Assessing Knowledge and Skills in Forensics with Alternative Assessment Pathways

Joseph Maguire
School of Computing Science
University of Glasgow
Glasgow, Scotland, United Kingdom
joseph.maguire@glasgow.ac.uk

ABSTRACT

Designing assessment for courses in computer science which are interdisciplinary by nature can be challenging. Challenging in making them interdisciplinary but also relevant within computing science. This paper presents the design and delivery of such an assessment for postgraduates in digital forensics that utilises assessment choice. Student teams were allowed to create either a program which implemented steganography or a report on the feasibility of such a tool being used to exfiltrate data by a whistle-blower in a fictional company. This paper reports on student feedback of this approach and provides a discussion on the benefits and concerns of utilising such an approach.

CCS CONCEPTS

• **Security and privacy**; • **Applied computing** → **Computer forensics**; **Education**;

KEYWORDS

forensics, assessment design

ACM Reference Format:
Joseph Maguire. 2022. Assessing Knowledge and Skills in Forensics with Alternative Assessment Pathways. In *Computing Education Practice 2022 (CEP 2022), January 6, 2022, Durham, United Kingdom.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3498343.3498351

1 INTRODUCTION

The general consensus among professionals, governments and educators is forensics from a cyber security perspective is interdisciplinary in nature [14]. Forensics contains concepts not just from computing science, but mathematics and law. Irons et al. argues that not only is forensics interdisciplinary, but is also a balance of skills [10]. Taylor et al. argues that this interdisciplinary content is a key component of high-quality forensic courses delivered by computing science departments [15]. Moreover, Govan argues that more emphasis should be placed on articulation of knowledge and findings as communication is central to forensics [7].

The application of one-way hash functions in the context of forensics is one such example, individuals not only need to comprehend the core conceptual elements, but also appreciate the interplay of ethical and legal concerns. Moreover, individuals may be required to articulate such knowledge in a manner accessible to a judge and jury.

Reflecting the interdisciplinary nature of forensics presents a distinct challenge to computing science educators in terms of devising effective assessments. The primary concern being that some students may perceive any assignment in computing science without programming as not authentic. Moreover, arguably, senior computing science students are likely to be more experienced at programming, than say academic writing.Consequently, an assignment that does not utilise programming could put *some* students at a disadvantage.

An alternative solution could be to utilise assessment choice, where students are able to select their own assessment pathway. In such a scenario, students could opt for a programming or non-programming route. Consequently, the contributions of this paper are:

- Assessment design for a digital forensics course that utilises assessment choice.
- Report preliminary results and feedback from students on the assessment.

2 BACKGROUND

Daniels et al. argues that while assessment is a crucial component of almost all learning designs, educators often become complacent about the value and purpose of it [5]. The concern is that educators largely rely on the same type of assessment design. Typically this includes assessment designs that educators have experienced as students as well as those that they have delivered successfully in the past. Such assessment designs are often chosen over exploring alternative assessment approaches [5].

Consequently, for forensics in computing science this could result in assessments that focus on programming and do not necessarily reflect the interdisciplinary nature of the topic. An assessment design that could result in students focusing on getting programmatic solutions working, rather than grasping the core theoretical concepts pertinent to forensics.

Cutts et al. argue that students in computing science often focus on technical concerns, such as getting a program working, rather than appreciating the underlying crucial concepts [4]. Cutts et al. go on to argue that getting students to focus on theoretical concepts, rather than compilation errors, reduces the temptation of students to randomly guess answers and compile programs to simply get them working. Similarly, Kim et al. demonstrated that paper and pen programming exercises are not only effective in improving logical

CEP 2022, January 6, 2022, Durham, United Kingdom

thinking, but are also effective in sustaining interest in learning computing science topics [12].

Kim et al. assigned 110 non-majors of computing science students either into a programming group or non-programming group that complete pen and paper exercises. Kim et al. report that performance was similar across both groups, but that students completing paper and pen exercises appeared to focus more on theoretical concepts. Similarly, Bell et al. report on the effective use of paper and pen exercises as well as other activities to drive the outreach and interest in computing science [1].

In examining cyber security assessment more specifically, Weiss et al. state that when monitoring the approaches used by individuals to complete cyber security assignments students used a variety of tactics that were often not predicted [16]. Weiss et al. also raise concerns that students focus on completing the assignment rather than considering core concepts. Consequently, a strong assessment for forensics may introduce assessment tasks that engage students in considering conceptual elements rather just getting a solution working.

Craddock and Mathias report on the novel use of assessment choice in a health skills course that may be relevant in the context of computing science [3]. Craddock and Mathias state some students would regularly fail the exam and perform poorly on the resit paper. Consequently, the course was redesigned to offer students the choice between two different types of assessment. The *first* choice or route was a closed book two hour examination where students were notified about a research scenario 14 days in advance. Students were then asked questions that probed relevant knowledge and skills. The *second* assessment route expected students to produce a 2,500 word report that outlined the design of a research study to tackle a specific question.

In total, 40 students enrolled on the course, 18 opted for the closed-book exam and 22 opted for the large coursework. Craddock and Mathias report that upon further analysis neither route was specifically advantageous with students performing roughly the same. Craddock and Mathias conducted a focus group after the assessment and feedback was largely positive with one student stating "*You know your strengths and weaknesses so when you are given an option you choose the one you think you will perform better in … so if you are not given the option you are not given the choice*".

Similarly, Hall explored the use of assessment choice in an economics course and the feedback from students about the experience was largely positive [8]. Hall stated that when students were given a choice in assessments, they typically favoured their strengths rather than their weaknesses, i.e. students did not select an assessment type based on the skill they wanted to learn or hone but rather one they felt experienced in. However, Hall cautioned that such a tactic was problematic when the assessment choice made by the student was not confirmed by the assessment, i.e. performance demonstrated by the student on the assessment was poor.

In contrast to Craddock and Mathias as well as Hall, Wood and Smith note that offering choice in assessment does not need to take the form of offering different assessment routes [17]. Wood and Smith suggest choice could be offered across a number of different dimensions, such as different timings, whether work is completed in groups or different styles, whether students could give a presentation or write an essay. Wood and Smith argue that the biggest concern with assessment choice is that it should not be a "free for all" where every student effectively passes, but an effective approach that engages students.

Having said that, assessment choice appears to have benefits and is generally well received by students in terms of positive feedback. However, designing and delivering assessment choice is not without challenge. Irwin and Hepplestone state there are many challenges around offering assessment choice, such as gaining approval from other academics and ensuring assessment validity [11].

Given that educators favour known and established assessment designs, gaining approval from other academics for novel assessment designs may be challenging. Henderson intended to offer assessment choice to support interdisciplinary students [9] on a data ethics course. Students with sufficient technical skills would have been offered an assessment that involved machine learning, while students with a non-technical background could complete a design study. However, the approach was ultimately discarded as it could not obtain sufficient approval to be delivered. Craddock and Mathias highlight similar challenges, but argue they were able to overcome such concerns through closely working with external examiners [3].

There is also the concern of the importance of some skills and knowledge to disciplines and degree programmes. Irwin and Hepplestone argue that if assessment choice was a regular occurrence within a degree programme, it may afford students an opportunity to avoid particular skills. Such skills may be essential for a student to qualify with the degree. This suggests that an effective assessment design may need to consider where assessment choices are suitable, and how such assessments are spread across degree programmes to ensure students are effectively assessed [11].

Nevertheless, assessment choice does appear a potential solution to offer assessments that can reflect the interdisciplinary nature of forensics while also supporting student strengths without reducing authenticity for some students.

3 CONTEXT

The assessment incorporating choice was delivered as part of a forensic taught Masters course in a research-led institution. The course covered several subject areas: anti-forensics, authentication of evidence, digital investigation models, regulatory and legal concerns, social and ethical concerns and tools. The 10-week course is offered in the second semester of the academic year and had a cohort of approximately 45 students. The course is accessible to senior undergraduate and postgraduate students enrolled on computing science, software engineering and specialist security degree programmes. The course was also accessible to postgraduate students enrolled on programmes from other disciplines, including law, politics and business. Consequently, prior computing science knowledge and skills varied widely between enrolled students.

4 ASSESSMENT DESIGN

The assessment was weighted at 20% of the overall course grade and was a team task. Teams were self-organising and could comprise of no more than three team members. Teams had the duration of the course, i.e. 10 weeks, to complete and submit the assignment. The assessment focused on a theoretically relevant but practically

challenging subject area of forensics as to stimulate interest and motivation among teams. Anti-forensics or countermeasures against forensic analysis was selected as the assessment area of focus as it was perceived as a timely and relevant area of interest for forensic practitioners [2, 13].

4.1 Scenario

Teams were presented with a fictional scenario where a former software engineer is accused of smuggling data out of a financial organisation through images on removable media for personal benefit. The financial organisation claims the software engineer used anti-forensic tactics to avoid detection.

4.2 Task

The financial organisation has recruited and authorised the student team to investigate the situation and report whether the software engineer performed such acts as well as identify any legal, social and ethical concerns.

English argues that video presentations can be an effective approach to support students in assessing student attainment of theoretical concepts [6]. Consequently, the primary deliverable of the assessment is a 10-minute video presentation explaining anti-forensic techniques and argue whether or not the former software engineer *could* and *would* have indeed exfiltrated data in the way claimed by the organisation. Teams are required to frame the presentation as if they are speaking to a non-specialised jury, i.e. the audience is not technically minded. The approach of using video presentations would also afford students the opportunity to refine their communication skills. An especially relevant skill in the context of the course as students may need to communicate findings to a judge and jury.

Teams were also required to research and identify potential legal defences the former employee may suggest for his suspected behaviour. The expectation is that students will investigate specific laws around whistle-blowing and Freedom of Information.

Asides from the presentation, teams were also required to provide additional supplementary material or artefacts to support the presentation. The required material was dependent on the assessment choice or route opted for by the team.

4.3 Routes

In terms of structure, the assessment offered teams to opt for one of two routes: the *Programming route* or the *Non-programming route*.

4.3.1 Programming route. The programming route required teams to construct a "light-weight" Java application that a software engineer could realistically construct rapidly without using any third-party or specialised libraries. The solution had to utilise anti-forensic techniques to exfiltrate data out of the organisation without detection as a demonstration of the possible actions taken by the software engineer. The expectation is that teams would implement steganography techniques to embed data in vessel images, as the topic is covered in the course.

4.3.2 Non-programming route. The non-programming route required students to produce a six-page research report that investigated at least four possible approaches to exfiltrate data out of the organisation while avoiding or hampering subsequent forensics analysis. Teams were expected to critically consider research literature as well as existing systems and tools.

4.4 Marking Scheme

The marking scheme comprised of eight criteria: Problem Recognition, Content Coverage, Intellectual Input, Rationality of Argument, Use of Visual Aids, Clarity of Speech, Written Quality and Team Performance. The criteria is the same across both routes with teams given guidance on how to fulfil criteria for their given route. For example, Content Coverage for the programming route requires thorough consideration of key steganography steps in source code and for the non-programming route it requires deep consideration of various areas of research into anti-forensics.

Team performance is recognised with grades and bands across a standard university-wide 22-point scale, the scale represents 8 grades (A through H) and each grade has a descriptor, for example Grade B is "very good" while Grade C is "good". There also various bands within each grade. The bands are used to be more precise within the grade, so for example B1 is a high B grade while a B3 is a low B grade. Lastly, each band has a weight on the scale, for example A1 is 22 out of 22, B1 is 17 out of 22 and C1 is 14 out of 22.

Teams were also provided the opportunity to provide a public *workload record* that all team members could observe as part of the final submission. The workload record detailed the contribution of each team member. Individual team members were also offered the opportunity to submit a private personal assessment of contribution for each team member via the course virtual learning environment (VLE), allocating points to individual members to indicate contribution. Teams were advised that the workload record and personal assessment of contribution would be used to inform the individual grade of team members.

5 DELIVERY

Teams were self-organising and comprised of three team members. Teams were given two weeks to confirm their route and members via the course VLE. Teams were permitted to change route at any point during the assessment. Students that were not able to self-organise into a team were advise they would be randomly allocated to a team and they would have to agree a route.

The assessment design required teams to have access to systems to produce a Java program as well as resources for teams to conduct research into anti-forensics, i.e. Internet systems, access to academic papers etc. Teams also required access to software which allowed them to produce a video recording of their presentation.

6 EXPERIENCE

15 teams completed the assessment, 11 teams opted for the non-programming route and four teams opted for the programming route. Teams were awarded a grade for overall performance, ranging between A to H. There was no significant difference in the overall grade awarded between routes, although it should be noted few teams opted for the programming route. However, performance did differ noticeably for some of the criteria in the marking scheme, outlined in §4.4. Those teams that adopted the programming route

typically demonstrated a stronger performance when considering key concepts, while non-programming teams demonstrated a stronger performance in the presentation component.

In terms of feedback, 27 students completed feedback questions on the assessment, after they had completed the assessment, but before they had received their grade. Feedback from a specific individual is connected to a feedback identification number, e.g. "F54". Students were initially asked why they had selected a particular route. The common theme from those in non-programming groups was that they felt they were not sufficiently skilled or lacked confidence in programming, F26 stated "*the reason is that we felt we could do a better job on it than on the programming approach*". Similarly, F27 stated "*I felt we - in particular myself - lacked the ability to do the programming route well. The non-programming route seemed like it would take less time*". However, some students stated that they selected the non-programming route, despite being sufficiently skilled in programming, as they felt it was more manageable, F10 stated "*Already had so much coursework and dissertation work to do. Non-programming seemed like less work as we wouldn't have to worry about chasing and fixing bugs. It felt more manageable given everything else*".

A common theme for those in the programming route was that they wanted to focus on something practical, F23 stated "*I think* [it] *is more interesting to do practical work than theoretical. It was a challenge for us*" while F18 stated "*Less writing and more of practical application*". However, some students felt it would give them a deeper insight into the problem, F21 stated "*We thought it would give us a better understanding of the case although we originally thought about doing the non-programming approach since two of us didn't feel quite as confident about the actual programming.*"

Students were also asked if they perceived any advantage in the use of assessment choice. A theme that emerged from both routes was that choice allowed students to lean on their strengths, F30 stated "*Great for people with different strengths. Programming or research*", F31 stated "*You get the choice to produce your best piece of coursework*" and F10 stated "*Gives people the ability to choose what they think will work best for them or what they would find more interesting or manageable*". However, there were also some students on the programming route that felt the use of choice accommodated those with weak writing skills, F20 stated "*I think the strengths are that people with more limited knowledge of the English language can do the programming assignment which is something that requires less writing*".

Students were also asked how they felt the assessment could be improved in the future. A common theme across all students was that they wanted more routes, F19 stated "*More alternatives rather having only two routes.*" and F14 reflected many students by stating "*more routes*". Students were generally positive about the existing routes, F20 stated "*It was really interesting I think it was one of the best programming assessments I had in the university. I don't see any improvement*".

Lastly, students were asked if the approach should be used in the future. F30 represents the thoughts of almost all students with the response "*Absolutely!*" F30 stated "*Yes. More [exercises] should be assessed like this*" and F12 stated "*of course, it gives us the freedom to choose*". Similarly, many students felt the approach was inclusive, F10 stated "*Yes! As not everyone taking this course is a computer science student the multi-route approach allows people to play to their strengths*".

7 CONCLUSION

There are many challenges in devising effective assessment design. The difficulty only increases when computing educators have diverse cohorts and they can not necessarily rely on all students possessing the same level of skill. In future, an alternative approach could be to offer more choice across multiple dimensions, as suggested by [17]. This could be decomposing aspects of the assessment further so that students could potentially explore some programming and more writing or more programming and less writing, rather than the binary choice that currently exists in many present assessment designs.

REFERENCES

[1] Tim Bell, Jason Alexander, Isaac Freeman, and Mick Grimley. 2009. Computer science unplugged: School students doing real computing without computers. *The New Zealand Journal of Applied Computing and Information Technology* 13, 1 (2009), 20–29.

[2] Peter Cooper, Gail T Finley, and Petteri Kaskenpalo. 2010. Towards standards in digital forensics education. In *Proceedings of the 2010 ITiCSE working group reports*. ACM, 87–95.

[3] Deborah Craddock and Haydn Mathias. 2009. Assessment options in higher education. *Assessment & Evaluation in Higher Education* 34, 2 (2009), 127–140.

[4] Quintin Cutts, Matthew Barr, Mireilla Bikanga Ada, Peter Donaldson, Steve Draper, Jack Parkinson, Jeremy Singer, and Lovisa Sundin. 2019. Experience Report: Thinkathon–Countering an" I Got It Working" Mentality with Pencil-and-Paper Exercises. In *Proceedings of the 2019 ACM Conference on Innovation and Technology in Computer Science Education*. ACM, 203–209.

[5] Mats Daniels, Anders Berglund, Arnold Pears, and Sally Fincher. 2004. Five myths of assessment. In *Proceedings of the Sixth Australasian Conference on Computing Education-Volume 30*. Australian Computer Society, Inc., 57–61.

[6] Rosanne English. 2019. Designing computer security assessments to reduce plagiarism. In *Proceedings of the 3rd Conference on Computing Education Practice*. ACM, 7.

[7] Michelle Govan. 2016. The application of peer teaching in digital forensics education. *Higher Education Pedagogies* 1, 1 (2016), 57–63.

[8] Chris Hall. 1982. Giving more choice to students in economic education; results and evaluation. *The Journal of Economic Education* 13, 1 (1982), 19–31.

[9] Tristan Henderson. 2019. Teaching Data Ethics: We're going to ethics the heck out of this. In *Proceedings of the 3rd Conference on Computing Education Practice*. ACM, 4.

[10] Alaisdair D Irons, Paul Stephens, and R Ian Ferguson. 2009. Digital Investigation as a distinct discipline: A pedagogic perspective. *Digital Investigation* 6, 1-2 (2009), 82–90.

[11] Brian Irwin and Stuart Hepplestone. 2012. Examining increased flexibility in assessment formats. *Assessment & Evaluation in Higher Education* 37, 7 (2012), 773–785.

[12] Byeongsu Kim, Taehun Kim, and Jonghoon Kim. 2013. and-Pencil Programming Strategy toward Computational Thinking for Non-Majors: Design Your Solution. *Journal of Educational Computing Research* 49, 4 (2013), 437–459.

[13] Laoise Luciano, Ibrahim Baggili, Mateusz Topor, Peter Casey, and Frank Breitinger. 2018. Digital Forensics in the Next Five Years. In *Proceedings of the 13th International Conference on Availability, Reliability and Security*. ACM, 46.

[14] Andrew McGettrick. 2013. Toward effective cybersecurity education. *IEEE Security & Privacy* 11, 6 (2013), 66–68.

[15] Carol Taylor, Barbara Endicott-Popovsky, and Amelia Phillips. 2007. Forensics education: Assessment and measures of excellence. In *Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'07)*. IEEE, 155–165.

[16] Richard Weiss, Michael E Locasto, and Jens Mache. 2016. A reflective approach to assessing student performance in cybersecurity exercises. In *Proceedings of the 47th ACM Technical Symposium on Computing Science Education*. ACM, 597–602.

[17] Leigh N Wood and Geoffrey H Smith. 1999. Flexible assessment. *The Challenge of diversity* (1999), 154–158.