CFRS 780 – Summer 2017 Syllabus
Linux Forensics
George Mason University

Administrative Information

Instructor:	David Loveall
Email:	dloveall@gmu.edu
Office hours:	By appointment
Classes:	TR, 19:20 – 22:00, Innovation Hall 317

Course Description

Presents the concepts, tools, and techniques used for forensic collection and analysis of Linux based operating systems and filesystems. Introduces, demonstrates, and discusses current research in the use of the Linux operating system and open source forensic tools, e.g. GNU Core Utilities, The Sleuth Kit, bulk_extractor, as digital forensic tools with emphasis on developing custom functionality from multiple components and extending functionality with Python. Course will consist of exercises conducted in a lab environment with lectures. Active participation of the students is encouraged in the form of discussion, writing papers, and presenting in various research areas associated with Linux Forensics. *Prerequisites: CFRS 500 and CFRS 661 or permission from instructor.*

Required Skills and Hardware / Software

Students are expected to have an understanding of the following items:

- Working knowledge of Linux command line
- A PC that can run virtual machines supporting current Linux releases
- Knowledge and understanding of digital forensics of offline filesystems

Textbooks

Note that these books are available to GMU students for free at the URLs listed.

Title:	*File System Forensic Analysis*
Author:	Brian Carrier
Print ISBN-13:	978-0-32126817-4

URL:	http://proquest.safaribooksonline.com.mutex.gmu.edu/book/networking/forensic-analysis/0321268172

Title:	*Digital Forensics with Open Source Tools*
Authors:	Cory Altheide, Harlan Carvey
Print ISBN-13:	978-1-59749586-8
URL:	http://proquest.safaribooksonline.com.mutex.gmu.edu/book/networking/security/9781597495868

Title:	*Automate the Boring Stuff with Python*
Author:	Al Sweigart
Print ISBN-13:	978-1-59327599-0
URL:	http://proquest.safaribooksonline.com.mutex.gmu.edu/book/programming/python/9781457189906

The following book was used in a previous offering of this class. While no longer required for the course material, it is included below as an optional reference.

Title:	*Wicked Cool Shell Scripts*
Author:	Dave Taylor
Print ISBN-13:	978-1-59327012-4
URL:	http://proquest.safaribooksonline.com.mutex.gmu.edu/book/operating-systems-and-server-administration/unix/1593270127

Topics

Linux filesystem forensics. Open source forensic tools. Developing scripts for forensic tools.

Technology

Because this is a computer classroom, we will frequently be using the internet as a means to enhance our discussions. We will also be using the computers for our in-class lab assignments. Please be respectful of your peers and your instructor and do not engage in activities that are unrelated to the class. Such disruptions show a lack of professionalism.

Goals

This course will present students with the basic tools and techniques used to conduct a forensic analysis of and using a Linux computer. Students will apply industry best practices to

both the collection and subsequent analysis of Linux computers, with an emphasis on hands-on exercises using currently available open-source tools. Development of basic scripts to combine tools into custom solutions will be used as an introduction to programming for the digital forensic examiner.

Participation

Throughout the semester there will be hands on exercises and labs to demonstrate the various tools and techniques covered in class. Students are expected to participate in the exercises. In-class assignments may be used as a factor in the overall grade.

Grading

Grades assigned will be assigned as A (>90%), B (>80%), C (>70%), and F. Grades will be assessed on the following components:

40%	Assignments	(Take home assignments)
30%	Midterm	(Short answer test)
30%	Final	(Paper and presentation)

Assignments

Assignments will be given throughout the course. The material covered will be first discussed in class, and then applied in the homework. Homework may have advanced topics not fully covered in class, but will be discussed in a future class. The advanced problems are for students to go above and beyond. All assignments are due when specified and late submissions will not be accepted.

The midterm will consist of a short answer test regarding the practical use of command line tools. It will be open book / reference, but **the time to complete will be limited**.

The final will consist of a research paper of approximately ten pages and a presentation of approximately 50 minutes on an advanced topic in the field of Linux forensics or open source forensic tools. Topics will be chosen to avoid overlap with other students. The presentations will be given during the second half of the class. Volunteers will be accepted to present first, and following that the presentation dates will be selected by lottery.

Important Dates

Please visit http://registrar.gmu.edu/calendars/ and view important dates for the current semester.

Call 703-993-1000 for recorded information on campus closings (e.g. due to weather).

Attendance Policy

Students are expected to attend each class, to complete any required preparatory work (including assigned reading) and to participate actively in lectures, discussions and exercises. As members of the academic community, all students are expected to contribute regardless of their proficiency with the subject matter.

Students are expected to make prior arrangements with Instructor if they know in advance that they will miss any class and to consult with the Instructor if they miss any class without prior notice.

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.

Communications

Communication on issues relating to the individual student should be conducted using email or telephone. Email is the preferred method – for urgent messages, you should also attempt to contact the Instructor via telephone. Email messages from the Instructor to all class members will be sent to students' GMU email addresses – if you use another email account as your primary address, you should forward your GMU email to that account. Lecture slides are complements to the lecture process, not substitutes for it - access to lecture slides will be provided as a courtesy to students provided acceptable attendance is maintained.

Academic Integrity

GMU is an Honor Code university; please see the Office for Academic Integrity for a full description of the code and the honor committee process. The principle of academic integrity is taken very seriously and violations are treated gravely. What does academic integrity mean in this course? Essentially this: when you are responsible for a task, you will perform that task. When you rely on someone else's work in an aspect of the performance of that task, you will give full credit in the proper, accepted form. Another aspect of academic integrity is the free

play of ideas. Vigorous discussion and debate are encouraged in this course, with the firm expectation that all aspects of the class will be conducted with civility and respect for differing ideas, perspectives, and traditions. When in doubt (of any kind) please ask for guidance and clarification. Students are required to be familiar and comply with the requirements of the GMU Honor Code @ http://oai.gmu.edu/the-mason-honor-code/. All assessable work is to be completed by the individual student. Students must NOT collaborate on the project reports or presentation without explicit prior permission from the Instructor.

Disability Accommodations

If you have a learning or physical difference that may affect your academic work, you will need to furnish appropriate documentation to the Office of Disability Services. If you qualify for accommodation, the ODS staff will give you a form detailing appropriate accommodations for your instructor. In addition to providing your professors with the appropriate form, please take the initiative to discuss accommodation with them at the beginning of the semester and as needed during the term. Because of the range of learning differences, faculty members need to learn from you the most effective ways to assist you. If you have contacted the Office of Disability Services and are waiting to hear from a counselor, please tell me.

Diversity

George Mason University promotes a living and learning environment for outstanding growth and productivity among its students, faculty and staff. Through its curriculum, programs, policies, procedures, services and resources, Mason strives to maintain a quality environment for work, study and personal growth.

An emphasis upon diversity and inclusion throughout the campus community is essential to achieve these goals. Diversity is broadly defined to include such characteristics as, but not limited to, race, ethnicity, gender, religion, age, disability, and sexual orientation. Diversity also entails different viewpoints, philosophies, and perspectives. Attention to these aspects of diversity will help promote a culture of inclusion and belonging, and an environment where diverse opinions, backgrounds and practices have the opportunity to be voiced, heard and respected.

The reflection of Mason's commitment to diversity and inclusion goes beyond policies and procedures to focus on behavior at the individual, group and organizational level. The implementation of this commitment to diversity and inclusion is found in all settings, including individual work units and groups, student organizations and groups, and classroom

settings; it is also found with the delivery of services and activities, including, but not limited to, curriculum, teaching, events, advising, research, service, and community outreach.

Acknowledging that the attainment of diversity and inclusion are dynamic and continuous processes, and that the larger societal setting has an evolving socio-cultural understanding of diversity and inclusion, Mason seeks to continuously improve its environment. To this end, the University promotes continuous monitoring and self-assessment regarding diversity. The aim is to incorporate diversity and inclusion within the philosophies and actions of the individual, group and organization, and to make improvements as needed.

Privacy

Students must use their MasonLive email account to receive important University information, including messages related to this class. See http://masonlive.gmu.edu for more information.

Tentative Schedule and Topics

As this class is an advanced topics class, including recent developments in the area of computer forensics, the class schedule is subject to change based on the need and interest of the class. Background material will be presented in order to better understand these emerging areas and to place them in the context of the overall discipline.

Date		Discussion Topics	Assignment
Week 1	6/6	Introductions, overview of the class. Discussion on topics to be included in course. Linux Live CD presentation.	
Week 2	6/8	Linux / Unix filesystem fundamentals. Bash command line. Compiling software.	Altheide Ch.2
Week 3	6/13	Discussion on final topics. Overview and discussion of various filesystems.	Carrier Ch.14
Week 4	6/15	Filesystem based analysis. The Sleuth Kit. Autopsy.	Altheide Ch.3
Week 5	6/20	Use of Python in digital forensics. Python modules for TSK. NumPy, SciPy.	**Assignment 1**
Week 6	6/22	Filesystem independent analysis. bulk_extractor, tcpflow.	Sweigart Ch.7
Week 7	6/27	Memory analysis. Volatility, Inception.	Sweigart Ch.8
Week 8	6/29	**MIDTERM.**	

Date		Discussion Topics	Assignment
	7/4	**INDEPENDENCE DAY**	
Week 9	7/6	Creating and acceessing disk images. libewf, dd_rescue, dd_rhelp.	Carrier Ch.15
Week 10	7/11	Filesystem unallocated data. ext2/3/4 Data Structures. extundelete.	**Assignment 2**
Week 11	7/13	Final Presentations. Additional topics TBD.	
Week 12	7/18	Final Presentations. Additional topics TBD.	
Week 13	7/20	Final Presentations. Additional topics TBD.	**Assignment 3**
Week 14	7/25	Final Presentations. Additional topics TBD.	
Week 15	7/27	Final Presentations. Additional topics TBD.	**Assignment 4**