SAND2015-5818R

UVI Cyber-security Workshop

Workshop Analysis

Jacob Allsop, Ben Anderson, Marc Boumedine, Cedric Carter Jr., Seanmichael Galvin, Oscar Gonzalez, Tommie Kuykendall, Wellington Lee, Han Lin, Tyler Morris, Kevin Nauer, Beth Potts, Kim Ta, Jennifer Trasti, David White

7/8/2015

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000

Table of Contents

Executive Summary

The cybersecurity consortium, which was established by DOE/NNSA's Minority Serving Institutions Partnerships Program (MSIPP), allows students from any of the partner schools (13 HBCUs, two national laboratories, and a public school district) to have all consortia options available to them, to create career paths and to open doors to DOE sites and facilities to student members of the consortium. As a part of this year consortium activities, Sandia National Laboratories and the University of Virgin Islands conducted a week long cyber workshop that consisted of three courses; Digital Forensics and Malware Analysis, Python Programming, and ThunderBird Cup. These courses are designed to enhance cyber defense skills and promote learning within STEM related fields.

The Digital Forensics and Malware Analysis program focused on raising awareness in Digital Forensics and Incidence Response (DFIR). The program was accomplished through multi-faceted approach of presentations, demonstrations, and hands on training to enable attendees to experience some actual day-to-day core activities within DFIR. Numerous forensics tools were utilized in the hands on training that contributed to the attendees' ability to participate in a mini Tracer Fire event at the end of the program.

The Python Training course was designed to teach an audience with little to no programming experience how to program in Python with an emphasis in developing cyber security codes. The Python Training Course consisted of four, hour-and-a-half long instructor-led classes. The course began with an introduction to the command line interface and branched to cover Python basics and Python for forensics and network programming. The course was presented in-person at the University of the Virgin Islands campus at St. Thomas and via video-teleconference to the University of the Virgin Islands campus at St. Croix.

The ThunderBird Cup program was primarily focused on boosting interest in STEM fields for students ranging from grade 6-12. The ThunderBird Cup is a cyber-security awareness exercise that uses hands on training to prepare students to compete in the CyberPatriot competition.

In addition, we also hosted a cyber-STEM forum discussion with members of the United States Virgin Islands (USVI) Education Department, community leaders, University of Virgin Islands (UVI) staff, STEM educators, and local technology business leaders to discuss how to best utilize the DOE/NNSA MSIPP's partnership and collaboration (Industry-education partnerships, project-based learning, and maximizing use of regional STEM resources) to train local students on key information technology (IT) and cyber skills for success in the 21st Century workplace, and connect workforce and education for mutual benefit.

Overall, the Digital Forensics and Malware Analysis and Python Training course attracted over 30 individuals with a wide variety of backgrounds. The ThunderBird Cup attracted 23 students from grades 6 – 11. The workshop and Cyber-STEM Forum received a great deal of positive feedback and press publicity while at the University of the Virgin Islands.

Cyber USVI Workshop

This workshop was hosted at the University of the Virgin Islands (St. Thomas and St. Croix campuses) from June 15-19, 2015, and was sponsored by the DOE Minority Serving Institution Partnership Program (MSIPP). The goal of the MSIPP is to establish a world-class workforce development, education, and research program that combine the strengths of Historically Black Colleges and Universities (HBCUs) and the DOE/NNSA National Laboratories to create and to train a stronger work force within the STEM fields. Cyber security is one of several funded consortiums within the overall DOE MSIPP.

Purpose Statement

The purpose of the workshop was to expose participants to what the field of cyber security is about and to highlight some of the challenging occupations within this exciting field such as Digital Forensics and Incident Response (DFIR). Staff members from Sandia National Laboratories introduced some of the basic DFIR techniques used by the Sandia Cyber Security Incident Response Team (CSIRT) during cyber-attacks and allow students to study a major malware campaign while playing the role of an incident response team member. The workshop fulfils its purpose through three educational modules including:

1. Digital Forensics and Malware Analysis
2. Python Programming
3. ThunderBird Cup

Goals

- Engage faculty, staff, and students at UVI in a cyber-security focused pre-workshop in preparation for a 5-week camp hosted by UVI that introduces cyber security and STEM topics for middle school students
- Interact with members of the high tech community in the United States Virgin Islands (USVI) to help UVI in its quest to become a hub of technology research and education in the Caribbean region
- Teach students, with little or no programming experience, how to program and perform forensics with Python
- Bring cyber awareness to students in grades 6-12
- Spark interest in the national youth cyber competition CyberPatriot

Entities Involved

- 33 attendees from the University of Virgin Islands; USVI law enforcement agencies, educators, students, and IT professionals participated

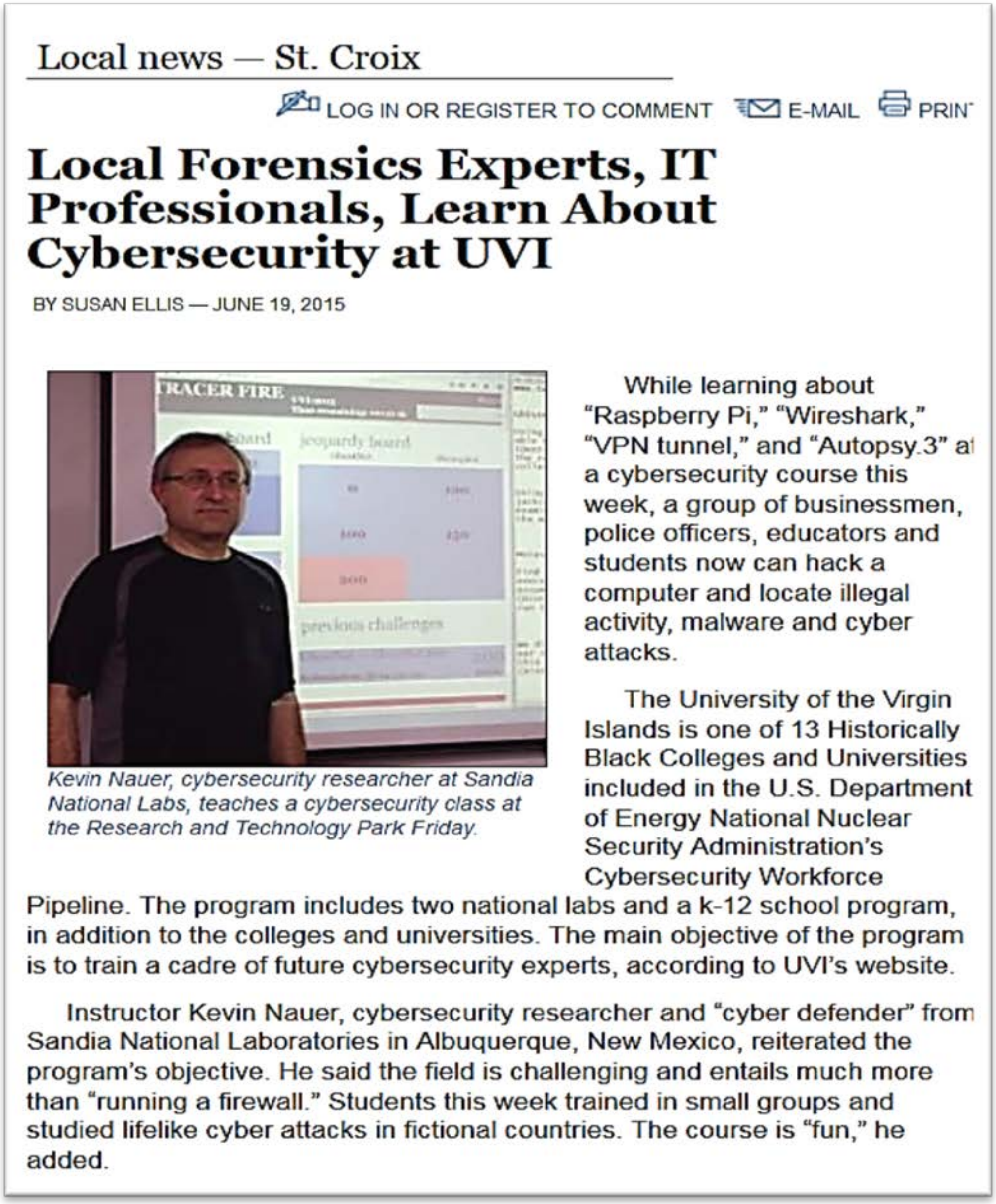
- Raised the visibility of the DOE/NNSA MSIPP and its potential positive impact on the USVI community, a community forum was hosted with members of the USVI Education Department, local tech business leaders, UVI staff, and interested participants
- A total of 23 students ranging from grades 6-11

Future Opportunities

Discussions were held between UVI, Sandia, and local community members to identify possible future collaboration. A number of ideas were offered during these discussions:

- Support the integration of capstone projects into the curriculum for the members of the consortium
- Explore collaboration with the United Negro College Fund (UNCF) and leverage its industrial partnerships, programs and activities, and funding support
- Review Sandia materials developed for the Tracer FIRE host forensics program and see how they may be translated into something appropriate for different computer experience levels with particular focus at the high school and middle school levels and where the crossover into the university level occurs
- Collaborate on co-advising student research on independent study and capstone research projects at both undergraduate and graduate levels, so students can benefit from working with SNL and other consortium member institutions on year-round basis in addition to summer internships
- Replicating/adapting the Tracer Fire competition and experimentation environment (with some components needing additional release approval by SNL) at UVI and NSU
- Investigate how NSU's Netlab+ can be utilized in some of the introductory level courses (both K-12 and university) which will help lower the bar for faculty wishing to offer forensics type of lab exercises in their courses without the additional overhead of setting up a more complex environment
- Authoring of cyber security training and workshop publications for shared use within the consortium
- Develop the workshop to involve other MSI Consortium schools to advance cyber security curriculums

News Release



Local news — St. Croix

Local Forensics Experts, IT Professionals, Learn About Cybersecurity at UVI

BY SUSAN ELLIS — JUNE 19, 2015

Kevin Nauer, cybersecurity researcher at Sandia National Labs, teaches a cybersecurity class at the Research and Technology Park Friday.

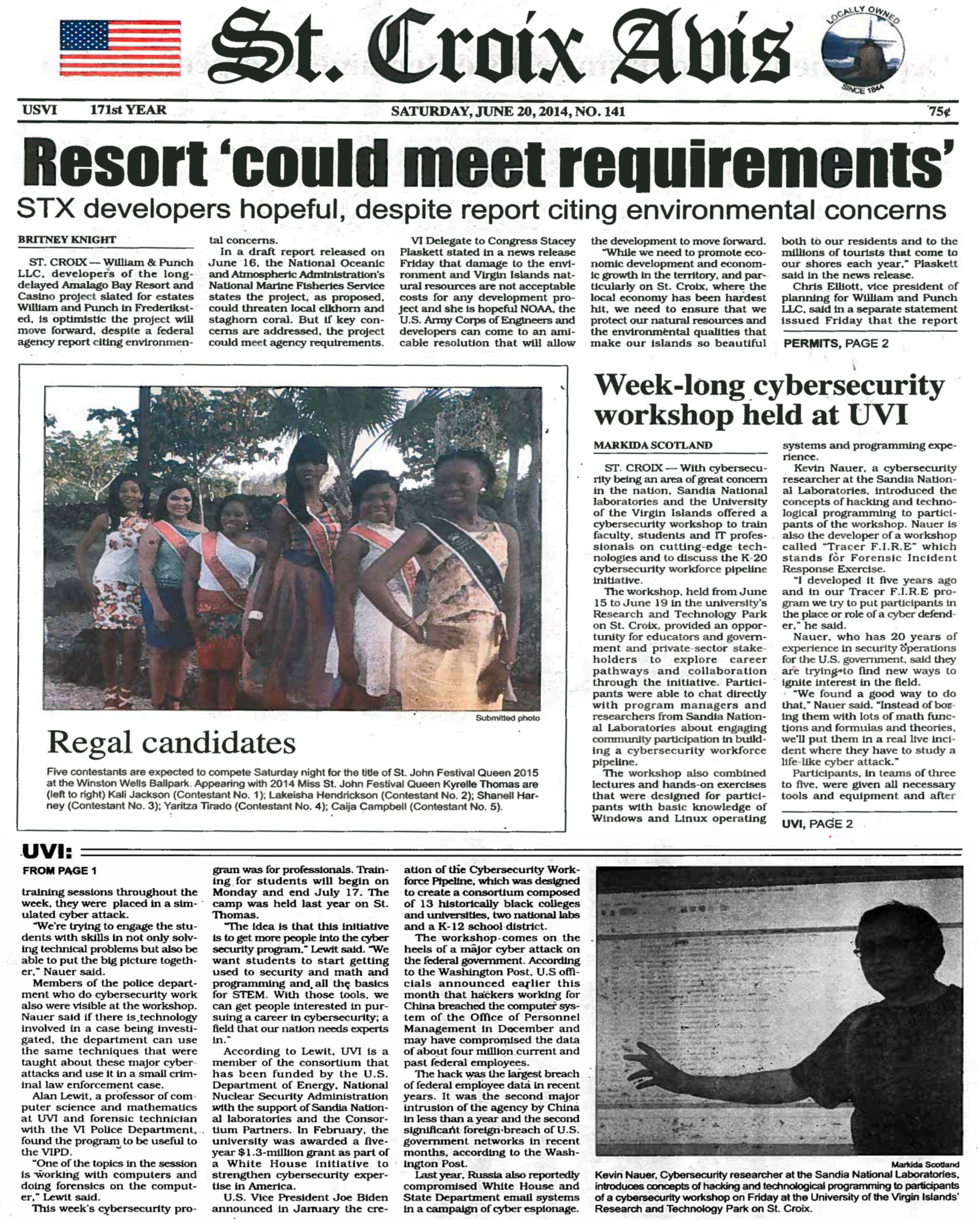
While learning about "Raspberry Pi," "Wireshark," "VPN tunnel," and "Autopsy.3" at a cybersecurity course this week, a group of businessmen, police officers, educators and students now can hack a computer and locate illegal activity, malware and cyber attacks.

The University of the Virgin Islands is one of 13 Historically Black Colleges and Universities included in the U.S. Department of Energy National Nuclear Security Administration's Cybersecurity Workforce Pipeline. The program includes two national labs and a k-12 school program, in addition to the colleges and universities. The main objective of the program is to train a cadre of future cybersecurity experts, according to UVI's website.

Instructor Kevin Nauer, cybersecurity researcher and "cyber defender" from Sandia National Laboratories in Albuquerque, New Mexico, reiterated the program's objective. He said the field is challenging and entails much more than "running a firewall." Students this week trained in small groups and studied lifelike cyber attacks in fictional countries. The course is "fun," he added.

Source:

http://stcroixsource.com/content/news/local-news/2015/06/19/local-forensics-experts-it-professionals-learn-about-cybersecurit



St. Croix Avis

LOCALLY OWNED · SINCE 1844

USVI 171st YEAR SATURDAY, JUNE 20, 2014, NO. 141 75¢

Resort 'could meet requirements'

STX developers hopeful, despite report citing environmental concerns

BRITNEY KNIGHT

ST. CROIX — William & Punch LLC, developers of the long-delayed Amalago Bay Resort and Casino project slated for estates William and Punch in Frederiksted, is optimistic the project will move forward, despite a federal agency report citing environmental concerns.

In a draft report released on June 16, the National Oceanic and Atmospheric Administration's National Marine Fisheries Service states the project, as proposed, could threaten local elkhorn and staghorn coral. But if key concerns are addressed, the project could meet agency requirements.

VI Delegate to Congress Stacey Plaskett stated in a news release Friday that damage to the environment and Virgin Islands natural resources are not acceptable costs for any development project and she is hopeful NOAA, the U.S. Army Corps of Engineers and developers can come to an amicable resolution that will allow the development to move forward.

"While we need to promote economic development and economic growth in the territory, and particularly on St. Croix, where the local economy has been hardest hit, we need to ensure that we protect our natural resources and the environmental qualities that make our islands so beautiful both to our residents and to the millions of tourists that come to our shores each year," Plaskett said in the news release.

Chris Elliott, vice president of planning for William and Punch LLC, said in a separate statement issued Friday that the report

PERMITS, PAGE 2

Submitted photo

Regal candidates

Five contestants are expected to compete Saturday night for the title of St. John Festival Queen 2015 at the Winston Wells Ballpark. Appearing with 2014 Miss St. John Festival Queen Kyrelle Thomas are (left to right) Kali Jackson (Contestant No. 1); Lakeisha Hendrickson (Contestant No. 2); Shanell Harney (Contestant No. 3); Yaritza Tirado (Contestant No. 4); Caija Campbell (Contestant No. 5).

Week-long cybersecurity workshop held at UVI

MARKIDA SCOTLAND

ST. CROIX — With cybersecurity being an area of great concern in the nation, Sandia National laboratories and the University of the Virgin Islands offered a cybersecurity workshop to train faculty, students and IT professionals on cutting-edge technologies and to discuss the K-20 cybersecurity workforce pipeline initiative.

The workshop, held from June 15 to June 19 in the university's Research and Technology Park on St. Croix, provided an opportunity for educators and government and private-sector stakeholders to explore career pathways and collaboration through the initiative. Participants were able to chat directly with program managers and researchers from Sandia National Laboratories about engaging community participation in building a cybersecurity workforce pipeline.

The workshop also combined lectures and hands-on exercises that were designed for participants with basic knowledge of Windows and Linux operating systems and programming experience.

Kevin Nauer, a cybersecurity researcher at the Sandia National Laboratories, introduced the concepts of hacking and technological programming to participants of the workshop. Nauer is also the developer of a workshop called "Tracer F.I.R.E" which stands for Forensic Incident Response Exercise.

"I developed it five years ago and in our Tracer F.I.R.E program we try to put participants in the place or role of a cyber defender," he said.

Nauer, who has 20 years of experience in security operations for the U.S. government, said they are trying to find new ways to ignite interest in the field.

"We found a good way to do that," Nauer said. "Instead of boring them with lots of math functions and formulas and theories, we'll put them in a real live incident where they have to study a life-like cyber attack."

Participants, in teams of three to five, were given all necessary tools and equipment and after

UVI, PAGE 2

UVI:

FROM PAGE 1

training sessions throughout the week, they were placed in a simulated cyber attack.

"We're trying to engage the students with skills in not only solving technical problems but also be able to put the big picture together," Nauer said.

Members of the police department who do cybersecurity work also were visible at the workshop. Nauer said if there is technology involved in a case being investigated, the department can use the same techniques that were taught about these major cyber-attacks and use it in a small criminal law enforcement case.

Alan Lewit, a professor of computer science and mathematics at UVI and forensic technician with the VI Police Department, found the program to be useful to the VIPD.

"One of the topics in the session is working with computers and doing forensics on the computer," Lewit said.

This week's cybersecurity program was for professionals. Training for students will begin on Monday and end July 17. The camp was held last year on St. Thomas.

"The idea is that this initiative is to get more people into the cyber security program," Lewit said. "We want students to start getting used to security and math and programming and all the basics for STEM. With those tools, we can get people interested in pursuing a career in cybersecurity; a field that our nation needs experts in."

According to Lewit, UVI is a member of the consortium that has been funded by the U.S. Department of Energy, National Nuclear Security Administration with the support of Sandia National laboratories and the Consortium Partners. In February, the university was awarded a five-year $1.3-million grant as part of a White House initiative to strengthen cybersecurity expertise in America.

U.S. Vice President Joe Biden announced in January the creation of the Cybersecurity Workforce Pipeline, which was designed to create a consortium composed of 13 historically black colleges and universities, two national labs and a K-12 school district.

The workshop comes on the heels of a major cyber attack on the federal government. According to the Washington Post, U.S officials announced earlier this month that hackers working for China breached the computer system of the Office of Personnel Management in December and may have compromised the data of about four million current and past federal employees.

The hack was the largest breach of federal employee data in recent years. It was the second major intrusion of the agency by China in less than a year and the second significant foreign breach of U.S. government networks in recent months, according to the Washington Post.

Last year, Russia also reportedly compromised White House and State Department email systems in a campaign of cyber espionage.

Markida Scotland

Kevin Nauer, Cybersecurity researcher at the Sandia National Laboratories, introduces concepts of hacking and technological programming to participants of a cybersecurity workshop on Friday at the University of the Virgin Islands' Research and Technology Park on St. Croix.

Source: St. Croix Avis Newspaper

Program: Digital Forensics and Malware Analysis

Purpose Statement

The program was created to raise awareness and to train faculty, staff, and professionals within the Cyber Security MSI Consortium of Digital Forensics and Incident Response (DFIR) - an applied discipline within cyber security - and to explore new educational approaches for integrating applied cyber security topics such as DFIR into the curriculum.

Goals

- Raise awareness of what the disciplines of DFIR and malware analysis are to students and local professionals
- Motivate the introduction of new curriculum oriented towards these topics (Digital Forensics and malware analysis) within cyber security educational programs hosted within the consortium (certificate programs, technical focused tracks, and cyber security degree programs)
- Help participants understand how organized criminal enterprises and nation states conduct cyber-attacks
- Provide breadth and depth into the technology and tools that professionals use in the field to conduct memory and disk forensics. Help faculty explore how these kinds of tools can be introduced into the curriculum
- Help participants understand how attackers exploit web browsers and the social engineering aspect of these threats
- Lead a discussion on how Sandia can help UVI to develop friendly malware for educational purposes

Steps Taken to Accomplish Goals

- Sandia technical staff members authored and presented a training course that included presentations and demonstrations to expose the participants to the various facets that make up the field of Digital Forensics and Incident Response (DFIR)
- Participants were also given hands-on training with forensic tools such as Volatility, Wireshark, Autopsy, Chopshop, Metasploit, and Browser Exploitation Framework
- Participants were required to actively take part in a live exercise
- Instructors offered assistance and mentoring during the training exercise

History

In FY14, as part of the MSIPP, Sandia and UVI created a program where subject matter experts in cybersecurity helped UVI to host a workshop on cybersecurity topics, with a focus on digital forensics. In July 2014, a team of technical staff members from Sandia/NM traveled to St. Thomas to conduct training for students, faculty, staff, and area professionals in a variety of areas of digital forensics including analysis of Windows registry, disk forensics, networks and system architecture. Some of the topics were originally developed for Sandia's Tracer FIRE live cyber exercise and modified for use at UVI. Tracer FIRE enables participants to experience what a real Cyber Security Incident Response Team (CSIRT) does on a daily basis by recreating a major cyber attack and allowing the participants to fill various roles of a CSIRT in a competition oriented event.

Program Explanation

The course focused on the exciting field of digital forensics and malware analysis in the hope of enabling the participants to think like an attacker. The course also enabled students to deliberately run malware in a safe environment in order to closely examine its behavior and determine how to detect this malware in a live environment.

Lessons Breakdown

- Lesson 1 - Cyber Kill Chain, Case Study Overview, Windows Credentials, IR workflow and Scot Collaborative Incident Response Tracker
- Lesson 2 – Wireshark and Network Packet Analysis, Malware Hunting with Sysinternals, and Memory Forensics with Volatility
- Lesson 3 - Disk Forensics with Autopsy, Analysis of Windows Registry Hives, Browser Forensics / Browser Credentials, Hands on Practical Lab Work
- Lesson 4 – Metasploit and Browser Exploitation Framework (BEEF), Armitage, IE Browser exploit demo
- Capstone - Mini Tracer FIRE – engaged participants with a hands-on team exercise where students from the St. Thomas campus competed against students from the St Croix campus.

Outcome

- Participants had opportunities to learn various facets of cyber security by taking part in several practical hands-on exercises that afforded them the opportunity to act as incident responders using the techniques and various forensic security tools that they received training on
- Participants learned how systems are attacked and compromised
- Participants were able to analyze memory and disk forensics
- Participants were capable of illustrating skills learned throughout the week in a mini Tracer Fire

Program: Python Course Training Overview

Purpose Statement

Teach students with no programming experience how to program with the Python language. This course provides students with two primary “takeaways.” The first takeaway is a week-long course, the focus of which is an introduction to the computer language Python. This introductory course requires students to start programming Python in the first hour and then write and modify code throughout. The second takeaway for students is a copy of the complete class materials containing examples, exercises, and labs to use for teaching others this introduction to programming with the Python programming language. These materials were created specifically copyright-free and were provided to all students on the first day.

Goals

- Teach students, with little or no programming experience, how to program with Python
- Provide course materials to curriculum creators and teachers
- Introduce students to using Python for computer forensics
- Introduce students to new cyber-resources

Steps Taken to Accomplish Goals

- Students were taught to program in Python through instructor-led discussions
- Students were given handouts and code to supplement discussions in class
- The students participated in lab sessions to create and modify Python code
- Instructors were available to answer students’ questions during discussions and lab work

History

In 2014, the authors of this course developed an internal Sandia Laboratories class called “Python for Experienced Programmers.” The class was taught to experienced programmers who are employees of several divisions across the labs. The authors of this course drew on the experiences gained in teaching a Python course to experienced programmers.

Early in development the authors were informed that some members of the class would not be familiar with the command line interface in Windows, yet would likely go on to teach the course to students at their universities. Unfamiliarity with the command line is a reasonable indicator of “no formal programming experience.” We therefore determined that our primary audience would be these students and started the course with an introduction to the command line interface.

Program Explanation

The MSI Introductory Python Programming Course is a set of four, hour-and-a-half long class sessions broken into learning “modules.” Each module focuses on one or more Python programs. There are no slides, only instructor-led discussion focusing on the code, followed by brief exercises that require the student to modify and add previous concepts to the current code. Students are given handouts with more detailed information than can be covered during class lectures, and encouraged to ask follow-up questions.

The course is geared primarily to those who have never programmed, but full course materials are provided on day one and advanced students are encouraged to work ahead and ask questions as needed. The instructors discourage competition between students to keep beginners motivated.

Following each course section is an hour-and-a-half laboratory session devoted to modifying and/or creating code to solve one or two problems related to the day's course module. Students are encouraged to work at their own pace and to continue with the module exercises if that is their comfort level.

This course borrowed some student handouts and techniques from a Sandia Free University (SFU) class, "Python for Experienced Programmers." It also drew upon the following for inspiration:

- Python For Kids: A Playful Introduction to Programming, Jason R. Briggs
- Black Hat Python: Python Programming for Hackers and Pentesters, Justin Seitz
- Violent Python: A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers, TJ O'Conner

Several of the code modules were provided as useful everyday tools for teachers and IT professionals including: a multiple-choice exam randomizer/creator, Comma-separated-value boilerplate code, a grading program, a bar-chart data display program, Windows registry analysis code, and Graphical User Interface sample code.

Lessons Breakdown

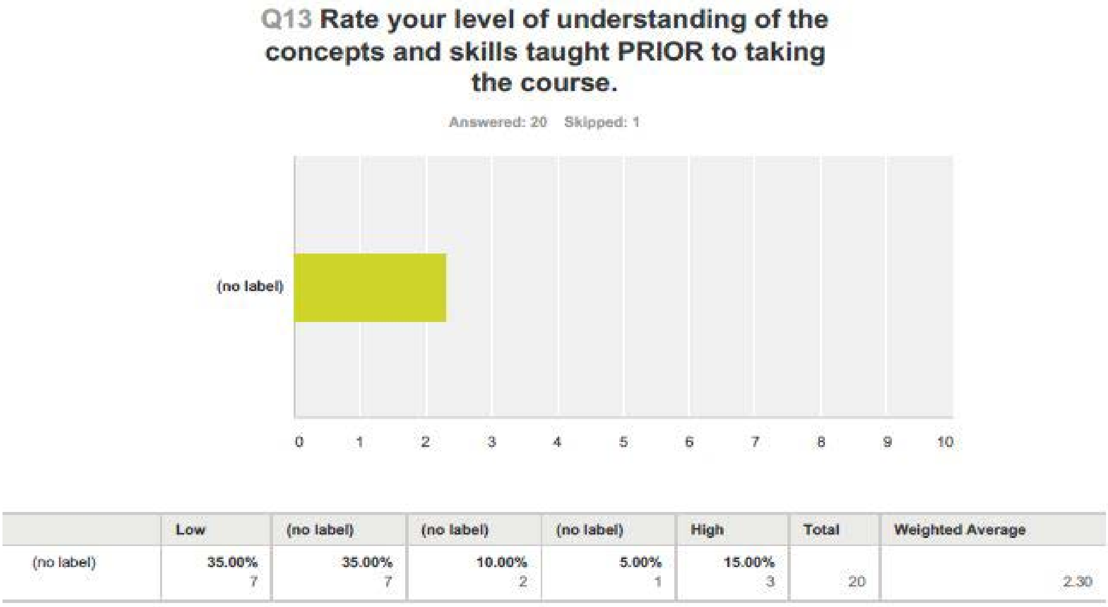
- **Day One**
    - Introduction to the command line
    - Opening Windows applications with Python
    - Interactive user I/O
    - File I/O
    - Labs
- **Day Two**
    - Processing forensic data
    - Labs
- **Day Three**
    - Code Reuse
    - Writing program from scratch
    - Labs
- **Day Four**
    - Bit twiddling
    - List slicing
    - Calling windows native functions with Ctypes
    - Lab

- **Videos**
    - How to install pipwheel
    - How to install python
    - How to install matplotlib

Each lesson included hands on code for students to use, modify, and learn based on the particular subject taught. In addition after each lesson, a lab that was given to harden the student's learning experience. Also, there were tutorial videos that showed the students how to install additional tools for use.

Outcomes

- Participants were able to program in Python
- The participants learned to compose Python code to perform computer forensic tasks
- Participants were given materials to incorporate into their own classes

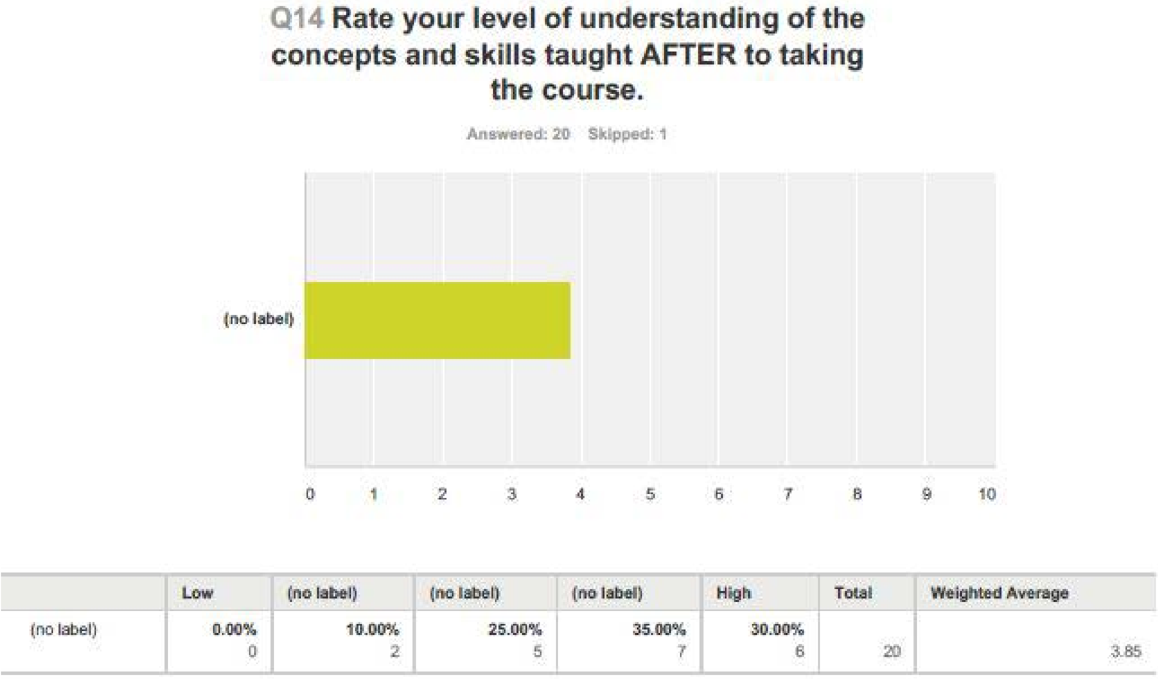


Q13 Rate your level of understanding of the concepts and skills taught PRIOR to taking the course.

Answered: 20 Skipped: 1

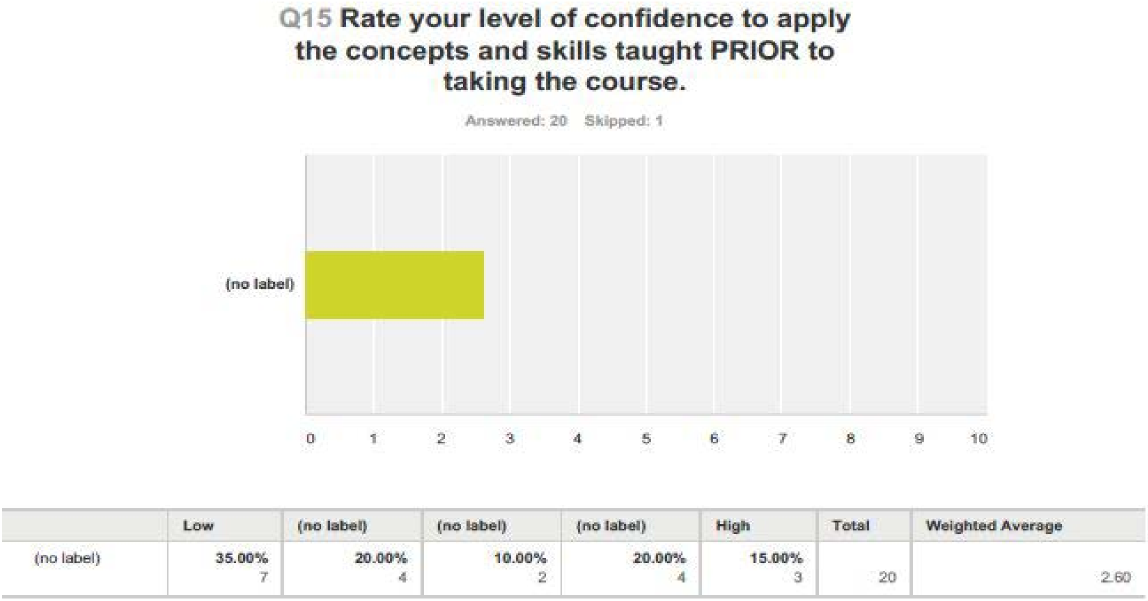
	Low	(no label)	(no label)	(no label)	High	Total	Weighted Average
(no label)	35.00% 7	35.00% 7	10.00% 2	5.00% 1	15.00% 3	20	2.30

Figure 1. Level of understanding prior to the course based on a scale of 1-5: '1' poor, '5' is best.



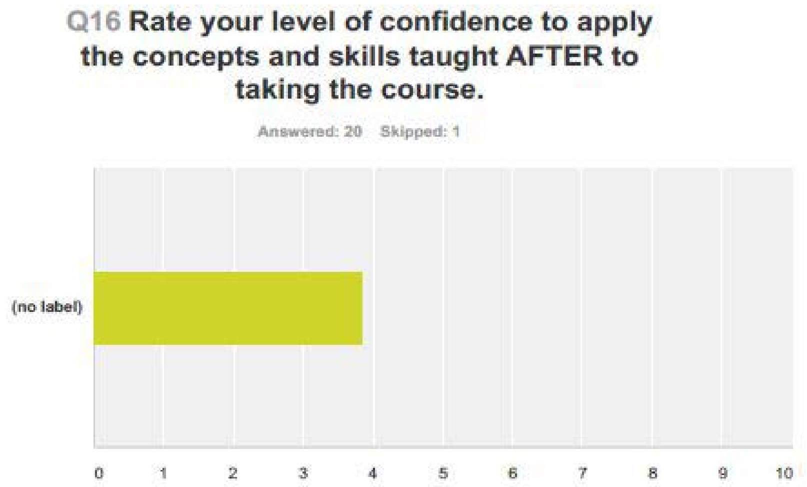
	Low	(no label)	(no label)	(no label)	High	Total	Weighted Average
(no label)	0.00% 0	10.00% 2	25.00% 5	35.00% 7	30.00% 6	20	3.85

Figure 2. Level of understanding after the course based on a scale of 1-5: '1' poor, '5' is best.



	Low	(no label)	(no label)	(no label)	High	Total	Weighted Average
(no label)	35.00% 7	20.00% 4	10.00% 2	20.00% 4	15.00% 3	20	2.60

Figure 3. Level of confidence before taking the course based on a scale of 1-5: '1' poor, '5' is best.



	Low	(no label)	(no label)	(no label)	High	Total	Weighted Average
(no label)	0.00% 0	10.00% 2	30.00% 6	25.00% 5	35.00% 7	20	3.85

Figure 4. Level of confidence after taking the course based on a scale of 1-5: '1' poor, '5' is best.

Conclusions

- Participants' feedback on level of understanding and confidence level prior/after was encouraging.
- There were a 10+% increase in both categories at the end of the workshop. However, it is too early to associate the increase to any variables, e.g., the instructors, materials, hands on exercise, etc., due to limited data point.

Recommendations

- Continue to work with consortium faculty to improve and enhance workshop materials
- Work with consortium partners to create effective survey questions
- Ensure there is alignment of workshop training to cyber security and IT pathway courses

Program: ThunderBird Cup Training

Purpose Statement

Provides students with a constructive learning environment that will encourage them to further their education in STEM related fields.

Goals

- Bring cyber awareness to students in grades 6-12
- Engage students in fields related to STEM
- Spark interest in the national youth cyber competition CyberPatriot

Steps Taken to Accomplish Goals

- Provided students with a hands on learning environment
- Gave them material that will spark interest in desired fields
- Provided opportunities for students to participate in the national youth cyber competition CyberPatriot

History

The ThunderBird Cup program was first tested in 2014 at University of the Virgin Islands. Students were given hands on experience in cyber security to help prepare them for the upcoming year of CyberPatriot. Those students created a middle school team and made it all the way to the semi-finals round of the competition.

Program Explanation

The ThunderBird Cup is a cyber-security awareness exercise created by Sandia National Laboratories. The program uses hands on training and competition to engage students in the exciting field of cyber security in the hope of leading them to further their education in STEM related fields.

Lessons Breakdown

- Lesson 0 –Fundamentals
- Lesson 1 –Windows Navigation
- Lesson 2 –Administrative tools
- Lesson 3 –Malware Protection/Passwords
- Lesson 4 –Remote/File Sharing
- Lesson 5 –Programs/Task Scheduler

Each lesson included tutorial videos on the related subject. Along with the videos, each lesson had pre and post questions to test the student's retention. At the end of each day's lessons, students were tasked with securing a virtual machine.

Outcomes

- Students gained a better understanding of cyber-security
- Students gained insight on what to prepare for to compete in CyberPatriot

All course participants (n = 23) had the chance to complete both the pre- and the post-course evaluations surveys. A total of 18 participants (ranging from incoming 6th to 11th grade) completed the pre-course survey; a subsample of 12 participants finished the post-course survey completely. Some survey items were not completed by all participants; hence the total number of responses for each survey item may vary.

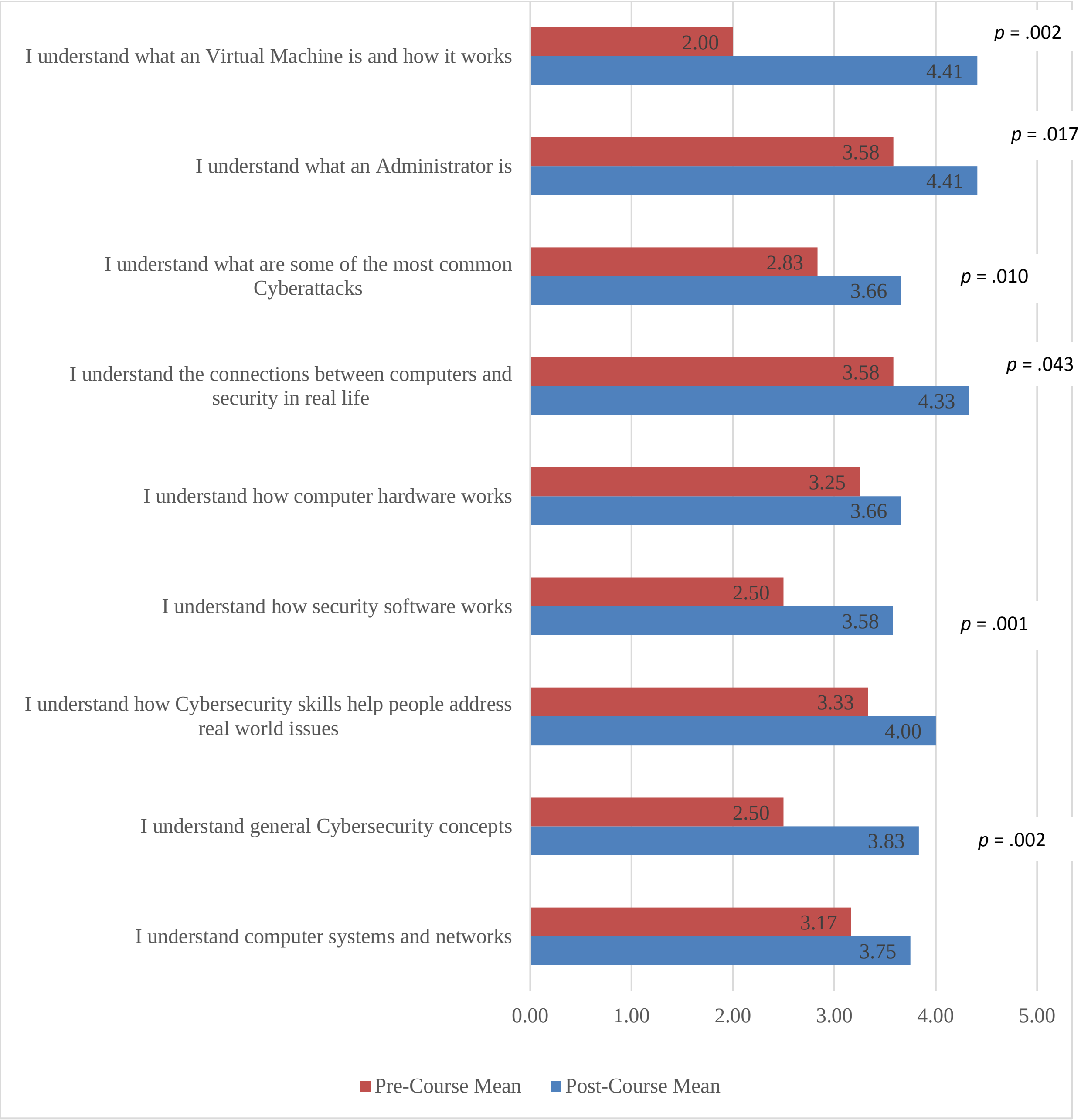


Figure 5. Understanding of Computer Science/Cybersecurity.

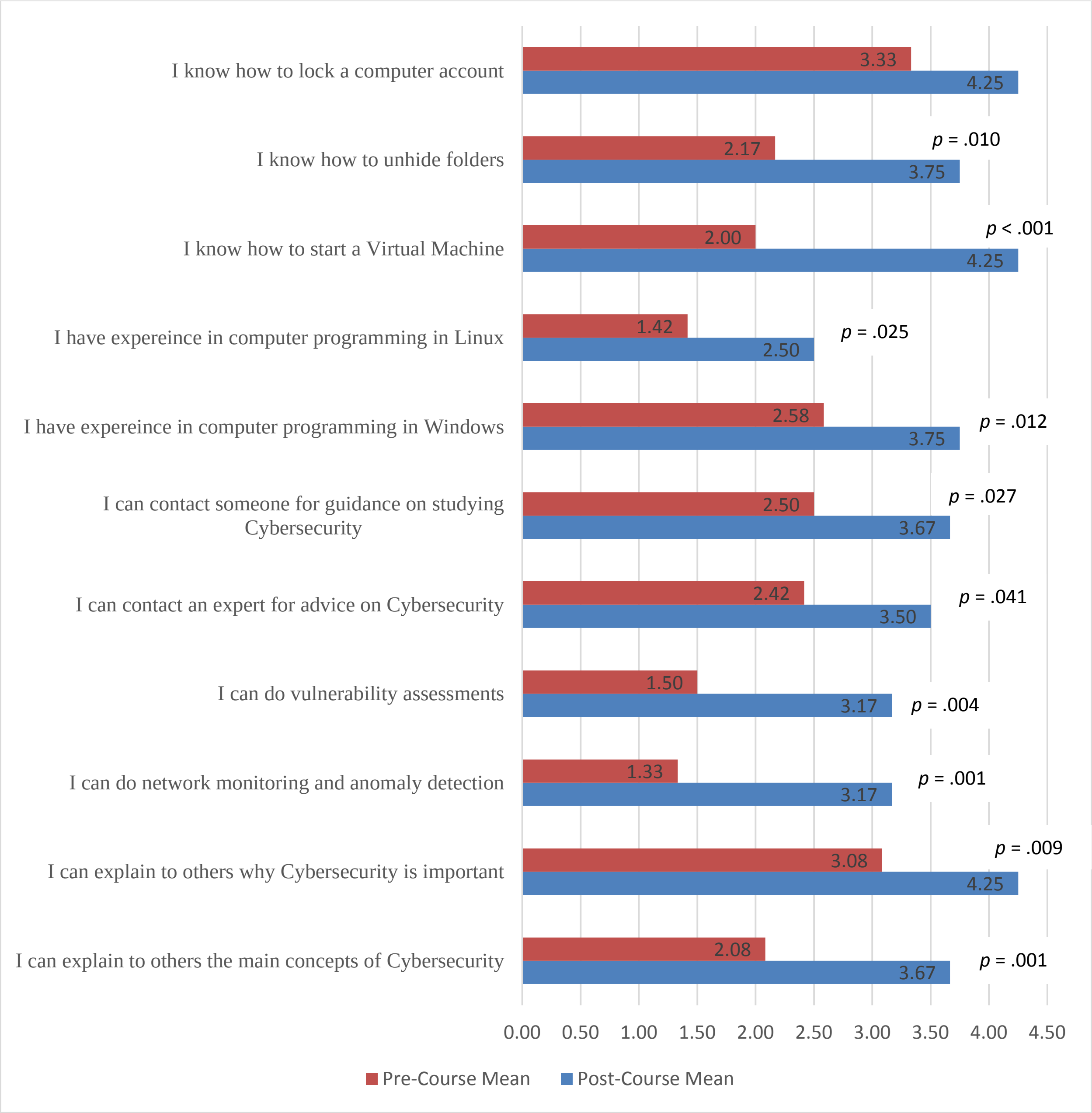


Figure 6. Experiences and skills of Computer Science/Cybersecurity.

Contrary to previous results, there were no statically significant differences found in relation to participants' pre/post-course "CS Motivations and Interests" and "Future Plans" as shown below.

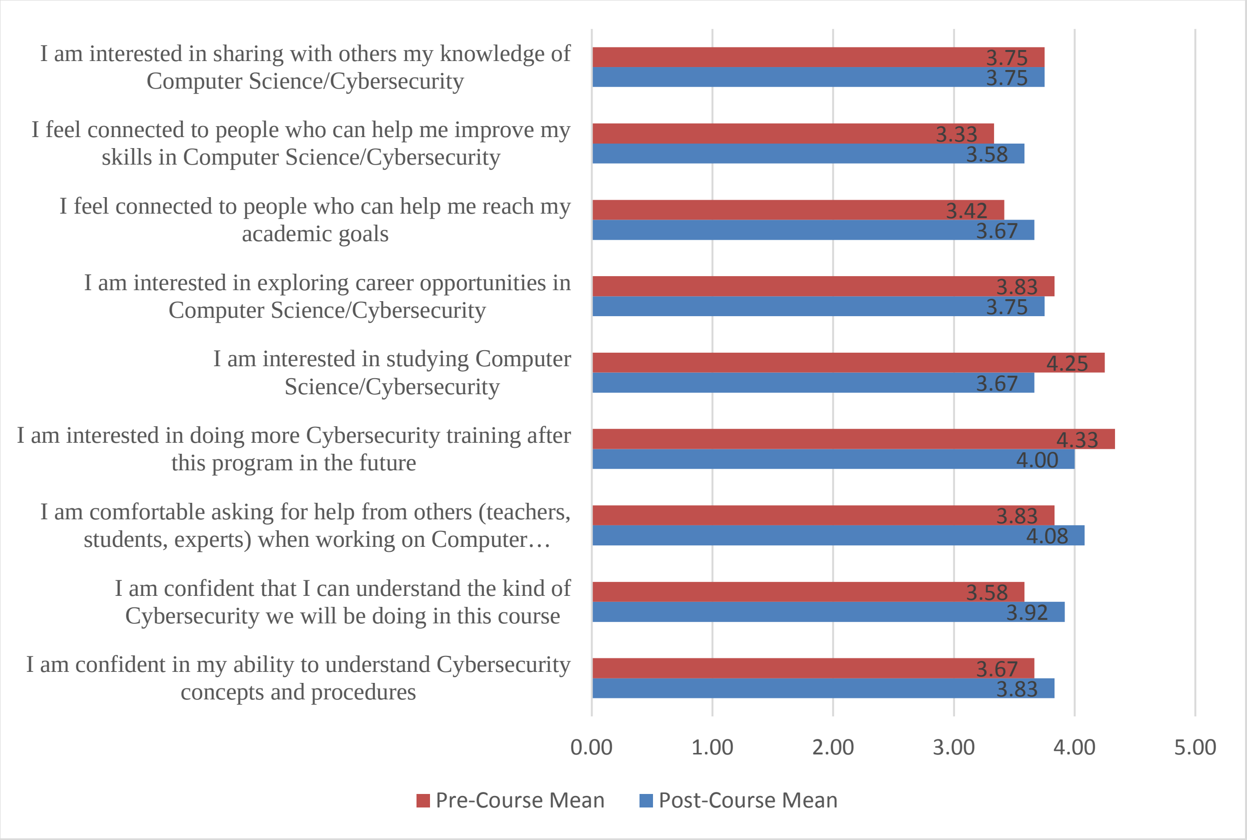


Figure 7. Motivations and Interests.

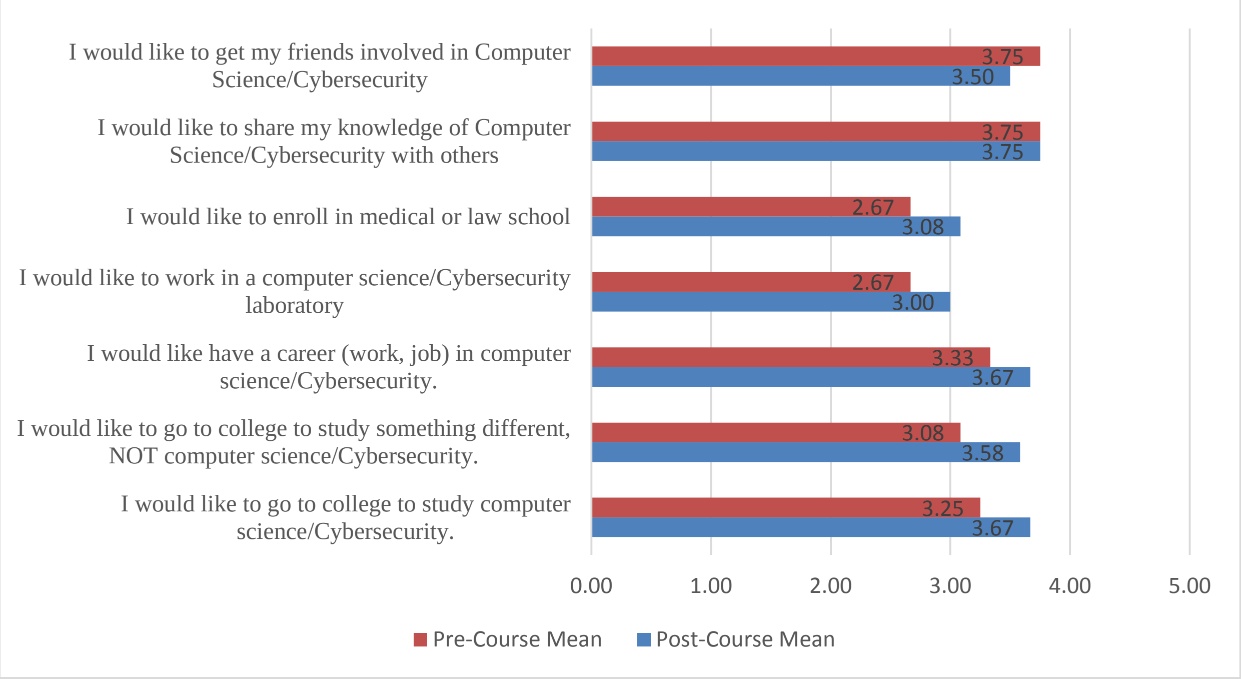


Figure 8. Future Plans.

Lastly, participants were also asked three open-ended questions about the course; answers are displayed below, unedited:

Table 1. Participants Course-related Feedback via Open-ended questions

What did you think about the Thunderbird Cup course?	*What did you like about the Thunderbird Cup course?*	*What did you NOT like about the Thunderbird Cup course?*
awesome I think I learned a lot	everything	How COLD the room was
I think it was fun I learned things that I have never learned before.	i get to spend time on a computer	i couldn't use my own computer
it is fun	i liked how we did things with the virtual machine	I have nothing to answer because I liked everything we did.
it was amazing	I liked that every machine had a theme for what was going on and what we had to fix.	nothing
It was ammazing I hope you come next year Sensei Tyler	I liked the lessons and the activities we did.	Nothing at all
It was an amazing expirence and i learned alot	it was fun and understanding	Nothing. The course was great.
it was interesting	that every one did it at their onw pace and was no rushing	there was nothing i didnt like
it was really fun learning about cyber security and i am happy i enrolled	The music, The expierience, The enoviorment, firends and the teachers	
it was very fun an interesting.	there were competions,prizes, a lot of learning.	
It,s good	Thursday's Virtual Machine	
nice		
This course was very fun and I enjoyed it.		

Conclusions

Encouraging findings were obtained -- statistically significant increases ($p < .05$) were observed in relation to numerous (16) key variables relating to individuals self-reported "C.S./Cybersecurity knowledge and skills" (see Figure 5 and Figure 6). Participants' feedback pertaining to the course was mostly very positive (see Table 1), participants often reported enjoying the course, learning and having fun. However, no significant changes were observed in relation to individuals self-reported

“C.S./Cybersecurity Motivations and Future Plans” (see Figure 7 and Figure 8). This unexpected finding may be due to numerous reasons, including a relatively small sample size (n = 12), participants may have already been highly motivated to study CS previous to taking the course, or other measurement-related issues. Results and associated implications are limited by the sample size/nature and the rate of missing data (due to participants not responding a question) in the survey.

Recommendations

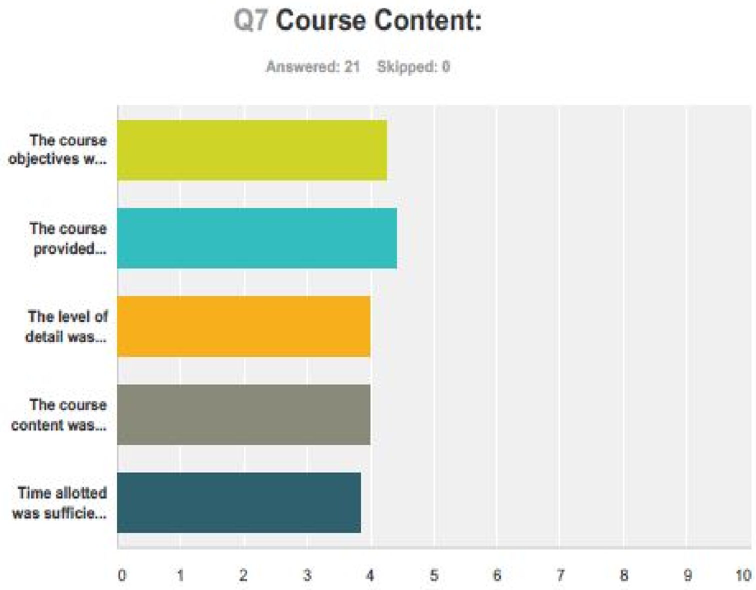
The unexpected finding of no significant increases in many items “C.S. motivations and future plans” warrants further consideration in order to improve future courses. Perhaps integrating additional C.S. career-related material (e.g. C.S. career paths and options) or presenting additional young scientists/programmers as role models may help participants view themselves as future CS/Cybersecurity agents and promote future interest in this field. A richer understanding of why participants did not report has CS in their future plans and motivations should help improve development of this and other CS-related educational courses. Participants’ attrition from the evaluation survey and missing data should be considered and efforts should be made to minimize these caveats. To address these issues, participants could be occasionally reminded during the course of the significance of completing the evaluation process to encourage participation and minimize drop-out/missing data.

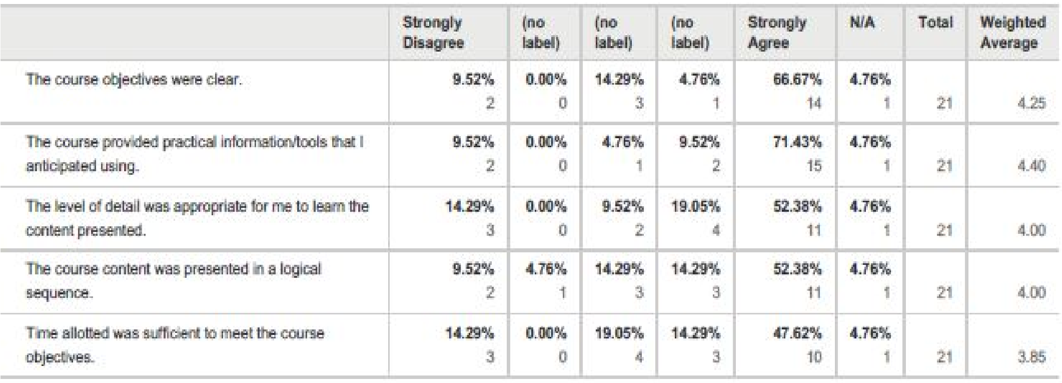
Appendix

Survey Results: Digital Forensics and Malware Analysis & Python Training Course

The survey results were conducted conjointly between the Digital Forensics and Malware Analysis and Python Training Course. The Survey results were based on a scale of 1-5: ‘1’ poor, ‘5’ is best.

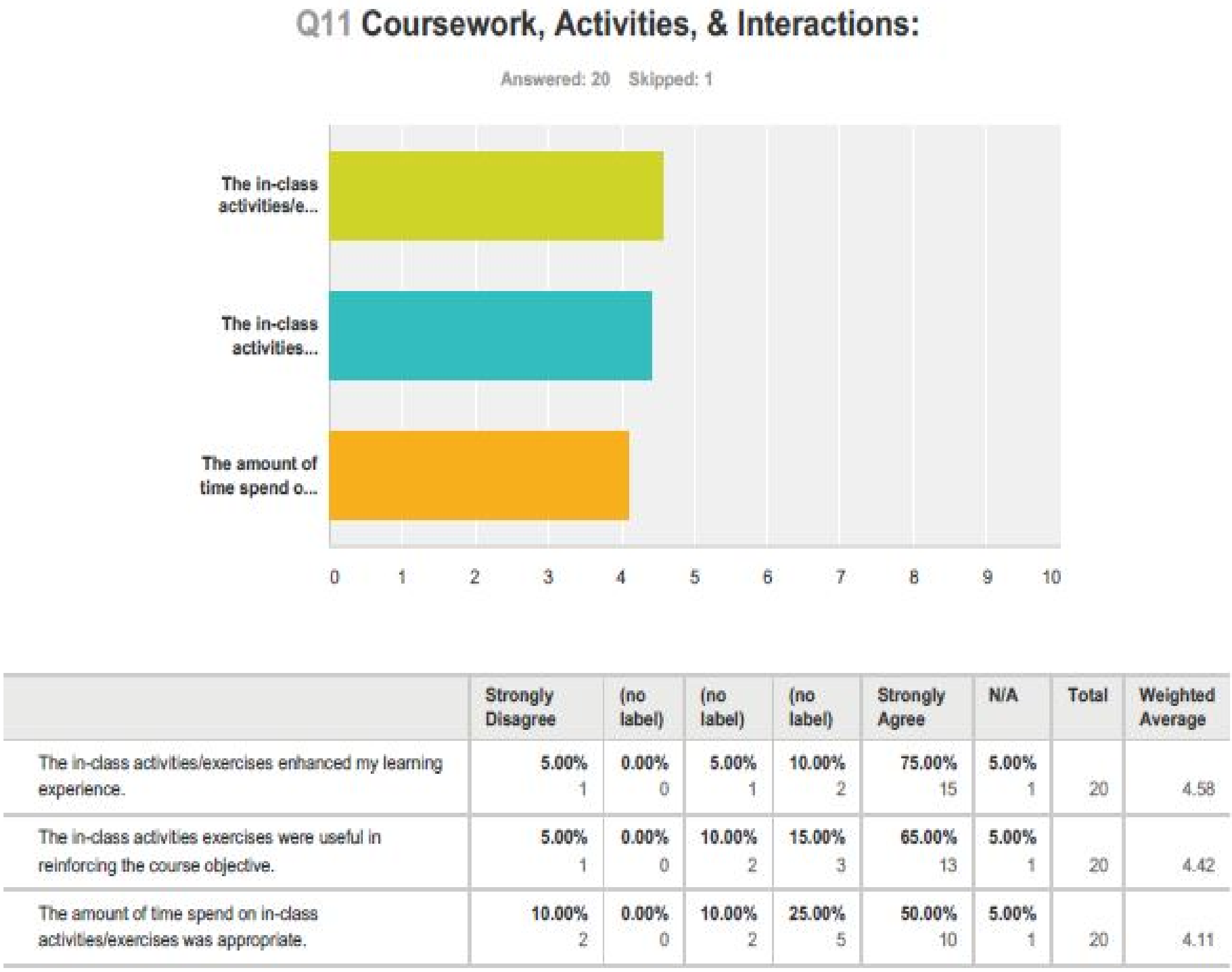
Course Content





	Strongly Disagree	(no label)	(no label)	(no label)	Strongly Agree	N/A	Total	Weighted Average
The course objectives were clear.	9.52% 2	0.00% 0	14.29% 3	4.76% 1	66.67% 14	4.76% 1	21	4.25
The course provided practical information/tools that I anticipated using.	9.52% 2	0.00% 0	4.76% 1	9.52% 2	71.43% 15	4.76% 1	21	4.40
The level of detail was appropriate for me to learn the content presented.	14.29% 3	0.00% 0	9.52% 2	19.05% 4	52.38% 11	4.76% 1	21	4.00
The course content was presented in a logical sequence.	9.52% 2	4.76% 1	14.29% 3	14.29% 3	52.38% 11	4.76% 1	21	4.00
Time allotted was sufficient to meet the course objectives.	14.29% 3	0.00% 0	19.05% 4	14.29% 3	47.62% 10	4.76% 1	21	3.85

Figure 9. Course Content.

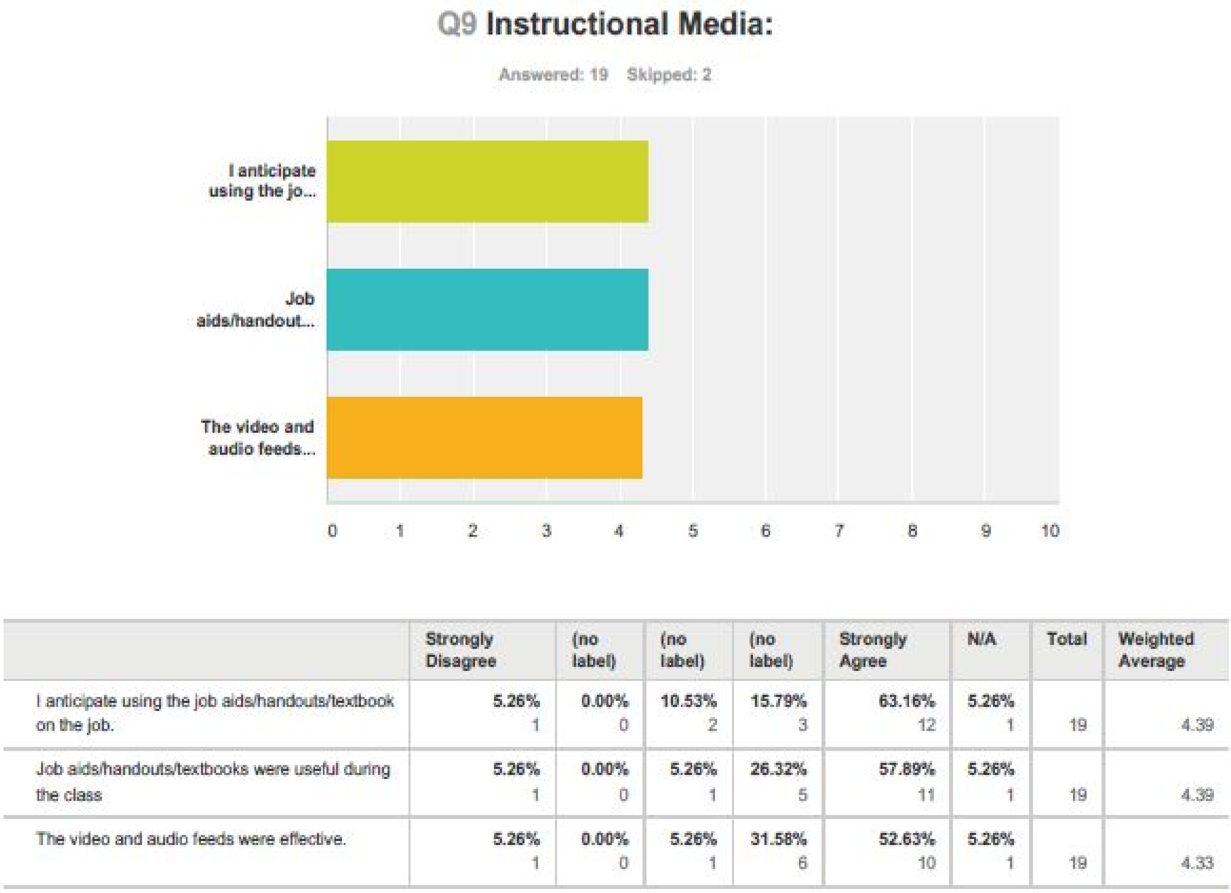

Q11 Coursework, Activities, & Interactions:

Answered: 20 Skipped: 1

The in-class activities/e...
The in-class activities...
The amount of time spend o...
0
1
2
3
4
5
6
7
8
9
10

	Strongly Disagree	(no label)	(no label)	(no label)	Strongly Agree	N/A	Total	Weighted Average
The in-class activities/exercises enhanced my learning experience.	5.00% 1	0.00% 0	5.00% 1	10.00% 2	75.00% 15	5.00% 1	20	4.58
The in-class activities exercises were useful in reinforcing the course objective.	5.00% 1	0.00% 0	10.00% 2	15.00% 3	65.00% 13	5.00% 1	20	4.42
The amount of time spend on in-class activities/exercises was appropriate.	10.00% 2	0.00% 0	10.00% 2	25.00% 5	50.00% 10	5.00% 1	20	4.11

Figure 10. Coursework, Activities, & Interactions.



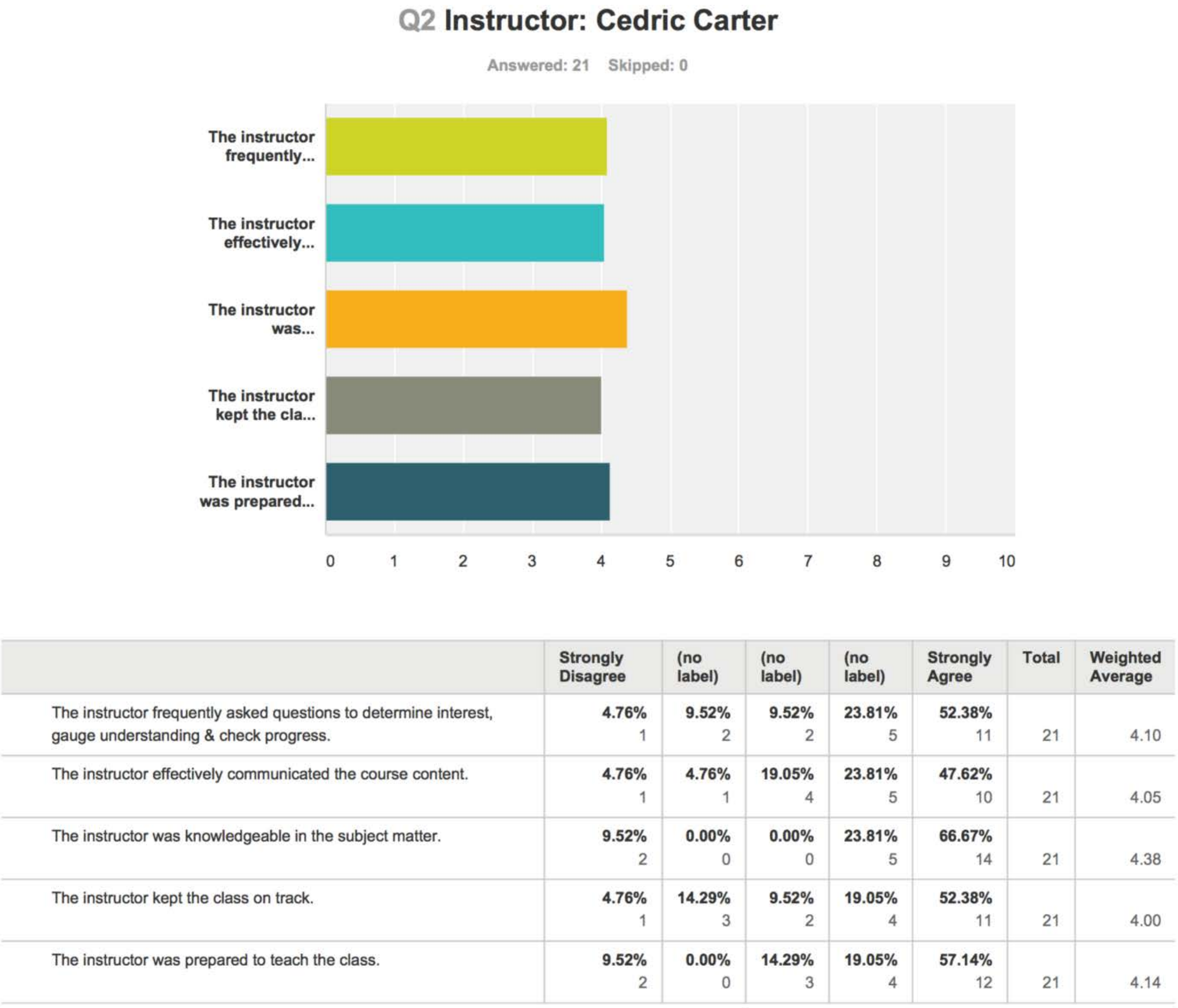
Q9 Instructional Media:

Answered: 19 Skipped: 2

	Strongly Disagree	(no label)	(no label)	(no label)	Strongly Agree	N/A	Total	Weighted Average
I anticipate using the job aids/handouts/textbook on the job.	5.26% 1	0.00% 0	10.53% 2	15.79% 3	63.16% 12	5.26% 1	19	4.39
Job aids/handouts/textbooks were useful during the class	5.26% 1	0.00% 0	5.26% 1	26.32% 5	57.89% 11	5.26% 1	19	4.39
The video and audio feeds were effective.	5.26% 1	0.00% 0	5.26% 1	31.58% 6	52.63% 10	5.26% 1	19	4.33

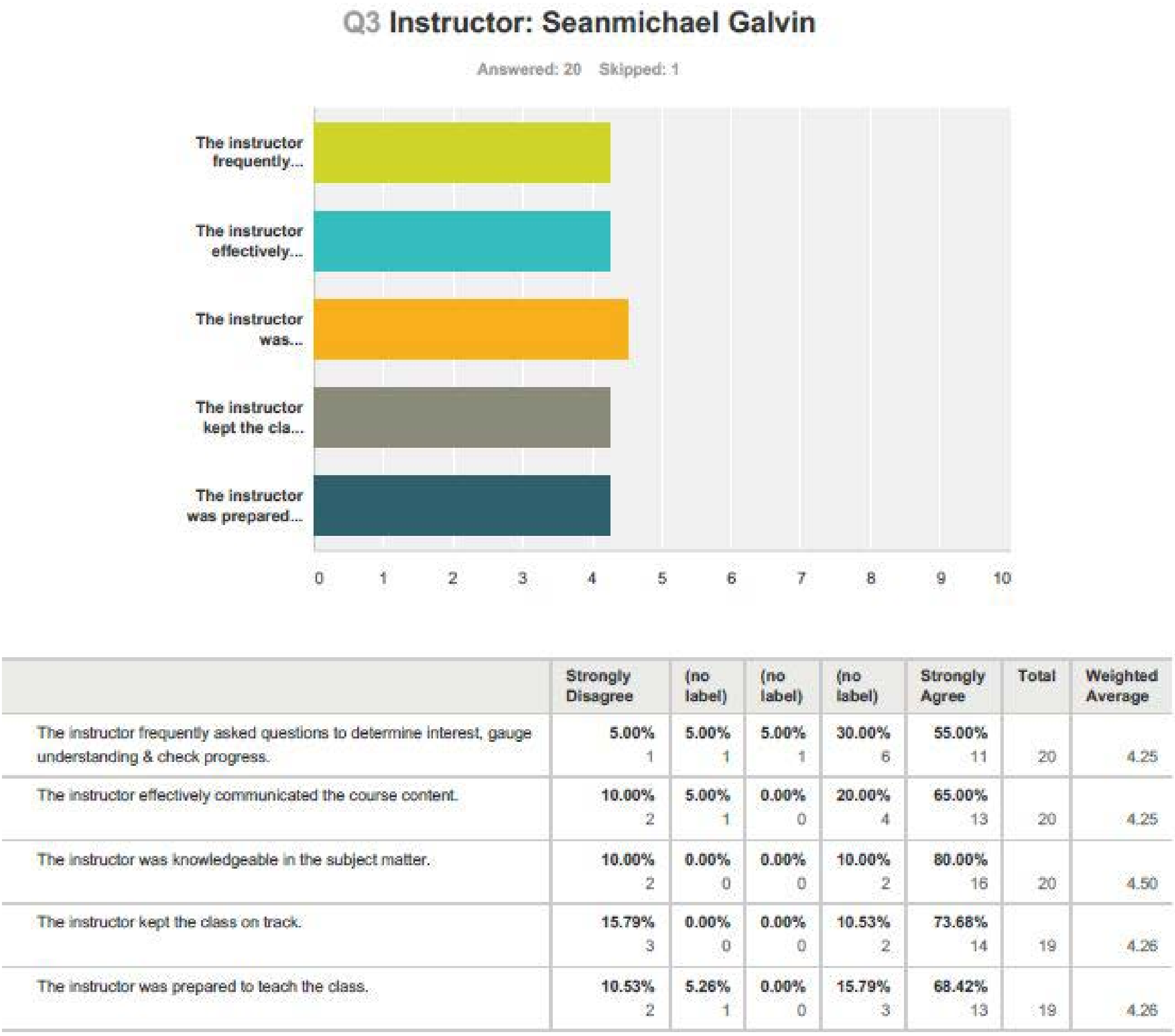
Figure 11. Instructional Media.

Instructors


Q2 Instructor: Cedric Carter
Answered: 21 Skipped: 0
The instructor frequently...
The instructor effectively...
The instructor was...
The instructor kept the cla...
The instructor was prepared...
0
1
2
3
4
5
6
7
8
9
10

	Strongly Disagree	(no label)	(no label)	(no label)	Strongly Agree	Total	Weighted Average
The instructor frequently asked questions to determine interest, gauge understanding & check progress.	**4.76%** 1	**9.52%** 2	**9.52%** 2	**23.81%** 5	**52.38%** 11	21	4.10
The instructor effectively communicated the course content.	**4.76%** 1	**4.76%** 1	**19.05%** 4	**23.81%** 5	**47.62%** 10	21	4.05
The instructor was knowledgeable in the subject matter.	**9.52%** 2	**0.00%** 0	**0.00%** 0	**23.81%** 5	**66.67%** 14	21	4.38
The instructor kept the class on track.	**4.76%** 1	**14.29%** 3	**9.52%** 2	**19.05%** 4	**52.38%** 11	21	4.00
The instructor was prepared to teach the class.	**9.52%** 2	**0.00%** 0	**14.29%** 3	**19.05%** 4	**57.14%** 12	21	4.14

Figure 12. Cedric Carter.

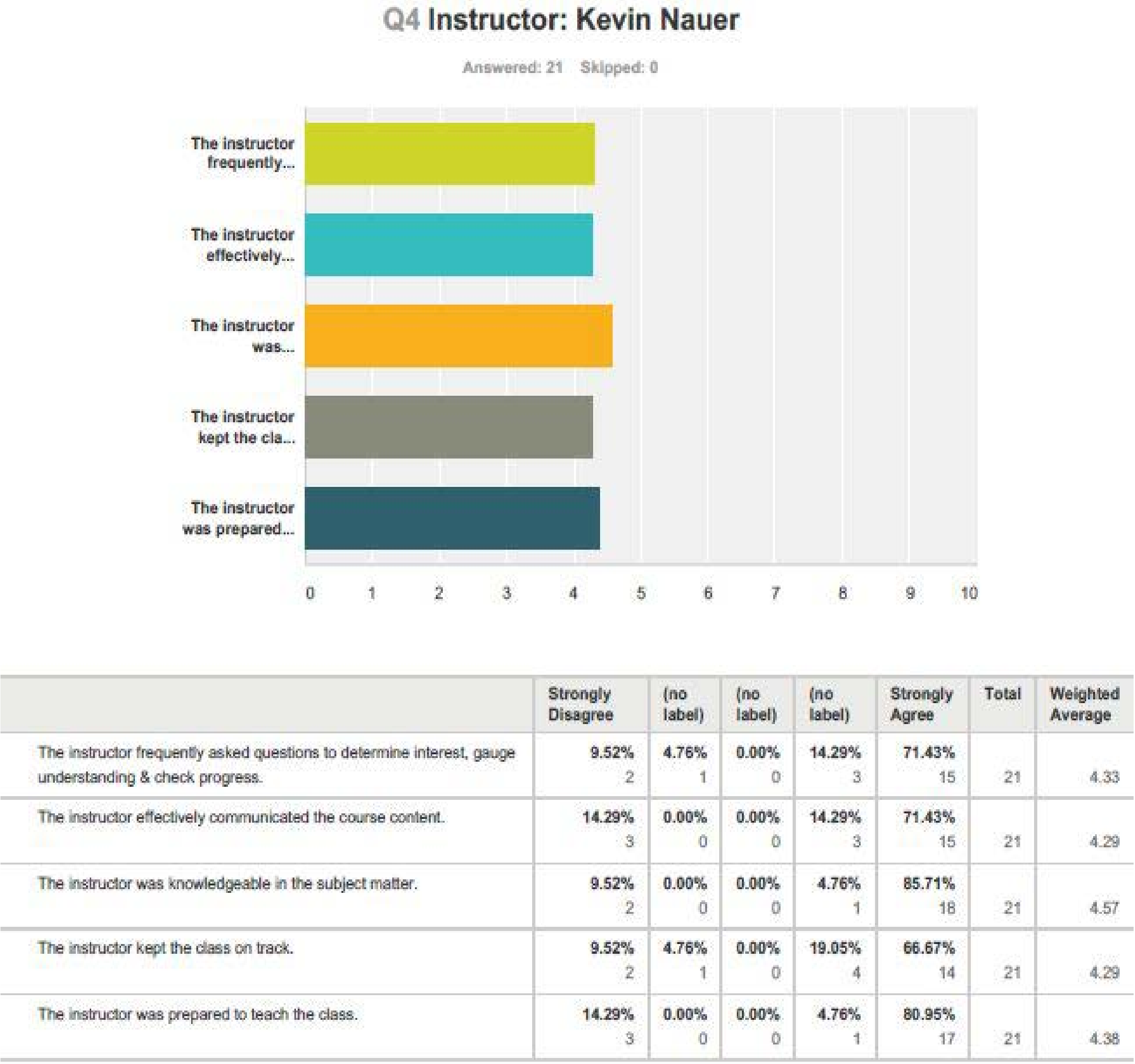

The instructor frequently...
The instructor effectively...
The instructor was...
The instructor kept the cla...
The instructor was prepared...
0
1
2
3
4
5
6
7
8
9
10

Q3 Instructor: Seanmichael Galvin

Answered: 20 Skipped: 1

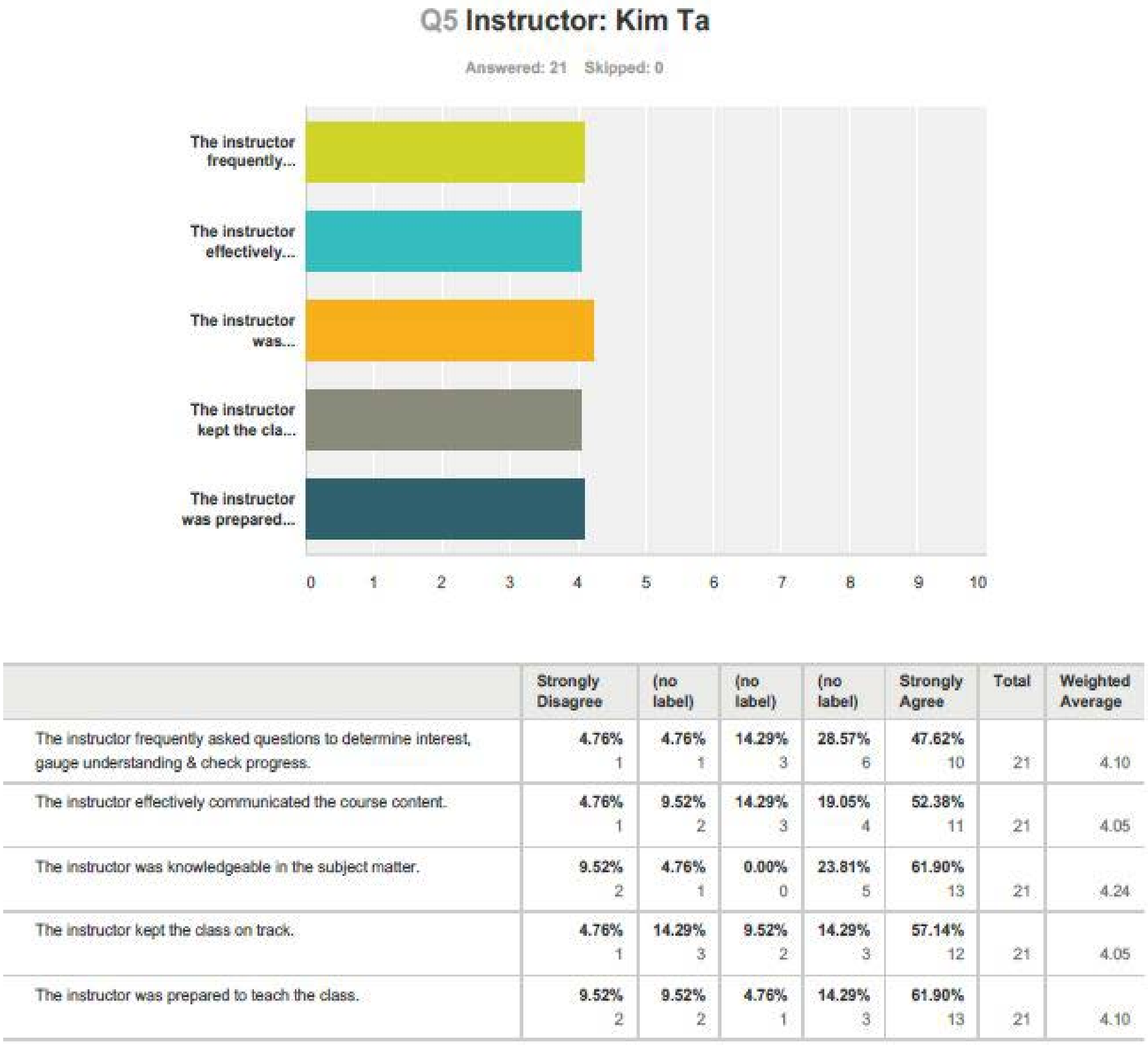
	Strongly Disagree	(no label)	(no label)	(no label)	Strongly Agree	Total	Weighted Average
The instructor frequently asked questions to determine interest, gauge understanding & check progress.	5.00% 1	5.00% 1	5.00% 1	30.00% 6	55.00% 11	20	4.25
The instructor effectively communicated the course content.	10.00% 2	5.00% 1	0.00% 0	20.00% 4	65.00% 13	20	4.25
The instructor was knowledgeable in the subject matter.	10.00% 2	0.00% 0	0.00% 0	10.00% 2	80.00% 16	20	4.50
The instructor kept the class on track.	15.79% 3	0.00% 0	0.00% 0	10.53% 2	73.68% 14	19	4.26
The instructor was prepared to teach the class.	10.53% 2	5.26% 1	0.00% 0	15.79% 3	68.42% 13	19	4.26

Figure 13. Seanmichael Galvin


Q4 Instructor: Kevin Nauer
Answered: 21 Skipped: 0
The instructor frequently...
The instructor effectively...
The instructor was...
The instructor kept the cla...
The instructor was prepared...
0
1
2
3
4
5
6
7
8
9
10

	Strongly Disagree	(no label)	(no label)	(no label)	Strongly Agree	Total	Weighted Average
The instructor frequently asked questions to determine interest, gauge understanding & check progress.	9.52% 2	4.76% 1	0.00% 0	14.29% 3	71.43% 15	21	4.33
The instructor effectively communicated the course content.	14.29% 3	0.00% 0	0.00% 0	14.29% 3	71.43% 15	21	4.29
The instructor was knowledgeable in the subject matter.	9.52% 2	0.00% 0	0.00% 0	4.76% 1	85.71% 18	21	4.57
The instructor kept the class on track.	9.52% 2	4.76% 1	0.00% 0	19.05% 4	66.67% 14	21	4.29
The instructor was prepared to teach the class.	14.29% 3	0.00% 0	0.00% 0	4.76% 1	80.95% 17	21	4.38

Figure 14. Kevin Nauer.



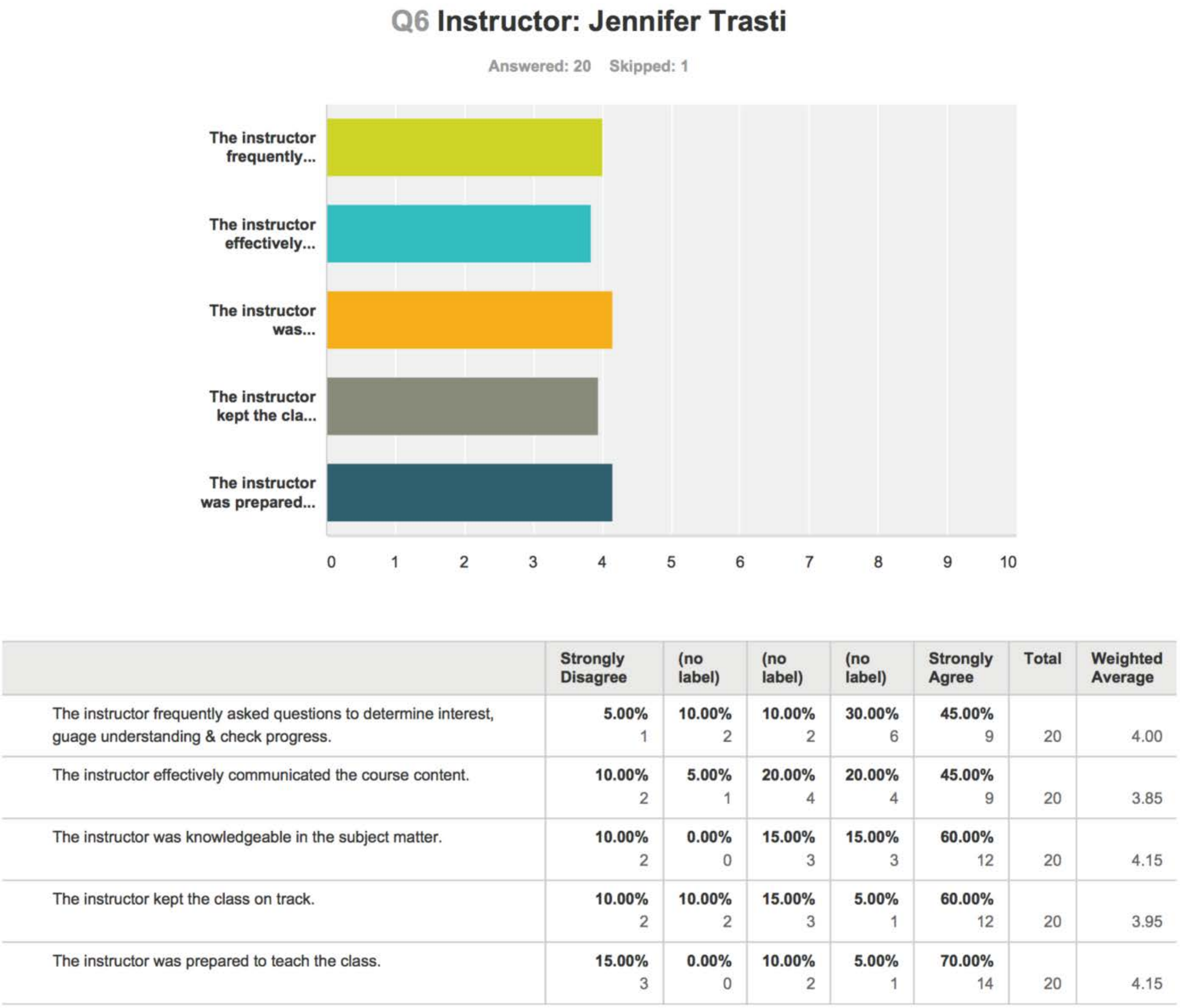
Q5 Instructor: Kim Ta

Answered: 21 Skipped: 0

The instructor frequently...
The instructor effectively...
The instructor was...
The instructor kept the cla...
The instructor was prepared...
0
1
2
3
4
5
6
7
8
9
10

	Strongly Disagree	(no label)	(no label)	(no label)	Strongly Agree	Total	Weighted Average
The instructor frequently asked questions to determine interest, gauge understanding & check progress.	4.76% 1	4.76% 1	14.29% 3	28.57% 6	47.62% 10	21	4.10
The instructor effectively communicated the course content.	4.76% 1	9.52% 2	14.29% 3	19.05% 4	52.38% 11	21	4.05
The instructor was knowledgeable in the subject matter.	9.52% 2	4.76% 1	0.00% 0	23.81% 5	61.90% 13	21	4.24
The instructor kept the class on track.	4.76% 1	14.29% 3	9.52% 2	14.29% 3	57.14% 12	21	4.05
The instructor was prepared to teach the class.	9.52% 2	9.52% 2	4.76% 1	14.29% 3	61.90% 13	21	4.10

Figure 15. Kim Ta.



	Strongly Disagree	(no label)	(no label)	(no label)	Strongly Agree	Total	Weighted Average
The instructor frequently asked questions to determine interest, guage understanding & check progress.	5.00% 1	10.00% 2	10.00% 2	30.00% 6	45.00% 9	20	4.00
The instructor effectively communicated the course content.	10.00% 2	5.00% 1	20.00% 4	20.00% 4	45.00% 9	20	3.85
The instructor was knowledgeable in the subject matter.	10.00% 2	0.00% 0	15.00% 3	15.00% 3	60.00% 12	20	4.15
The instructor kept the class on track.	10.00% 2	10.00% 2	15.00% 3	5.00% 1	60.00% 12	20	3.95
The instructor was prepared to teach the class.	15.00% 3	0.00% 0	10.00% 2	5.00% 1	70.00% 14	20	4.15

Figure 16. Jennifer Trasti.