Course: CCBC: Mobile Forensics

Cyber Pathways Across Maryland SME Rubric

Reviewer Name: Jeff Hague
Date: 9/23/2018

This course is offered by Community College of Baltimore County (http://www.ccbcmd.edu/Programs-and-Courses/Schools-and-Academic-Departments/School-of-Technology-Art-and-Design/Network-Technology-and-Cybersecurity.aspx). The goal for this review is to validate that the curriculum is complete, current, and relevant to industry cybersecurity needs. Please use the comments sections for each category to explain your overall impressions, whether positive or negative.

COURSE STRUCTURE AND SYLLABUS	Y	N	N/A
Course description is factually complete and accurate	x		
Course structure includes major lessons and assignments	x		
Prerequisite requirements are included and appropriate	x		
Required facilities and equipment are included and appropriate	x		
Required course texts are listed	x		
Appropriate supplementary materials and resources are provided	x		
Course organization and design is clear, coherent, and appropriately structured	x		
Concepts and skills build logically, with appropriate transitions between course sections	x		
Learning outcomes are clearly stated, measurable, and appropriate for the level of the course	x		
Learning outcomes emphasize application of knowledge and skills	x		

Comments about the course structure and syllabus:
Summarize your impressions of the syllabus and course structure including errors, suggestions for revisions, or gaps in the curriculum in regard to industry standards and needs:

READ ME FIRST" doc
In the "READ ME FIRST" doc, a placeholder on page 5 for "CYBERSECURITY DIAGRAM WILL GO HERE; TO BE PROVIDED LATER" is still present. If this is just clip art, it could be removed, but the term "diagram" indicates that this should be present to help illustrate the structure of the course.

The link “Cyber Pathways Across Maryland section of SkillsCommons.org” goes to a page with the message “No data available for this page. ” If this will be populated once all the courses are reviewed, you can ignore this comment.

Good call in limiting the scope of the course to iOS and Android. Windows just doesn't have the market share to be relevant.

Under Learning Objectives, it would also be good call out the relation to mobile apps, not just mobile devices, i.e. How secure app development practices can make data unavailable for forensic retrieval, or poor app development practices can make data very easy to obtain.

In the Course Outline, chapters 3, 4, 5 are skipped. A brief note on why that is would be helpful for students (e.g. focusing on other material given limited time, left as an exercise for the reader, etc.)

The project approach of having teams load and switch devices for analysis is good, as long as there is a consistent way to grade work done for teams both loading data and retrieving data (devices are bound to vary in their level of difficulty).

The textbook listed (*Practical Mobile Forensics* (2nd ed.).) covers up to iOS 9.2 and Android 6, but a later version (3rd edition) covers up to iOS 11 and Android 8. As the major versions increase every year, this can be tough to keep up with, but the later the better (especially on iOS) if the goal is to stay current with the industry.

The iOS security whitepaper should be required reading:
https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf

Syllabus
A fair amount of content overlaps between the “READ ME FIRST” doc and the Syllabus, so comments from the former apply to the latter as well.

In the project section of the syllabus, the named devices specified are tablets. Unless there is a compelling reason to avoid phones, those should be permitted as well.

Under Part 6: College Policies and Resources, there is a list of terms. Should these be linked to the appropriate websites?

LECTURE MATERIALS: INSTRUCTOR SLIDES OR AUDIO/VIDEO PRESENTATIONS	Y	N	N/A
Content is accurate.	x	x	
Materials accurately reflect course content.	x		

Materials are presented in a logical order.	x		
Materials reflect the major learning points and objectives for the related lesson.	x		

Comments about the instructor slides or video presentations:
Summarize your impressions of the instructor slides including errors or suggestions for revisions:

Lesson 1

Slide 9: “Problems with multijurisdictional” is unclear and looks like it was cut off.

Slide 14: The phrase “legal authority” is fairly vague. Specifically mentioning and discussing the 4th amendment would be beneficial in the context of criminal cases. For penetration testing use cases, covering a scope of the test and ownership of the devices, apps and data involved would be beneficial.

Slide 17: The term “TransFlash” is dated. Just “Micro SD” is good.

Slide 18: It is unclear if this is referring to physical biological evidence on the device (e.g. hair, blood, physical fingerprints, etc.) or an electronic representation of a biometric used for device authentication (e.g. Touch ID). That should be made clear. If this is referring to an electronic representation of a biometric, it should be noted that a majority of devices would prevent this.

Slide 44: Spelling out CC = Country Code, NDC = National Destination Code, and SN = Subscriber Number would be helpful.

Lesson 2

Slide 3: This question is unclearly worded: “What information does service provider need to provide the PIN or PUK to an investigator?” Perhaps reword as: “What information does the service provider need to provide to a forensic investigator? (the PIN or PUK?)”

Slide 9: To future-proof the course somewhat, link to iFixit's general teardown page (https://www.ifixit.com/Teardown). If linking to a specific model is still desired, use the latest (iPhone XS and XS Max). The iPhone 6 example used is now 4 years old (a very long time in mobile years).

Slides 13-18: The HFS Plus/HFSX info is a few years old. As of macOS High Sierra and later and iOS 10.3 and later, Apple File System (APFS) became the current file system. The WWDC video and other resources are at https://developer.apple.com/videos/play/wwdc2016/701/

Slide 25: The phrase “Touch ID fingerprint as passcode” would be more accurate as “Touch ID fingerprint authentication”. Also another bullet under that: “Face ID for 3D depth map facial authentication”

Slide 27: The bullet “Limits an app’s access to... network resources, hardware, and more” strays outside sandboxing and into permissions. Either that bullet should be trimmed down to just files, or the title expanded to include permissions.

Slide 35: Include the Pangu jailbreak tool as well for a more complete list (there are also many others). The statement “Jailbreaking iPad is illegal” is incorrect. In 2015, this exemption was granted. See:
https://copyright.gov/1201/2015/fedreg-publicinspectionFR.pdf
http://www.idownloadblog.com/2015/10/27/now-ok-to-jailbreak-ipad/
The 2018 exemptions have not been announced, but existing exemptions are planned to be readopted: https://www.copyright.gov/1201/2018/

Lesson 3

Slides 2-3: Not all answers to the review questions are covered in the previous slide deck. If they are covered in the verbal lecture, please disregard this comment.

Slide 16: Some of these statements are dated. e.g. Cellebrite can extract up to iOS 11: https://www.cellebrite.com/en/services/advanced-extraction-services/

Slides 21-27: These are duplicated from the previous lesson. If this is not intentional, they should be removed. If kept, the comments from the earlier lesson apply.

Slide 28: See previous comment on HFSX being replaced by APFS.

Slide 37: Clarify “Intended to aid user in typing” by expanding to “Intended to aid user in typing via word prediction”

Slide 39: Add a caveat that this location only contains SMS messages, not messages from encrypted chat apps (e.g. WhatsApp, Signal, Telegram)

Lesson 4

General note for all slides with paths: The filesystem locations given can (and often do) change with each iOS version. A note that some navigating would be needed for the particular version being analyzed would be helpful.

Slide 6: Name update needed: From “Mac X” to “MacOS”

Slide 11: “com.apple...” is broken into two lines. It should be continuous on a single line.

Slide 12: “Data of purchase” should be “Date of purchase”

Slide 13: “/private/var/mobile/Library/Caches/com.apple.mobile.installation.plist” is only valid up to iOS 7. Another method would be needed, e.g. https://blog.elcomsoft.com/2017/10/obtaining-detailed-information-about-ios-installed-apps/

Slide 28: Also note the screenshot method for devices without a home button: https://www.imore.com/how-to-screenshot-iphone-x

Slide 29: The URL provided is a dead link.

Lesson 6

Slide 4: The http://faqoid.com link is rather dated. Wikipedia's is maintained up to date: https://en.wikipedia.org/wiki/Android_version_history Market share should link to current stats, e.g.: https://www.statista.com/statistics/266136/global-market-share-held-by-smartphone-operating-systems/

Slide 10: Under User-installed apps, remove the two stores listed (both are pre-installed depending on the device) and list example apps that wouldn't be pre-installed, e.g. Facebook, WhatsApp, Dropbox, etc.

Slide 14: Typo: Change “updates” to “update”.

Slide 19: “...gaining privileged access...” would be more accurate as “...gaining root access...”. A decent comparison to link to: https://www.androidpit.com/jailbreak-android

Slide 22: Clarify that this is the “external SD card” (vs. adopted storage: https://source.android.com/devices/storage/adoptable)

Lesson 7

General note for all slides with paths: The filesystem locations given can (and often do) change with each Android version as well as for each Android OEM. A note that some navigating would be needed for the particular version being analyzed would be helpful.

Slide 4: Name update needed: From “OS X” to “MacOS”

Slide 9: On newer versions of Android, the device may not appear as a drive until authorized to on the device: https://support.google.com/android/answer/9064445?hl=en

Slide 11: Missing words. Change “...and build Number field...” to “...and tap the Build Number field...”

Slide 14: Should this say “shell command” or “pull command” instead of “is command”? Including a link to the adb command reference would be helpful: https://developer.android.com/studio/command-line/adb#issuingcommands

Slide 26: Typo. Change “...data/date/com....” to “...data/data/com....”

Lesson 10

General note for all slides with paths: The filesystem locations given can (and often do) change with each Android version as well as for each Android OEM. A note that some navigating would be needed for the particular version being analyzed would be helpful.

Slide 3: Typo. Update “files systems” to “file systems”.

Slides 8-17: These are duplicated from the previous lesson. If this is not intentional, they should be removed. If kept, the comments from the earlier lesson apply.

Slide 25: This isn't quite accurate: “Owner can choose which applications to back up”. Suggest rewording to “Application developer can choose if the application can be backed up.” See android:allowBackup at https://developer.android.com/guide/topics/manifest/application-element#allowbackup

Slide 26: Missing word. Update ““.ab” file “.tar” file” to ““.ab” file to “.tar” file”

Slide 34: Edit for clarity: “Use the Linux “dd” command”

Slides 44-47: These are duplicated from the previous lesson. If this is not intentional, they should be removed.

Lesson 12

Slide 11: Files are not always on the SD card. Refer to https://faq.whatsapp.com/en/android/30004992/

Slide 21: This is no longer true: “All Android apps written in Java programming language“. Reword to “Android apps are written in either the Java programming language or Kotlin. Kotlin and Java are both compiled into bytecode.” Also, replace “Dalvik Virtual Machine (DVM)” with “Android runtime (ART)”

Slide 22: Replace “Dalvik bytecode” with “Dex bytecode”

Slide 23: Remove the old “Android Market” reference. Google Play replaced this in 2012.

Slide 25: Update “dex2.jar” to “dex2jar”. Also link to https://github.com/pxb1988/dex2jar
Also add “apktool” and link to https://ibotpeaches.github.io/Apktool/documentation/

Slide 26: The article referenced and the bullets are rather dated. Instead mention a few current points:

- Examples of Android malware (2017): https://nakedsecurity.sophos.com/2017/08/24/malware-rains-on-googles-android-oreo-parade/
- Trending of malware families: https://www.statista.com/statistics/494974/android-new-malware-families/
- Google Play Protect for defense: https://security.googleblog.com/2018/05/keeping-2-billion-android-devices-safe.html

Slide 28: Important items to add to the list would be “Root the device” and “Log keystrokes”

Slide 32: Edits for clarity: “a flashlight app does not need read/write access to your SD card data or access to make a call”

STUDENT ACTIVITIES: LABS/EXERCISES/HOMEWORK			
Activities as a whole:	Y	N	N/A
• Contribute to the achievement of the stated course objectives.	x		
• Are comprehensive enough to reinforce course objectives.		x	
• Are current.		x	
Individual activities:	Y	N	N/A
• Have a clearly explained purpose and learning goals.	x		
• Promote the achievement of their stated learning goals.	x		
• Include access to all necessary resources.	x		

Comments about student activities:
Please summarize your impressions of the student activities including errors or suggestions for revisions:

Lab 1: Under the extra activity, a reminder should be added that students may want to review the Privacy Policy at https://www.numberingplans.com/?page=analysis&sub=simnr before entering their own ICCID or IMSI.

Lab 5: The Sony Xperia X10 mini can't be considered a modern device. The lab would be a better exercise if it was against a more modern, popular smartphone such as a recent Samsung Galaxy. For reference:
https://deviceatlas.com/blog/most-popular-smartphones#us
https://deviceatlas.com/blog/most-popular-android-smartphones#us

The other labs didn't name a device or OS version, so this feedback may or may not apply to those.

EXAMS AND ASSESSMENTS	Y	N	N/A
Assessments measure the stated learning objectives.	x		
Assessments are consistent with module activities and resources.		x	
Assessments are varied	x		
Assessments are appropriate to the student work being assessed.	x		

Comments about exams and assessments:
Please summarize your impressions of the assessments and any suggestions including errors or suggestions for revisions:

Mid-Term Exam

The exam only tests knowledge of iOS regarding application data discovery, not any of the SIM card material.

Final Exam

Step 1: XRY, Blacklight and Cellebrite are each listed twice.

Question 23 is unclearly worded.

Working with an iPhone 5 image is technically valid, but is rather dated. A newer device should be chosen.

The exam only tests knowledge of iOS, not of Android.

Overall Summary:
Based on your expertise and knowledge of the course, please write a summary of your overall impressions, the strengths of the material, and your recommendations for future iterations. Please keep in mind suggestions for revisions or gaps in the curriculum in regard to industry standards and needs. If your course is meant to prepare students for a certification exam, please indicate whether or not you feel the course will do so.

The course seems geared toward law enforcement investigations, but careers that use these skills for penetration testing (or similar assessments) or mobile application security/defense are important to mention as well.

Some related topics are notably absent:

- IMSI catchers and their use (pros, cons, legal issues, etc.) would be worth a slide somewhere, likely in Lesson 1.
- The role of OS vulnerabilities in the context of malware and insecure mobile usage is worth citing some examples, e.g. goto fail (2014), Stagefright (2015), Pegasus malware/Trident vulnerabilities (2016), etc.
- Secure hardware should be included in the list of challenges to forensic examination, i.e. iOS' Secure Enclave and the Secure Element/Trusted Execution Environment (TEE) on Android.
- Reverse engineering Android apps is covered, but reverse engineering iOS apps is not. Tools like Cycript, class-dump, Hopper, etc. should be covered.
- For continued learning after the course, it should be noted that:
    - Forums can be a helpful reference, e.g. https://forum.xda-developers.com
    - Staying current with operating system changes and threat developments is needed. Events like WWDC and Google I/O and ongoing news media reports of threats, malware, operating system vulnerabilities, etc. are a must to consume.

Overall, this is a good exposure to mobile forensics and should start students off with a technical framework on which to build experience. For the portions of material that touch on legal concepts and procedures, a reviewer with law enforcement experience should evaluate the material presented there.