Your name: ______________________________ Your UPI: _________

Quiz #1 for CompSci 725, S2 2019

Quoting from the introduction of Quick (2014): “It is is important to have a rigorous methodology and set of procedures for conducting digital forensic investigations and examinations that are also flexible enough to be able to work with future providers offering new cloud storage services.”

Discuss: does this article provide its reader with a “rigorous methodology” and a “set of procedures”? Please write two or three sentences in the space below. Your goal is to convince your marker that you have read this article before arriving in class today.

Your name: _____________________________ Your UPI: _________

Quiz #2 for CompSci 725, S2 2019

Quoting from the conclusion of De Bock (2016): “A major additional advantage of the proposed tool is that the carving search space is considered both an input and an output parameter of the tool.”

Discuss: do you agree with the authors’ assertion that this is a major advantage? Please write two or three sentences in the space below. Your goal is to convince your marker that you have read this article before arriving in class today.

Your name: _____________________________ Your UPI: _________

Quiz #3 for CompSci 725, S2 2019

Quoting from the introduction of Oriwoh (2013): "Digital forensics is a field that deals with the investigation of technology-related crimes. These crimes cover those perpetrated against, using or perpetrated through technology. With the IoT, a key addition would be crimes perpetrated by and originating solely from technology."

Compare and contrast the definition of digital forensics in Oriwoh (2013) with the definition of digital forensics presented in the lecture slides for CompSci 725.

Please write two or three sentences in the space below. You will get a mark on this quiz if your answer convinces your marker that you have read this article before arriving in class today, *or* if your answer convinces your marker that you have been keeping up with the lectures in this course and are able to integrate the knowledge you derive from disparate sources.

Your name: ____________________________ Your UPI: _________

Quiz #4 for CompSci 725, S2 2019

Write two or three sentences, explaining which of the following possibilities is the most accurate description of how Ahmad (2018) validated their prototype of a Virtual Machine Forensic Artefact Collector (VMFAC):

1. Evidence from VMFAC was accepted into a courtroom proceedings.
2. Evidence from VMFAC assisted a forensic investigation of an incident which involved the criminal use of a VM.
3. VMFAC was tested against a benchmark set of forensic cases.
4. VMFAC produced a report whose validity and utility were confirmed by an independent forensic expert.
5. VMFAC produced a report with plausible validity and utility.
6. VMFAC produced a report which did not convince you of its validity or utility.
7. None of the above.

You will get a mark on this quiz if your answer convinces your marker that you have read this article before arriving in class today.

Your name: ______________________________ Your UPI: _________

Quiz #5 for CompSci 725, S2 2019

Recall that Li (2019) distinguishes three types of IoT-related crimes:

1. "IoT device as a target (e.g. cyberattacks where vulnerabilities in IoT devices are exploited)…
2. "IoT device as a tool… For example, a compromised IoT device [has] been used to facilitate other malicious activities such as a botnet attack…
3. "IoT device as a witness (e.g. data stored in the IoT device can directly implicate an individual accused of a crime)…"

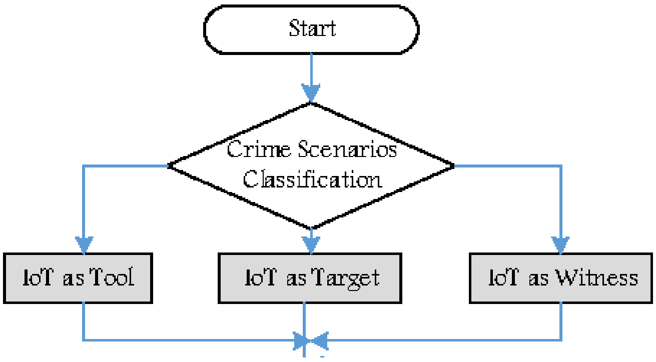

Figure 1. Initial step in an IoT forensic investigation, from Figure 2 of Li (2019).

Now recall the forensic investigation described in Domingues (2016). In this investigation, was the Windows 10 device being examined for evidence that it had been a criminal's target, that it had been a tool used for criminal intent, or that it had been a witness in a crime scene? Discuss briefly.

You will receive full marks if your answer persuades your marker that you are able to use the terminology and concepts from one article (Li 2019) in an accurate and understandable discussion of an aspect of another article (Domingues 2016).

Your name: ______________________________ Your UPI: _________

Quiz #6 for CompSci 725, S2 2019

Briefly discuss the privacy threat being addressed in “e-PRNU: Encrypted Domain PRNU-Based Camera Attribution for Preserving Privacy” (Mohanty 2019).

You will get a mark on this quiz if you describe the threat understandably, concisely, and accurately, using at least two of the following words: confidentiality, integrity, availability, interception, interruption, modification, fabrication, stegocommunication, repudiation.

Your name: ____________________________ Your UPI: _________

Quiz #7 for CompSci 725, S2 2019

You are being interviewed for an entry-level position as a security analyst. Your interviewer has no technical skill whatsoever, and is only able to provide you with the information below. They will collect your written answer within 10 minutes. (Good luck and best wishes in your interview!)

Scenario: You have been asked to provide technical advice, in writing, on the first step in a proposed process for deleting video surveillance recordings.

Goal of the proposed process: To decrease the expense of storing video recordings, by automatically deleting recordings which are highly unlikely to be of forensic relevance in any future investigation. The process should err on the side of retention rather than deletion, because the cost of retaining a videotape is very small in comparison to the value of relevant forensic evidence.

Retention rule: A videotape segment should be retained if it was recorded within the last 24 hours, if it shows a person's face, or if it was recorded within 30 minutes of a person's face being shown to any video camera within a 10 metre distance.

First step of the proposed process: Identify frames of video that contain a cluster of pixels which might (upon further processing) be found to represent a recognisable human face.

Advice required: Which of the methods listed in Table 1 below is most worthy of further investigation, to confirm that it is an appropriate skin-tone recognition method for the proposed process? Your advice should include a brief discussion of: 1) the reason why you selected this method, and 2) ***one*** important reason why further investigation of your selected method would be appropriate, before the design of the proposed process is finalised. You should ***not comment*** on the scenario, the goal, the retention rule, or the proposed process after its first step.

Table 1. Results of skin detection using different methods, from Al Mohair (2015).

	Recall (***R***, %)	Precision (***P***, %)	***F1*** (%)
Method of Al Mohair (2015)	88.00	87.65	87.82
MLP ANN + dynamic threshold [35]	85.51	79.32	82.30
Explicit rules (YCbCr + YUV) [9]	91.16	41.71	57.24
Explicit rules (RGB + YUV) [9]	89.62	59.12	71.25
ANN (RGB + texture) [17]	81.26	77.31	79.23
Bayesian network (YCbCr) [48]	62.87	41.28	49.83
Bayesian network (YIQ + texture)	85.79	50.82	63.83

Note: Recall ***R*** is the number of accurate decisions (***TP***) divided by the total number of forensically-relevant videotape segments (***TP*** + ***FN***). Precision ***P*** is the number of accurate decisions (***TP***) divided by the total number of retained videotapes (***TP*** + ***FP***). ***F1*** is the arithmetic mean of recall ***R*** and precision ***P***.

You will get a mark on this quiz if your response shows an ability to provide advice on the design of a secure system, in which you demonstrate a level of professional expertise which might reasonably be expected of a newly-hired security analyst.