TECH THROUGH
THE LENS OF
SECURITY

ARTIFACT GENOME PROJECT

Expanding Digital Forensics Education With Artifact Curation And Scalable, Accessible Exercises Via The Artifact Genome Project

CINTHYA GRAJEDA, JESSICA BERRIOS, SANKOFA BENZO, EMMANUEL OGUNWOBI, & DR. IBRAHIM BAGGILI

DFRWS

USA 2023 Conference, Baltimore, MD

LSU BiT Lab

University of New Haven
CONNECTICUT INSTITUTE OF TECHNOLOGY

UNHcFREG

AUTHOR INFORMATION

Cinthya Grajeda

Cybersecurity Lab & Grants Manager
Artifact Genome Project Manager

Jessica Berrios

SFS Scholar
M.S. Cybersecurity 2025
B.S. Cybersecurity 2023

Sankofa Benzo

SFS Scholar
B.S. Cybersecurity 2024

Emmanuel Ogunwobi

M.S. Computer Science 2023
Cybersecurity & Networks

Dr. Ibrahim Baggili

Former Director, UNHcFREG
AGP Grant PI
Director, BiT Lab
Professor of Cybersecurity & Computer Science at LSU

This material is based upon work supported by the National Science Foundation under Grant Numbers 1900210 and 1921813. 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.

TABLE OF CONTENTS

UNDERSTANDING ARTIFACTS

"Information or data created as a result of the use of an electronic device that shows past activity."

The Scientific Working Group on Digital Forensics (SWDGE), 2015

- Registry Keys
- Logs
- Databases

INTRODUCTION

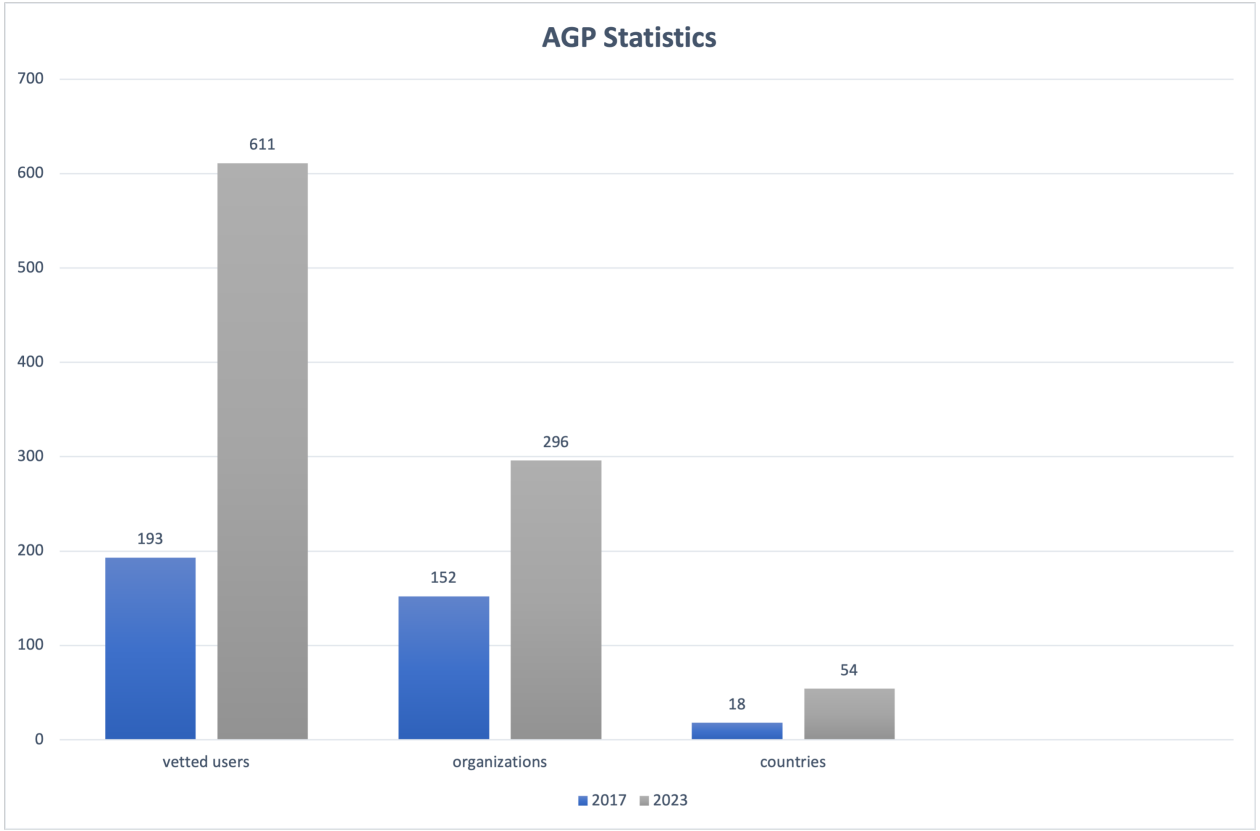
- The Artifact Genome Project launched in 2017.
- Presented ***Experience Constructing The Artifact Genome Project (AGP): Managing The Domain's Knowledge One Artifact At A Time,*** DFRWS USA 2018.
- At the time first of its kind.
- A look to the past:

User/System Statistics	
Vetted Users	193
Organizations	152
Countries	18

USER GROWTH

An overall growth of:

- 216.6% Vetted Users
- 94.7% Organizations
- 200% Countries



RELATED WORKS

- Grajeda, C., Sanchez, L., Baggili, I., Clark, D. and Breitinger, F. (2018), '*Experience constructing the artifact genome project (agp): managing the domain's knowledge one artifact at a time*', Digital Investigation 26, S47–S58.
- Mahr, A., Cichon, M., Mateo, S., Grajeda, C. and Baggili, I. (2021), '*Zooming into the pandemic! a forensic analysis of the zoom application*', Forensic Science International: Digital Investigation 36, 301107.
- Balon, T., Herlopian, K., Baggili, I., & Grajeda-Mendez, C. (2021, August). '*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).
- Mahr, A., Serafin, R., Grajeda, C., & Baggili, I. (2021, December). '*Auto-Parser: Android Auto and Apple CarPlay Forensics.*' In International Conference on Digital Forensics and Cyber Crime (pp. 52-71). Cham: Springer International Publishing.
- Johnson, H., Volk, K., Serafin, R., Grajeda, C. and Baggili, I. (2022), '*Alt-tech social forensics: Forensic analysis of alternative social networking applications*', Forensic Science International: Digital Investigation 42, 301406.
- Berrios, J., Mosher, E., Benzo, S., Grajeda, C., & Baggili, I. (2023). *'Factorizing 2FA: Forensic analysis of two-factor authentication applications.'* Forensic Science International: Digital Investigation, 45, 301569.

TYPES OF PLATFORMS

- Platforms range from traditional to non-traditional with an emphasis on game-based learning
- The inception of many of these platform occurred after AGP
- Many popular platforms are paid-only or are limited freemium
- Gamified platforms are often not available on public platforms

TYPES OF LEARNING

SELF PACED

AGP educational modules permit users to solve artifact challenges at their own pace over a web browser using open-source tools.

INQUIRY BASED

AGP platform contains scavenger hunt exercises that permit students to search for answers through browsing the AGP system for artifacts

CHALLENGE BASED

AGP platform contains challenges that users have to solve.

REAL WORLD DATA

AGP, all artifacts (CuFAs) pose potential forensic value to investigations, making them realistic.

FEATURES & FUNCTIONALITIES

SEARCH

This allows the users to search, by keyword, phrase, or title.

MY ASSIGNMENTS

Users can track the assignments that they have created and note the status of the assignments

CREATE ASSIGNMENTS

Provides the form where the assignment can be created.

REPORT CARD

Lists all assignments that have been taken by the user as well as the ones that are in progress.

FEATURES & FUNCTIONALITIES

LEADERSHIP

Presentation of communication tools that can be used as demonstration.

CLASSES

Students can join classes that are posted by their instructors.

CONFERENCES

Conferences that are hosted will be posted and archived here.

LEADERBOARD

Global leaderboard dependent on the number of points that individual users gain from completing assignments.

EDUCATIONAL MODULES

LEARN BY DOING

Users are provided with one or more artifacts, and the answers to the quiz questions are within the artifacts themselves.

LEARN ABOUT TOOLS

Educates the user on various types of tools used within cybersecurity.

LEARN ABOUT LINUX

Provides users an overview of features and functionalities of the Linux OS.

EDUCATIONAL MODULES

SCAVENGER HUNT

In these modules the users are quizzed on existing artifacts. The questions are multiple choice or flags.

LEARN ABOUT ARTIFACTS

These modules teach users about what an artifact is through recorded videos implemented into AGP.

LEARN ABOUT CYBER FORENSICS

This educational module introduce users to the field of Cyber forensics. Modules range from explaining cyber forensics to how to search and seize evidence at a crime scene

CREATION PROCESS

THE IDEA

Introduces the primary purpose of the assignment.

RESEARCH

Ensures idea is feasible and encompasses the full scope of the topic.

IDEA APPROVAL

Once idea is solidified by team lead and manager, student begins to create first draft.

FIRST DRAFT

Draft will go through initial review by team lead and student begins making necessary changes.

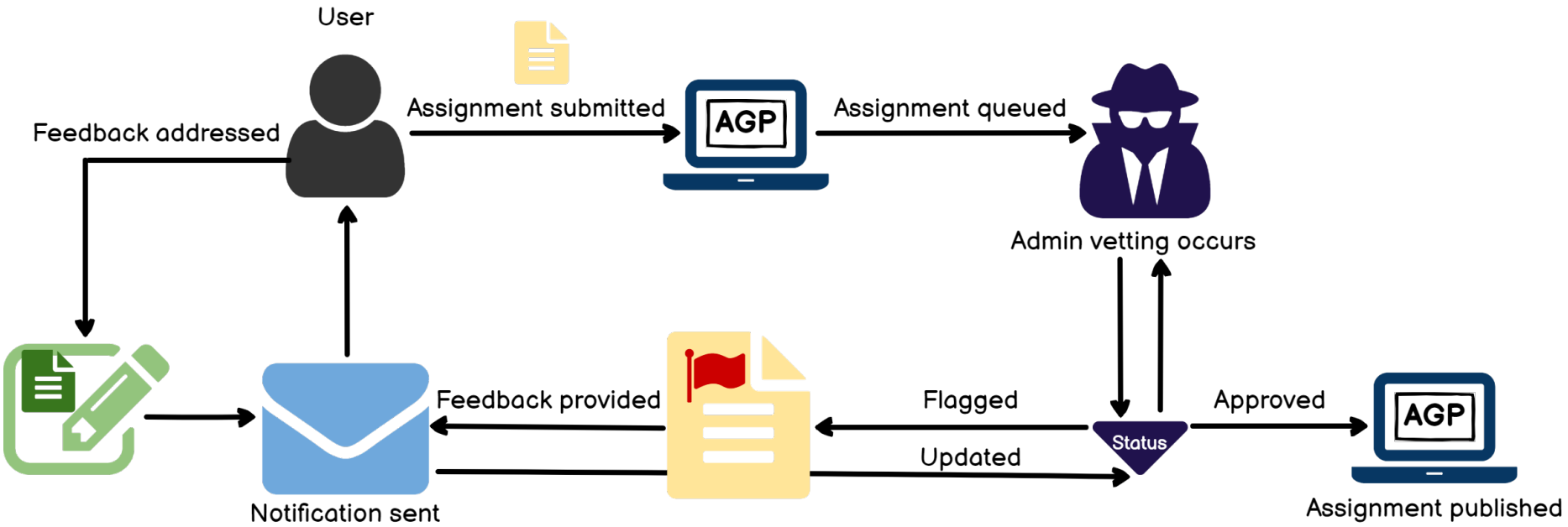
SECOND DRAFT

The student presents the second draft for AGP manager to review. During this stage team lead and manager also vet artifacts.

UPLOAD TO AGP

Once assignment is approved it is uploaded to AGP, the team lead will test the module to ensure it works as expected.

VETTING PROCESS



INTERPOL DIGITAL FORENSICS EXPERT GROUP

Methodology:

- 14 educational modules were selected
- One week to complete the challenge
- Users were vetted before participation

Sample:

- 14 conference participants

Survey Design:

- 14 questions
  - 6 Likert Scale
  - 2 Multiple Choice
  - 6 Free Response.

DIGITAL FORENSIC RESEARCH WORKSHOP ASIA-PACIFIC

Methodology:

- 15 educational modules were selected
- Three days to complete the challenge
- Users were vetted before participation

Sample:

- 15 conference participants

Survey Design:

- 19 questions
  - 6 Multiple Choice
  - 1 Likert Scale
  - 4 Net Promoter Score
  - 8 Free Response

UNIVERSITY COURSE

Background:

- Employed at the University of New Haven through its Small-Scale Digital Forensic Science course in the Fall semester of 2020 and 2021

Sample:

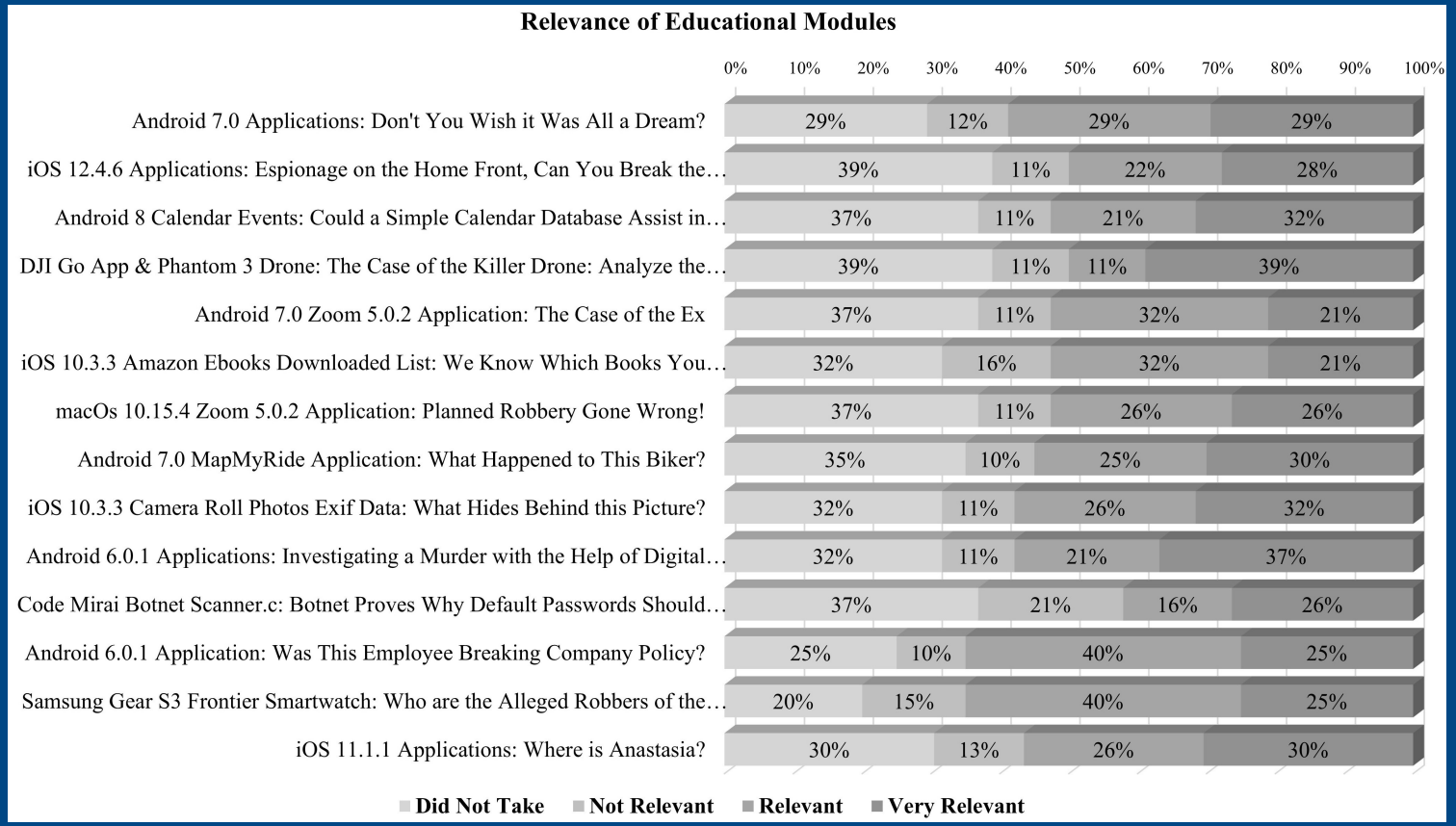
- Two sets of 19 and 24 students

Survey Design:

- 16 questions containing
  - 5 Multiple Choice
  - 1 Likert Scale
  - 4 Net Promoter Score
  - 6 Free Response.

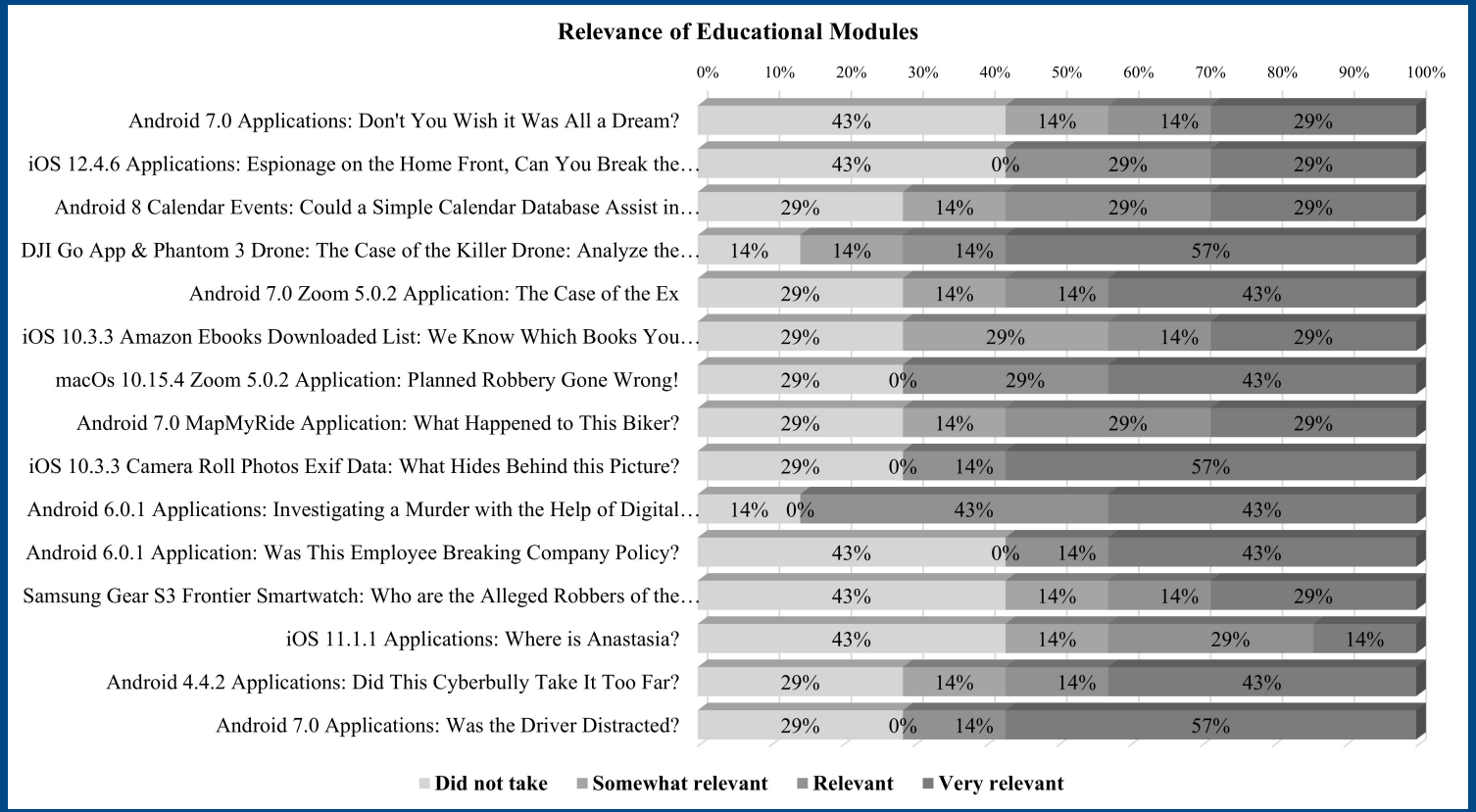
Number	Feedback
1	I learnt how to use artefacts in several ways, the open source tools were very helpful. Plist files, sqlite files and so on.
2	Zoom, Kik, iOs camera roll artifacts.
3	To me as an NCB, this event is very unique and full of experts to share most of the knowledge that I have never known 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.2: Key Takeaways from the DFEG Conference's AGP Challenge & Overall Experience


Relevance of Educational Modules
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
Android 7.0 Applications: Don't You Wish it Was All a Dream?
29%
12%
29%
29%
iOS 12.4.6 Applications: Espionage on the Home Front, Can You Break the…
39%
11%
22%
28%
Android 8 Calendar Events: Could a Simple Calendar Database Assist in…
37%
11%
21%
32%
DJI Go App & Phantom 3 Drone: The Case of the Killer Drone: Analyze the…
39%
11%
11%
39%
Android 7.0 Zoom 5.0.2 Application: The Case of the Ex
37%
11%
32%
21%
iOS 10.3.3 Amazon Ebooks Downloaded List: We Know Which Books You…
32%
16%
32%
21%
macOs 10.15.4 Zoom 5.0.2 Application: Planned Robbery Gone Wrong!
37%
11%
26%
26%
Android 7.0 MapMyRide Application: What Happened to This Biker?
35%
10%
25%
30%
iOS 10.3.3 Camera Roll Photos Exif Data: What Hides Behind this Picture?
32%
11%
26%
32%
Android 6.0.1 Applications: Investigating a Murder with the Help of Digital…
32%
11%
21%
37%
Code Mirai Botnet Scanner.c: Botnet Proves Why Default Passwords Should…
37%
21%
16%
26%
Android 6.0.1 Application: Was This Employee Breaking Company Policy?
25%
10%
40%
25%
Samsung Gear S3 Frontier Smartwatch: Who are the Alleged Robbers of the…
20%
15%
40%
25%
iOS 11.1.1 Applications: Where is Anastasia?
30%
13%
26%
30%
Did Not Take
Not Relevant
Relevant
Very Relevant

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


Relevance of Educational Modules
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
Android 7.0 Applications: Don't You Wish it Was All a Dream? 43% 14% 14% 29%
iOS 12.4.6 Applications: Espionage on the Home Front, Can You Break the… 43% 0% 29% 29%
Android 8 Calendar Events: Could a Simple Calendar Database Assist in… 29% 14% 29% 29%
DJI Go App & Phantom 3 Drone: The Case of the Killer Drone: Analyze the… 14% 14% 14% 57%
Android 7.0 Zoom 5.0.2 Application: The Case of the Ex 29% 14% 14% 43%
iOS 10.3.3 Amazon Ebooks Downloaded List: We Know Which Books You… 29% 29% 14% 29%
macOs 10.15.4 Zoom 5.0.2 Application: Planned Robbery Gone Wrong! 29% 0% 29% 43%
Android 7.0 MapMyRide Application: What Happened to This Biker? 29% 14% 29% 29%
iOS 10.3.3 Camera Roll Photos Exif Data: What Hides Behind this Picture? 29% 0% 14% 57%
Android 6.0.1 Applications: Investigating a Murder with the Help of Digital… 14% 0% 43% 43%
Android 6.0.1 Application: Was This Employee Breaking Company Policy? 43% 0% 14% 43%
Samsung Gear S3 Frontier Smartwatch: Who are the Alleged Robbers of the… 43% 14% 14% 29%
iOS 11.1.1 Applications: Where is Anastasia? 43% 14% 29% 14%
Android 4.4.2 Applications: Did This Cyberbully Take It Too Far? 29% 14% 14% 43%
Android 7.0 Applications: Was the Driver Distracted? 29% 0% 14% 57%
Did not take
Somewhat relevant
Relevant
Very relevant

ACADEMIC IMPACT

- Students are the main contributors to educational modules
- AGP has had a workforce of over 41 students varying between interns, paid students, and volunteers
- Students have grown their skills and gained new knowledge and experience in different disciplines
- AGP helps to provide students with various opportunities such as scholarships
- Students have become contributors to academia by publishing papers

PROFESSIONAL IMPACT

- Significant contribution to the cybersecurity community to help balance the growth in cybercrimes with the need for knowledgeable individuals
- Repository for digital forensic artifacts
- Provide users with a more granular understanding of digital forensic artifacts

FUTURE WORK

- Focus on continuous improvement and evolution
- Transfer of the system to Louisiana State University
- Partnerships with academia and other organizations will be a priority to pursue
- Development on a new system portal is underway
- Allow universities and conferences to host their events and courses

DEMO

CONCLUSION

- Invaluable resource to the cybersecurity community
- Offers a plethora of assignments with a focus on using digital artifacts with nuance
- Has served as a springboard with which other cybersecurity learning platforms have used to emerge.

CONTACT

Jessica Berrios	jberr6@unh.newhaven.edu
Sankofa Benzo	sbenz1@unh.newhaven.edu
Cinthya Grajeda	cgrajedamendez@newhaven.edu
Ibrahim Baggili	ibaggili@lsu.edu
Emmanuel Ogunwobi	eogun1@unh.newhaven.edu
AGP	agp@newhaven.edu
AGP Website	www.agp.newhaven.edu

THANK YOU