CFRS 510

CFRES 510: Digital Forensics Analysis
Spring 2016 • Garfinkel

Spring 2016
Wed 7:20-10:00pm
Fairfax Campus
Nguyen Engineering Bld. 4457

Instructor: Simson L. Garfinkel, Ph.D.
E-Mail: sgarfin2@gmu.edu
Phone: 202-649-0029
Office Hours: by appointment

Overview

"Explains computer forensics crime scene procedures, beginning with initial walk-through and evaluation; identification, collection and handling of potential evidence; aspects of working with investigators and attorneys; reverse engineering with file identification and profiling; application of critical thinking in determination of significance of artifacts; and analysis and reporting of evidence."

Learning Outcomes:

At the end of this class, you will be able to:

- Explain the process of digital forensics analysis, from the crime scene, through investigation, to the writing of a report.
- Describe the representation and organization of data and metadata within modern computer systems, from the level of bytes and Unicode characters, through the arrangement of data in files (including document, image, multimedia, database, and archive file formats), to the storage of files in modern file systems.
- Create disk images from physical devices.
- Recover deleted files from disk images.
- Extract metadata and data from files and file systems.
- Read, present, and evaluate information from papers describing digital forensics research in academia and industry.

Materials

Digital Evidence and Computer Crime, 3rd Edition, Eoghan Casey, Academic Press, 2011

Assigned papers

Open source software

Photo Forensics, Hany Farid, MIT Press (selected chapters distributed by professor)

Milestones

Thu Jan 21
First Day of class

Thu Apr 28
Last day of class.
In class presentations.
Projects due.

Prerequisites and Requirements

Students should have a working knowledge the Unix command line. Students should have a laptop with at least 100GB of free disk space, 8GB of RAM, and VMWare Player, Workstation or Fusion. VMWare can run on Mac, Windows and Linux machines and runs best on computers with at least 2 cores and an SSD or 7200RPM hard drive. (An external 7200RPM or SSD connected via USB3 is fine; a USB3 thumb drive is not.)

Students should bring their laptops to class on the first day so that lab work can be started on the computer (data will be handed out on USB sticks). Laptops are also available in the classroom for students who do not have a suitable machine.

Materials and Student Deliverables

Required Readings are due on the date for which they are appear on the syllabus so that they can be discussed in class. Students are responsible for the content of these readings. Other than the textbook, readings will be made available on Blackboard. **This course expects that you will spend 2-3 hours of preparation time for each hour of class time.**

Homework and Problem Sets are assigned in class and due on a specified date. Problem sets must be turned in via Blackboard. Students are encouraged to turn in their homework on time. Late homework will be accepted for up to 1 week at the cost of 1 point per day, unless arrangements to turn in an assignment late have been made in advance..

Each student is expected to make two *Presentations* during this course. 1) Each student will identify, prepare, and present a digital forensics article from the open literature. (Articles should be submitted and approved in advance by the instructor.) 2) Each student will identify and test a publicly available digital forensics tool, such as an open source tool, a demonstration tool, or an appropriate website. Tools should be tested with publicly available data. Dates for student presentations will be proposed early in the course.

Students will be responsible for a *Final Project.*

References and Additional Materials are optional and provided for students that are interested in delving further. Students are not responsible for the content of these materials.

Grading

Homework assignments, individual presentation, mid-term exam, and group presentations will be combined to create the final grade. Students may collaborate on a problem set or presentation, but all group members will receive the same grade, and each group may only collaborate on a single project.

Grading will be consistent with the GMU Graduate Grading Policy[1], with a 100% of all possible credit being equivalent to 4.0 quality points and a grade of A+.

Credit in this course will be apportioned as follows:

Student Deliverable	Assigned	Due	Weight
Problem Set #1: File System Analysis and Deleted File Recovery	Jan 28	Feb 10	10%
Problem Set #2: M57 Email Investigation	Feb 11	Feb 24	10%
Problem Set #3: File Carving and File Analysis	Feb 25	Mar 16	10%
Problem Set #4: bulk_extractor and encryption cracking	Mar 17	Mar 30	10%
Midterm		Mar 31	20%
Proposed dates for two presentations	Jan 21	Jan 27	2%
Presentation #1 — An open source software program	*Jan 27*		4%
Presentation #2 — A digital forensics research paper	*Jan 27*		4%
Final Project Proposals (2)		Apr 1	1%

[1] http://catalog.gmu.edu/content.php?catoid=15&navoid=1172#gradgrading

Student Deliverable	Assigned	Due	Weight
Final Project Group Proposal		Apr 6	1
Final Project Presentation	*Apr 6*	Apr 26	5
Final Project Paper	*Apr 6*	Apr 26	13%
Classroom Participation			10%
Total:			100%

Syllabus and Schedule

Thu Jan 21 — M01: Welcome to CFRS 510 – Digital Forensics Analysis

- Class organization, requirements, and materials
- Foundations of Digital Forensics
- Digital forensics tools, trust, and tool testing.
- Documenting what you have learned
- Challenges facing digital forensic analysis
- Forensic Integrity, Cryptographic Hashing, and Media Wiping.

In Class Lab: Setting up Virtual Box and SIFT; imaging a 512MB USB Drive

Homework: Identify the date and topic for two presentations. Submit online by January 27th.

Optional Reading:

- "Testing the forensic soundness of forensic examination environments on bootable media," Mohamed, Marrington, Iqbal and Baggili, DFRWS 2014.
- "Quality Standards for Digital Forensics," Council of the Inspectors General on Integrity & Efficiency Investigations Committee, Council of the Inspectors General on Integrity and Efficiency, December 2011. https://www.ignet.gov/content/investigations-0
- "Digital Forensics and the Futuristic Scene-of-the-Crime," John Walker, The State of Security (TripWire Blog), May 26, 2015. http://www.tripwire.com/state-of-security/incident-detection/digital-forensics-and-the-futuristic-scene-of-crime/

References:

- Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition, US DOJ.

Wed Jan 27 — Due: Date and Topics for two presentations

Thu Jan 28 — M02: Organization of Data in the Computer

- Review of Casey chapter 1 and 16:
  - Initial walk-through and evaluation
  - Identification of Digital Evidence: Devices; Volatile vs. non-volatile;
- Organization of computer hardware and data storage*
- ASCII, Unicode, and codes

Required Readings:

☐ Casey Chapter 1: Foundations of Digital Forensics Analysis

- ☐ Casey Chapter 16: Applying Forensic Science to Computers
- ☐ Digital Forensics Research: The Next 10 Years, Garfinkel, DFRWS 2010.
- ☐ A Cyber Forensics Needs Analysis, Harichandran, Breitinger, Baggili and Marrington, Computers & Security 57 (2016), 1-13
- ☐ The Unicode Standard: A Technical Introduction, The Unicode Consortium. http://unicode.org/standard/principles.html

Optional Readings:

- Casey Chapter 15: Computer Basics for Digital Investigators
- Some Practical Thoughts Concerning Active Disk Antiforensics and Other Entertaining Stories, Travis Goodspeed, presentation, DFRWS 2014. http://www.dfrws.org/2014/proceedings/presentations/DFRWS2014-keynote2.pdf (presentation, 43 pages)
- Conference d'ouverture [titre à venir], Travis Goodspeed, June 4, 2014. https://www.sstic.org/media/SSTIC2014/SSTIC-actes/ouverture/SSTIC2014-Slides-ouverture-goodspeed_2.pdf (presentation, 51 pages) (lots of overlap with previous presentation)
- Implementation and Implications of a Stealth Hard-Drive Backdoor, Zaddach et al, ACSAC 2013.
- Eric Muller's Unicode Tutorial: http://www.unicode.org/notes/tn23/
- The Absolute Minimum Every Software Developer Absolutely, Positively Must Know About Unicode and Character Sets (No Excuses!), Joel Spolsky, Joel on Software, October 8, 2003. http://www.joelonsoftware.com/articles/Unicode.html

Problem Set #1 Assigned: File System Analysis and Deleted File Recovery. Due February 10th.

Thu Feb 4 — M03: File Systems and File Recovery

- Language of Computer Crime Investigations
- Digital Evidence in the Courtroom
- Drives: HD, USB, SSD, Floppy
- Disk Wiping, Residual, and Remnant Data
- Disk Partitions
- File systems: FAT32 and NTFS (in detail); EXT3 and HFS+ (overview)
- File recovery with The SleuthKit and Autopsy.

Required Readings:

- ☐ Casey Chapter 2: Language of Computer Crime Investigation
- ☐ Casey Chapter 3: Digital Evidence in the Courtroom
- ☐ Casey Chapter 17: Digital Evidence on Windows Systems

Optional Readings:

- Autopsy User Document 3.1, http://sleuthkit.org/autopsy/docs/user-docs/3.1/
- Autopsy 3 Quick Start Guide, June 2013. http://www.sleuthkit.org/autopsy/docs/quick/index.html

Wed Feb 10 — Problem Set #1 Due

Thu Feb 11 — M04: Email

- Review of reading:
    - Conducting digital investigations

    - Handling a digital crime scene
- Email Headers
- Email Bodies: MIME
- Creating a Digital Forensics Experiment

Problem Set 2 Assigned: M57 Email Investigation (Due Feb 24)

Required Readings:

- ☐ Casey Chapter 6: Conducting Digital Investigations (Review)
- ☐ Casey Chapter 7: Handling a Digital Crime Scene (Review)
- ☐ M. Tariq Banday, Technology Corner: Analysing E-Mail Headers for Forensic Investigation, Journal of Digital Forensics, Security and Law, 6:2, 2014.
- ☐ Pasupatheeswaran, Email 'Message-IDs' hepful for forensic analysis? Australian Digital Forensics Conference, 2008

Optional Reading:

- ☐ M. Tariq Banday, Techniques and Tools for Forensic Investigation of E-Mail, International Journal of Network Security & Its Applications, 3:6, Nov. 2011

Thu Feb 18 — M05: Metadata and Timelines

- Review of Reading
- Residual data in GPS Devices
- Metadata in JPEGs
- Datamining with Metadata
- Timeline analysis with SleuthKit

Required Readings:

- ☐ Casey Chapter 10: Violent Crime and Digital Evidence
- ☐ Casey Chapter 11: Digital Evidence as Alibi
- ☐ Garfinkel, S., Parker-Wood, A., Huynh, D., and Migletz, J., A Solution to the Multi-User Carved Data Ascription Problem, IEEE Transactions on Information Forensics & Security, December 2010, pages 868--882.

Optional Reading:

- Alfredo De Santis, Aniello Castiglione, Giuseppe Cattaneo, Giancarlo De Maio, and Mario Ianulardo. 2011. Automated construction of a false digital alibi. In *Proceedings of the IFIP WG 8.4/8.9 international cross domain conference on Availability, reliability and security for business, enterprise and health information systems* (ARES'11), A Min Tjoa, Gerald Quirchmayr, Ilsun You, and Lida Xu (Eds.). Springer-Verlag, Berlin, Heidelberg, 359-373.
- Beyer, Mulazzani et al, "Towards Fully Automated Digital Alibis with Social Interaction,"
- Eric Kee, Micah K. Johnson, Hanry Farid, "Digital Image Authentication from JPEG Headers", IEEE Transactions on Information Forensics and Security, 17 March 2011, pp. 1066-1075

Wed Feb 24 — Problem Set #2 Due

Thu Feb 25 — M06: Files and File Type

- Image Files and Document Files
- File Type Identification
- File Carving

Optional Reading:

- Klaus Knopper, "Rescuing Lost Files with TestDisk and PhotoRec," Linux Magazine, 2016. http://www.linux-magazine.com/Online/Features/Rescuing-Lost-Files-with-TestDisk-and-PhotoRec

Problem Set #3 Assigned: File Carving (Due March 16)

Thu Mar 3 — M07: Time, Registry and Memory

- Time — Where does time come from on the machine? How do we authenticate time?
- Registry analysis with RegRipper
- Memory analysis with Volatility

Assigned Readings:

☐ Casey Chapter 8: Investigative Reconstruction with Digital Evidence

Curated material from the Web:

- "Windows Registry Forensics using 'RegRipper' Command-Line on Linux," INFOSEC Institute, August 16, 2014. http://resources.infosecinstitute.com/registry-forensics-regripper-command-line-linux/
- "INTERPOL's face programme for a safer world," (slides) Mark Branchflower, March 17, 2014.

Thu Mar 10 — No class (Spring Break)

Wed Mar 16 — Problem Set #3 Due

Thu Mar 17 —M08: Analysis with bulk_extractor

- Review: Digital Evidence as Alibi
- Bulk data analysis with bulk_extractor
- Browsers and Browser Artifacts
- KML
- Decoding the browser cache

Required Readings:

☐ "Digital media triage with bulk data analysis and bulk_extractor," Garfinkel, Computers and Security 32:56-72 (2013).
☐ "In Lieu of Swap: Analyzing Compressed RAM in Mac OS X and Linux," Richard and Case, DFRWS 2014

Optional Readings Readings:

Problem Set #4 Assigned: bulk_extractor and encryption cracking (Due March 30)

Thu Mar 24 — M09: Encryption, Steganography, and Password Cracking

- Steganography and application-level encryption
- Hash function construction and cracking.

Required Reading:

☐ John the Ripper Manual, including, "doc" (http://www.openwall.com/john/doc/), INSTALL, OPTIONS, MODES, EXAMPLES, and FAQ,
☐ "John the Ripper Tutorial," Jan-Henk, EthicalHackingCentral, January 22, 2015. http://ethicalhackingcentral.com/tutorials/john-the-ripper-tutorial/

Problem Sets:

☐ Final project proposals due. (Will be returned at the end of the midterm.)

Optional Readings:

- "How a security ninja cracked the password guarding his most valued assets," Dan Goodin, ArsTechnica, Feb 9, 2013. http://arstechnica.com/security/2013/02/how-a-security-ninja-cracked-the-password-guarding-his-most-valued-assets/

Final Project Deliverable #1:

☐ Final Project Proposal — 1 page, Due March 31

Wed Mar 30 — Problem Set #4 Due

Thu Mar 31 — M10: Midterm and Rump Session

Required Readings:

☐ "Privacy Preserving Email-Forensics" Frederik Armknecht, Andreas Dewald and Michael Gruhn, DFRWS 2015.

☐ Final Project Group Proposal — 1-2 pages, Due April 4

Wed Apr 6 — Final Project Proposal Due

Thu Apr 7 —M11: Database Forensics

- MySQL Record Carving
- SQLite3

Required Reading:

☐ Stahlberg, Miklau and Levine, Treats to Privacy in the Forensic Analysis of Database Systems, SIGMOD '07, June 11-14, 2007, Bejing, China

☐ "Database Forensic Analysis through Internal Structure Carving," James Wagner, Alexander Rasin and Jonathan Grier, DFRWS 2015.

Optional Reading:

- InnoDB Database Forensics, Peter Frühwirt and Markus Huber, 24th IEEE International Conference on Advanced Information Networking and Applications (AINA), 2010, April 2010.
- Securing History: Privacy and accountability in database systems, Miklau, Levine and Stahlberg, 3rd Biennial Conference on Innovative Ddata Systems Research (CIDR), January 7-10, 2007, Asilomar, CA.
- Chavan and Khanuja, Database Forensic Analysis Using Log Files, International Conference on Industrial Automation And Computing (ICIAC-12th &13th April 2014)
- Alexander Grebhahn, Martin Schäler, Veit Köppen, Secure Deletion: Towards Tailor-Made Privacy in Database Systems. BTW Workshops 2013: 99-113
- Wit and van Duijn "MySQL Record Carving," February 5, 2014.

Thu Apr 14 — M12: Forensics Analysis at Scale

- Approaches for analysis of massive data
- Forensics in the cloud
- Forensics as a service
- Text Processing
- Cloud Forensics

Required Readings:

- ☐ "Rapid Forensic Imaging with Large Disks with Sifting Collectors," Jonathan Grier and Golden Richard, DFRWS 2015.
- ☐ "Fast contraband detection in large capacity disk drives," Penrose, Buchanan, and Macfarlane, DFRWS EU 2015.

Optional:

- XIRAF—XML-based indexing and querying for digital forensics, W. Alink, R.A.F. Bhoedjang, P.A. Boncz, A.P. de Vries, DFRWS 2006.

Thu Apr 21 — M13: Child Exploitation and Presenting Evidence in the Courtroom

- Analysis and reporting of evidence.

Required Readings:

- ☐ "Misuse of Web Cameras to Manipulate Children within the so-called Webcam Trolling," Kamil Kopecký, Telematics and Informatics, June 2015.
- ☐ Casey Chapter 12: Sex Offenders on the Internet
- ☐ Casey Chapter 14: Cyberstalking

Optional Readings:

- "Hash-Based Carving: Searching media for complete files and file fragments with sector hashing and hashdb," Garfinkel and McCarrin, DFRWS 2015.

Thu Apr 28 — M14: Final Projects

- Presentation of final projects

Note: This schedule is subject to change. If changed, a revised schedule shall appear on the class Blackboard website and will be distributed to students via email.

What's Missing

With only 14 classes this course necessarily leaves some stones unturned. In particular, the following topics will receive minimal treatment in this class; you are expected to learn this material elsewhere if you wish to pursue a career in digital forensics practice or research:

- ⦿ Criminal and civil law that governs digital forensics analysis.
- ⦿ Courtroom testimony and moot court.
- ⦿ Approximate matching (similarity functions)
- ⦿ Authentication of JPEGs and other multimedia files using content

Problem Sets (Labs & Homework)

Problem sets are research-oriented tasks that begin in class and are completed at home. These tasks will typically take between 1 and 4 hours to complete, depending on the skill of the student, and involves the investigation of digital objects provided in class. Students are to submit a PDF file that is structured as a laboratory report clearly indicating what they did and what they discovered. Each report should include the sections: Executive Summary, Apparatus, Procedures, Problem Solving, Conclusions & Recommendations. A standard rubric will be used to grade the lab report.

Late labs will only be accepted in exceptional circumstances.

Online Materials and Communications

All materials will be accessible through Blackboard, and Blackboard will be used to collect all student assignments. All class announcements will be sent through Blackboard. You are responsible for either having announcements delivered to a mailbox that you check, or monitoring Blackboard for information. You can access Blackboard at https://mymasonportal.gmu.edu/.

According to university policy, students and faculty are to use their GMU.EDU email addresses for all course-related communications, as some commercial email systems may be filtered out by the GMU.EDU system.

Attendance Policy

GMU Policy: "Students are expected to attend the class periods of the courses for which they register. In-class participation is important not only to the individual student, but also to the class as a whole. Because class participation may be a factor in grading, instructors may use absence, tardiness, or early departure as de facto evidence of nonparticipation. Students who miss an exam with an acceptable excuse may be penalized according to the individual instructor's grading policy, as stated in the course syllabus." (University Catalog, p. 35)

Students are expected to attend each class, to complete all preparatory work (including assigned reading), and to participate actively in lectures, discussions and exercises. Students should bring laptops to class—some classes may feature pop quizzes for personal assessment. Students are expected to contact the Instructor in advance for planned absences, and after class as soon as possible in the event of a medical or personal emergency. Work-related absences can be accommodated if the Instructor is notified in advance.

Departmental policy requires students to take exams at the scheduled time and place, unless there are truly compelling circumstances supported by appropriate documentation. Except in such circumstances, failure to attend a scheduled exam may result in a grade of zero (0) for that exam.

Academic Integrity and the Honor Code

The Mason Honor Code: Student members of the George Mason University community pledge not to cheat, plagiarize, steal, or lie in matters related to academic work. [2]

Academic integrity on the part of students is an important part of professional performance. The policy for labs, homework, tests and final projects is simple: no assistance may be obtained from any person, by any means including conversation, copying written work, phone conversations, or any electronic communication, unless specifically approved in advance by the instructor. Open book exams include: use of all books, notes, and on-line sources that do not involve interaction with a person.

Accommodations for Disabilities

If you have a documented learning disability or other condition that may affect academic performance you should: 1) make sure this documentation is on file with Office for Disability Services (SUB I, Rm. 2500; 993-2474; http://ods.gmu.edu) to determine the accommodations you need; and 2) talk with me to discuss your accommodation needs.

[2] http://oai.gmu.edu/the-mason-honor-code-2/