*This syllabus is subject to changes and revisions throughout the course.*

**CFRS 773 – 001 – Spring, 2017**
**Advanced Topics - Mobile Application Forensics & Analysis**
**George Mason University**

# Syllabus

## Administrative Information


Instructor: **Tahir Khan**
Email: tkhan9@gmu.edu subject=CFRS 780-MAFA-Your name

Office hours: By appointment
Classes: Thursday, 19:20 – 22:00 – Innovation Hall 317

## Course Description

**CFRS 773-001 - Mobile Application Forensics and Analysis (3:3:0)**
*Prerequisites: CFRS 780 (Forensic Artifact Extraction) and CFRS 660/CFRS 661; working knowledge of computer operating systems (e.g. CS 471 or equivalent), networking or permission from instructor.*
The course will analyze mobile applications and configurations on Android and iPhone platforms in a lab environment. The course goal is to explore what mobile application forensic artifacts are left behind by analysis and inspection of applications on emulated devices.

## Required Skills and Hardware/Software

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

- Working knowledge of TCP/IP and its underlying protocols including
  - Routing and other basic networking knowledge (HTTP, DNS, etc)
- A fundamental understanding of Java or C/C++ or OOP
- Windows / Linux command line knowledge
- Scripting/Programming (Bash, Python, PowerShell/C,C++,.NET)
- Knowledge and understanding of virtual machines and their operation
- A PC that can run VMWare (v10) **AND** VirtualBox (4.3.x) with at least 6GB RAM
- *An old Android Phone (If you have one!)*
- *A jailbroken/old iPhone (If you have one!)*

## Tools used during the course

- Kali Linux
- Genymotion
- Snoop-IT
- Dex2jar
- Baksmali/Smali
- Android SDK
- ApkTool
- JD-gui
- ClassDumpZ
- Sqlite browser
- Burpsuite
- Appuse VM

*This syllabus is subject to changes and revisions throughout the course.*

## Textbook

N/A

## Topics

Mobile application forensics / Mobile application analysis.

## 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 and may affect your participation grade.

## Goals

The goal of this course is to teach students the fundamentals of how mobile applications work and how to identify what artifacts are left behind. Students will learn a variety of methods to disassemble and analyze mobile applications as well as determine forensic artifacts left behind. By the end of this course, students should have the knowledge to analyze mobile applications for simple and intermediate weaknesses, determine if traditional mistakes have been made in application design, and ultimately, what artifacts are left behind.

## 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 are a factor in the overall grade.

## Grading

Grades will be assessed on the following components:

(40%) Assignments (Take home assignments)
(10%) Presentation (A presentation on a mobile forensic analysis tool)
(20%) Midterm (Forensic report and presentation)
(30%) Final (Forensic report and presentation)

*This syllabus is subject to changes and revisions throughout the course.*

## Assignments

Assignments will be given throughout the class. The material covered will be first discussed in class, and then applied in the homework. All programming assignments must be in Python. All assignments are due when specified and late submissions will not be accepted. Students will present their assignments on the day they are due.

## Tool Presentation

Students will choose a tool from a list in blackboard and will create a presentation on how the tool works, the features and a demonstration of the tool in action. See the tool attachment for further details

## Midterm Project

Students will utilize the various skills and techniques learned in class to reverse and analyze mobile applications. The midterm project will consist of analyzing at least two similar public mobile applications and determine any forensic artifacts left behind. A short report and presentation will be the deliverable for the project. See the midterm attachment for further details.

## Final Project

The final project will be similar to the midterm project, students will continue their analysis of the mobile applications, and in addition will find any network forensic artifacts that are left behind, application vulnerabilities and indicators of application use. By understanding the application, and how it works, students will be more prepared to understand what the application does and therefore what it leaves behind. The final report will consist of all information gathered and presented in a paper. The paper should be summarized in a presentation as well. See the final attachment for further details.

## Final Presentation

Each student must present their final paper in a presentation format. Students are expected to know the material they are presenting and to expect a question and answer session. A soft copy of the PowerPoint (.ppt) file must be submitted prior to the presentation.

## Resources

| | |
|---|---|
| Kali Linux | → http://www.kali.org/ |
| Genymotion | → http://www.genymotion.com/ |
| Appuse VM | → https://appsec-labs.com/AppUse |
| Burpsuite | → http://portswigger.net/burp/ |
| ZAP | → https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project |
| ClassDumpZ | → https://code.google.com/p/networkpx/downloads/list |
| Snoop-IT | → https://code.google.com/p/snoop-it/ |
| Virtual Box | → https://www.virtualbox.org/ |
| IDA PRO | → https://www.hex-rays.com/products/ida/support/download_demo.shtml |
| Android SDK | → http://developer.android.com/sdk/index.html |
| HOPPER | → http://www.hopperapp.com/download.html |
| APKs | → http://www.androiddrawer.com/ |
| Virtuous Ten | → http://virtuous-ten-studio.com/downloads/ |

*This syllabus is subject to changes and revisions throughout the course.*

## Schedule

| Lecture | Date | Topic | Reading Assignments | Assignments Info |
|---|---|---|---|---|
| | | | *Read up on HTTP, IP and network protocols and Read Chapter 1*<br>http://net.tutsplus.com/tutorials/tools-and-tips/http-the-protocol-every-web-developer-must-know-part-1/<br>http://www.tutorialspoint.com/http/what_is_http.htm<br>http://www.symantec.com/page.jsp?id=how-ssl-works | |
| Week 1 | 1/26 | Introduction, overview and review of web technologies. Topics such as HTTP/HTTPS, obfuscation and encryption will be visited as well as the top issues facing mobile devices.<br>A brief introduction to python. | Please review and become familiar with Genymotion, the android SDK and AppUse. You should read about the various platforms and understand their basic properties. We will be installing them in the next class.<br><br>*Please download APPUse before next week | |
| Week 2 | 2/2 | Overview of the various mobile analysis platforms. Students will learn the various platforms that are currently in the environment and the pros and cons of each environment.<br>**Android**<br>Configuration of the android mobile testing environment. This week will consist of setting up and verifying the Android testing environments. Overview of the various tools available. | Please become familiar with the tools installed in this class. You should be able to start up your VM, start up Genymotion and start up Burpsuite. | **Tool signup due @ 19:20 EST** |
| Week 3 | 2/9 | Understanding the APK file format. The lecture will consist of the format of the APK file and its various components.<br>Initial analysis on the android platform will occur. Students will install applications from the Google Play store and learn how to copy the application to their VM for analysis. | Please view https://sites.google.com/site/io/inside-the-android-application-framework for next week.<br><br>Please read about bulk_extractor for next week.<br><br>In class lab: Python script to automate application acquisition | **Assignment 1 issued** |
| Week 4 | 2/16 | Students will unpack the APK file and perform simple analysis on the files within. This will consist of extracting actionable information such as web addresses, IP addresses, names, etc. | Use APK: com.aiguo.handydiary-1.apk<br>Use APK: cg.diary-1.apk<br><br>In class lab: Python script to search for actionable information.<br>In class lab: aapt – Searching for package names and rights.<br>In class lab: Using bulk un an unpacked APK | **Midterm topics due @ 19:20EST** |

*This syllabus is subject to changes and revisions throughout the course.*

| | | | | |
|---|---|---|---|---|
| Week 5 | 2/23 | Student presentations of a mobile forensic analysis tool.<br><br>Students will learn how to decode the android APK XML encoding format. This will allow students to further understand the structure of the application. If time allows students will disassemble code modify it and reassemble it. (Part 1) | Please have eclipse downloaded and installed for next week<br>Use APK: com.aiguo.handydiary-1.apk<br>Use APK: cg.diary-1.apk<br><br>In class lab: Creating/Destroying AVDs<br>In class lab: Installing and Uninstall APKs<br>In class lab: Python script to assist in timelining | **Tool PPT due @ 19:20 EST**<br><br>**Assignment 2 issued** |
| Week 6 | 3/2 | Student presentations of Assignment 1: Students will present in alphabetical order by first names.<br><br>Students will learn how to decode the android APK XML encoding format. This will allow students to further understand the structure of the application. If time allows students will disassemble code modify it and reassemble it. (Part 2) | Please read https://code.google.com/p/dex2jar/ and various resources about dex2jar for next week.<br><br>Please have eclipse downloaded and installed for next week<br>Use APK: com.aiguo.handydiary-1.apk<br>Use APK: cg.diary-1.apk<br><br>In class lab: Creating/Destroying AVDs<br>In class lab: Installing and Uninstall APKs<br>In class lab: Python script to assist in timelining | **Assignment 1 due @ 19:20 EST** |
| Week 7 | 3/9 | Students will extract DEX files from the APK and convert them to a JAR file. Students will analyze the jar file in eclipse. This will allow the students to see the program flow and identify and potential weaknesses. | Please read http://developer.android.com/tools/help/logcat.html for next week.<br><br>Use APK: com.aiguo.handydiary-1.apk<br>Use APK: cg.diary-1.apk<br><br>In class lab: Dex2Jar and JDGui/Eclipse<br>In class lab: Identification of weak cryptographic functions<br>In class lab: Searching the jar file for sensitive information | **Assignment 3 issued** |
| NO CLASS | 3/16 | NO CLASS | NO CLASS | **NO CLASS** |
| Week 8 | 3/23 | Student presentation of Assignment 2: Students will present in alphabetical order by last names.<br><br>Students will learn how to view and influencing debugging parameters on the android virtual devices they create. Students will learn how to view the debug logs with the purpose of identifying forensic artifacts. | In class lab: Debugging an application and bypassing a password lock on an application via the Java Debugger<br>In class lab: Debugging an application and changing the expected values via the Java debugger | **Assignment 2 due @ 19:20 EST** |

*This syllabus is subject to changes and revisions throughout the course.*

| | | | | |
|---|---|---|---|---|
| Week 9 | 3/30 | Student presentations of the Midterm: Students will present in alphabetical order by first names. | Please have Burpsuite/ZAP installed for next week and read the tutorials on how to set it up for AVD. You can also look on blackboard for a resource sheet. | **Project 1 due @ 19:20 EST** |
| Week 10 | 4/6 | Android application traffic interception and analysis. The lecture will consist of intercepting and analyzing traffic to and from android applications, with the goal of understanding the functionality of the application. Identification of certificate pinning and countermeasures.<br>Part I – Wireless security threats and threat analysis in mobile environment. | In class lab: Client side Heartbleed<br>In class lab: Bypassing certificate pinning<br>In class lab: Kali (Aircrack-NG, BeEF) | |
| Week 11 | 4/13 | Student presentation of Assignment 3: Students will present in alphabetical order by first names.<br>Part II - Wireless security threats and threat analysis in mobile environment. | Please read several articles on Android based malware for next week<br><br>In class lab: DNS Interception/Modification<br>In class lab: Malicious APKs | **Assignment 3 due @ 19:20 EST** |
| Week 12 | 4/20 | Android Malware – Students will look at current malware trends on the Android platform.<br>Students will learn how to identify various artifacts left behind from mobile applications. Students will be able to determine if applications were ran or not ran based on these artifacts. | Please read about the IPA format and Mach-O format for next week.<br>Please install bitvise SSH (Free version) for next week<br><br>In class lab: Learner Lesson 6<br>In class lab: Identification of application usage. Students will install APKs and identify the files touched/modified as well as artifacts left behind. Then students will create a new VM and install the same applications and log into them. Students will identify forensically interesting artifacts left behind. | |
| Week 13 | 4/27 | **iPhone**<br>Students will learn how to analyze IPA files from iPhones. Students will learn how to dump class information and view the basic layout of the application to determine any potential weaknesses. | In class lab: ClassDump and ObjDump<br>In class lab: iRet and iNalyzer<br>In class lab: Snoop-IT | |
| Week 14 | 5/4 | Student presentations of Assignment 4: Students will present in alphabetical order by first names.<br>iPhone application analysis and file system monitoring and iPhone traffic interception. | In class lab: filemon.iOS<br>In class lab: Dumping iPhone traffic | **Assignment 4 due @ 19:20 EST** |
| Week 15 | 5/11 | Final Presentations | | **Final Due** |

*This syllabus is subject to changes and revisions throughout the course.*

## 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://honorcode.gmu.edu/. 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.

*This syllabus is subject to changes and revisions throughout the course.*

## 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.