Forensic Science International: Digital Investigation 45 (2023) 301566

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi

DFRWS 2023 USA - Proceedings of the Twenty Third Annual DFRWS Conference

Expanding digital forensics education with artifact curation and scalable, accessible exercises via the Artifact Genome Project

Cinthya Grajeda [a, *], Jessica Berrios [a], Sankofa Benzo [a], Emmanuel Ogunwobi [a], Ibrahim Baggili [b]

[a] Samuel S. Bergami Jr. Cybersecurity Center, Connecticut Institute of Technology, University of New Haven, 300 Boston Post Rd., West Haven, CT, 06516, USA
[b] Baggil(i) Truth (BiT) Lab, Center for Computation & Technology, School of Electrical Engineering & Computer Science, Louisiana State University, USA

ARTICLE INFO

Article history:

Keywords:
Artifacts
Education
Forensics
Cybersecurity
Modules
Challenges
Training
Learn

ABSTRACT

Digital Forensics (DF) is a multidisciplinary domain that involves computing, law, criminology and other disciplines. At the core of the domain, however, is the Acquisition, Authentication and Analysis (AAA) of digital evidence. In the real world, practitioners typically find data of forensic value in DF artifacts. While this is true, educational programs and resources have not kept up with DF artifacts - which are the cornerstone of real-world investigations. Our work transforms and expands DF education by focusing the community's attention to artifacts. By leveraging our past work on the Artifact Genome Project (AGP), we expanded the platform to house educational modules that can be created and taken by any user or organization that has been vetted and met our standards to do so. Hundreds of curated DF artifacts have been added to the platform, and along with other educational resources, they have been employed to design scalable, self-paced, open, online DF educational modules. Our work was tested and put into practice in real-world scenarios around the world. This includes using the AGP platform to host the first DF challenge at the 2020 Interpol Digital Forensics Expert Group (DFEG) Conference and the 2021 DFRWS APAC Conference's annual Forensics Rodeo. Furthermore, we implemented the platform in DF courses at our own university. Feedback from these experiences was collected through surveys and in summary, the results show that there is a need for these type of educational resources in our community. While we observed that some improvements needed to be made either in the materials or platform, overall, participants benefited from the experience regardless of having zero to many years practicing on the field.

1. Introduction

Digital Forensics (DF) is a multidisciplinary domain that continues to advance. As DF investigators, researchers, educators and other stakeholders in the field adapt to ever evolving technologies, academia has struggled to prepare students to enter the field after graduation (McCullough et al., 2021).

One of the major challenges instructors face in DF education is the vast amount of artifacts generated by different technologies. A digital artifact is defined as *"Information or data created as a result of the use of an electronic device that shows past activity"* (SWGDE, 2016). Nowadays, just a single individual might own several devices ranging from smartphones, wearables, voice assisted and more. It is clear the diverse amount of digital devices, operating systems, filesystems and software may intimidate educators. Thus, integrating up to date, diverse digital artifacts into educational environments is a difficult task to accomplish.

With minimal focus devoted to creating scalable educational resources of artifact curation and analysis, the learning gap in academic programs widens and the possibility of students graduating with critical skills upon graduation decreases. Forensics educators may use data dumps extracted from different devices such as hard drives, smartphones, network traffic in their teaching programs, but these materials do not fully expose students to the variety of DF evidence found in artifacts. This problem is not unique to DF and exists in cybersecurity broadly. Other platforms have been developed to offer cybersecurity education and some examples are

* Corresponding author.
E-mail addresses: cgrajedamendez@newhaven.edu (C. Grajeda), jberr6@unh.newhaven.edu (J. Berrios), sbenz14@newhaven.edu (S. Benzo), eogun1@unh.newhaven.edu (E. Ogunwobi), ibaggili@lsu.edu (I. Baggili).

https://doi.org/10.1016/j.fsidi.2023.301566

discussed in Section 2. These platforms come with some limitations, for example, many are surrounded by a paywall to have full access to their content. At the time of writing, there are no platforms that serve as a centralized repository for Curated Forensic Artifacts (CuFA)s. Instead, most platforms use datasets or disk images. Additionally, some are not accessible to the general public and are privately used by specific institutions.

The Artifact Genome Project (AGP)[1] (Grajeda et al., 2018) was launched in 2017 with the goal of providing the community with a granular and sanitized DF artifact database, allowing practitioners and academics to leverage them in their investigations and research (Balon et al., 2021), while also allowing them to contribute any artifacts. As a centralized repository for curated artifacts, the AGP has had a major impact in the professional and educational communities. As a result, it now houses over 1200 curated artifacts, and almost 600 registered users that are affiliated to over 280 organizations from academia, federal, local and state law enforcement, and private companies residing in 54 countries around the world.

Consequently, integration of educational modules in the AGP happened in 2020. The approach was to leverage current and future CuFAs to catalyze scalable, self-paced, self-assessed educational material related to DF artifacts.

Our work provides the following contributions:

- **An educational platform created by and for students to learn about DF artifacts.** Before this work, there was no organized platform allowing students, educators, and practitioners to share their artifact knowledge.
- **An approach that allows instructors to implement self-paced, automatically assessed learning modules related to DF artifacts.** Given that the AGP is the platform used to curate artifacts, we now empower instructors to create self-paced learning modules related to DF artifacts by consuming CuFAs in their learning exercises.
- **An online educational community made up of industry professionals, students, and instructors.** While the AGP focuses on artifacts and educational modules, the system grants users the ability to communicate with other users via a messaging functionality to inquire about certain artifacts or educational material.
- **Free access to the artifacts and DF artifact instructional material.** The system is available to anyone who can meet our standards and pass the vetting process after registration.
- **Catalyze the study of DF artifacts over time.** Given that rigorous scientific endeavors require large datasets, and longitudinal data, the curation of DF artifacts over time enables us to gain scientific insight into how artifacts and their ontology change over time.
- **Training and mentorship of undergraduate and graduate students.** Students were hired, or completed their internships, or volunteered to conduct research in various technologies at the AGP. They acquired artifacts, created educational exercises and some even published any research that resulted from their work.

This paper is organized as follows: Section 2 presents related work. Section 3 discusses Educational Material Development & Design. Section 4 details the Educational Module System Design & Functionality. Assessment of the educational modules is discussed in Section 5, followed by Sections 6 and 7 which presents the conclusion and future work.

[1] https://agp.newhaven.edu/.

2. Related work

The constant rise of cybercrime and the rapid advancement of technology are an ever evolving challenges that have increased the demand for professionals in Cybersecurity and DF. With this in mind, traditional teaching methods are no longer viable for providing swift learning experiences. This paired with findings highlighting the lack in offering in-demand DF courses, like memory forensics across universities in the United States seems to be a challenge (McCullough et al., 2021). Although cybersecurity education can be commonly associated with in-class learning, there has been a surge in online platforms that provide educational resources in diverse areas within cybersecurity (Balon and Baggili, 2023).

The Artifact Genome Project's initial purpose was to provide an online system for uploading and viewing digital forensic artifacts acquired either through scientific research or real world investigations (Grajeda et al., 2018). The main drivers of producing these artifacts became our own students. The AGP not only became a portal for them to contribute their findings, but also a project to take on and learn the process to properly conduct research and gain technical skills.

2.1. Forensic artifact analysis

Prior to discussing related educational methods, it is essential to highlight the bread and butter of the AGP. Over the last decade, there has been an increased amount of research involving DF artifacts. Some of this research has also contributed artifacts to the AGP. Some examples include, mobile forensics (Bader and Baggili, 2010) (Al Marzougy and Marrington, 2012) (Iqbal et al., 2013), smart watches (Baggili et al., 2015), drones (Clark et al., 2017), cloud storage (Hale, 2013) (Roussev and McCulley, 2016), (Roussev et al., 2016) and mobile and desktop applications (Al Mutawa et al., 2012) (Walnycky et al., 2015) (Zhang et al., 2017) (Marrington et al., 2012) (Mahr et al., 2021) (Johnson et al., 2022).

2.2. Educational cybersecurity systems

Back when the AGP was launched, it was noted that new systems geared towards cybersecurity training started to appear online. Some of them have been software prototypes stemming from scientific research that have either been implemented online or that are no longer updated. Many have focused on innovating the way users could best learn through online exercises. In the next subsections, a few different examples of these platforms are categorized to provide an idea of the state of the field at the time of this writing. Note that these examples are not indicative of the total amount of systems currently available or whether they have been updated by the time this article goes public. These include traditional and non-traditional online learning, which can include the use of Virtual Machine (VM)s, gamified and Capture The Flag (CTF) like platforms.

2.2.1. Traditional & non-traditional

These platforms are categorized as traditional and non-traditional as they might involve instructors providing the training or the sole use of training through videos and hands-on exercises that might implement the use of VMs individually or through a Cyber Range. Some of these platforms are considered “freemium” as they allow users to access the introductory materials, but once the user reaches a certain limit, a paid subscription is required. While the focus of these systems is to provide cybersecurity training for users, none of them focus on artifacts. Instead, resources are provided which in some cases could be considered

artifacts or datasets depending on the exercise.

Security training portals such as HackTheBox (HackTheBox, 2017) and TryHackMe (Tryhackme, 2018) were released in 2017 and 2018 respectively. Both platforms provide users with cybersecurity "hands-on" training experience using virtual machines to complete challenges. TryHackMe uses a guided model for learning, while HackTheBox is a more aggressive approach that encourages users to learn by hacking their boxes (VMs). Similarly, LetsDefend (LetsDefend (2020) is another challenge based platform to understand the Security Operation Center (SOC) environment with both blue team and red team skills. All three offer limited free content, but a paid subscription is necessary for full access.

Other more traditional platforms offering freemium or paid training include (CYBRARY, 2015), which motivates users to focus on specific cybersecurity career paths such as penetration tester to systems administrator. This platform offers mentoring as well as certifications. On the other hand, Offensive Security (OFFSEC for Orgs, 2012) directly sells training and certifications with no freemium access. It includes complex subjects such as exploit development, web application security and more.

2.2.2. Gamified learning platforms

With the steady increase of gamified learning in lectures and the integration of gaming in digital learning environments, it is normal to inquire whether or not this framework is an adequate way to teach. A number of studies have explored the effectiveness of gamified cybersecurity learning through different metrics: student's self-perception of success, quantitative grades, and student enthusiasm (Ros et al., 2020) (Demmese et al., n.d.). While each platform is different in how they approach gamified learning, the basic conclusion is the same: there is a strong correlation between gamified learning and increased memorization, retention, and success. Some examples of these platforms are discussed below.

The transition from traditional Cybersecurity learning to gamified learning is demonstrated in the computer video game, CyberCIEGE (Thompson and Irvine, 2015). The project was supported by several federal organizations with the goal to teach computer and network security concepts to students. The game was assessed in an Introduction to Computer Security course, and has been used in hundreds of educational institutions worldwide. Although the game is fairly outdated, it is still available to US government organizations and educational institutions per request. Cyberspace Odyssey (CSO) (Graham et al., 2020) is another online game that supports supplemental learning of network security concepts though speed-based challenges. This game has been evaluated for four years through the Advanced Cyber Education (ACE) program, a leadership training course teaching cybersecurity principles to cadets in the United States.

More recently, there have been efforts to utilize different gaming styles. PenQuest (Luh et al., 2020) (Luh et al., 2022), which was funded by the Austrian Science Fund and others, is a role-playing game that utilizes the attacker/defender model using an IT infrastructure. The game is based on MITRE ATT&CK, D3FEND, and the National Institute of Standards and Technology (NIST) SP 800-53 security standard. The beta version of this game was evaluated in a classroom environment as well as with independent security experts.

2.2.3. Capture the flag (CTF) platforms

CTF competitions have become ubiquitous and very popular among the Cybersecurity community worldwide. Their popularity stems from being one of the main methods of competition in testing and practicing Cybersecurity skills. Nowadays, CTF's are easily accessible, and even when the competitions have passed, some platforms remain active to offer a method to continue practicing one's skills. Take the case of picoCTF (Owens et al., 2019; Research, 2013), which is an online CTF-style platform targeted towards middle and high school students. The challenges offered range from beginner to advanced and include, password cracking, reverse engineering, etc.

3. Educational Material Development & Design

3.1. Research-based best practices

In order to create educational materials, the AGP team has implemented research-based best practices. Previous research has demonstrated the following:

- **Automatic Assessment (AA).** In virtual education, it has proven to be effective, especially when used by a large number of students (Malmi et al., 2002). In the AGP platform, *automatic answer verification* is employed. Users can submit their answers to problems repeatedly and the system provides immediate grading. Additionally, some types of questions receive up to three tries to answer them correctly (See Fig. 2).
- **Self-paced learning.** Depending on the situation, this method is effective as research shows that people who control their study-time have performed better compared to those without it (Tullis and Benjamin, 2011). *The AGP educational modules permit users to solve artifact challenges at their own pace* over a web browser using open source tools.
- **Challenge-Based Learning (CBL).** This enhances the educational experience and has demonstrated effectiveness in cybersecurity education (Cheung et al., 2011). This might be a hands on approach where students use a diverse number of resources and tools to solve complex problems.
- **Inquiry-Based Learning (IBL).** This method allows students to learn using an inquiry approach (Lim, 2004; Kim and Yao, 2010; Woolf et al., 2002). Active learning provides questions, challenges, or scenarios where students seek for the answer. In contrast to having an instructor directly training the student. The AGP platform contains different types of scenario based educational modules where students will need to search for answers in the resources provided. For example, *scavenger hunt* exercises permit students to search for answers through browsing the AGP system for artifacts.
- **Real world data.** This is one of the most important aspects for digital forensics and cybersecurity education as students have an opportunity to experience complexities they might face in the real world (Woods et al., 2011). *At the AGP, CuFA by definition pose potential forensic value to investigations, making them realistic.* Our team of researchers invest a lot of time to ensure the most realistic case scenarios are created to provide this educational experience through educational modules.

3.2. Creation of educational modules

At the time of writing, the AGP platform contains 35 submitted educational modules that are organized in six different types, Learn About Linux, Learn About Cyber Forensics, Learn by Doing, Scavenger Hunt, Learn About the AGP and Learn About Artifacts with the option to create new types as needed. These exercises have been created by our research students under the guidance and evaluation of the AGP manager and Principal Investigator (PI). The team is composed of paid students, volunteer researchers, paid/unpaid interns, and developers. The students' grade level ranges from Undergraduate Freshmen to Graduate.

Educational modules in some cases take a lot of time to create.

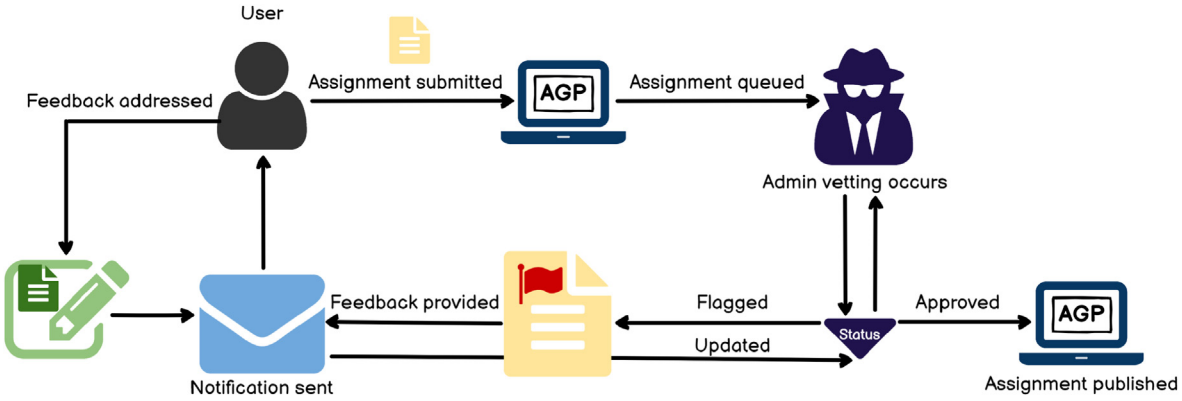

Fig. 1. General assignment vetting process.

This is due to the vast amount of research and quality review invested when creating them. The following steps portray this process as employed by our team:

1. The first step in the creation process is an idea. This concept introduces the primary purpose of the assignment. For example, creating a module that would teach users about malware network forensics by using the tool Wireshark.[2] This idea can be a costly one depending on the type of research being conducted. For example, this can involve the purchase of devices (i.e., drones) and software to investigate.
2. The second step involves conducting preliminary research to ensure the idea is feasible and encompasses the full scope of the topic.
3. Once the idea is solidified with the guidance of the AGP team lead and manager, the student starts their official research and a first draft is created in Overleaf[3] following the standards pertaining to the type of exercise being created.
4. The first draft goes through a review cycle. The team lead reviews the exercise and interacts directly with the student. The AGP manager might also provide feedback as needed. This process might take several days due to the feedback provided and the necessary corrections needed from the user until the draft is ready to move on to the next phase.
5. The second draft is reviewed by the AGP manager. At this point, another review cycle starts between the three parties. During this review process, the team lead and manager are also involved in vetting artifacts if they are part of the assignment, which also prolongs this process.
6. The final steps involve the student creating the assignment and uploading any artifacts in the AGP platform. The student would also test the assignment to ensure no issues are encountered. Moreover, the team lead also tests the module to ensure that it works in the platform as expected before being approved for public use by the manager.

3.3. General process for vetting educational modules

While the guidance provided above to create assignments applies only to our current group of researchers, it is important to describe the vetting process that applies to the general audience when submitting educational modules to the platform to ensure standards are met. For instance, this could be anyone with enough experience, such as an instructor at a university. A high level process of vetting this type of assignments is demonstrated in Fig. 1.

From this flowchart, it is important to note that the vetting cycle does not stop until the user has addressed all the feedback provided by the administrator. Some of the things that could cause an assignment to be flagged include not submitting artifacts when the assignment explicitly uses them, artifacts submitted not meeting artifact submission or sanitation standards, missing context and failing to demonstrate how the assignment leads users to learn or practice a certain skill or subject. There are more standards to know before starting the research to produce an educational module. For more details proceed to register at https://agp.newhaven.edu and/or contacts us in the Contact page.

4. Educational Module System Design & Functionality

The AGP platform was first designed to host digital artifacts. The concept of hosting educational modules using artifacts came later. The modules were first launched to the public in 2020 via a digital forensics conference challenge (See section 5). The educational modules' features and functionalities in the portal followed a similar concept as artifacts. The next subsections will briefly address these functionalities and features.

4.1. Educational module design

The educational modules in the AGP are designed to allow easy interaction between the users and the system. As previously described (See Section 3), the design of these modules allows anyone qualified in the platform to easily build the module using different resources to include artifacts.

The notable aspects of educational module design are shown in Fig. 2 and A.4 and are briefly described below:

- *Assignment Type*: The assignment types are based on what/how the assignment aims to teach the subject. Currently, there are six types in the system, (i.e., Scavenger Hunt) and new categories can be created by the admin as needed.
- *Assignment Overview*: The overview describes the case details and sets up the immersion for the user.
- *Learning Objectives*: The objectives are used to guide the focus of the assignment and describe the expected outcomes of completing this assignment.
- *Tools Needed*: The tools listed in this section must be open-source and compatible with different operating systems (i.e.,

[2] https://www.wireshark.org/.
[3] https://www.overleaf.com.

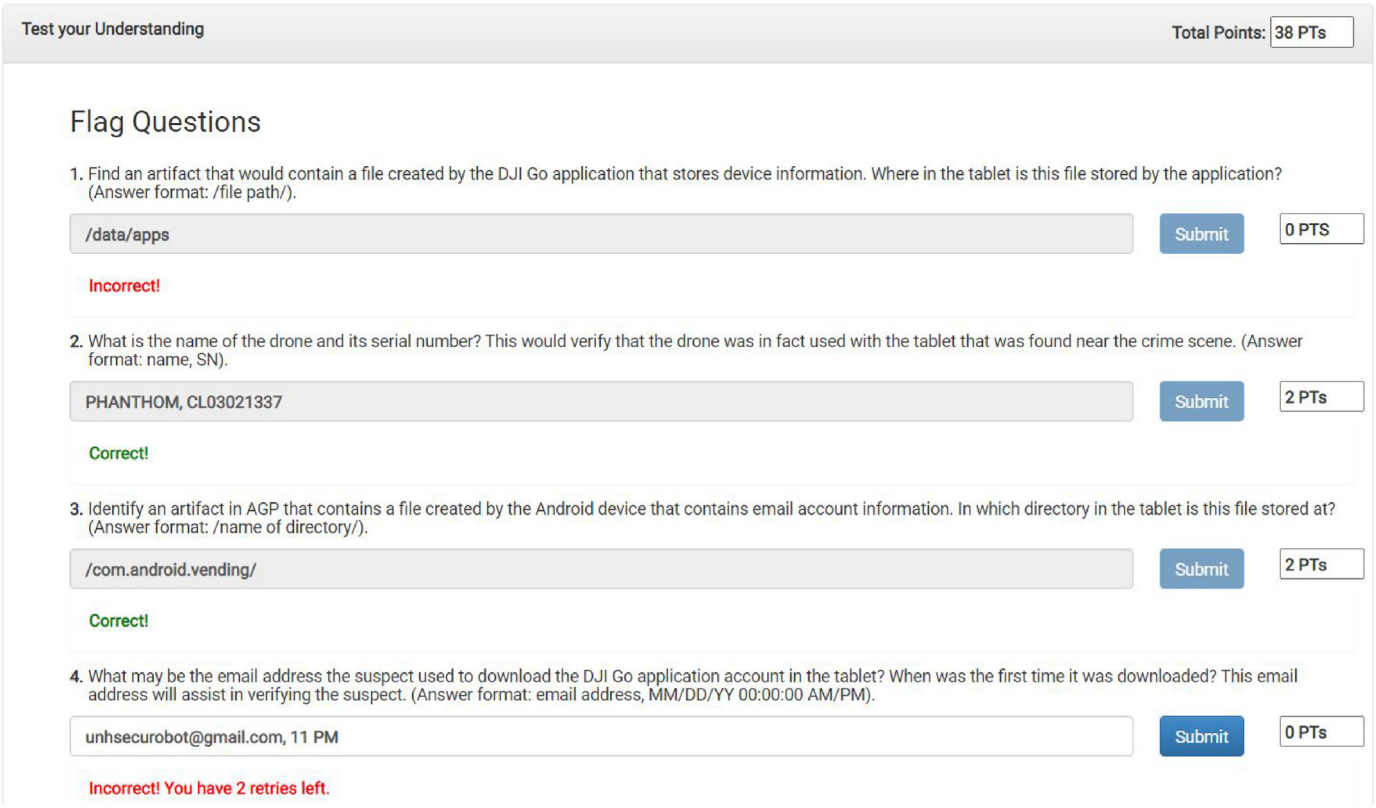

Fig. 2. Test sample with questions & answers.

macOS). The AGP strives to have assignments that are easily accessible and by extension, the tools have to be as well.

- *Artifact Tags*: This directly links the relevant artifacts to the assignment. When users click on this, they will be able to see the entire artifact page and cross-reference it with questions located in the "Test Your Understanding" section. Note that some modules might not need artifact tags listed depending on their type, such as Scavenger Hunt.
- *Adding Media (pictures and videos) & other resources*: The creators have the option to add images, videos, and other educational materials to the assignment. These might serve as pieces of evidence, instructional videos, or other educational sources that might aid the user in answering the questions or learning more about a certain topic.
- *Test Your Understanding*: This section is a key aspect of the design of the educational module as it allows the user to take the overview, the supplied artifacts and/or other resources and apply practical applications to them. This section has the option to add different types of question formats, such as *multiple choice, flag, and thought questions.* The multiple choice and flag questions require the creator to add the correct answers and to provide a description of the answer, how to obtain it, or where to locate it in the sources provided. This helps the admin vet the authenticity of the assignment. Flag questions are the hardest to grade as they require the user/creator to obtain the answer from the resources provided. The answer will have to be text that the user will have to input in a text box. Thus, probability of error is high. The AGP system allows creators to adjust the matching percentage from 0 to 100% for each answer so there is room for error, but not enough to make the answer unreliable. Additionally, in both types of questions a difficulty level can be assigned (easy, intermediate, hard) as well as allowing the question to be answered multiple times. The questions also indicate the amount of points they are worth. Finally, Thought Questions are different as they are not graded and the answer is provided. These are added at the end of the assignment and provide the user with the conclusion of the case scenario. Users are encouraged to solve the "case" on their own and come to a conclusion before looking at the answers provided.

4.2. Other features and functionalities

In conjunction with the design of the assignment itself, there are other features used to enhance the experience and the feasibility of creating or taking assignments. These features are similar to creating and viewing artifacts. These features include:

- *"Search" for assignments:* This allows the user to search by keyword, phrase, or title for an educational module. Additionally, an advanced search option is provided to filter by assignment type, creator, dates and more.
- *Create an Assignment:* This provides the form where the assignment can be created. This form also allows the user to select the type of assignment they want to create.
- *My Assignments:* This is where users can track the assignments they have created and note the status of the assignments (queued, updated, flagged, and approved). The assignments can be edited and resubmitted during the vetting process.

- *Report Card:* The "Report Card" (See Fig. A.5) list the scores of all completed assignments the user has taken as well as the ones in progress. The modules are self-paced, and users can start taking an assignment and finish it later. Users can export this report card as a PDF certificate.
- *Leaderboard for Assignments:* This is a global leaderboard displaying the total points individual users have gained from completing assignments. As new assignments are added, there is a higher chance for people to climb up in the ranks. As of now, about 100 users have been added to the leaderboard.

5. Educational modules assessment

Assessment of the educational modules was a critical goal to measure the efficacy of the materials presented. The objective was to reach a diverse audience with different levels of experience in Cybersecurity and Digital Forensics. Qualitative data was collected after each assessment and analyzed. Any feedback suggesting improvements were carefully considered and applied wherever it was possible.

A diverse amount of modules were compiled and presented as a Cyber Forensics challenge and evaluated within two groups of people, conference attendees and university students. The assessments happened in 2020 and 2021. The conferences involved were the Interpol Digital Forensics Expert Group (DFEG) 2020 Conference[4] and the Digital Forensic Research Workshop (DFRWS) Asia-Pacific (APAC) 2021.[5] The challenge was also implemented at the University of New Haven through its Small-Scale Digital Forensic Science course in the Fall semester on both years. The methodology and survey results from these events are discussed in the following subsections.

5.1. Methodology

Two different methodologies were employed for hosting conference challenges and university courses. These are described as follows:

5.1.1. Conferences

Hosting digital forensic challenges for conferences was not an initial goal of the AGP. These separate occasions presented themselves after the Covid-19 pandemic.[6] As work and school began to be remotely conducted, even major events such as conferences switched to virtual over video conferencing applications such as Zoom.[7]

The two major digital forensics conferences previously mentioned were affected during this time. The first time the educational modules were introduced to the public happened during the Interpol DFEG Conference. This event was supposed to be hosted on campus at the University of New Haven in the Summer of 2020, but became one of the first conferences hosted over Zoom. As co-hosts of this conference and creators of the Artifact Genome Project, the idea of using the AGP educational modules to conduct the first Interpol DFEG Conference Forensics challenge[8] made the shift from in-person to digital more compelling.

For the second conference, DFRWS APAC,[9] the AGP was recommended to the organizers by an attendee of the Interpol DFEG conference. Eventually, the AGP was also used to host the conference's annual Forensics Rodeo. Both of these forensic challenges were hosted by the AGP at no cost to the conferences' organizers. In return, the AGP was able to introduce the educational modules to a bigger, more diverse and more experienced audience to test the effectiveness of the challenges and provide feedback about them via a survey. The following methodology was applied to both conferences when conducting the AGP Forensics Challenge:

1. To form each forensic challenge, approved educational modules were selected. 14 were chosen for the DFEG conference and 15 for the DFRWS conference. Most of these modules were the same with the exception of three. They were largely based on digital forensics investigations using artifacts about mobile applications, desktop applications, drones, and smart watches.
2. The amount of time provided to complete each challenge varied depending on the duration of each conference. The DFEG conference lasted for four days total, but was implemented over two weeks, two days per week. Thus, one week was provided to complete the challenge. The DFRWS conference lasted three days, and about the same time was provided to complete the challenge.
3. A presentation was given to introduce the challenge in each conference and how to participate. Information was also posted into the conferences' programs.,[10] [11]
4. Users were vetted before approving them for registration and participation into the AGP to ensure they were conference registered attendees. A guide was also provided in the portal to ensure users understood how to take the challenge.
5. Our AGP team was on call to assist users anytime. Users could reach our team via the Zoom chat (DFEG) and Discord (DFRWS), our contact page or email inbox messaging system through the portal, and via direct email. Any issues users encountered were addressed as soon as possible to maximize available time for the challenge.
6. Surveys were designed based on the type of conference and materials presented. See Survey Design 5.2 subsection for details. Surveys were distributed to every registered user of the challenge.
7. Data was collected by exporting recorded responses as PDF and CSV files. The data was analyzed and any feasible feedback that proposed changes were implemented on either the educational content or the AGP portal.

5.1.2. University course - mini pilot

The challenge was employed at the University of New Haven through its Small-Scale Digital Forensic Science course in the Fall semesters of 2020 and 2021. Note that each year, a different instructor taught the course. This was only an optional mini-pilot for students to test the efficacy of the challenges. The challenge was introduced to each class of roughly 20 students each year. The challenge was categorized as optional extra credit to be completed by the end of each semester. Since this was not a requirement, the final score students received on the challenge did not have an impact in their course's grade. The method these challenges were implemented in each course differed depending on what the professor desired. On the first year, students had a choice of taking any type of assignment out of nineteen. On the second year, students were given a total of fourteen assignments to take. Ten of those were hand picked by the professor and the other four were

[4] https://dfeg.newhaven.edu/.
[5] https://dfrws.org/conferences/dfrws-apac-2021/.
[6] https://www.cdc.gov/coronavirus/2019-ncov/index.html.
[7] https://zoom.us/.
[8] https://dfeg.newhaven.edu/digital-forensics-challenge/.
[9] https://dfrws.org/conferences/dfrws-apac-2021/.
[10] https://dfeg.newhaven.edu/schedule/.
[11] https://dfrws.org/apac-2021-program/digital-forensics-rodeo/.

randomly assigned to each student. After the students completed the challenge, they were asked to provide feedback via a survey. The survey's design and results are discussed in the next subsections.

5.2. Survey design

The surveys constructed for conferences and university courses did not vary significantly as the goal of each survey was to get an idea about the users' experience. The questions were designed to address a particular need in the field and in our research: understanding whether the materials presented were relevant according to their current skill level and whether they actually learned anything from them. The amount and type of questions asked in each survey was adjusted depending on previous feedback and event type. The types,[12,13] [14] of questions per conference and courses were as follows:

- DFEG Conference: 14 questions containing, 6 Likert Scale, 2 Multiple Choice, and 6 Free Response. This survey was disseminated after each conference challenge was completed, the same is true for university courses at the end of the semester. Surveys were created using Google Forms and Microsoft Forms.
- DFRWS Conference: 19 questions containing, 6 Multiple Choice, 1 Likert Scale, 4 Net Promoter Score and 8 Free Response.
- University courses: 16 questions containing, 5 Multiple Choice, 1 Likert Scale, 4 Net Promoter Score, and 6 Free Response.

5.3. Survey results

The results of the surveys will be summarized in the following subsections.

5.3.1. Interpol DFEG & DFRWS APAC conference forensic challenge

The results from these two conferences will be discussed jointly due to the similarities and the amount of respondents. The DFEG conference had the most participants registered to take on the challenge with a total of 64. However, only 39% ($n = 25$) of those provided some feedback in the survey. The DFRWS APAC had lower participation with a total of 21 registered users, but only 33% ($n = 7$) provided some feedback. The following sections will discuss the results.

5.3.2. Demographics

Results relating to demographics (Appendix B, Table B.1 and Appendix C, Table C.4) show the majority of the sample population were very diverse and came from various countries. This is no surprise as both conferences were international. The majority of respondents in the DFEG conference came from Portugal (12%), while the DFRWS conference's majority came from China (43%).

For the DFEG conference, no demographics questions were asked. For the DFRWS conference, the majority of respondents were male (71%) and ranged from ages 26–34 year old (43%). The level of education for attendees of DFRWS varied. The highest was a masters degree; most respondents were in technology related fields. At least one correspondent did not have a technical related major and another did not provide a major. The question about profession and years of experience was asked in both conferences. In the DFEG conference, the majority of participants were Digital Forensics Examiners/Investigators (32%) with 4–15 years of experience. DFRWS participants had different professions. One participant was a Digital Forensic Analyst, with 18+ years and another one was a Sr. Technical Advisor with 20+ years of experience.

Lastly, the questions about level of expertise in Cybersecurity and/or Cyber Forensics field and years of experience in them were asked in the DFRWS conference only. The majority were either intermediate to advanced (58%) with over three years of experience (57%) in the field.

5.3.3. Relevance of Educational Modules

To understand how relevant the educational modules were to respondents in both conferences, they were asked to rank each assignment they took and also note whether they took them or not. The answers when ranking these assignments were mixed and it was noted that some respondents took some assignments more than others as well as response rate was not 100%. Therefore, a short summary of the most relevant results is discussed by conference below.

For the DFEG conference's results refer to Fig. 3. The educational modules that were ranked the most relevant in this conference were titled, *Samsung Gear S3 Frontier Smartwatch: Who are the Alleged Robbers of the Iron Bank of Braavos?* and *Android 6.0.1 Application: Was This Employee Breaking Company Policy?* Both assignments' combined relevant and very relevant scores were a total of 65% and 80% of the survey respondents answered these two questions. Most assignments had a combined relevancy score of 50% or higher with the exception of one (*Code Mirai Botnet Scanner.c: Botnet Proves Why Default Passwords Should Always Be Changed!*), which had a combined relevancy of 42%. This demonstrates that the material provided was relevant to most respondents in their careers. Lastly, there were two assignments *(..The Case of the Killer Drone and Espionage on the Home Front..)* that respondents did not take the most (39%) each and were probably the most difficult ones amongst them all.

Subsequently, for the DFRWS conference's results refer to Fig. C.6 in Appendix C. All respondents answered all the relevancy questions. The assignment that was ranked the most relevant with 86% combined relevant and very relevant scores was *(Android 6.0.1 Applications: Investigating a Murder with the Help of Digital Artifacts.* Furthermore, similar to the DFEG conference, most assignments were relevant to the respondents in their field.

5.3.4. Key Takeaways & recommendations

Key takeaways from both conferences were very positive as reflected in Tables B.2 and C.5 in Appendix B and Appendix C respectively. There were 36 responses participants provided that involved questions regarding their experience in participating in the AGP Challenge and any benefits in using the platform. Based on the feedback, it is clear that the challenge was a success. One of the main things respondents seem to enjoy was the vast amount and diversity of the digital artifacts. Moreover, some benefited from gaining knowledge or validating their skills, while experiencing real world scenarios with open source tools they might be able to add to their own arsenal. Additionally, one even mentioned that it was important to be exposed to artifacts as nowadays most individuals rely on 'push-button' forensics or tools. The feedback provided in both surveys strongly correlates with other questions posted to participants on whether they found the challenges' educational material relevant to their job and/or career and whether they would recommend others to use the AGP. As expected, most found it very relevant and very likely to recommend it to others.

[12] For details about question types, see footnotes 15 and 16.

[13] https://www.qualtrics.com/support/survey-platform/survey-module/editing-questions/question-types-guide/question-types-overview/.

[14] https://segmanta.com/blog/difference-nps-likert-scale-questions/.

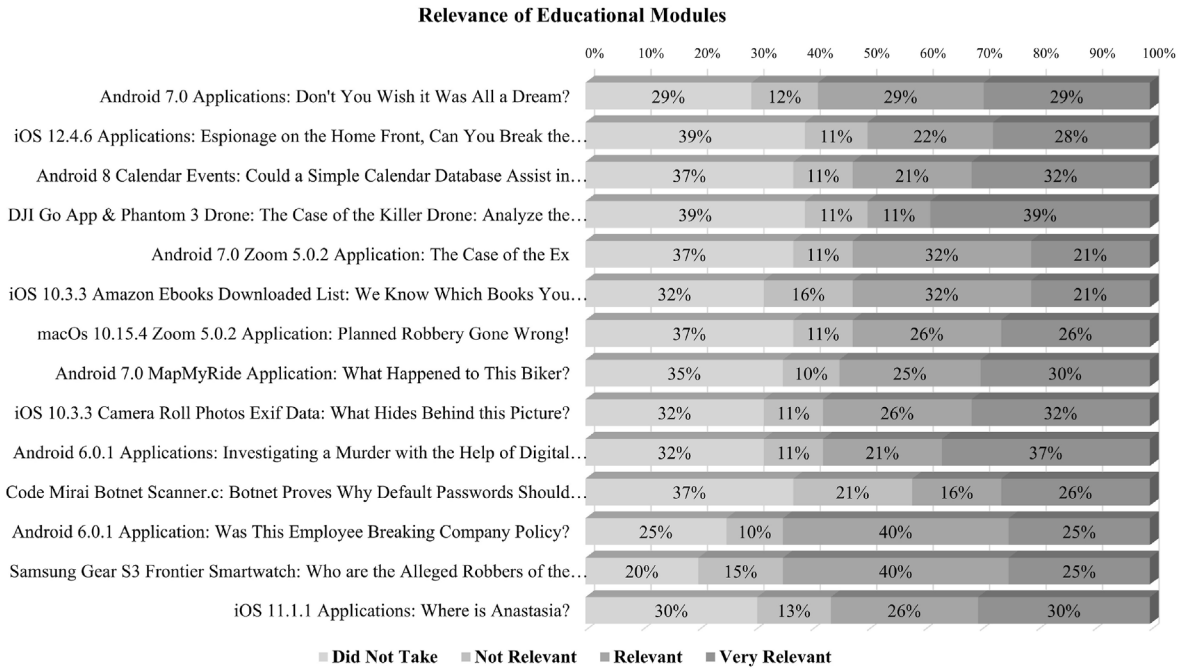

Fig. 3. Interpol dfeg conference - relevance of educational modules.

On the other hand, respondents were also asked for their recommendations to improve the AGP's educational module's content (see Tables B.3 and C.6 in Appendix B and Appendix C). Seventeen responses were provided on both conferences combined. The major recommendation was to be consistent on answer format, precisely on dates and times. Due to individuals being located around the world, it would make sense to use a timestamp standard such as ISO 8601 or UTC format. UTC is something we applied as part of our changes in the platform. Other feedback, especially from the DFEG conference since it was involved testing the modules in the platform more. Due to this being the first time the modules were launched to the public, there were indeed a few bugs that we had to correct in the fly. Those were reported by some users during the challenge and they were addressed immediately to minimize any setbacks. This was actually a great and helpful experience in making the system more reliable. Most of these recommendations were also addressed and some applied to the content and system after the conference was over.

5.3.5. University courses - mini pilot results

The mini pilot was a concept to evaluate the efficacy of the AGP educational modules in a Cyber Forensics course. The idea was for the professors to make the modules an optional forensic challenge that would be completed at the end of the semester for extra credit. Due to the nature of the method used to take the assignments, as they were not required, low participation from students resulted from this. As a result, in both evaluations, a combination of twelve students provided feedback on our survey. It is also possible some students might have taken the educational modules, but decided not to respond to the survey. Therefore, a short summary of the results will be provided in this section.

As far as demographics, most students were male (67%) between the ages of 17–25 years old (83%). All students were enrolled in the Cybersecurity and Networks major with 58% being graduate students. Furthermore, based on the feedback from the assignments that were taken, most were relevant. However, due to students choosing which modules to take, calculating a percentage of this was not applicable. The same is true when asking about how significant the materials were to their career and whether they had learned something new, which in both cases most of them felt strongly about the significance and that they had indeed learned something new. Finally, some of the biggest takeaways were the diversity of the materials and artifacts as they enjoyed the experience, while the major recommendation was to improve the answer format, similar to the feedback provided in the conferences.

6. Conclusion & discussion

The Artifact Genome Project is an invaluable resource to the cybersecurity community. It offers a plethora of educational information about cyber forensics, cybersecurity and technology as a whole. With the addition of educational modules in the platform, there has been a significant impact on not only on the AGP users, but also the AGP student team. Students have been and continue to be the main contributors of artifacts to the platform with now over 1200 added to the portal, and now they are also the main contributors to the educational modules created with 35 of them added so far. This has been a driving force in the success of the platform and in the students' professional careers. It has helped students grow their skills and gain new knowledge and experience in different disciplines within cybersecurity and research. As a result, students have become more proficient and competitive,

providing them a better chance to display their skills when searching for internships or postgraduate positions. Some students have even published their work in peer-reviewed journals as part of this project, giving them a higher chance to extend their network and present their work in conferences such as this one and landing them the job of their dreams.

Consequently, our main goal continues to be the same, to be able to offer this platform to the community and that use it in the best way they can. However, this platform cannot survive without the engagement of the community as a whole. Our hope with this work is to reach out to the Cyber community and encourage them to continue using this powerful resource and to spread the word to others to utilize it and help contribute to it. With the addition of educational modules, our hope is also to reach out to academia and others who wish to use it to train others. As it has been demonstrated, using the educational modules as forensics challenges has worked not only in major forensic conferences, but in the educational environment.

7. Future work

The AGP will continue to focus on improving the platform as well as the educational materials offered. The system will also be transferred to the Louisiana State University as its Principal Investigator is now working there. With the transfer, a new wave of leadership and students will be taking over to continue supporting the cause. Moreover, partnership with academia and other organizations will be a priority to pursue. The contributions could be in different ways, to include offering research internships to students at other organizations as we did in the University of New Haven. Finally, the development of a new system has been in the works at the University of New Haven. In this new portal, the emphasis will be to offer a different experience than what it is now. In the future version, entities such as universities and cybersecurity conferences will be able to use the platform to host their events and courses separately.

Acknowledgements

This material is based upon work supported by the National Science Foundation under Grant Number 1900210. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Appendix A. AGP Educational Modules Design & Functionality

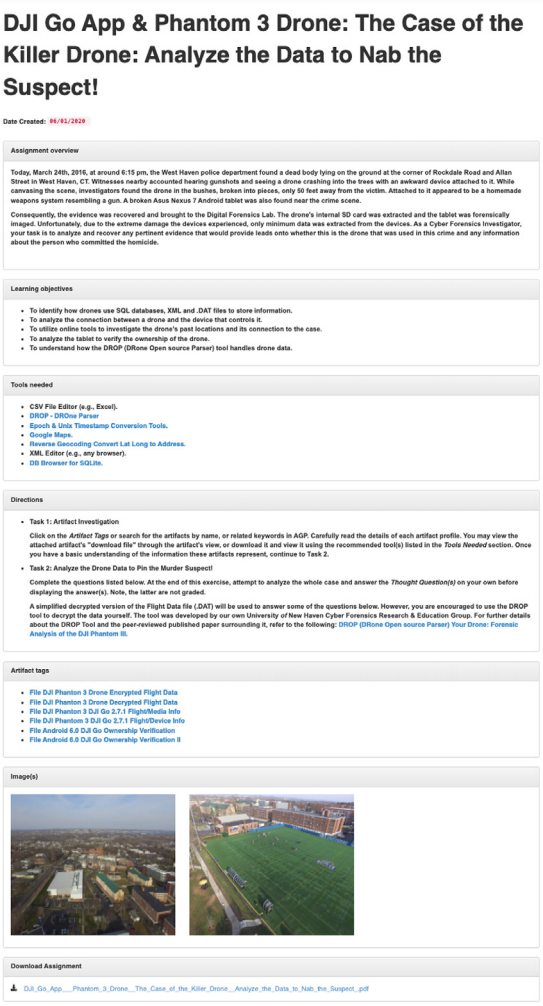

Fig. A.4. Educational Module Sample

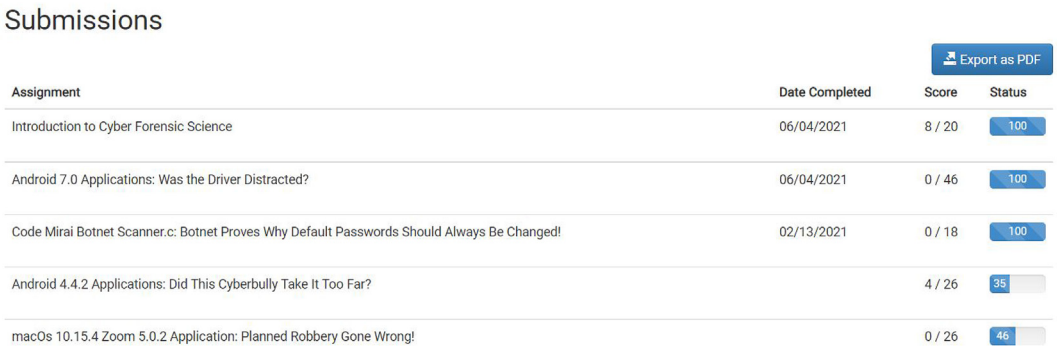

Fig. A.5. Educational Module Report Card

Appendix B. DFEG Survey Results

Table B.1
Demographics from the (DFEG) Conference. *Any percentage disparities due to rounding.

	Count	Percentage
Country		
Australia	1	4%
Bahrain	1	4%
Cambodia	1	4%
El Salvador	1	4%
Estonia	1	4%
France	1	4%
Greece	2	8%
India	2	8%
Italy	2	8%
Jordan	1	4%
Mexico	1	4%
Myanmar	2	8%
Nepal	1	4%
Nigeria	1	4%
Portugal	3	12%
Sudan	1	4%
Trinidad	1	4%
United States	2	8%
Profession & Years of Experience		
Academic-Telecoms/Investigator, 26 years	1	4%
Digital Forensics Examiner/Investigator, 15 years	2	8%
—- 12 years	2	8%
—- 8 years	1	4%
—- 6 years	2	8%
—- 4 years	1	4%
Information Systems and Forensic Expertise on Digital Equipment, 20 years	1	4%
Law Enforcement, 15 years	1	4%
—- 20+ years	2	8%
—- No years provided	3	12%
Computer Engineer, no years provided	1	4%
Faculty in Computer Science, no years provided	1	4%
INTERPOL Cambodia, no years provided	1	4%
Social Media Investigation and Digital Forensics, no years provided	1	4%
No profession provided, 2 years	1	4%

Table B.2
Key Takeaways from the DFEG Conference's AGP Challenge & Overall Experience

Number	Feedback
1	I learnt how to use artefacts in several ways, the open source tools were very helpful. Plist files, sqlite files and so on.
2	Zoom, Kik, iOs camera roll artifacts.
3	To me as an NCB, this event is very unique and full of experts to share most of the knowledge that I have never known before.
4	Diversity of artifacts.
5	Many keys.
6	The AGP library of Artifacts!
7	How much information is store and how many places it is duplicated in our devices.
8	Excellent event.
9	It is important to stay informed about the resources out there.
10	Other tools to experiment and work with.
11	I have to go over everything again, extremely helpful.
12	In particular, the knowledge acquired from the Digital Forensic Challenge from AGP.
13	Partnership with the academia is a key.
14	That other members in this community face similar daily challenges as we do.
15	It is a new area in my work. I must try even more.
16	Great experience. Great artifacts discovered. Great support from Cinthya. Gained a lot even being an experienced examiner.
17	I can say most of the things are very new to me as an NCB and I am grateful to have the opportunity to join with the experts around the world.
18	I'll be signing up students to take the challenge!
19	Very informative and useful on the field.
20	Congratulations on a very good tool and thank you for making this fun challenge.
21	Adding new artifacts looks like little bit difficult at first time.
22	Amazing experience and looking forward to many to come. Thank you.
23	I found the CHALLENGE, a keyword searching exercise, Even though the purpose behind was good (to learn about the artifacts). My personal view, It Would have been bit more interesting, If there were few questions to answer on a evidence (acquired image).
24	Network issues.
25	No. Great job overall.
26	It was a great contribution to my functions. I hope to continue participating with you and INTERPOL and learn much more.

Table B.3
Interpol DFEG Conference - Recommendations to Improve AGP's Challenges' Content

Number	Recommendation
1	Questions must be more elaborate, smaller and the error % must be reduced.
2	Stress Test the challenges for bugs before opening the contest.
3	I've provided extensive feedback around clarity of questions, answer formats, data formats, validation etc. Critical but constructive - a really useful resource.
4	Add more forensics in IoT.
5	1). Because of the range of people who participate (different languages) more clear answers format in some cases or not very strict format (i.e. - just to clear it out "YES" = "Yes" = "yes) 2). Perhaps, more tests before releasing (from someone who did not involved in building it).
6	I would like that the correct answer will be show after an error.
7	I would like to see artifacts in category view.
8	A more step by step work process, I had problems working through them (new to digital forensics).
9	The event should be available online after the pandemics.s
10	Step actions on the use of the open source tools utilized in the acquisition. Area for additional hints and subsequent answer but if accessed results in diminished or no points awarded for the specific question.

Appendix C. DFRWS APAC Forensic Rodeo Survey Results

Table C.4
DFWRS APAC Conference Survey - Demographics. *Any percentage disparities due to rounding.

	Count	Percentage
Gender		
Male	5	71%
Female	1	14%
Prefer not to say	1	14%
Age		
26–34 years old	3	43%
35–43 years old	2	29%
44–52 years old	2	29%
Country		
Australia	1	14%
Austria	1	14%
China	3	43%
Singapore	1	14%
United States	1	14%
Level of Education		
B.E. Computer Engineering	1	14%
B.A. Languages and Cultures of South Asia and Tibet	1	14%
M.S. Information Security	1	14%
B.E. Computer Science	1	14%
B.A. Management Information Systems	1	14%
B.S. Information and Communications Technology	1	14%
M.S. No major provided	1	14%
Profession & Years of Experience		
Associate Consultant, 3+ years	1	14%
Digital Forensic Analyst, 18+ years	1	14%
Engineer, 3 years	1	14.29%
Forensics Researcher, 11 years	1	14%
Junior IT Security Analyst, 2 years	1	14%
Sr. Technical Advisor, 20+ years	1	14%
Did not provide occupation, 20 years	1	14%
Level of expertise in Cybersecurity and/or Cyber Forensics field		
Beginner	3	43%
Intermediate	2	29%
Advanced	2	29%
Years of experience in the Cybersecurity and/or Cyber Forensics field		
Two	2	29%
Over three	4	57%
None	1	14%

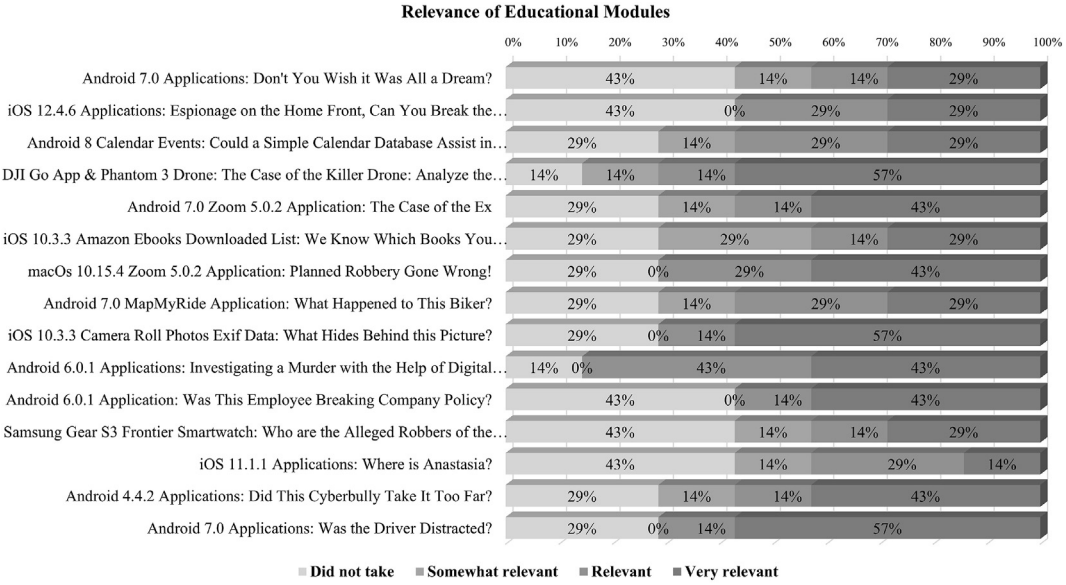

Fig. C.6. DFRWS APAC Conference - Relevance of Educational Modules

Table C.5
Key Takeaways from the DFRWS APAC Conference's Forensic Rodeo & Benefits in Using the AGP Platform

Number	Feedback
1	It was a fun way validating my knowledge.
2	Figuring out that phone forensics is not as hard as I thought, but mostly sqlite:D I really enjoyed working on so many different applications, especially on the ones like Zoom which are heavily used and rather new.
3	What artifacts are related to certain scenario.
4	Most assignments are good practice for real works. The designing of case background.
5	Did not complete any assignments due to schedule unavailability (US Time Zone); I reviewed the AGP site afterwards and find it be a useful resource for forensic investigators to use as a training platform and learn more. I have passed onto my colleagues as well and look forward to engaging with the AGP team on potential follow-on research.
6	The importance of being able to manually identify and understand artifacts. Is very important in this era of 'push-button' forensics.
7	Yes certainly beneficial for participants of the conference.
8	For me, it was very beneficial, I think it's a great addition to the conference. I definitely think this would be great for educational institutions and other conferences. However, with conferences I suppose it would be hard to provide knew challenges all the time and this can quickly turn into a problem if people solve problems quickly just because they already know them.
9	I've participated in previous DFRWS Rodeo activities and this one followed a similar type model with challenges across a wide spectrum of topics as in past RODEOS. I just didn't have the time to work through the challenges, but I did like the diversity across looking at different platforms and applications in more depth. Additional conferences (OSDFcon) and educational institutions can gain great insights from AGP.
10	It was an extremely good idea. The AGP would benefit everyone involved with digital forensics.

Table C.6
DFRWS APAC Conference's Forensic Rodeo - Recommendations to Improve AGP's Educational Module's Content

Number	Recommendation
1	The general interface is good imho, but the leaderboard was a bit strange, as I couldn't find the one for the DFRWS itself, just a global one.
2	Sqlite contents should below the file information (e.g. path), which cannot load under bad network condition. As for a international challenge, time format should use ISO format rather than USA format, and not so many questions for the time format converting, which is boring.
3	Worked across Windows & Mac systems and browsers. did not try on iPad or Surface tablet - probably need to have access to various tools to complete the challenges, so might think about a future expansion enhancement to spin up cloud-based VM environment to complete the challenge (for those organizations in the education/academic market that cannot afford to reconstitute a laptop/desktop at scale).
4	Consistency in the way the data is input, mostly in regard to dates in which many questions asked for the date to be inputted in different formats.
5	The only thing I didn't like were the different timestamp formats, that was really a hassle. I'd suggest using standardized ISO 8601 timestamps in UTC. Bad enough that we all have to struggle with the different vendor formats, but at least for a forensic challenge consistency would be great)
6	Attached files can be stored in the cloud like GDrive, since I had to try several times to download a file. The "Reverse Geocoding Convert Lat Long to Address" website has a daily quota which is not enough for solve all of these questions.
7	It was a bit too much of a distraction from the main conference. I got so hooked on completing the AGP assignments that I missed out on some sessions in the conference. For me, it was too difficult to do both.

References

Al Marzougy, M., B, I., Marrington, A., 2012. Blackberry Playbook Backup Forensic Analysis. Springer, pp. 239–252.

Al Mutawa, N., Baggili, I., Marrington, A., 2012. 'Forensic analysis of social networking applications on mobile devices'. Digit. Invest. 9, S24–S33 (The Proceedings of the Twelfth Annual DFRWS Conference).

Bader, M., Baggili, I.M., 2010. Iphone 3gs Forensics: Logical Analysis Using Apple Itunes Backup Utility.

Baggili, I., Oduro, J., Anthony, K., Breitinger, F., McGee, G., 2015. Watch what you wear: preliminary forensic analysis of smart watches. In: '2015 10th International Conference on Availability, Reliability and Security', pp. 303–311.

Balon, T., Baggili, I., 2023. Cybercompetitions: A Survey of Competitions, Tools, and Systems to Support Cybersecurity Education. Education and Information Technologies, pp. 1–33.

Balon, T., Herlopian, K., Baggili, I., Grajeda-Mendez, C., 2021. Forensic artifact finder (forensicaf): an approach & tool for leveraging crowd-sourced curated forensic artifacts. In: Proceedings of the 16th International Conference on Availability, Reliability and Security', pp. 1–10.

Cheung, R.S., Cohen, J.P., Lo, H.Z., Elia, F., 2011. Challenge based learning in cybersecurity education. In: Proceedings of the 2011 International Conference on Security & Management, 1.

Clark, D.R., Meffert, C., Baggili, I., Breitinger, F., 2017. Drop (drone open source parser) your drone: forensic analysis of the dji phantom iii. Digit. Invest. 22, S3–S14.

CYBRARY, 2015. The leading cybersecurity professional development platform. https://www.cybrary.it/.

Demmese, F., Yuan, X. and Dicheva, D. (n.d.), 'Evaluating the effectiveness of gamification on students' performance in a cybersecurity course', Journal of the Colloquium for Information System Security Education 8(1). **URL:** https://par.nsf.gov/biblio/10290874.

Graham, K., Anderson, J., Rife, C., Heitmeyer, B., R Patel, P., Nykl, S., C Lin, A., D Merkle, L., 2020. Cyberspace odyssey: a competitive team-oriented serious game in computer networking. IEEE Transactions on Learning Technologies 13 (3), 502–515.

Grajeda, C., Sanchez, L., Baggili, I., Clark, D., Breitinger, F., 2018. Experience constructing the artifact genome project (agp): managing the domain's knowledge one artifact at a time. Digit. Invest. 26, S47–S58.

HackTheBox, 2017. A massive hacking playground. https://www.hackthebox.com/.

Hale, J.S., 2013. Amazon cloud drive forensic analysis. Digit. Invest. 10 (3), 259–265.

Iqbal, A., Obaidli, H.A., Marrington, A., Baggili, I.M., 2013. Amazon kindle fire hd forensics. In: 'ICDF2C'.

Johnson, H., Volk, K., Serafin, R., Grajeda, C., Baggili, I., 2022. Alt-tech social forensics: forensic analysis of alternative social networking applications. Forensic Sci. Int.: Digit. Invest. 42, 301406.

Kim, D.W., Yao, J., 2010. A web-based learning support system for inquiry-based learning. In: Web-based Support Systems. Springer, pp. 125–143.

LetsDefend, 2020. Lets defend. https://letsdefend.io.

Lim, B.-R., 2004. Challenges and issues in designing inquiry on the web. Br. J. Educ. Technol. 35 (5), 627–643.

Luh, R., Temper, M., Tjoa, S., Schrittwieser, S., Janicke, H., 2020. Penquest: a gamified attacker/defender meta model for cyber security assessment and education. Journal of Computer Virology and Hacking Techniques 16.

Luh, R., Eresheim, S., Großbacher, S., Petelin, T., Mayr, F., Tavolato, P., Schrittwieser, S., 2022. Penquest Reloaded: A Digital Cyber Defense Game for Technical Education.

Mahr, A., Cichon, M., Mateo, S., Grajeda, C., Baggili, I., 2021. Zooming into the pandemic! a forensic analysis of the zoom application. Forensic Sci. Int.: Digit. Invest. 36, 301107.

Malmi, L., Korhonen, A., Saikkonen, R., 2002. Experiences in automatic assessment on mass courses and issues for designing virtual courses. ACM SIGCSE Bulletin 34 (3), 55–59.

Marrington, A., Baggili, I., Ismail, T.A., Kaf, A.A., 2012. Portable web browser forensics: a forensic examination of the privacy benefits of portable web browsers. In: '2012 International Conference on Computer Systems and Industrial Informatics', pp. 1–6.

McCullough, S., Abudu, S., Onwubuariri, E., Baggili, I., 2021. Another brick in the wall: an exploratory analysis of digital forensics programs in the United States. Forensic Sci. Int.: Digit. Invest. 37, 301187.

OFFSEC for Orgs, 2012. https://www.offensive-security.com/offsec-for-orgs/.

Owens, K., Fulton, A., Jones, L., Carlisle, M., 2019. Pico-Boo!: How to Avoid Scaring Students Away in a Ctf Competition, 2013.

Research (2013). https://picoctf.org.

Ros, S., González, S., Robles, A., Tobarra, L., Caminero, A., Cano, J., 2020. Analyzing students' self-perception of success and learning effectiveness using gamification in an online cybersecurity course. IEEE Access 8, 97718–97728.

Roussev, V., McCulley, S., 2016. Forensic analysis of cloud-native artifacts. Digit. Invest. 16, S104–S113. DFRWS 2016 Europe.

Roussev, V., Barreto, A., Ahmed, I., 2016. Forensic Acquisition of Cloud Drives. *ArXiv* **a***bs/1603.06542*.

SWGDE, 2016. Swgde digital & multimedia evidence glossary. https://www.swgde.org/documents/published.

Thompson, M.F., Irvine, C.E., 2015. Cyberciege: a Video Game for Constructive Cyber Security Education.

Tryhackme, 2018. A fun way to learn cyber security. https://tryhackme.com/.

Tullis, J.G., Benjamin, A.S., 2011. On the effectiveness of self-paced learning. J. Mem. Lang. 64 (2), 109–118.

Walnycky, D., Baggili, I., Marrington, A., Moore, J., Breitinger, F., 2015. 'Network and device forensic analysis of android social-messaging applications'. Digit. Invest. 14, S77–S84 (The Proceedings of the Fifteenth Annual DFRWS Conference).

Woods, K., Lee, C.A., Garfinkel, S., Dittrich, D., Russell, A., Kearton, K., 2011. Creating realistic corpora for security and forensic education. In: Proceedings of the Conference on Digital Forensics, Security and Law. Association of Digital Forensics, Security and Law, p. 123.

Woolf, B.P., Reid, J., Stillings, N., Bruno, M., Murray, D., Reese, P., Peterfreund, A., Rath, K., 2002. A general platform for inquiry learning. In: International Conference on Intelligent Tutoring Systems. Springer, pp. 681–697.

Zhang, X., Baggili, I., Breitinger, F., 2017. Breaking into the vault: privacy, security and forensic analysis of android vault applications. Comput. Secur. 70, 516–531.