Readings forensics 2 v0.1

- In general there are a lot of articles on the course web site and in the docs directory on the digitalbrott share that have relevant content that fits in to the course.
- The book Windows Forensic Analysis 2e got a lot of suggested readings after each chapter as well.
- The document may get updated as the course progress.

Week 1 - Carving and Python

- Measuring and Improving the Quality of File Carving Methods – Kloet_2007.pdf
- A Frugal, High Performance File Carver - http://dfrws.org/2005/proceedings/richard_scalpel.pdf
- Digital Forensics File Carving Advances - http://www.korelogic.com/Resources/Projects/dfrws_challenge_2006/DFRWS_2006_File_Carving_Challenge.pdf
- ANALYSIS OF 2007 DFRWS FORENSIC CARVING CHALLENGE – dfrws2007_carving_challenge.pdf
- Tutorials for Python, check out the laboration.

Week 2 – RAM memory analysis

- An Introduction to Windows memory forensic - Introduction_to_windows_memory_forensic.pdf
- Using Every Part of the Buffalo in Windows Memory Analysis - buffalo.pdf
- Physical Memory Forensics - mburdach_physical_memory_forensics_bh06
    - Including videos to the presentation
- Memory Forensic Acquisition and Analysis 101
    - http://sansforensics.wordpress.com/2008/11/19/memory-forensic-analysis-finding-hidden-processes/
- The Acquisition and Analysis of Random Access Memory - The Acquisition and Analysis of Random Access Memory.pdf
- Memory Analysis Q-CERT Workshop - forensics-waits-live-memory-forensics-doha-feb-08.pdf
- Pool Allocations in Windows Memory Forensics - IMF2006-PoolAllocations.pdf

Week 3 – Windows registry 1

- Forensic Analysis of the Windows Registry in Memory - Brendan Dolan-Gavitt, http://www.dfrws.org/2008/program.shtml **[**SESSION 2: In-Depth Analysis #2**]**
- Recovering Deleted Data From the Windows Registry – Timothy Morgan, http://www.dfrws.org/2008/program.shtml **[**SESSION 2: In-Depth Analysis #2**]**
- Explanation of win3.11, win95 and NT registry files, http://home.eunet.no/pnordahl/ntpasswd/WinReg.txt
- Accessdata white papers about registry on [server]\forensics\docs\AccessData\White Papers*registry*.pdf, also on http://accessdata.com/downloads.html [Download Resources]
- Mark Russinovich - "Inside the Registry", http://technet.microsoft.com/en-us/library/cc750583.aspx
- FORENSIC ANALYSIS OF UNALLOCATED SPACE IN WINDOWS REGISTRY HIVE FILES, http://sentinelchicken.com/data/JolantaThomassenDISSERTATION.pdf

Week 4 - Windows registry 2

- ?

Week 5 – File analysis and Reverse Code Engineering

- Executable and Linking Format (ELF) Specification - http://refspecs.freestandards.org/elf/elf.pdf
- Microsoft Portable Executable and Common Object File Format Specification - http://www.microsoft.com/whdc/system/platform/firmware/PECOFF.mspx
- Reverse Engineering Linux ELF Binaries on the x86 Platform - http://www.linuxsa.org.au/meetings/reveng-0.2.pdf
- Reverse Engineering Malware - http://www.zeltser.com/reverse-malware-paper/reverse-malware.pdf
- RCE links and video tutorials about IDA Pro and OllyDbg found in presentation.

Week 6 – GIS and location

- Getting started with GIS at MIT, An exceptional good resource for GIS! Check out the current and previous workshops - http://libraries.mit.edu/gis/teach/index.html
- Windows Sensor and Location Platform - http://www.microsoft.com/whdc/device/sensors/default.mspx

Week 7

- Expert witness presentation and report example (USA)
- IDG.se Positionerings special - http://www.idg.se/2.1085/1.190260/positioneringsspecial
- The books at Stiftelsen Den Nya Välfärden - http://dnv.se/
- www.stoppa-storebror.se - http://stoppastorebror.se/