and their low level file system (TrueFFS, extremeFFS,...) affect forensics
- File systems advanced, NTFS vs. WinFS etc.?
- Database forensics

Tools and forensics

- 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 course books or alternative literature
- Examine forensic file analysis (carving/memory dump) tools, check with forensic wiki
- Encase vs. FTK (We have Encase 5 demo which may work) (**buy one Encase license?).**
- Forensic analyze with FTK 3 in a distributed environment, new functions **(if we get license)**
- Construct a Perl/Python forensic toolbox or module to the Mobius Forensic Toolkit
- Make your own COFFE++ USB tool
- Anti-forensics
- Prepare a forensic image with hard to find evidence – a challenge in some way
- OSSEC - Open Source Host-based Intrusion Detection System (Hans J. har mer info)

Programming (crypto)

- GPGPU – parallel programming, OpenCL, Direct Compute, CUDA etc. building a suitable computer for this and explain the technology, (Hans J. har mer info).
- CPU – parallel programming, OpenMP, VisualStudio 2010, Java 7.
- CrypTool tricks and tips, challenge etc.

Reverse Code Engineering

- RCE - obfuscation and anti-debugging technologies
- RCE – advanced new stuff
- RCE - Malware

Other

- GIS, spatial databases and data mining, BI, GRASS etc.
- Russian Business Network (RBN) and other cybercrime organizations
- How prove that a root-kit not existed on the computer (ch7 WFA)
- Bleeding edge forensics idea from forensic blog or own proposal...
- Välja ett arbete som man kan fortsätta med senare som examensarbete, t.ex.
    - Utveckling av en programmodul som kan automatisera detektering av ”naken hud” som förekommer i bilder eller i film-sekvenser.
    - Utveckla någon form av ”webcrawler” som kan hämta specifika ord/slanguttryck kopplade till vissa grupper (t.ex. mc-gäng) för att sedan kunna skapa ett ”riktat” dictionary som kan användas vid forcering av lösenord etc.
    - Utveckla en programmodul som tar fram meta-data kopplat till bilder (kameratyp, tid, datum m.m. m.m.) och katalogiserar dessa för att få en överblick av kameratyper när det är många bilder i ett case.
    - Skapa en standard för en forensisk rapport (rapport-mall)
    - Eget förslag