3-22-2018

Assessing and Expanding Extracurricular Cybersecurity Youth Activities' Impact on Career Interest

Michael H. Dunn

ASSESSING AND EXPANDING EXTRACURRICULAR CYBERSECURITY YOUTH ACTIVITIES' IMPACT ON CAREER INTEREST

THESIS

Michael H. Dunn, Captain, USAF

AFIT-ENG-MS-18-M-021

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT-ENG-MS-18-M-021

ASSESSING AND EXPANDING EXTRACURRICULAR CYBERSECURITY YOUTH ACTIVITIES' IMPACT ON CAREER INTEREST

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Cyber Operations

Michael H. Dunn, MPA, BS

Captain, USAF

March 2018

AFIT-ENG-MS-18-M-021

ASSESSING AND EXPANDING EXTRACURRICULAR CYBERSECURITY YOUTH ACTIVITIES' IMPACT ON CAREER INTEREST

Michael H. Dunn, MPA, BS
Captain, USAF

Committee Membership:

Laurence D. Merkle, PhD
Chair

Maj Jason M. Bindewald, PhD
Member

Maj Daniel J. Casey, PhD
Member

AFIT-ENG-MS-18-M-021

Abstract

This thesis assesses and expands the potential of extracurricular activities to address the shortage of cybersecurity workers by increasing secondary school students' interest in these careers. Competitions and badges, two forms of gamification often applied in extracurricular educational activities, have potential to improve motivation and increase interest in related careers, but are significantly understudied in the context of cybersecurity activities.

CyberPatriot is the largest cybersecurity competition in the United States for secondary school students. Impact on participants' career interests is assessed by analyzing responses to recent surveys conducted by the competition organizers. Analysis demonstrates significantly increased interest in cybersecurity in several dimensions relevant to career selection, significantly larger increases for females than males, and persistence of increased interest over time. A survey of U.S. Air Force enlisted members is designed to gauge the impact of cyber-related education activities on developing its cyber workforce. Cybersecurity activity options are expanded by creating a flexible age-appropriate digital forensics activity in which students analyze forensic evidence in folders and files, reconstructing user activity to answer some basic questions. A cybersecurity merit badge is proposed for the Boy Scouts of America with suggested requirements modeled on other successful technology-related merit badges.

To my wife, who has sacrificed so much for me to be able to do this,

and who has always believed in me. Thank you for everything.

Acknowledgments

First and foremost, I would like to acknowledge and thank my research advisor, Dr. Larry Merkle. I am grateful for the many hours spent reading my drafts, giving feedback, and generally guiding me on this long and winding academic journey. I also appreciate your willingness to work with me on such an unconventional thesis topic.

My thanks also to the other members of my committee, Maj Jason Bindewald and Maj Dan Casey, for your assistance in this process, including reviewing my conference submissions.

I am extremely grateful to Ms. Rachel Zimmerman of the CyberPatriot Program Office for providing so much information on the CyberPatriot program, including the survey data used in this thesis.

Finally, I could not have done much of this work without support from my sponsor, the Air Force STEM Outreach Office, represented by Mr. Rick Baker, and later by Ms. Vicki Stoneking. I appreciated the discussions we had and the insights and experience you both provided. I also would not have been nearly as productive without the conference attendances you enabled. Most of all, I am just glad to be able to do work that matters. I hope in some small way I've been able to assist with your mission.

Michael H. Dunn

Table of Contents

Page

List of Figures

Page

List of Tables

Page

ASSESSING AND EXPANDING EXTRACURRICULAR CYBERSECURITY YOUTH ACTIVITIES' IMPACT ON CAREER INTEREST

I. Introduction

1.1 General Issue/Motivation

Modern society has become dependent on a wide range of networked computer systems, and addressing the many security problems inherent to this dependence is an increasingly difficult challenge. One of the key components to doing so is employing enough appropriately skilled cybersecurity workers. However, organizations across all sectors of industry are having difficulty filling the existing cybersecurity jobs. Furthermore, the worker shortage is only getting worse as growth in the number of cybersecurity jobs significantly outpaces the number of workers entering the field. The Center for Cyber Safety and Education, affiliated with the International Information System Security Certification Consortium ("$(ISC)^2$"), estimates that the cybersecurity worker shortage will grow to 1.8 million by 2022 [1, p. 3]. Among professionals surveyed in North America, 68% said there were too few cybersecurity workers in their department, and the majority believe that one of the main reasons is a difficulty in finding qualified personnel [1, p. 4]. The United States (U.S.) President's Commission on Enhancing National Cybersecurity also identified this challenge, concluding that building the cybersecurity workforce was one of its strategic imperatives for bolstering the nation's cybersecurity posture [2].

The U.S. government is not exempt from the cybersecurity worker problem. The same $(ISC)^2$ study cited above found that responses from U.S. federal government and military mirrored the overall results: 69% of respondents reported that there were too few information security workers in their organization, and the number one stated reason was that it was "difficult to find qualified personnel" [3, p. 20]. Furthermore, 64% of respondents said they expected to increase the number of information security personnel within the following year. They also reported that this shortage greatly impacts not only other security workers, but the organization as a whole and its customers [3, pp. 21–22].

The cybersecurity worker shortage has wide-ranging effects on our society, from loss of private information to threats to national security. Experts estimate that cybercrime causes tens of billions of dollars of damage each year to the U.S. economy alone and hundreds of billions globally [4]. This problem impacts everyone. In recent Congressional testimony on the cybersecurity workforce, one industry leader put it this way:

> The cybersecurity talent issue isn't limited to a few sectors; it runs across the board from government to education to healthcare and all industries. Strong talent is needed in all communities from rural farms that increasing rely on information technology to financial service companies in large urban areas. [5, p. 1]

A 2017 Presidential Executive Order, recognizing that a skilled cybersecurity workforce is essential "for achieving [the U.S. government's] objectives in cyberspace," reaffirmed that it is the policy of the U.S. federal government to support the development of the cyber workforce [6, p. 22395].

The National Security Strategy [7] and the National Military Strategy [8] both acknowledge cyber attacks as a threat to national security and highlight the need for action. The cybersecurity labor shortage makes it even more difficult to meet these challenges, and demands more proactive measures to grow and strengthen the cybersecurity workforce within the Department of Defense [9]. The U.S. military service's efforts to attract or build cyber expertise have been varied. Cybersecurity lessons are incorporated into existing military training, from boot camp to military service academies to professional military education [10]. The Air Force is offering enlistment bonuses of up to ten thousand dollars for Airmen that enter a cyber career field with an industry certification [11], and the Army is testing a program to fast-track talented individuals into cyber officers (a process known as "direct commissioning") [12].

Exacerbating this problem is a severe gender imbalance in the cybersecurity workforce. The same $(ISC)^2$ study found that only 11% of the global cybersecurity workforce are women [13], and multiple studies have shown that female students have much more negative views of cybersecurity and other computing careers than their male counterparts do [14], [15]. Clearly, addressing the cybersecurity worker shortage must include improving female students' perceptions of cybersecurity as a potential career.

1.2 Background for Research

Several approaches to solving this are being pursued by various government, industry, and academic organizations, including scholarships, internships and apprenticeship programs, cybersecurity training camps, increasing the number of

cybersecurity degree programs, and integrating cybersecurity into other related curricula. One approach that is generating growing interest is cybersecurity competitions. Such competitions at the college and professional level have become a well-established and prominent part of the cybersecurity landscape, often in the form of “capture the flag” type challenges [16]–[18].

Cybersecurity competitions for pre-college students (i.e. middle and high school) have also been growing in popularity over recent years [19], [20]. With over 14,000 registered participants during the 2016-2017 school year [21], the Air Force Association’s CyberPatriot [22] is the largest such program, and the only truly national cybersecurity competition for middle and high school students [16]. In the CyberPatriot cyber defense competition, teams of up to six middle or high school students scour a virtual computer for vulnerabilities, such as viruses, backdoors, and incorrect security settings, then eliminate those vulnerabilities for points. These teams can come from public or private schools, homeschool groups, Junior ROTC programs, Civil Air Patrol units, or other approved youth organizations serving middle and high school students [22]. The goal of CyberPatriot and similar programs is to increase the number of young people who pursue cybersecurity-related careers, as well as increase awareness of cybersecurity more broadly. However, it is unclear whether this approach is accomplishing this goal, and if so, to what extent.

1.3 Research Goals and Hypothesis

The goal of this thesis is to develop the potential of extracurricular cybersecurity activities to address the shortage of cybersecurity workers by increasing interest in these

careers amongst middle and high school students. This will be done by assessing the impact of such programs on students' career interests, particularly the CyberPatriot cyber defense competition, and to explore ways to expand these offerings. The research hypothesis is that extracurricular cybersecurity programs like CyberPatriot have a significant and meaningful positive impact on participants' inclinations to pursue an education and/or career in cybersecurity or a related field.

1.4 Approach

The research approach is in two parts, each with two elements. First, the potential of extracurricular programs to impact the cybersecurity worker shortage is assessed by analyzing survey results for CyberPatriot participants and by formulating a survey of enlisted Airmen. Second, this potential is expanded by creating a digital forensics educational activity to add to the CyberPatriot program and by designing and proposing a Cybersecurity merit badge for the Boy Scouts of America.

In the first element of assessing the potential of extracurricular cybersecurity activities, results from a survey of past participants in the CyberPatriot cyber defense competition are analyzed. The research assesses the impact of this competition on participants' interest in cybersecurity careers. Survey data previously collected by the competition organizers is analyzed with rigorous statistical methods. Results show that participants' interest in cybersecurity increased meaningfully in several dimensions relevant to career selection. Further analysis also finds that despite lower initial interest in cybersecurity careers among female participants, this interest increased by an even greater amount than it did for male participants.

The second element is a survey of enlisted Airmen regarding their experiences with cybersecurity or other computing outreach activities prior to entering military service, designed to assess the impact of these activities specifically on those who would eventually enlist in the Air Force. The survey is designed to test two basic hypotheses: one, that participation in a cyber or computing extracurricular activity increases the likelihood that an individual who enlists in the Air Force will express preference for a cyber-related career field; and two, that participation in a cyber or computing extracurricular activity, for those that do enter a cyber-related career field in the Air Force, increases average academic performance (as measured by grade point average) in their initial cyber-related technical training. These hypotheses can also be tested for individual gender and ethnic demographic sub-groups. Additional research questions can be analyzed from the resulting survey data, including factor analysis of specific educational programs reported and qualitative analysis of responses to opinion-based questions. The survey has not yet been approved for distribution, so the contribution for this portion of the thesis is the design of the survey. Analysis of the results are left for future work.

The other aspect of the research approach is expanding the potential of extracurricular cybersecurity activities. One element of this is the design and creation of a digital forensics educational activity. Since cybersecurity competitions have proven to be effective at increasing students' interests in cybersecurity careers, this research seeks to broaden the scope of offerings in an underrepresented subset of cybersecurity. Through analyzing existing cyber forensics competitions and challenges, it is demonstrated that there are few if any opportunities for most students to be exposed to digital forensics

through engaging extracurricular activities. Thus, a digital forensics challenge is designed and created as a model for the type of activity that could be adapted for use in CyberPatriot, classrooms, or other youth education settings. Due to administrative and regulatory barriers, the activity could not be tested with the target population (middle and high school students), so this is left for future work.

The second element of expanding extracurricular cybersecurity activities is the development of a proposal for a Cybersecurity merit badge for the Boy Scouts of America. Although competitions have proven effective at increasing career interest in cybersecurity, they are not the only method that can be used to incorporate cybersecurity into extracurricular youth activities. Badges, another form of gamification growing in popularity among educational researchers, are also considered. Scouting is one of the most well-established and effective contexts for the use of educational badges. While the Girl Scouts of the USA have already announced plans to introduce cybersecurity badges, the Boy Scouts of America (BSA) have no such program in the works. Therefore, a Boy Scout merit badge for Cybersecurity is designed and proposed to the BSA. First, several existing technology-related badges are analyzed, then suggested requirements are drafted for the proposed badge. A full proposal is put together, in consultation with a diverse team of experts and with the endorsement and support of leading information security professional organizations, and sent to the BSA national offices for consideration.

1.5 Organization of Thesis

This introduction is followed by four chapters. Chapter II, Related Research, discusses the research literature on extracurricular activities, especially STEM (science,

technology, engineering, and mathematics) activities, competitions, badges, cybersecurity extracurriculars specifically, and frameworks for evaluation.

Chapter III, Methodology, explains in detail the research design for each of the four elements of the research design described above.

Chapter IV, Results and Discussion, presents the results of the research described in chapter 3, along with analysis and discussion of the significance of those results.

Chapter V, Conclusion, summarizes the research, presents conclusions that can be drawn, identifies limitations in this research, and suggests future work.

Several Appendices contain supplementary material, including Institutional Review Board (IRB) exemption request and approval for the CyberPatriot survey data, IRB paperwork for the survey of enlisted Airmen, complete questionnaires from the surveys discussed, more detailed information regarding the digital forensics activity, and the full merit badge proposal sent to the BSA.

II. Related Research

2.1 Introduction

This chapter reviews the literature and related work relevant to the research of this thesis. The general benefits of extracurricular activities on the development of young people is briefly surveyed, followed by the impact of activities specifically related to STEM. Narrowing the focus, the research on academic competitions, a specific form of educational extracurricular activity, especially as it pertains to impact on career interest, is thoroughly reviewed. Narrowing further, the state of extracurricular cybersecurity education activities is discussed, and what little research exists on the topic is examined. A related method also used in educational extracurricular activities – badges – is also considered. Finally, two alternate frameworks for evaluation are considered.

2.2 Extracurricular Activities

This thesis focuses on the impact of extracurricular activities. Structured extracurricular activities (also sometimes referred to in the literature as “organized activities”) have been shown to have a number of benefits for young people. Adolescents who participate in extracurricular activities have fewer behavioral problems, are less likely to abuse alcohol and drugs, have higher levels of school engagement, and are less likely to drop out of school [23]. They are also more likely to have positive developmental outcomes, including higher school engagement and attachment, higher academic performance and achievement, college attendance, better careers, and

more [23]. Studies have found a positive correlation not only with mere participation, but also with the number of activities participated in and with the number of hours spent participating in activities; in other words, the more activities a student participates in and the more time devoted to those activities, the greater the positive outcomes are likely to be. Researchers have also found a positive correlation between greater "breadth" of participation – i.e. participating in multiple types of activities – and "greater school attachment, higher GPA, and greater likelihood of college attendance" [23].

There has been some limited work on deciphering the particular aspects of extracurricular activities that contribute to these positive developmental outcomes, and of the mechanisms by which they do so. One positive aspect of participation in voluntary (also "discretionary") extracurricular activities is that it contributes to a young person's development of their identity. Voluntary activities allow a young person to express their identity, while at the same time exploring implications and opportunities of that. As a result, "consistency" between a young person's chosen activities and their personal identity has been found to lead to better outcomes [23]. A related aspect of such activities is that they foster opportunities for initiative, to set goals, and to take on challenging tasks. Arts and sports have been reported to offer more of this, but all extracurricular activities in general offer more than standard classes in school [23].

A study of graduates of a particular STEM-focused charter school in Texas found a strong positive correlation between the number of after school STEM clubs that students participated in and their rate of matriculation into STEM majors in college [24]. While this research suggests a correlation, it says nothing of the cause of this correlation. It is possible and arguably likely that students who participated in multiple STEM clubs were

already interested in majoring in a STEM field, and probably would have done so anyway even if those clubs were not available. Nevertheless, participation in STEM clubs may have fostered and supported pre-existing aspirations, and may contribute to successfully pursuing a STEM career. After-school STEM clubs can be more flexible and dynamic than classroom curricula, and they have the potential to be more engaging for those students that have some interest in STEM, but may find their science and math classes boring [25]. Research on learning environments has consistently found that active participation increases motivation, and this has shown to apply to hands-on science outreach activities as well [26]. Engaging, participatory, non-standard learning activities clearly have significant potential within STEM education.

Analysis of data from the U.S. Department of Education's Educational Longitudinal Study (ELS) found a link between extracurricular participation in high school and college persistence [27]. Students who reported no participation in extracurricular activities in high school were more likely to have dropped out of college within two years of graduating high school than students who did participate in extracurriculars. The authors' hypothesis is that extracurricular participation in high school prepares a student to participate in extracurricular activities in college, which makes the student feel more engaged with their school community, and thus more likely to persist. It appears the researchers did not control for other factors, such as family income, so it cannot be ruled out that both college persistence and extracurricular participation have a common cause. It is possible that students from a lower-income background are less likely to participate in extracurricular activities (due to not being able to afford them or needing to work more hours in paid employment) and also more likely

to drop out of college. However, the authors' hypothesis is also plausible, since other research has asserted a connection between academic and social engagement in college – to which participation in extracurricular activities can contribute – and persistence to graduation [28], [29].

2.3 Competitions

Competitions are a popular format for extracurricular activities, especially in cybersecurity. In particular, the largest cybersecurity education program in the United States, CyberPatriot, is structured around a competition. Therefore this section reviews research on the impact of extracurricular academic competitions on student participants. Competitions are a sort of "gamification," a scheme of incorporating elements of game design into other, typically non-gamelike contexts [30], that is often used in extracurricular education activities. Gamification can, in certain contexts, positively impact the motivation of participants toward the thing being gamified [31]. In particular, academic competitions offer the same overall benefits as any extracurricular educational activity, plus several that are special to the competition format. Researchers and practitioners have articulated several specific affective benefits of academic competitions for young people.

Academic competitions can serve to motivate students to pursue a subject, and to strive for excellence in that scholarship. While intrinsic motivation, i.e. based on a student's internal drive, is preferred and is the ultimate goal of an educational activity, competitions can be used as an extrinsic motivation (from outside the student) to help

develop a healthy intrinsic motivation [32]. The competition can serve as an impetus to get the student started, and to help drive them toward success when they get bored or frustrated. Lepper's "minimal sufficiency principle" articulates the idea that only the minimum amount of extrinsic motivation be used to help get the student to intrinsic motivation [33] (cited in [32, p. 49]). Key to this development is "abundant meaningful, positive feedback" from caring adults [32, p. 50]. This effect can be particularly potent when positive feedback is coming from professionals in the field (rather than just teachers and parents). Participation from outside professionals is particularly common in academic competitions, where they often serve as mentors and judges.

Another "affective outcome" of academic competitions is the fostering of healthy "self-concepts": self-confidence, self-awareness, self-esteem, etc. [32]. The competitive nature of such activities drive participants to prove themselves, and gives them realistic feedback on their talents and abilities. Students can have their talents affirmed and validated, leading them to internalize those abilities as part of their identity. They can also receive a dose of reality by seeing that there are others their age who are just as good at something, maybe even better. However, academic competitions, especially at the middle and high school level, give students an opportunity to learn to deal with competition – both its positive and negative aspects – in the relatively safer, "softer" context of school. Caring adults are there to help a student deal with the stress and anxiety of the competition, or navigate the disappointment of failure, and help build confidence and resilience [32], [34], [35].

Along with enabling the benefits of receiving affirmation from professionals in the field, academic competitions also foster a role-model relationship between those

professionals and the students. Meaningful interaction with “real” practitioners of a subject or industry can have a powerful impact on a young person. This is especially important for students who do not often receive exposure to a wide range of careers, and to students who may have difficulty seeing themselves in a particular career because that student’s race or gender is underrepresented [32].

Evidence from field studies has suggested that academic competitions can have a significant impact on students’ educational and career choices, and they can be an effective avenue for stimulating interest in specific career fields, particularly in the sciences. A study of past participants in the National Ocean Sciences Bowl found that 41% of respondents indicated that participation influenced their choice of career, and 39% said that it influenced their choice of college major [36].

Academic competitions have been shown to be a positive experience for students. Science fair and science Olympiad participants reported that their number one reward for participating was “fun,” followed by “learning new things.” External motivators such as pleasing teachers and parents and winning prizes were ranked much lower. Students in both competitions said that given a choice of activities in the future, the competition they just participated in would be their top choice [37].

A study of a robotics competition called “Robofest” found that participation in the competition had a positive impact on students’ math and science scores [38]. Researchers analyzed results of pre- and post-assessments in math, science, and engineering of students who participated in an autonomous robotics competition, compared to students who did not participate. They found an increase in scores for both groups, though the

students in the robotics competition scored higher overall. However, weaknesses in the study methodology limit the amount of insight can be drawn from it.

Academic competitions can also help launch talented students into highly successful careers. A study of past winners of academic Olympiad competitions found they significantly outperformed their peers in various measures, including doctorates earned and number of publications. A significant majority of both participants and their parents agreed that the Olympiad programs helped develop their talent and fostered their future accomplishments [39].

2.4 Cybersecurity Activities

Competitions have become a popular way for professionals and students to practice and hone their cybersecurity skills, and prove to current or potential employers that they are skilled. The pioneer event in this field is the DEF CON Capture the Flag (CTF), and in many ways it is still the most famous and prestigious [40]. There are now dozens of cybersecurity competitions, both large and small, for varying skill levels [16]. One of the most popular is the Collegiate Cyber Defense Competition (CCDC), a national cybersecurity tournament for college students, with affiliated regional competitions [41]. CCDC has gained popularity especially for its value in creating hands-on learning experiences for students in cyber and computing related fields. It also has the potential to increase the inflow of new students into the cybersecurity profession, by recruiting, retaining, and identifying students who would be interested and adept in cybersecurity roles [16], [17]. The National Cyber League [42], a more recent addition to the cyber

competition pantheon, is modeled loosely on sports league competitions: it has "preseason" games to sort individuals into skill levels, a "regular season" where participants compete for rankings within their skill level, and a team-based "postseason" bracket; it has "gymnasiums" where participants practice between competitions; and "scouting reports" tell competitors and their potential employers how they performed in the competition. Analysis of participation in the first year of the league suggests that engagement – defined by measures of dedication, absorption, and vigor – dropped off measurably from new competitors to those with just one previous experience, but after that engagement increased proportionally with more experience [43]. It is unclear to what extent any of these competitions actually recruit new people into the cybersecurity profession, or if they are merely good at attracting those who are already interested.

Below the collegiate level, however, options for extracurricular cybersecurity activities become much scarcer. Many colleges and universities host cybersecurity camps for local middle or high school students. One of the more prominent programs supporting this type of activity is GenCyber [44], sponsored by the National Security Agency (NSA) and the National Science Foundation (NSF), and administered by the NSA. GenCyber awards funding grants to colleges, universities, and other organizations to run locally-organized cybersecurity camps for local students and/or teachers. New York University's (NYU) multi-faceted cybersecurity competition CyberSecurity Awareness Week (CSAW) includes a digital forensics competition for high schoolers (in what is otherwise geared solely for university students) [45]. Iowa State University has hosted a regional cyber defense competition for high school students in Iowa, including a training program in the run-up to an in-person competition event [19].

The only truly national program of cybersecurity extracurricular activities for middle and high school students is CyberPatriot [16], [20]. Run by the Air Force Association, CyberPatriot bills itself as "The National Youth Cyber Education Program" [22]. The central element of the CyberPatriot program is the annual cyber defense competition, in its tenth season as of the 2017-2018 school year. Teams of two to six middle school or high school students, sponsored by schools, Junior ROTC programs, Civil Air Patrol units, and other youth organizations, compete in tiered rounds culminating in a national championship. The early rounds (qualification, state, and semifinals) are conducted remotely, each team at its own location. Each team receives two or three virtual machines, preconfigured with vulnerabilities, and race to find and fix these vulnerabilities; a scoring system built in to the virtual machines awards points for each vulnerability fixed and communicates the results to a central scoring server [20], [46], [47].

However, little is known about the impact of computing and cybersecurity competitions as a means of attracting young people to these fields. One study of past participants in Cybersecurity Awareness Week evaluated personality profiles of competitors, and found that the high levels of "perceived self-efficacy in cybersecurity tasks, rational decision-making style, and investigative interests" correlated with a higher likelihood of participants later choosing a cybersecurity career [48]. A relatively large-scale survey by McGill, Decker, and Settle [14] studies the long-term effects of pre-college outreach activities, especially in relation to students' choice of major (specifically, computing vs. non-computing). These researchers found that there is a strong link between participating in computing educational activities and later choosing

to major in a computing field. This correlation is stronger when participation is voluntary than when it is required, and stronger for males than for females [14].

A small pilot study of cybersecurity engagement and self-efficacy among participants in a GenCyber summer camp found modest increase in male participants and a large increase among female participants [49]. Female students started the week with significantly lower scores than males, but by the end of the week had completely caught up.

A cybersecurity summer program at California State University, Bakersfield, garnered markedly mixed results from its participants [50]. Based on a set of pre- and post-activity survey questions, researchers found that male participants had a slight (negligible) increase in their interest in computer/cyber security, while female participants showed a slight decrease in interest. However, on a separate question on the post-activity survey asking how the program affected their interest, 100% of female and 81.3% of male respondents indicated that the program had made them more interested in computer/cyber security. Another question asked about their interest in cryptography, and had similar results. When asked about possible college majors, interest in cybersecurity majors increased from pre-survey to post-survey in males, but decreased in females. Interest in "technology" majors (including computer science and information systems) decreased for both male and female respondents. The researchers concluded that while female participants indicated an increase in interest, their "planned career trajector[ies]" did not change; they hypothesize that for most of the students who participated, they were too far along in their college and career planning for the program to have made a significant impact [50]. However, it should be noted that the sample size

is fairly small (n = 45), and the authors present no statistical analysis of their survey results, so it is unclear how significant their findings really are.

2.4.1 Digital Forensics Activities

For reasons discussed in section 3.4, this thesis reviews and evaluates digital forensics competitions and challenges available to pre-college students. The activities considered either specifically target secondary school students or are open to anyone and are of an appropriate skill level for students in that age range. One such program is the High School Forensics component of New York University's CyberSecurity Awareness Week [45], discussed in section 2.4 above. The largest digital forensics competition found is the Black T-Shirt Cyber Forensics Challenge [51]. Sponsored by sixty academic institutions and ten industry partners, it was designed to be an annual competition [52]. Competitors produced written reports in response to the challenges, which were then graded on a rubric by judges from the sponsoring organizations [53], [54]. However, that approach did not scale well, and after its inaugural competition in 2016, it was discontinued indefinitely [51]. The Digital Forensics Security Treasure Hunt [55] was part of the Security Treasure Hunt game sponsored by Counter Hack Challenges. In early rounds, participants viewed images or files and answered basic questions via a quiz engine on the game's website. Later rounds required some more in-depth analysis, but still relied on the same quiz engine. This program has become inactive, and the entire website has not been updated in several years [56]. Moraine Valley Community College in northern Illinois hosts an annual Youth Forensics Competition in the form of a summer day camp for local sixth through eighth graders [57]. The Digital Forensics Consortium, a

digital forensics education organization, organizes two different challenges. One is the Digital Crime Scene Challenge [58], a packaged event that can be set up a conferences, schools, etc. and runs a local challenge for attendees. The other is the US Digital Forensics Challenge [59], an online competition designed to replace the Digital Forensics Challenge run by the Department of Defense Cyber Crime Center (DC3) [60], [61]. Finally, the Civil Air Patrol's Cyber Defense Training Academy has created a Cyber Forensics Challenge [62] that is available online for local groups to download and implement locally. It consists of shell scripts and instructions for running them, as well as instructional materials for conducting the activity. However, implementing the activity requires some special equipment, which costs approximately $200 per kit for the basic challenge or $500 for the basic and advanced challenges [63].

2.5 Badges

This thesis also considers other formats that could be used to increase interest in cybersecurity through extracurricular activities. Another form of gamification getting more attention lately is badges [30]. In this method, the target audience – in the context of this research, students or other youth learners – is incentivized to participate in an activity by being awarded a "badge," either for mere participation or for achieving some level of skill. Badges can be virtual, displayed on an online profile, as in the case of many online

learning systems (e.g. Khan Academy [64]), or they can be physical, like the classic Boy Scout merit badge patch (Figure 1).

Figure 1. Merit Badges in the Boy Scouts of America

Educational badges in the context of an intelligent tutor system were found in one study [65] to increase interest in the subject being taught as well as decrease negative motivations (i.e. not wanting to look bad compared to other students, which is considered to be a counter-productive form of extrinsic motivation). However, this effect depended on the skill of the learner and the type of badge. For example, these changes in motivation were only detected for low-performing students; high-performing students had no discernable change in motivation or interest. Additionally, earning a greater number of participation badges (as opposed to skill badges) correlated to less of a decrease in negative motivation, though again, only for low-performing students. For high-performing students, however, earning skill badges increased their level of expectancy of success. The conclusion drawn from this study is that there can be a complex interplay between type of badges, skill levels of learners, and different forms of motivation outcomes.

Experts warn that if gamification is done poorly, gamification will fail to have the desired motivational impact, and could even discourage users. A frequent example of

poor gamification is merely adding points and badges or leaderboards to an otherwise unexciting activities and expecting that to make them exciting [30]. Some researchers have criticized Khan Academy for taking just such an approach: adding points and badges, but failing to fundamentally alter the structure of the learning activity [66].

Badges cannot by themselves create value, but they can deepen engagement and interest in something that already has intrinsic value. This is most effective in the right social context, where the social capital embodied by the badges is the reward that drives motivation [30]. Scouting is a prime example of just such a context. In fact, the merit badge program of the Boy Scouts of America (BSA) is held up by experts as a model of the positive impact badges can have [30], [67].

Scouts who complete science-based merit badges retain content knowledge, they report doing better in school, and many who go on to science careers credit Scouting with helping them get there [68], [69]. One university that conducted computing workshops for Boy Scouts, based on the Computer merit badge, found increased positive attitudes about computers across multiple dimensions [70].

Girl Scout STEM programs have also been incredibly successful, increasing girls' positive attitudes and interest in STEM subjects and careers [71], [72]. Earning badges was one of the most widely-reported positive experiences in a survey of Girl Scout alumnae, as were learning new skills and trying new things (also things like fun, friendship, crafting, and camping) [73].

2.5.1 Cybersecurity Badges in Scouting

The Girl Scouts of the USA has recently announced that they will be introducing a series of age-appropriate cybersecurity badges to their programs, projected to start in the fall of 2018 [74]. The Boy Scouts of America has a handful of badges that relate either directly or indirectly to computing [75]. Two of them – Digital Technology [76] and Programming [77] – include elements of online safety in the requirements and brief sections on security in the associated merit badge booklets. The BSA's primary program for personal online safety education is the Cyber Chip [78]. However, BSA merit badge program leadership has indicated that they may be interested in expanding these options at some point in the future, writing in a newsletter to local Scout leaders that "developing merit badges that expand Scouts' horizons into technological careers … will be the merit badge trend of the future" [79].

2.5.2 BSA Merit Badge Requirements

As discussed in section 3.5, the first step in creating a Cybersecurity merit badge for use in the Boy Scouts of America (BSA) is to analyze the structure of existing merit badges. Eight merit badges were selected, all of which relating to technology or technical careers, and all of them created or updated within the past few years [75], [80]: Animation (updated 2015), Aviation (2014), Digital Technology (2014), Game Design (2017), Mining in Society (2016), Programming (2017), Robotics (2011), and Welding (2012). Requirements for these merit badges generally fall into one of the following types:

- Safety – safety precautions the Scout should know before engaging in the activities described in the merit badge, including first aid for possible injuries; most merit badges start with one or more safety requirements;
- Knowledge – terms and concepts that the Scout must define, explain, discuss, etc.; for this analysis, a separate knowledge requirement is counted for every term or concept a Scout is required to know, regardless of how they are consolidated and presented in the official requirements booklet;
- Activity – something that the Scout must *do*, hands-on; requires little-to-no planning; relatively easy to accomplish;
- Project – a hands-on requirement, but more involved than a single simple activity; requires some planning; and
- Large project – a complex, hands-on project consisting of multiple steps or sub-projects; requires more extensive planning; for merit badges that contain a large project, it is the central focus of the requirements.

Further analysis of the number and type of requirements for the selected merit badges is presented in section 4.7.1.

2.6 Frameworks for Evaluation

Various methods of evaluating academic competitions have been used or suggested over the years, depending on the purpose and perspective. Program evaluation is an entire field and cannot be effectively summarized here. Rather, this section will

present a few select examples that can be drawn upon to evaluate the impact of cybersecurity competitions for middle and high school students.

The vast majority of cybersecurity competitions are digital – i.e. computer based – and by their very nature as competitions they are types of games. One approach, therefore, is to view cybersecurity competitions as a type of digital game-based learning. All, Castellar, and Van Looy [81] investigated the perspectives of a wide variety of stakeholders in order to develop a framework for evaluating the "effectiveness" of digital game-based learning. They proposed three categories of effectiveness: learning outcomes, efficiency outcomes, and motivational outcomes. Learning outcomes relate to how a student interacts with the subject matter being taught. They include attaining pre-defined learning objectives, being able to apply what they learned to real-world contexts, and increasing their general interest in a subject. Efficiency outcomes measure cost savings, both in terms of time spent teaching/learning, and monetary cost. To be useful, both of these types of efficiency outcomes must be measured against a traditional learning method achieving the same or similar learning outcomes. The final category, motivational outcomes, relates to the students' attitudes toward the medium – the game itself – and the game-based instructional approach. The effectiveness framework described by All, Castellar, and Van Looy is holistic, designed to evaluate the overall effectiveness of a digital game-based learning program. If a cybersecurity competition or other extracurricular activity were to be evaluated strictly for its impact on students' career interests based on this framework, it would be solely under the learning outcomes category. Knowledge of and interest in cybersecurity careers could be designated a learning objective, and the competition or activity evaluated on its effectiveness at

meeting those objectives. However, this narrow use of the digital game-based learning effectiveness framework cuts it down to be essentially no different from evaluating any other educational program.

In their study of the National Ocean Sciences Bowl, Walters and Bishop identified fourteen separate dimensions of the subject competition [82], [83]. Half of these dimensions are from Mary Tallent-Runnels' seven "characteristics of good competitions" [84], put forward as a guide for students and their parents when considering whether to get involved in an academic competition. The other seven dimensions from Walters and Bishop are factors identified from the literature, and confirmed by their study, as affecting a student's career decisions [82], [85], [86]. These seven factors are:

- "perceptions of career tasks" – a student's understanding of what a particular career actually entails
- "perception of role models" – the attitudes and beliefs of individuals the student knows and respects
- "previous career experiences" – a student having engaged in a real-world interaction with the career
- "view of self" – a student's perception of their own abilities and capabilities as they relate to the career; whether they can "see themselves" doing that job
- "difficulty of attainment" – student's perception of how difficult it would be to enter the field and succeed in a career
- "personal support" – a student's network of peers, mentors, and family members supporting their pursuit of a the career
- "interest and awareness" – the extent to which a student is even aware of a career field and how interested they are in it

2.7 Summary

Organized extracurricular activities have been shown to have positive effects on the development of children and young adults. Academic or career-oriented activities can also have an impact on students' future educational and career choices. In recent years this has been studied with special emphasis on STEM subjects, activities, and related careers. Participation in certain STEM-focused extracurricular activities has a positive correlation with higher interest in STEM subjects and careers, and there is evidence to suggest that participating in such activities does increase this interest.

Competitions are a specific subset of extracurricular activity and seem to have several additional benefits as well, such as developing motivation, building self-confidence, and fostering relationships with professionals in a specific field. Research on some of these competitions has found that they have the potential to have significant positive impacts on participants' career interests. The use of educational badges is another approach used successfully in some extracurricular contexts. Research findings on the effectiveness of educational badges have been mixed, depending on the pre-existing skills of the learner, the intrinsic value of the content of the badge, and the social context. One context that seems to be consistently successful at using badges is Scouting. Research has found positive results from the use of badges in both Girl Scout and Boy Scout organizations.

Cybersecurity-specific extracurricular activities are becoming more popular, particularly in the form of summer camps and cyber defense and capture-the-flag competitions. CyberPatriot is by far the largest such program in the United States for middle and high school students, and the only truly national cybersecurity competition

for that age group. However, these activities have been studied to a much more limited degree than their traditional STEM counterparts. A few limited studies have found mostly positive evidence that cybersecurity competitions and other extracurricular activities can increase interest in cybersecurity subjects and careers. Prior to the work in this thesis there had been no published peer-reviewed studies of the CyberPatriot program's impact on the career interests and aspirations of its participants.

In their study of the National Ocean Sciences Bowl, an ocean science themed academic competition, Walters and Bishop identified a framework for evaluating the impact of an academic competition. Their framework included seven factors that contribute to students' career interests. These seven factors offer a useful framework for use in evaluating the impact of a cybersecurity competition like CyberPatriot.

III. Methodology

3.1 Introduction

This chapter details the methodologies used in approaching the elements of this thesis research. The first part of the research approach is to assess the potential of extracurricular activities to increase interest in cybersecurity careers. Section 3.2 describes the analysis conducted of CyberPatriot survey data in order to assess the impact of that program on career interest. Section 3.3 covers the details of a survey designed to collect data on enlisted Airmen's experiences with cyber-related educational activities prior to entering the Air Force and the impact those activities had on their careers. The second part is to expand the potential of extracurricular cybersecurity activities. Section 3.4 outlines the design process for creating a digital forensics activity to add to CyberPatriot or a similar program; it starts with a discussion of the activity criteria, then a review of related programs, then a description of the design choices, and concludes with the process used to create the activity. Section 3.5 finishes off this chapter with the methodology for adding a new cybersecurity component to an existing extracurricular youth program, by putting together a proposal for a Cybersecurity merit badge for the Boy Scouts of America.

3.2 CyberPatriot Survey Analysis[1]

The first element of assessing the potential of extracurricular cybersecurity activities is to analyze data on the impact of the CyberPatriot cyber defense competition on participants' interest in cybersecurity careers. The data used for this part of the research was constructed from responses to various surveys conducted by the CyberPatriot Program Office over the past several years. In 2014, 2015, and 2017 the organization conducted "post-season" competitor surveys asking students about their experiences with the program in the preceding school year. Also, in 2014 and 2016 they surveyed all students who had participated in any year of the program ("alumni") and asked them about their current educational and career situations. Summaries of a few of the surveys have been published in reports by the CyberPatriot Program Office [87]–[89], including basic descriptive statistics; however, this research is the first statistically rigorous analysis of the collected survey data.

The questionnaires for the post-season surveys, which were sent to all students who had participated during the immediately preceding school years, begin with a series of six retrospective questions asking students to "think back to before [they] had ever heard about CyberPatriot." Unfortunately, there were no pre-season surveys to gauge the opinions of students before they participated in the CyberPatriot competition. These retrospective questions inquire about students' perceptions of their knowledge of basic

[1] Portions of sections 3.2, 4.2, 4.3, and 4.4 were adapted for presentation at the *49th Association for Computing Machinery (ACM) Technical Symposium on Computing Science Education (SIGCSE 2018)* and publication in the conference proceedings as "Assessing the Impact of a National Cybersecurity Competition on Students' Career Interests" [101].

cybersecurity principles, their knowledge of and interest in cybersecurity careers, their likelihood of pursuing an education or career in a STEM field, and how "welcoming and accessible" to females they perceived cybersecurity careers to be before they participated. Those six questions are then posed again, with the time considered changed to "now" or "currently." Finally, the questionnaires ask participants two questions about how "engaging" and "fun" they thought the competition was. The 2017 survey added several questions about students' reasons for participating, elements of the competition that were most impactful, how much time they spent training, etc.

Questionnaires for the alumni surveys were sent to CyberPatriot alumni and the questions focus on the individuals' educational and/or career status and plans. After collecting some basic demographic data, these questionnaires ask respondents if they have graduated from high school yet (i.e. at the time of the survey). High school graduates are then asked if they are enrolled in higher education, and if so, what field they are studying. Others are asked if they plan on pursuing higher education after high school and in what field. All respondents are then asked if they are employed, and if so, in what sector (public/private/military). They are also asked in what field they are currently employed or hoping to be employed. Finally, respondents are asked to what extent participation in the CyberPatriot program has impacted their education and career goals (none/somewhat/significant).

Three of the five surveys studied collected some personally identifiable information (PII), including name, mailing address, and email address, for use in a random drawing as an incentive for completing the survey. To meet legal and regulatory

requirements, the survey data must be anonymized before it can be used for this research. This requirement could be met by merely removing all potential PII fields; however, it is desirable to be able to link participants across multiple survey responses. This is achieved by replacing each respondent's PII with a unique Hashed Message Authentication Code (HMAC) generated via SHA-256 hashing algorithm and a randomly-generated secret key. A set of Microsoft Excel macros was written to automatically replace all data in identified PII fields with this uniquely-generated HMAC. The macros standardize all PII fields by first setting all letters to lowercase and removing all punctuation and whitespace, and then running the HMAC algorithm on the result. These macros were given to the staff of the CyberPatriot Program Office, who ran them on copies of their datasets and then transferred the anonymized datasets to the author. In this way the data was de-identified, but respondents could still be linked across different survey responses by matching the unique HMAC generated from a participant's mailing or email address. This allowed measurement of reliability of certain responses by comparing an individual's responses to the same question across multiple instances of the survey, as well as to construct a semi-longitudinal study by linking individuals' responses in the 2015 post-competition survey to their responses in the 2016 alumni survey.

A complete list of questions asked in the post-season and alumni surveys, including which fields were anonymized using the above process, is contained in Appendix A: IRB Exemption Request Memo. The approved exemption from IRB human experimentation requirements is in Appendix B: Approved IRB Exemption Memo.

The 2014 post-season competitor survey (following CyberPatriot VI) had 639 respondents, and the 2015 post-season survey (following CyberPatriot VII) had 790 respondents (see Table 1). The 2017 post-season survey (following CyberPatriot IX) had 2,161 respondents – an increase of 274% over the 2015 survey. The 2014 alumni survey had 254 respondents, and the 2016 alumni survey had 2,870 respondents – an increase of 1,130%. Due to the significantly larger number of respondents, the 2016 alumni survey and 2017 post-season competitor survey are the primary sources for this analysis. The 2015 post-season survey is used primarily to measure reliability of certain questions by linking responses from individuals who responded to both the 2015 and the 2017 surveys.

Table 1. Survey response numbers

Survey	Total Responses	Male	Female	Decline to Specify
2014 Post-Season	639	516 (80.8%)	115 (18.0%)	8 (1.3%)
2015 Post-Season	790	608 (77.0%)	168 (21.3%)	14 (1.8%)
2017 Post-Season	2161	1553 (71.9%)	576 (26.7%)	32 (1.5%)
2014 Alumni	254	218 (85.8%)	34 (13.4%)	2 (0.8%)
2016 Alumni	2870	2174 (75.7%)	660 (23.0%)	36 (1.3%)

A discussion of the demographic characteristics of the respondents to the 2017 post-season survey, as well as analysis of the reliability of responses to the “before” questions described above, is found in Section 4.1.

To measure impact on career interest, responses to the cybersecurity career perception questions are analyzed. The mean value of the responses to each question is calculated, and the means of the “before” and “after” versions compared. A paired t-test

is performed for each to determine statistical significance. Effect size is measured by calculating Cohen's d for the difference of means [90, pp. 20–21].

The effect size d for use with t-test for means is defined by Cohen as the ratio of the difference in means to the standard deviation. Assuming two independent samples of populations with equal standard deviations, the effect size for a one-tailed test is thus

$$\mathrm{d} = \frac{\mathrm{m_A} - \mathrm{m_B}}{\sigma} \tag{1}$$

where $\mathrm{m_A}$ and $\mathrm{m_B}$ are the two sample means and σ is the standard deviation of the populations [90, p. 20]. If the standard deviation is not equal in the two populations, σ is replaced by σ', the root mean square of the two standard deviations:

$$\sigma' = \sqrt{\frac{\sigma_\mathrm{A}^2 + \sigma_\mathrm{B}^2}{2}} \tag{2}$$

where σ_A and σ_B are the standard deviations of their respective populations [90, p. 44]. This formula could also be described as the square root of the mean of the variances of both populations. Since the population standard deviations are not known, they are estimated with the sample standard deviations, S_A and S_B, respectively.

The final formula for calculating the effect size thus becomes

$$\mathrm{d} = \frac{\mathrm{m_A} - \mathrm{m_B}}{\sqrt{\frac{S_\mathrm{A}^2 + S_\mathrm{B}^2}{2}}} \tag{3}$$

where $\mathrm{m_A}$ and $\mathrm{m_B}$ are the two sample means and S_A and S_B are the sample standard deviations.

The value of d as calculated for each t-test pair is then evaluated against Cohen's conventions for "small," "medium," and "large" effect sizes [90, pp. 24–26]:

small: $d = .20$

medium: $d = .50$

large: $d = .80$

The results of these calculations are presented and discussed in Section 4.3.

Part of filling the cybersecurity worker shortage should be increasing the diversity of the talent pool, and one of the most significant diversity challenges is the gender imbalance. The impact that participation in CyberPatriot had on female students' perceptions of how accessible a career in cybersecurity is to them is assessed in two ways. First, in the post-season survey, a pair of before and after questions was posed, asking how "welcoming and accessible to females" they thought a career in cybersecurity is. The change in perception from before to after is measured, using a paired t-test, for both male and female students, and the effect size (Cohen's d) calculated for both. Second, the change in the before and after responses to the other career-perception questions is calculated with a paired t-test and Cohen's d specifically for the subgroup of female participants, and compared to the overall group of respondents. Results of this analysis are in Section 4.3.

3.3 Survey of Enlisted Airmen

To study the impact of cyber educational activities specifically on the U.S. Air Force, a survey of enlisted Airmen is constructed. The purpose of the survey is to gain insight into the effectiveness of computing and cyber-related educational outreach activities at fostering the Air Force cyber workforce and guide decisions about Air Force STEM outreach programs. The specific research objectives of the survey are twofold: first, to assess the impact of computing-related educational and outreach activities on the career decisions of enlisted Airmen; second, to assess the impact of computing-related educational and outreach activities on the academic performance of enlisted Airmen in cyber initial skills training ("tech school").

The target population selected for this survey is enlisted Airmen on active duty in the U.S. Air Force, with less than 4 years' time-in-service and under 24 years of age. These criteria are selected to focus the study on the impact of the studied activities on initial recruitment and accession into the Air Force cyber workforce. Past this point in an Airman's career, many additional confounding factors such as on-the-job experiences and opportunities would obscure the impact of activities participated in during middle and high school. That is an internal personnel management matter, which is beyond the scope of this thesis.

The survey is conducted online with invitations sent out via email. A participant list is generated by the Air Force Survey Office based on the criteria described above. The survey is open for two weeks to allow ample time for responses. The survey software tracks responses by email address, and reminders are sent out as needed to those who

have not yet responded. The email address is also recorded along with each individual's responses, in order to correlate to other data sources as described below. The first page of the survey is an informed consent statement. Participants must click a button to agree to the terms of the consent statement; declining to consent will terminate the survey before it starts.

The questionnaire first asks respondent Airmen to choose their Air Force Specialty Code (AFSC) from a dropdown list, and indicate how many years they have been on active duty. If they select more than 4 years of service, the survey is ended and their responses are discarded. The AFSC is used in the analysis to classify Airmen as either "cyber" – defined as AFSCs 3D0X2, 3D0X3, 3D1X1, and 3D1X2 – or "non-cyber." The "cyber" AFSCs reflect the AFSCs with an enlistment bonus for those entering with an industry cybersecurity certification [11]. Respondents are asked if they initially felt this AFSC was a good match; non-cyber Airmen are also asked if they would have preferred a cyber AFSC. Respondents are then asked to select from a list which computing and cyber-related educational activities they participated in prior to entering the Air Force; they can select as many as apply, and lines are provided to fill in activities not listed. For each of the activities a respondent selects, they are then asked a series of questions about their experience, including: timeframe, classroom or extracurricular, how they felt about the activity, the activity's impact on their career choices, and how well they feel the activity prepared them for their job. Finally, respondents are asked for ethnic and gender demographics. Many of the questions are based on the questionnaire from the McGill, Decker, and Settle survey [14], and some of the narrative language is adapted

from that questionnaire, with the permission of the authors. The complete questionnaire is in Appendix C: Questionnaire for Enlisted Airmen Survey.

There are two sets of statistical tests to be run on the resulting survey data, one for each of the main objectives described above in the first paragraph of this section. To meet the objective of assessing the impact of computing-related educational and outreach activities on the career decisions of enlisted Airmen, the following question is posed: Does previous participation in a computing extracurricular activity affect the likelihood an individual will prefer a cyber-related career field when enlisting in the Air Force? Preference for a cyber-related career field is operationally defined as either Airmen in cyber AFSCs who indicate they were pleased with this match or non-cyber Airmen who indicate they would have preferred a cyber AFSC. To answer this question, a difference of proportions test is performed. Activities are classified as either classroom-based or extracurricular, and respondents are categorized into one of four populations based on their participation (or non-participation) in these activities:

Population 1: those who participated in both classroom and extracurricular computing activities

Population 2: those who participated only in classroom computing activities (and *not* extracurriculars)

Population 3: those who participated only in extracurricular computing activities (and *not* classroom activities)

Population 4: those who participated in *neither* classroom-based *nor* extracurricular computing activities

These four populations are summarized in Figure 2 below, categorized by participation in classroom and extracurricular computing activities.

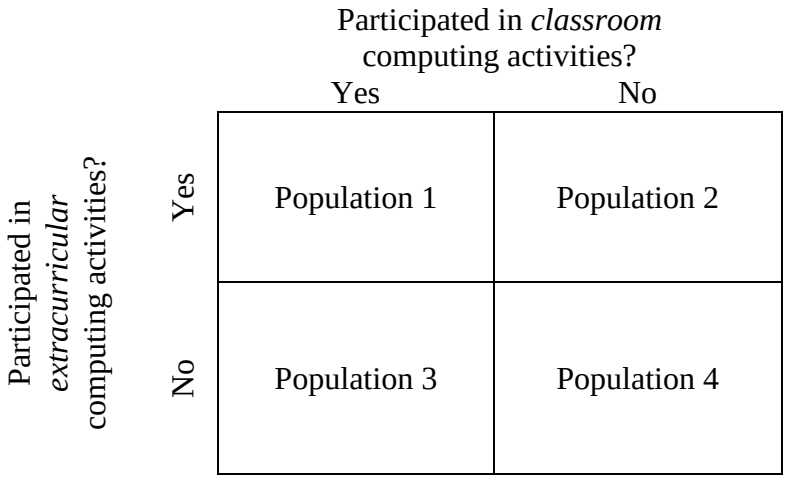


Figure 2. Populations by Participation in Classroom and Extracurricular Computing Activities

The statistic to be tested for each population is the proportion p_x of those who preferred a cyber career, as operationally defined above. The following hypotheses are tested against their respective null hypotheses:

$$p_1 - p_2 > 0 \quad (4)$$

$$p_3 - p_4 > 0 \quad (5)$$

$$p_3 - p_2 \geq 0 \quad (6)$$

The other set of tests addresses the second study objective, to assess the impact of computing-related educational and outreach activities on the academic performance of enlisted Airmen in cyber tech schools. Specifically, the research question posed is: Does previous participation in a computing extracurricular activity serve as a predictor of higher performance in a cyber-related tech school? The test here is a t-test for means, using the mean cumulative grade point average (GPA). Respondents who indicated they are in a cyber AFSC are divided into the same four sub-populations as before (see

Figure 2). Non-cyber respondents are not relevant to this question. The statistic used is m_x, the mean adjusted cumulative GPA from tech school. First, an average GPA for each AFSC must be established, since each of these have separate schools, and their GPAs cannot be assumed to be equivalent. Each respondent's cumulative GPA is then adjusted by dividing it by that tech school's average GPA. Finally, m_x is calculated from the adjusted cumulative GPAs for each of the four sub-populations defined above. A t-test is performed for a difference of means. The following hypotheses are tested against their respective null hypotheses:

$$m_1 - m_2 > 0 \quad (7)$$

$$m_3 - m_4 > 0 \quad (8)$$

$$m_3 - m_2 \geq 0 \quad (9)$$

The number of survey invitations sent out is determined by conducting a power analysis for the desired statistical tests. The power analysis is conducted according to the formulas and sample size tables developed by Jacob Cohen in *Statistical Power Analysis for the Behavioral Sciences*, Second Edition [90].

The sample size for cyber Airmen is based on the t-test measuring the difference in mean tech school GPA between those who had participated in a computing extracurricular activity (population 3) and those that had not (population 4).

Hypothesis tests:

$$H_0: m_3 - m_4 = 0 \quad (10)$$

$$H_A: m_3 - m_4 > 0 \text{ (one-tailed test)} \quad (11)$$

Parameters:

$$\alpha = .05 \text{ (one-tailed)}$$

$$\beta = .20 \text{ (power = .80)}$$

$$d = .20 \text{ (“small” effect size)}$$

The sample size table in [90, p. 54] gives a sample size required of n = 310.

Based on a previous study by McGill et al. [14], it is estimated that about one-third of cyber Airmen will have participated in a qualifying extracurricular activity. Thus the total number of responses needed to get at least 310 in population 1 is three times that: 930. With a predicted response rate of 20% or less, the number of survey invitations to be sent out should be no fewer than 4,650.

The sample size for non-cyber Airmen is based on a difference of proportions test, measuring the difference in proportion of respondents who chose or preferred a cyber AFSC, between those who had participated in a computing extracurricular activity (population 3) and those that had not (population 4).

Hypothesis tests:

$$H_0: \ p3 - p4 = 0 \tag{12}$$

$$H_A: \ p3 - p4 > 0 \ \text{(one-tailed test)} \tag{13}$$

Parameters:

$$\alpha = .05 \text{ (one-tailed)}$$

$$\beta = .20 \text{ (power = .80)}$$

$$h = .20 \text{ (“small” effect size)}$$

The sample size table in [90, p. 205] gives a sample size required of n = 309.

Based on the same previous study by McGill et al. [14], it can be estimated that about 15% of non-cyber Airmen will have participated in a qualifying extracurricular activity. Thus the total number of responses needed to get at least 309 in population 1 is 6.67 times that: 2,060. With a predicted response rate of 20% or less, the number of survey invitations to be sent out should no fewer than 10,300.

As part of the IRB approval process, a risk/benefit analysis is performed. Two risks are identified: participants being uncomfortable with researchers having access to their data, and tech school grade data being leaked. Appropriate measures to mitigate these risks are taken.

The first risk analyzed is that participants may feel uncomfortable with researchers having access to data about their performance in tech school. To minimize this risk, an informed consent statement is provided at the beginning of the survey for participants to read and agree to before continuing. The informed consent statement makes it very clear that tech school performance data will be anonymized and the researchers will not keep copies of identifiable training or performance data. Additionally, the informed consent statement will make it clear that participation in the survey is voluntary and that an individual can exit the survey at any time prior to completion and their tech school records will not be accessed. The informed consent statement also complies with human subject research regulatory requirements.

The second risk analyzed is a leak of the tech school data. If participant grade data were to leak and be obtained by participants' coworkers who otherwise would not have had access to that data, it could affect those coworkers' impressions of the participants

and their knowledge, skills, and abilities. To minimize this risk, survey responses and participant tech school grades must be protected. Initial survey response data is identified by the official email address to which the survey was sent. Once retrieved, the survey data is kept in the investigators' secured accounts on the Air Force Institute of Technology (AFIT) internal network, accessible only to the investigators. Tech school grade data is sent securely by staff at the Headquarters Air Education Training Command (AETC/A3PS). This data contains only names and grades; no other personal information (e.g. SSN) is sent. Once the survey response data and the grade data are correlated, the associated personal information is deleted. The investigators do not store any personal information past the initial downloading and correlation steps.

The complete paperwork for IRB review is attached in Appendix D: IRB Protocol for Enlisted Airmen Survey. Once approved by the IRB, the survey plan must also be submitted to the Air Force Survey Office for approval and assignment of a Survey Control Number (SCN). To be considered by the Survey Office, the survey needs to be sponsored by a general officer responsible for the program being studied. Since Air Force support for extracurricular STEM activities is managed by the Air Force STEM Outreach Program Office within the Air Force Research Laboratory (AFRL), the AFRL Commander is the appropriate general officer. He has expressed enthusiastic support for this survey, and will be the sponsor when the paperwork is submitted to the Air Force Survey Office.

3.4 Expanding Cybersecurity Competitions with a Digital Forensics Activity

The second aspect of this thesis is to expand the scope of current cybersecurity extracurricular activities. As discussed in sections 4.2 through 4.4, the CyberPatriot national cyber defense competition is demonstrated to be an effective model for increasing interest in cybersecurity careers. Therefore the first approach used in this research to expand the potential of cybersecurity extracurricular activities is to build an educational activity that can be added to CyberPatriot or a similar program.

To select a topic for this activity, the knowledge units from the National Security Agency's (NSA) Center of Academic Excellence (CAE) in Cyber Operations [91] are used as a guide (see Table 2) . Of the twenty-seven mandatory and optional knowledge units, nineteen are specifically related to cybersecurity (the other eight are foundational math or computer science/engineering topics). Four of the knowledge units are already covered by CyberPatriot to some degree, six are generally not well-suited for secondary school students (due to difficulty level or age-appropriateness), and two are not interesting or engaging enough for a hands-on extracurricular competition like CyberPatriot. Of the remaining seven potential candidate topics, digital forensics was selected due to its ease of implementation and perceived potential interest with young people. Table 2 lists the complete set of CAE-Cyber Operations knowledge units broken out by the categories described above.

In studying the landscape of extracurricular cybersecurity educational activities widely available for middle and high school students, it becomes apparent that there is a significant deficiency in the area of digital forensics. The rest of this section describes the

Table 2. NSA's CAE-Cyber Operations Knowledge Units

Not cybersecurity	Covered by CyberPatriot	Not age/grade appropriate	Not interesting or engaging	Potential candidates
Low Level Programming Languages	Networking	Software Reverse Engineering	Legal and Ethics	Cellular and Mobile Technologies
Operating System Theory	Overview of Cyber Defense	Virtualization	Risk Management of Information Systems	Wireless Security
Discrete Math and Algorithms	Security Fundamental Principles	Software Security Analysis		Cloud Security/ Cloud Computing
Programmable Logic	Vulnerabilities	Secure Software Development		**Digital Forensics**
Computer Architecture		Offensive Cyber Operations		Applied Cryptography
Microcontroller Design		Hardware Reverse Engineering		Industrial Control System
Embedded Systems				User Experience/ Human Computer Interface Security
Systems Programming				

methodology to create a digital forensics challenge that can complement CyberPatriot's current offering. First, a systematic review is conducted of the field of current programs. All available digital forensics competitions and challenges for middle and high school students that could be found are identified and analyzed based on relevant criteria. Next, a simple activity is designed and created to meet those criteria, which can be used as either a standalone introductory digital forensics challenge or part of a larger educational competition or program like CyberPatriot.

3.4.1 Criteria for the Activity

The criteria for the activity – the goals that it should be attempting to meet – are fourfold: engaging, scalable, introductory, and low-cost. First, the activity must be engaging, or hands-on. Research and experience in extracurricular education has demonstrated that students benefit from engaging, hands-on educational activities (see Chapter II). Since the digital forensics activity is intended to fit this model, it too must be hands-on. Students must *do* something as part of the exercise, not merely answer questions.

The purpose of finding or creating the activity is to expand young people's exposure to the field of digital forensics, thus it must be able to reach the widest possible audience. This means being scalable to both large and small audiences, and accessible to students with a wide range of backgrounds and with a wide range of available resources. It must be flexible enough to be scaled to serve any size audience, no matter how small or (more importantly) large. This requirement rules out any activity requiring manual grading, such as writing a report or answering open-ended or short essay type questions. To be accessible to students who may not already have interest in computers or cybersecurity, the activity must be at the introductory level. It should be appropriate for students in grades 6-12 and require only basic computer skills. The level of specific knowledge required should be such that a student could succeed at the activity after a brief lesson on digital forensics or some simple internet searching. Finally, the activity must be low-cost, accessible to students of any means and background. As such, it cannot require any special hardware or software to accomplish. A computer will be required, of

course, but the activity ought to be able to be completed on the types of computers common to schools, libraries, etc.

3.4.2 Review of Current Programs

The first step on this line of effort is to conduct a systematic review of all available digital forensics competitions and challenges available to middle and high school students. Each competition is evaluated on the following four factors (to the extent possible given the available data), based on the four criteria discussed in section 3.4.1:

- Age/Grade Level. What is the age and grade or skill level the activity is designed for?
- Scalability. What is the potential for growth? This includes not just the size of the target audience, but how easily the program could handle a larger number of participants.
- Cost. Since behind-the-scenes program costs would not be expected to be available, this criterion is focused primarily on cost to participants.
- Engagement level. How interesting and hands-on is the activity?

The results of this review are presented in Section 4.6.1.

3.4.3 Design of the Activity

First and foremost, the activity is designed to meet the four criteria discussed in section 3.4.1 above. Additionally, the activity should accomplish certain educational or learning objectives. Since the purpose of this research is to increase interest in cybersecurity careers, and for this part more specifically cyber forensics, that aim informs the learning objectives chosen. As reviewed in Chapter II, perception of career tasks is one of the key factors influencing career decisions [82]. Therefore the first learning objective is related to the core task of digital forensics, at its most basic level, to find

evidence on a computer. The second objective is the next step, which is to actually foster interest in digital forensics careers. Formally stated, the following primary learning objectives will be used:

- Gain an understanding of evidence left on a computer from everyday activities
- Inspire further exploration/consideration of digital forensics

Since the majority of students who may be exposed to this activity will not actually end up pursuing a cybersecurity-related career, the activity should have additional educational value beyond consideration of digital forensics careers, so it can benefit everyone who participates. Therefore, the activity will also aim to accomplish these secondary learning objectives:

- Practice systematic thinking and problem solving
- Improve practical computer skills

The scenario for the activity is inspired by the popular Carmen Sandiego series of games and television shows [92]. A criminal mastermind (here named “Carla Sanfrancisco”) has just committed a theft and is on her way to her next burglary. The suspect got away, but detectives captured her laptop and extracted the user profile directory. The student is given a ZIP file containing this directory (and the files and sub-directories it contains) to analyze for clues. The student will then answer simple questions based on the evidence, with the ultimate objective of identifying where the suspect is headed next and what will be the target of her next heist.

Since one of the requirements for the activity is to be at an introductory level, only basic computer skills should be required to complete it. Specifically, a participant need only know the basics of how to work with folders and files. To answer the questions and solve the challenge, a student will need to extract a compressed folder (ZIP file), navigate a directory structure, view file properties, use a simple tool to view browser history, and correlate two activities based on date and time. These skills can either be taught in a classroom or laboratory setting beforehand, or left for the participants to figure out on their own based on previous experience and internet searches, depending on the audience. For most situations, it would be recommended that facilitators either provide the browser history viewer tool or a link to download it.

3.4.4 Setup and Creation of the Activity Files

To create the evidence needed for the activity, a virtual machine is created with a clean install of Windows 7. Essential updates are installed, and Internet Explorer upgraded to the latest version (IE11) to ensure compatibility with current versions of websites; however no other modifications, updates, or additions are made. Internet Explorer 11 is used to browse several websites to simulate the suspect's activities: scoping multiple possible locations on Wikipedia, downloading an image of the selected target, and booking a flight to the target location. A simulated "draft email" is composed indicating that the suspect has selected the next target and booked a flight. The following day, the virtual machine is run again, and the browser used again to download more photos of potential targets to serve as decoys.

To extract the user profile, first the built-in Administrator account is enabled using the following command (run in command prompt as Administrator):

```
net user administrator /active:yes
```

The account on the virtual machine is logged off and logged back in with the Administrator account. The following command is used to copy the entire user profile to a test folder in the `C:\` drive:

```
robocopy <user profile directory> <target directory>
/e /copyall /dcopy:T /xj
```

This command copies the entire contents of the directory, including all files and sub-directories, and preserves file properties (except file creation date, which is replaced with file modification date); it does exclude junctions[2], however, as those cause problems with the copy. Windows' built-in ZIP function cannot handle the Unicode characters in the Temporary Internet Files directory, so the content folders must be deleted (they are not needed for this activity). The folder is compressed into a ZIP file using the built-in function, and the ZIP file is copied out of the virtual machine onto the host computer.

The completed activity created using the methodology outlined above is presented in Section 4.6.2, with further discussion in Section 4.6.3. The resulting activity is evaluated against the stated goals and learning objectives in Section 4.6.4.

---

[2] A junction in a Windows NTFS file system is a method of referencing a single directory by multiple paths on the local system [102].

3.5 Cybersecurity Merit Badge[3]

The final element of developing the potential of extracurricular activities to increase interest in cybersecurity careers is to expand the reach of cybersecurity activities by adding a cybersecurity component to another popular youth program. As described in Section 2.5 of Chapter II, competitions are only one form of gamification that is found in extracurricular educational activities. Badges are another, very popular technique for motivating learners. Badges have been used effectively in a number of extracurricular educational settings, most prominently in Scouting. The largest Scouting organization in the United States – and the third largest youth organization in the U.S. of any type – is the Boy Scouts of America (BSA). Furthermore, the BSA has been particularly successful at implementing badges related to science and technology topics and modern STEM-related careers [30], [67], [68], [79], [93], [94]. This makes the BSA a logical place to expand extracurricular cybersecurity education opportunities for pre-college youth through badges.

Therefore, as part of this thesis's contribution to the state of extracurricular cybersecurity education, a Cybersecurity merit badge is designed and proposed to the BSA. First, a selection of current badges related to technology or technical careers is analyzed. The requirements for earning each badge are broken out and categorized by

[3] Portions of sections 3.5 and 4.7.2 were adapted for a poster, "Proposed Cybersecurity Merit Badge for the Boy Scouts of America," presented at the *49th ACM Technical Symposium on Computing Science Education* [103].

type. For each category of requirement across the selected badge set, a few basic descriptive statistics are computed: mean, median, low value, and high value. This analysis can then be used to guide the development of a set of requirements for the proposed Cybersecurity merit badge. The merit badges analyzed and the types of requirements found are discussed in section 2.5.2, and a breakdown of the number of requirements by type is presented in Section 4.7.1.

The BSA receives over a hundred suggestions for new badges every year, and as such has established a very formal process for considering new ideas [94]. To ensure the best chance of success, the proposal for a Cybersecurity merit badge must include a description of the badge, rationale as to why it ought to be created, a draft set of requirements, and information pertaining to feasibility, age appropriateness, recruitment of merit badge counselors, and funding [95].

In order to accomplish all this, and to make sure the proposal represents the broader cybersecurity community rather than just one student at one institution, a diverse team of experts is recruited to contribute. One of these experts was a coauthor on two previous computing merit badges, Digital Technology [76] and Programming [77], as well as the BSA's Internet safety program, the Cyber Chip [78]; he provides expertise not only in commercial cybersecurity but also in merit badge development. Further experts from academia and secondary education are recruited through personal networking at cybersecurity education conferences. Another significant group of stakeholders that needs to be involved are cybersecurity professional associations. These organizations are needed to add further legitimacy to the proposal, and provide sponsor funding as needed.

Two of the most prominent cybersecurity associations – $(ISC)^2$ and the Information Systems Security Association (ISSA) – became involved in the project through their educational foundations, the Center for Cyber Safety and Education and the ISSA Education Foundation, respectively. $(ISC)^2$ and the Center for Cyber Safety and Education serve as the originating entity; that is, they actually send the final copy of the proposal, with a cover letter signed by their leadership. The ISSA Education Foundation is providing donor funding to sponsor development costs, and will advocate to the BSA separately, in coordination with the Center for Cyber Safety Education and the proposal authors.

The proposed badge requirements are developed in three basic categories: safety, knowledge, and activities. The safety requirement is met with BSA's existing program, the Cyber Chip, by simply requiring a Scout to show proof of having completed the Cyber Chip.

Knowledge requirements help a Scout understand key cybersecurity terms and topics. This is important not only for laying the foundation for the activity requirements but also for helping the Scout become a well-informed citizen. Many of these concepts have impacts in everyday life, and greater understanding of them is of benefit not only to the individual, but to society. The first set of knowledge requirements pertain to ethics. Security professionals often have access to sensitive data and systems, making it imperative that they be ethical. The technical and creative skills possessed by many young people interested in computer technology can easily be used for illegal and/or unethical purposes when pursued outside the context of a strong ethical framework. The

next three sets of requirements cover fundamental cybersecurity terms and concepts, a few different aspects of cyber defense, and a survey of common types of threats and attacks against information systems. A short set of requirements hits on the basic categories of encryption and examples of their uses. Moving beyond traditional computers and networks, a set of requirements covers mobile security. Mobile devices are such a ubiquitous part of life, especially for young people, that it is important to know how to keep mobile devices secure when accessing both cellular and WiFi networks. Two brief sets of requirements help raise a Scout's awareness of the importance of security in the context of the Internet of Things (IoT) and critical infrastructure.

Activity requirements give Scouts hands-on experience with real-life cybersecurity. Most of them revolve around the devices and networks a Scout is likely to have or use in his day-to-day life. They help a Scout learn to secure his computer, his home network, and his mobile device. They also empower the Scout to help others secure their devices.

As with the knowledge requirements, the first activity prescribed for this badge is about ethics. A current events requirement prompts the Scout to consider how cybersecurity (or lack thereof) impacts the world around him. The next two sets of requirements cover the most foundational elements of securing any system: installing updates and virus scanning. The next set of requirements includes a variety of options to explore additional aspects of system (host) security. The next set of requirements focuses on network security, such as home WiFi settings and open network ports. The next requirement set provides an option to learn one of three ways a Scout can use

cryptography in his everyday computer use: encrypting a file, encrypting an email, or hashing a file. The next set prompts the Scout to explore further learning opportunities, either through cybersecurity competitions or by teaching a cybersecurity topic to their peers. Finally, the Scout examines career opportunities in cybersecurity. The requirements developed for this proposed merit badge are discussed further in Section 4.7.2. The full set of proposed requirements are detailed in Appendix G: Proposal for Cybersecurity Merit Badge as Sent to BSA National Office.

To gain better insight on the target audience, an informal focus group is conducted. Boy Scouts from a local troop are presented with the proposed set of requirements for their assessment and criticism. The Scouts are asked questions about their general impressions, what they liked, and what they did not like. An informal poll is taken of how many of the Scouts would want to earn the proposed merit badge if it were offered today. No personal information of any kind is collected on any of the focus group participants and only general, non-attributable opinions are recorded.

After the draft of recommended requirements is finalized, in consultation with the team of experts and sponsoring organizations described above, a formal proposal is sent to the BSA national offices to be reviewed by a committee of volunteers. In addition to the draft requirements, the proposal includes all of the additional information described earlier in this section: a description and rationale for the new badge, feasibility, age appropriateness, recruitment of merit badge counselors, and sponsorship/funding. The full and complete proposal is attached as Appendix G: Proposal for Cybersecurity Merit Badge as Sent to BSA National Office.

3.6 Summary

To assess the impact of participating in the CyberPatriot cyber defense competition, survey data of past participants is analyzed. This survey data was previously collected by the competition organizers, and is anonymized for use in this research. A series of "before" and "after" questions is posed to competition participants, and a paired t-test performed for each to determine the statistical significance of the difference in responses. The effect size is also calculated, to measure how large the change is relative to the standard deviations of the samples. The impact of the competition specifically on female students' perceptions is also measured, by looking at their responses to a question about accessibility of cybersecurity careers to females, and by comparing the change in female participants' attitudes compared to male participants.

To gauge the impact of extracurricular cybersecurity activities and related computing outreach efforts specifically on developing the U.S. Air Force's enlisted cyber workforce, a survey of enlisted Airmen is designed. The survey addresses two basic research questions: first, assessing the impact of computing-related educational and outreach activities on the career decisions of enlisted Airmen; second, measuring the impact of computing-related educational and outreach activities on the academic performance of enlisted Airmen in cyber tech schools.

There is a significant deficiency in the area of digital forensics. To address this, first systematic review is conducted of the field of current programs. All available digital forensics competitions and challenges for middle and high school students are identified

and analyzed. Subsequently, a simple activity is designed and created that can be used as either a standalone introductory digital forensics challenge, or part of a larger educational competition or program. Goals are defined for this activity: it should be engaging (hands-on), scalable, introductory, and low-cost. The activity is designed as a puzzle, where students must figure out where a super-thief is headed and what her next target is, based on the evidence they find in an extracted user profile directory. The files for the activity are created using a virtual machine, then copied and compressed into a ZIP file.

The fourth piece of the research is the construction of a proposal for a Boy Scout merit badge in Cybersecurity. A selection of current technology and career-related merit badge is analyzed, and a new badge designed to fit with the other badges. A team of experts and cybersecurity professional organizations recruited to support the development. Then a proposal is built with everything the Boy Scouts of America national staff might need to fully consider the idea. A set of suggested requirements is drafted, along with a number of pieces of additional information needed to create and implement a new merit badge. The results of implementing the research elements described in this chapter are presented and discussed in Chapter IV next.

IV. Results and Discussion

4.1 Introduction

This chapter presents and analyzes the results of the research described in Chapter III. Section 4.2 gives an overview of the CyberPatriot survey respondents, including basic demographic data, and a brief discussion of the reliability of responses. Section 4.3 presents the findings on the impact of the CyberPatriot competition on students' career interests, and Section 4.4 analyzes the impact of the competition specifically on female students' perceptions of the accessibility of cybersecurity careers. The survey of enlisted Airmen described in Section 3.3 of Chapter III is currently being considered by Air Force authorities; if they elect to go forward with it, analysis of the results is left for future work. Section 4.6 starts with the results of the review of available digital forensics activities, then presents the digital forensics activity created for this thesis. An overview of the evidence that the students will find is given, and methods of delivery discussed. Finally the activity is evaluated against the criteria established at the beginning of Section 3.4.1. Section 4.7 begins with the results of analysis of selected current merit badge requirements, then covers the details of the Cybersecurity merit badge proposed to the Boy Scouts of America.

4.2 CyberPatriot Survey[4]

The 2017 post-season survey (following CyberPatriot IX) had 2,161 respondents – an increase of 274% over the 2015 survey. The 2014 alumni survey had 254 respondents, and the 2016 alumni survey had 2,870 respondents – an increase of 1,130% (see Table 3).

Table 3. Survey response numbers

Survey	Total Responses	Male	Female	Decline to Specify
2014 Post-Season	639	516 (80.8%)	115 (18.0%)	8 (1.3%)
2015 Post-Season	790	608 (77.0%)	168 (21.3%)	14 (1.8%)
2017 Post-Season	2161	1553 (71.9%)	576 (26.7%)	32 (1.5%)
2014 Alumni	254	218 (85.8%)	34 (13.4%)	2 (0.8%)
2016 Alumni	2870	2174 (75.7%)	660 (23.0%)	36 (1.3%)

4.2.1 Demographics

Of the 2161 respondents to the 2017 post-season survey, 187 only answered the first three questions, which were mandatory. These responses are excluded, leaving 1974 responses for further analysis (n = 1974). Of those respondents, 71.2% were male, 27.3% were female, and 1.5% declined to respond. Ethnicity data was also collected, as summarized in Table 4. The majority (55.0%) were White non-Hispanic, followed by Asian/Pacific Islander (21.2%) and Hispanic (13.1%). The mean age of respondents was 15.8 years; the median age was 16 years, and the mode was 17 years (25.6% of respondents).

[4] See footnote 1.

Table 4. Respondents by ethnicity

Ethnicity	Frequency	Percentage
American Indian/Alaskan Native	29	1.5%
Asian/Pacific Islander	419	21.2%
Black (non-Hispanic)	83	4.2%
Hispanic	258	13.1%
White (non-Hispanic)	1086	55.0%
Prefer not to answer	99	5.0%
Total	1,974	100.0%

Grade level is determined by what year respondents indicated they would graduate high school (Table 5). The median grade level of respondents that specified a graduation year is 10th grade (i.e. having two years left in high school), and the mode is 11th grade (23.7% of respondents).

Table 5. Respondents by grade level (just completed)

Grade level	HS grad year	Frequency	Percentage
12th grade	2017	350	20.8%
11th grade	2018	468	27.8%
10th grade	2019	340	20.2%
9th grade	2020	267	15.8%
8th grade	2021	138	8.2%
7th grade	2022	91	5.4%
6th grade	2023	32	1.9%
Total		1686	100.0%

These demographics are similar to those of the sampled population, registered participants in the 2016-2017 CyberPatriot competition season [21]. Females are slightly

overrepresented in this survey (27.3% vs 23.0%), as are Asians/Pacific Islanders (21.2% vs 17.8%). Underrepresented demographics include Black non-Hispanic (4.2% vs 6.2%), Hispanic (13.1% vs 17.9%), and 12th-graders (20.8% vs 26.9%).

4.2.2 Reliability

To measure reliability for the retrospective questions in the survey (described in Section 3.1), participants are identified who responded to both the 2015 post-season survey and the 2017 post-season survey. The Pearson *r* is computed as the reliability coefficient for each question.

Unfortunately, only 16 repeat respondents are identifiable, representing just 2.0% of the respondents to the 2015 survey. Even so, based on one-tailed *t* tests, all questions but one ("What was your knowledge of possible cybersecurity careers at the time?") are reliable at the $p < 0.05$ level of significance.

4.3 Impact of CyberPatriot Participation on Career Interest[5]

Participants in the post-season survey were asked before and after versions of four different questions related to perceptions of cybersecurity careers: (1) knowledge of possible cybersecurity careers, (2) how "cool" it would be to work in cybersecurity, (3) likelihood to pursue education or career in cybersecurity, and (4) how welcoming cybersecurity careers are to women. The first three questions are used here as measures

[5] See footnote 1.

of general interest in cybersecurity careers; the fourth is considered separately in a later section.

4.3.1 Survey Results

Participants rated their "knowledge of possible cybersecurity careers" at an average of 3.77 on a 1-to-5 scale, somewhere between "some" and "a lot of" knowledge, up from 3.08 before participating in the CyberPatriot program (see Table 6 and Figure 3). To gauge the size of the effect from before to after, Cohen's d is calculated for the mean difference and compared to Cohen's definitions of small, medium, and large effect sizes [90, pp. 20–26]. By this measure, the effect size d = 1.06 far exceeds Cohen's threshold of 0.80 for large effect sizes.

Table 6. Differences between reported beliefs "before" and "after" participation in CyberPatriot. N = 1,895, $p \ll 0.001$

	"Before"		After		Paired *t*-Test			Effect Size
	μ	σ	μ	σ	*t*	*d.f.*	*p*	*d*
Knowledge of cybersecurity principles (1-5)	2.43	0.98	3.76	0.81	57.7	1,894	0.00	1.33
Likely to pursue education/career in STEM (1-4)	3.16	0.96	3.50	0.73	17.4	1,894	0.00	0.40
Knowledge of cybersecurity careers (1-5)	2.58	0.99	3.72	0.87	46.1	1,894	0.00	1.06
How "cool" it would be to work in cybersecurity (1-5)	3.08	1.03	3.77	0.92	28.8	1,894	0.00	0.66
Likely to pursue education/career in cybersecurity (1-4)	2.24	0.93	3.05	0.83	37.7	1,894	0.00	0.87

Participants' opinions about how "cool" it would be to work in cybersecurity also increase, from 3.08 to 3.77, again on a 1-to-5 scale. The effect size is not as large (d = 0.66), but still comfortably exceeds the 0.50 threshold for a medium effect size [90, p. 26].

The most direct question about participants' career interest straightforwardly asks "how likely [they are] to pursue an education or career in cybersecurity." Here again, there is a marked increase, from a mean of 2.24 before to a mean of 3.05 after, this time on a 1-to-4 scale. The number of participants indicating "somewhat likely" went from 29.6% before to 45.2% after, and the number marking "very likely" rose from 9.4% to 32.3%. The Cohen's d effect size for this question (d = 0.87) comfortably qualifies as a large effect size.

Related to their opinions specifically about cybersecurity careers is participants' perceptions of their own abilities in the field. Respondents were asked to rate their cybersecurity knowledge both before and after participating in CyberPatriot. The mean response increases from 2.43 before to 3.76 after, on a 1-to-5 scale. The effect size of d = 1.33 is the largest effect size observed in this question set, and is much larger than Cohen's requirement to qualify as a large effect size.

Participants were also asked about their likelihood to pursue an education or career in the much broader category of Science, Technology, Engineering, and Mathematics (STEM). While this also increased (3.16 before to 3.50 after, on a 1-to-4 scale), the effect is much smaller than the cybersecurity specific questions. Cohen's d = 0.40, which does not quite reach the level of a medium effect size. This is primarily

due to the fact that the “before” average is already significantly higher than the cybersecurity-specific version of the question (3.16 vs 2.24 on a 1-to-4 scale). This makes sense given that CyberPatriot participants chose to volunteer for an activity that they knew would be somewhat technical.

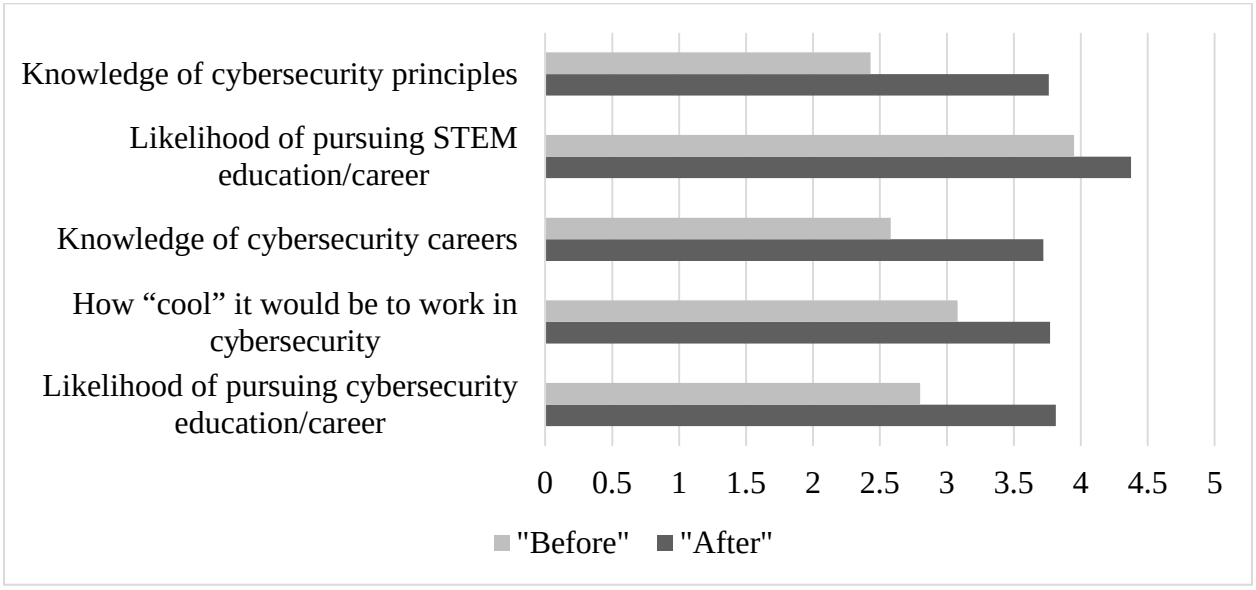


Figure 3. Mean reported beliefs “before” and “after” participation in CyberPatriot

To gauge the extent to which respondents’ self-reported likelihood to enter a cybersecurity field persisted over time, responses to the 2015 post-season survey are linked to responses to the 2016 alumni survey by the same individual. Of the 790 total responses in the 2015 survey, 61 (7.7%) are able to be linked to their responses in the 2016 survey. Of the 17 that had responded in 2015 that they were “very likely” to pursue an education or career in cybersecurity, 13 (76.5%) individuals reported one year later that they were doing so (if they had graduated) or that they still planned on doing so (if they had not yet graduated). Two others (11.8%) were pursuing or planning to pursue a degree in a computer science field.

4.3.2 Discussion

Responses improved on all five questions related to participant perceptions of cybersecurity and cybersecurity-related careers. These increases are both statistically significant ($p \ll 0.001$) and practically significant, with effect sizes ranging from medium to very large. The question then, is can these responses really tell us anything about participants' likelihood to enter the cybersecurity workforce? The factors influencing career selection identified by Walters and Bishop [82] can be used as a framework to judge the relevance of the CyberPatriot survey questions and responses. Of the seven factors they identify from the literature and their own study, four are at least partially addressed by the CyberPatriot post-competition survey questions.

Participants' self-reported "knowledge of cybersecurity careers," which increased with a large effect size, is a key dimension of the career selection factors "perception of career tasks" and "interest and awareness" [82]. This is supported by the finding that a self-reported increase in career knowledge is positively correlated with an increase in expressed likelihood to pursue a cybersecurity career ($r = 0.46$). Also contributing to these factors – especially "interest and awareness" – are the students' perceptions of how "cool" a career in cybersecurity would be. These increased by a smaller amount, due in large part to the fact that they started with a higher average (3.08 vs. 2.58). Increases in the response value to this question have the highest correlation with increases in the likelihood to pursue a career ($r = 0.60$), likely because the two questions are the most similar in the sentiment they express. The factor "difficulty of attainment" is partially addressed by the "knowledge of cybersecurity careers" question; 19.8% of respondents answering this question selected "I know a lot about cybersecurity career opportunities,

as well as how to pursue them" after participating, up from just 4.2% before. Understanding how to pursue a career in cybersecurity, combined with the increased knowledge of cybersecurity principles, could significantly decrease the perceived difficulty of attaining a career in the field.

Participants' responses to the question of how they would rate their "knowledge of cybersecurity basic principles" is also directly relevant to career selection. One of the factors influencing career selection is "view of self", which is essentially whether the student perceives their abilities, aptitudes, etc. as being sufficient to be successful at a particular career [82]. In fact, in studying past participants of the National Ocean Sciences Bowl, Walters and Bishop found that this self-perception had the strongest influence on students' selection of a career [36], [82]. Perceived competence in a subject has also been found to be a predictor of future achievement [96]. It is noteworthy, therefore, that responses to this question saw the greatest increase of all six career perception questions, with a very large effect size. It did not have the strongest correlation to increased likelihood of pursuing a cybersecurity career, but it was positively correlated ($r = 0.31$).

Summing up the participants' perceptions of cybersecurity as a likely career choice, responses to the question of "how likely [the participant is] to pursue education or career in cybersecurity" increased from 2.24 to 3.05 on a 4-point scale. This increase is statistically significant and has a large effect size. After participating, 32.3% of respondents indicated they were "very likely" to pursue cybersecurity, and 45.1% said they were "somewhat likely" to do so; this is up from 9.4% and 29.5%, respectively, that

indicated they were very or somewhat likely to pursue cybersecurity before participating in CyberPatriot. These results are consistent with previous years' surveys [88].

Ultimately, the goal of the CyberPatriot program is not truly fulfilled unless students follow-through with these intentions and actually enter the cybersecurity workforce. Observing participants' responses to multiple surveys over time is the best way to measure if this is really happening. From the limited results found in this study, it appears that the majority of participants do follow-through on their stated intentions. This is also supported by the overall number of CyberPatriot participants who have entered a cybersecurity-related field. The 2016 alumni survey found that 59.2% of those enrolled in higher education were majoring in a cybersecurity or computer science field, and 82.4% of high school grads were employed in or seeking work in a cybersecurity or computer science related field [87].

4.4 Impact of CyberPatriot Participation on Female Perceptions of Career Accessibility[6]

Since an important part of filling the cybersecurity worker shortage is increasing the diversity of the talent pool, it is relevant to consider CyberPatriot's impact on female participants. Although participation in CyberPatriot suffers from a significant gender imbalance, it is not as severe as the imbalance in the current cybersecurity workforce (23.0% of participants in the 2015-2016 season were female [21] vs. only 11% in the

[6] See footnote 1.

current workforce [13]). Furthermore, it is important to assess how well the program does at influencing those female students that do participate.

4.4.1 Survey Results

Responses to the question of "how welcoming and accessible to females" participants think a career in cybersecurity is rose from a mean of 3.46 before to 3.83 after, on a 1-to-5 scale (see Table 7). Although statistically significant ($t = 19.7$, $p \ll 0.001$), the effect size is not quite medium ($d = 0.45$). When considering just the sub-population of female participants, however, that increases to $d = 0.58$, which constitutes a medium effect size.

Table 7. Perceptions of how "welcoming and accessible" cybersecurity careers are to females

		"Before"		After		Paired t-test ($p \ll 0.001$)		Effect size
	N	*μ*	*σ*	*μ*	*σ*	*t*	*d.f.*	*d*
All	1,895	3.46	1.07	3.83	0.99	19.7	1894	0.45
Female	523	3.02	1.07	3.56	1.04	13.2	522	0.58
Male	1,343	3.64	1.01	3.94	0.94	14.5	1342	0.40

Another way to assess how female participants' perceptions of cybersecurity careers changed is to compare their responses on the career perception questions to the responses of male participants. For every single question, although the overall mean response values of the 523 female respondents are lower than those of the 1343 male respondents, the change in their responses from before to after is greater (see Table 8). The difference in mean change is statistically significant for every question (t between

2.85 and 5.79, $p \leq 0.002$), however the effect size is small (two of the questions are close, though just shy of the "small" effect size convention).

Table 8. Mean changes in response, by gender

	Female (N = 523)		Male (N = 1,343)		Independent t-Test			Effect Size
	μ	σ	μ	σ	t	$d.f.$	p	d
Knowledge of cybersecurity principles (1-5)	1.55	1.00	1.26	0.99	5.79	950	0.00	0.30
Likely to pursue education/career in STEM (1-4)	0.52	0.93	0.27	0.82	5.45	855	0.00	0.29
Knowledge of cybersecurity careers (1-5)	1.26	1.11	1.10	1.04	2.85	898	0.002	0.15
How "cool" it would be to work in cybersecurity (1-5)	0.82	1.10	0.65	1.02	3.02	891	0.001	0.16
Likely to pursue education/career in cybersecurity (1-4)	0.99	0.99	0.75	0.89	4.84	871	0.00	0.25
Welcoming and accessible to females (1-5)	0.54	0.92	0.30	0.77	5.11	815	0.00	0.27

4.4.2 Discussion

According to female participants' survey responses, their perception of how "welcoming and accessible" cybersecurity careers are for females improved in a meaningful way; the improvement in their responses is statistically significant and has a medium effect size. However, perhaps a more meaningful measure is how much female students' opinions changed regarding cybersecurity careers as it relates to *them* specifically. It is possible for a female student to think that a career may be accessible to females generally, but still not think they themselves are "cut out for it." The general

trend in the literature that girls tend to perceive themselves as less capable in technical fields than boys do holds for CyberPatriot participants as well. Mean responses to the career perception questions were lower for female respondents than for their male counterparts across the board, both in the "before" questions and in the "after" questions. However, the change in mean response value was higher for female respondents than for males on every question ($p \ll 0.01$). As discussed in the previous section, perceptions improved meaningfully for all students overall, but the improvement was greater for females.

Bolstering the notion that participation in CyberPatriot narrows the gap between male and female students with regard to their interest in cybersecurity careers, female respondents to the alumni survey reported pursuing cybersecurity and computing majors and careers in very similar proportions. Among females enrolled in higher education, 53.6% were majoring in a cybersecurity or computer science field (compared to 59.2% overall), and 80.6% of female high school grads who reported a career field were in cybersecurity or computer science related fields (compared to 82.4% overall [87]).

4.5 Survey of Enlisted Airmen

As of this writing, the plan for the survey of enlisted Airmen, as detailed in Section 3.3, is being reviewed by the Wright-Patterson Air Force Base IRB. Once the survey is executed, the results will be analyzed and presented in a separate venue.

4.6 Digital Forensics Educational Activity

4.6.1 Review of Current Programs

After extensive internet searches, a total of seven programs were identified for further analysis. The results of this analysis are compiled in Table 9 on page 72 below. Each activity is evaluated on the following five criteria, described in further detail in Section 3.4.1: scope, size, scalability, cost, and engagement level. None of the activities had any data on impact, so that criterion is omitted from the evaluation matrix.

The trend for digital forensics competitions and challenges is clear: activities come and go, but most activities are discontinued after just a few years, if they get off the ground at all. The one exception to this seems to be NYU's CyberSecurity Awareness Week High School Forensics challenge. However, no data was available about how many participants they have actually had, or the impact of participating.

4.6.2 Results of Creating the Activity Files

Following the procedures detailed in Section 3.4.4, the activity files for the digital forensics educational activity were created on 21-22 August 2017, using VMWare Workstation on a computer in the AFIT Center for Cyberspace Research (CCR) Cyber Defense Lab. This section describes the evidence created for participants to find and use to answer the challenge questions listed in Appendix E: Example Prompt, Questions, and Answers for Digital Forensics Educational Activity. A more detailed breakdown of available evidence is in Appendix F: Detailed Description of Evidence for Digital Forensics Education Activity.

Table 9 Digital Forensics Activity Evaluation Matrix

Activity	Age/Grade Level	Scalability	Cost	Engagement
Black T-Shirt Cyber Forensics Challenge https://cyberforensicschallenge.com/ *Inactive – only ran one year* [51], [52]	Anyone	Entries graded by hand ("countless hours of grading" [54]); rubric, written report [53]; judges from academic and industry partners [53]	Free to participants [52]	Data not available
Digital Forensics Security Treasure Hunt [55] http://digitalforensics.securitytreasurehunt.com/ *Inactive – site has not been updated since 2013* [56]	Anyone	Very high	Free to participants	Low – participants look at images and answer questions about them [55]
CSSIA Youth Forensics Competition [57] (Moraine Valley Community College)	6th-8th grades	In-person camp – not scalable	Data not available	Very high – on-location immersive hands-on scenarios
US Digital Forensics Challenge [59] (Digital Forensics Consortium) http://www.usdfc.org/us-digital-forensics-challenge.html (continuation of the DC3 Challenge, discontinued due to budget cuts, taken up by private non-profit) [60], [61] *In the works for years, but has yet to launch. Seems to have stalled.*	Anyone	High – challenges conducted online/remotely [59]	Data not available	Medium-High – series of progressively harder hands-on exercises [59]
Digital Crime Scene Challenge [58] (Digital Forensics Consortium) http://www.usdfc.org/digital-crime-scene-challenge.html	Not specified	Limited – physical challenge must be set up on location; limited to no more than 5 participants per team, 15 minutes per team	Data not available	Very high – on-location immersive hands-on scenarios
CSAW High School Forensics [45], [48] (NYU Cybersecurity Awareness Week) https://csaw.engineering.nyu.edu/hsf	High school	Medium-High – qualification rounds consist of online quizzes, but finals are in-person (limited) [45]	Online qualification rounds are free; costs for in-person finals vary [45]	Medium – qualification rounds are just answering questions; finals are hands-on and involve solving a mystery [45]
Cyber Defense Training Academy Cyber Forensics Challenge [62] (Civil Air Patrol) https://github.com/cap-cdta/cyber-forensics-challenge	Middle and high school [62]	Medium – open source materials allow local implementation of challenge anywhere, but requires special equipment and set-up [62]	Approx. $200 per kit for basic challenge, additional $300 for advanced challenge (kit can be reused) [63]	High – on-location hands-on challenge [62]

The file `email.txt`, located in the `Documents` folder, contains text that appears to be a draft email, stating “I selected our next target and booked a flight yesterday. I’ll be there the day after tomorrow.” From the file properties (Figure 4), the student can see the file was modified August 22; therefore any true evidence of target selection and booking a flight must be dated before that.

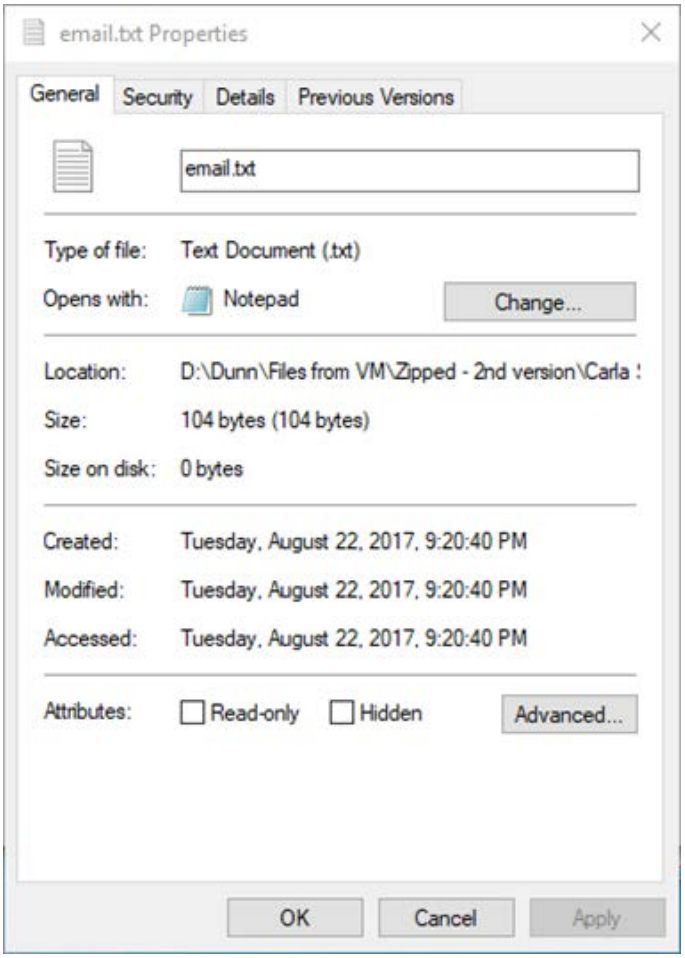


Figure 4. File Properties, `Documents\email.txt`

Also in the `Documents` folder is a file named `Andersen.txt`, containing a text version of Hans Andersen’s Fairy Tales, Second Series, from Project Gutenberg (www.gutenberg.org). The relevant information can be found in the Table of Contents,

which shows that “The Little Mermaid” is one of the stories contained in it. This connection will only become evident once the student has pieced together a couple more of the clues.

The `Downloads` folder (Figure 5) contains several photos of iconic public statues around the world.

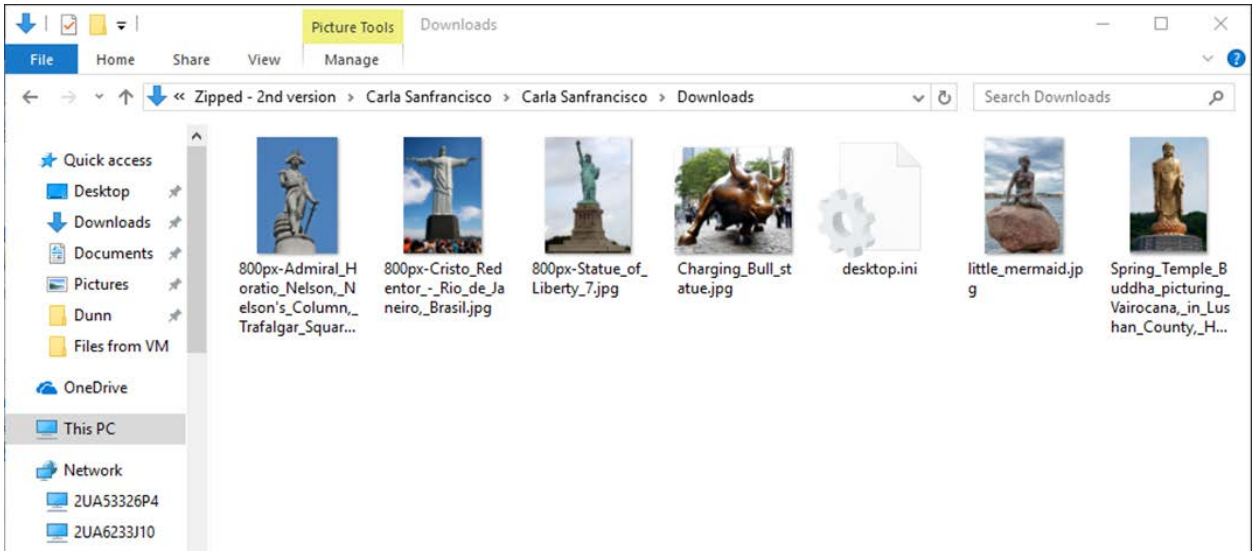


Figure 5. `Downloads` folder

If the student views the file properties of each file, either one at a time or by switching to details view, she will see that all but one were created on August 22. Only one (`little_mermaid.jpg`) was created August 21. This suggests – though so far does not prove – that `little_mermaid.jpg` is related to the target. Viewing the extended file properties shows that the file has a tag “Kopenhagen”. Now, at this point a sharp student may be able to guess that next target is The Little Mermaid statue in Copenhagen, Denmark. However, the point of the exercise is not merely to solve a geography clue, but rather to gather a variety of evidence and correlate it together.

Therefore answering the all of the questions (Appendix E: Example Prompt, Questions, and Answers for Digital Forensics Educational Activity) will require participating students to go a step further.

Web browsing history is also contained in the user profile directory (`AppData\Local\Microsoft\ Windows\History\`). However, it is not directly viewable in Windows, so students will have to use a digital forensics tool to extract and view it. The tool used in testing this activity was BrowsingHistoryView v2.10, from NirSoft [8], though any similar tool should work too. When this tool is run on the extracted user profile, a list of URLs visited is displayed, along with visit date and time. These entries can be sorted chronologically by clicking the Visit Time column header, allowing the student to reconstruct the suspect's web browsing activity, as shown in Figure 6.

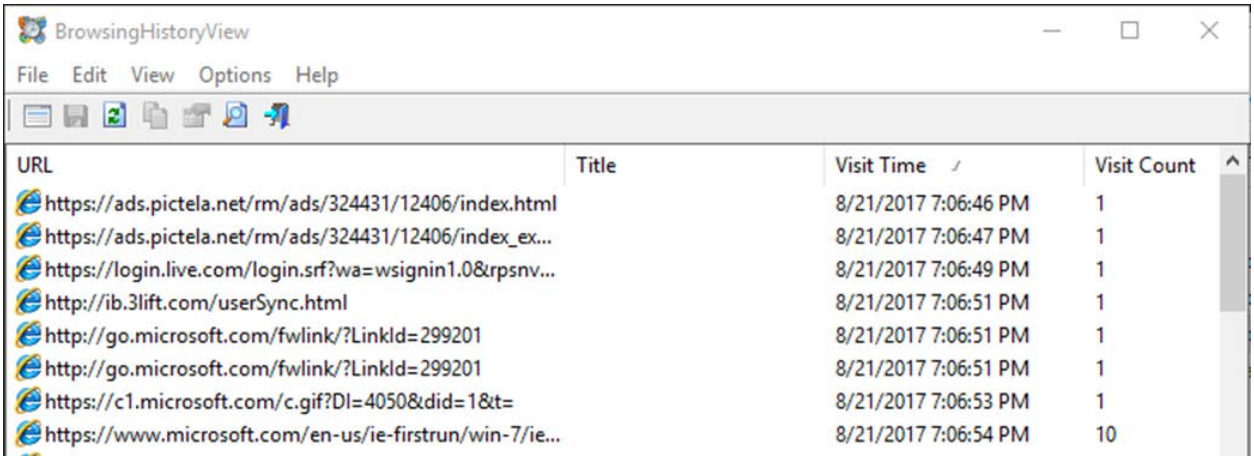


Figure 6. NirSoft browsing history, sorted by visit time

From this browsing history, the student should be able to see the following (for a more detailed breakdown, including screenshots for each item, see Appendix F: Detailed Description of Evidence for Digital Forensics Education Activity):

Open browser: August 21, 2017, 7:06 PM

- Loads default page(s)

Wikipedia

- Main_Page (default)
- Chicago-style pizza
- Sydney
- Milan
- Dublin
- Copenhagen
- The Little Mermaid (statue) (visiting this URL confirms that this is the source of the `little_mermaid.jpg` file in the `Downloads` folder)

Gutenberg.org (free public domain books)

- Search for Hans Andersen
- Selected *Hans Andersen's Fairy Tales, Second Series*
- Downloaded text file, saved as `Andersen.txt` (file modified time can be correlated to browsing history visit time)

Google

- Searched "united airlines"
- Clicked link to https://www.united.com/ual/en/us (United Airlines U.S. homepage)

United Airlines

- Searched for flight from ORD (Chicago O'Hare) to CPH (Copenhagen) departing August 23, 2017 (this can be seen from the format of the URL, shown in Figure 7)

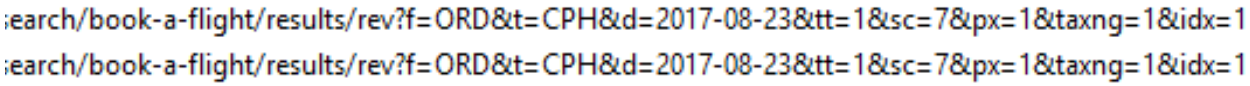


Figure 7. Detail of URL in browser history

- Selected flight (exact flight unknown)
- Continued through booking process

Open browser: August 22, 2017, 8:46 PM

- Loads default page
- Lots of built-in advertisements

Wikipedia

- Christ the Redeemer (statue)
- Downloaded photo

Bing

- Searched "iconic statues" (using the IE Search Box)

Wikipedia

- Statue of Liberty → downloaded photo
- Trafalgar Square
- Nelson's Column → downloaded photo
- Charging Bull → downloaded photo
- Angel of Grief
- Spring Temple Buddha → downloaded photo

- Visit times can be correlated with file properties

4.6.3 Discussion

From these pieces of evidence, students participating in the activity should be able to deduce that the thief is headed to Copenhagen, Denmark, and her next target is the iconic waterside statue of *The Little Mermaid*. However, as noted earlier, as a digital forensics activity and not just a computer-based mystery game, students should be required to go a level deeper and look at multiple pieces of evidence to support a conclusion. Furthermore, there are enough data in this evidence to go into more detail, such as which airport she is flying out of, what date she will arrive, and more.

There are three basic approaches that a teacher or facilitator could take, depending on the size and nature of the target audience. For an informal activity with a fairly small group, the students can be given a fixed time to analyze the evidence, then discuss what they found as a group. For a more formal competition, or even a graded school assignment, but still with a relatively small group, students could be asked to write up a simple report detailing the evidence they found and the conclusions they made from it, perhaps with a few prompting questions drawn from Appendix E: Example Prompt, Questions, and Answers for Digital Forensics Educational Activity. However, since the goal is scalability, the activity has been designed in such a way that it can be adapted for an arbitrarily large number of participants. By turning the pieces of evidence into questions on a quiz, the challenge can be delivered remotely on the Internet, and entries can be scored automatically. Since this is such a simple exercise, multiple entries with

perfect scores should be anticipated, at which point time could be used as a tiebreaker (e.g. first correct entry wins, or completed in shortest time after download if the system enables this). An example of suitable quiz questions is in Appendix E: Example Prompt, Questions, and Answers for Digital Forensics Educational Activity.

4.6.4 Evaluation of the Activity against the Goals

At the outset of the activity design, four goals or parameters were established. First, that the activity be engaging and hands-on. This activity meets that intent by giving participants real files to explore and analyze, including using a real-world tool. Clues have to be found by actually doing something, not just looking up some facts. The activity achieves the scalability goal by being adaptable to different size groups. While the activity would work great in smaller settings like classrooms, it works just as well with a very large disperse audience by being distributed online, with participant entries scored automatically via multiple-choice or similar type quiz. The activity also stuck to introductory level skills, building upon very basic computer skills. The additional techniques needed, such as viewing file properties and using a tool to view web browsing history, can be taught in a short classroom lesson, or left for students to figure out with web-based resources, a little trial-and-error, and problem solving. Finally, the activity is very low cost, requiring no expensive software or equipment. A participant can accomplish everything needed to solve the case using any Windows computer, an Internet connection, and a free web browsing history tool. Additionally, since the exercise files do not include any software (such as would be the case with a virtual machine image), the facilitator does not incur any licensing expenses.

The activity created in this project would be appropriate for use in various settings, such as an introductory computing class. It could also be integrated into a larger computing or cybersecurity competition, such as CyberPatriot. The activity files could be distributed with the competition images, and questions from Appendix E: Example Prompt, Questions, and Answers for Digital Forensics Educational Activity included in the competition round.

4.7 Cybersecurity Merit Badge

4.7.1 Analysis of Current Merit Badges

The first step in creating a Cybersecurity merit badge for use in the BSA is to analyze the structure of existing merit badges. As first discussed in section 2.5.2, eight merit badges were selected, all of which relating to technology or technical careers, and all of them created or updated within the past few years. Requirements for these merit badges generally fall into one of the following types: safety, knowledge, activity, project, and large project. The number of requirements in each of these categories for the selected merit badges, along with some basic descriptive statistics, is in Table 10 below.

4.7.2 Design of Proposed Cybersecurity Merit Badge[7]

In keeping with the pattern found in existing BSA merit badge requirements, the proposed badge requirements are developed in three basic categories: safety, knowledge, and activities. All requirements presented here have been established by consensus of the

Table 10. Merit Badge requirements analysis

Merit Badge	Safety	Knowledge	Activity	Project	Lg. Project
Animation	0	11	1	2	0
Aviation	0	24	3	1	0
Digital Technology	1	31	5	3	0
Game Design	0	15	2	1	1
Mining in Society	4	19	4	0	0
Programming	2	28	2	2	0
Robotics	2	17	1	0	1
Welding	5	19	1	0	1
Mean	1.75	20.5	2.375	1.125	0.375
Median	1.5	19	2	1	0
Low	0	11	1	0	0
High	5	31	5	3	1

team of experts assembled as described in Section 3.5. In addition to the discussion below, the complete set of suggested requirements can be found in the proposal document

[7] See footnote 3.

sent to the BSA national office, attached as Appendix G: Proposal for Cybersecurity Merit Badge as Sent to BSA National Office.

The safety requirement is met with BSA's existing program for online safety, the Cyber Chip [78], by simply requiring a Scout to show proof of having completed the Cyber Chip.

Knowledge requirements help a Scout understand key cybersecurity terms and topics. This is important not only for laying the foundation for the activity requirements but also for helping the Scout become a well-informed citizen. Many of these concepts have impacts in everyday life, and greater understanding of them is of benefit not only to the individual, but to society. A list of key terms and concepts covered by the knowledge requirements is in Table 11 below. The complete set of knowledge requirements is in Appendix G: Proposal for Cybersecurity Merit Badge as Sent to BSA National Office, starting on page 159.

Table 11. Summary of Key Terms and Concepts in Knowledge Requirements

Acceptable behavior in cyberspace	Vulnerability disclosure	Vulnerability	Exploit	Identity
Confidentiality	Integrity	Availability	Authentication	Authorization
Firewall	Antivirus	Intrusion Detection/Prevention Systems	Access control list	Multi-factor authentication
Threats to computer systems	Types of malware	Botnet	Online scams	Symmetric encryption
Asymmetric encryption	Hashing	Public Key Infrastructure	Public Wi-Fi risks	Mobile device security
Jailbreaking	Application sideloading	Application permissions	Internet of Things	Critical infrastructure

The first set of knowledge requirements pertain to ethics. Security professionals often have access to sensitive data and systems, making it imperative that they be ethical. The technical and creative skills possessed by many young people interested in computer technology can easily be used for illegal and/or unethical purposes when pursued outside the context of a strong ethical framework. The next three sets of requirements cover fundamental cybersecurity terms and concepts, a few different aspects of cyber defense, and a survey of common types of threats and attacks against information systems. A short set of requirements hits on the basic categories of encryption and examples of their uses. Moving beyond traditional computers and networks, a set of requirements covers mobile security. Mobile devices are such a ubiquitous part of life, especially for young people, it is important to know how to keep mobile devices secure when accessing both cellular and WiFi networks. Two brief sets of requirements help raise a Scout's awareness of the importance of security in the context of the Internet of Things (IoT) and critical infrastructure.

Activity requirements give Scouts hands-on experience with real-life cybersecurity. Most of them revolve around the devices and networks a Scout is likely to have or use in his day-to-day life. They help a Scout learn to secure his computer, his home network, and his mobile device. They also empower the Scout to help others secure their devices. A summary of these activity requirements is listed in Table 12 on page 84. The full set of activity requirements is on pages 161 to 165 of Appendix G: Proposal for Cybersecurity Merit Badge as Sent to BSA National Office.

As with the knowledge requirements, the first activity prescribed for this badge is about ethics. A current events requirement prompts the Scout to consider how cybersecurity (or lack thereof) impacts the world around him. The next two sets of requirements cover the most foundational elements of securing any system: installing updates and virus scanning. The next set of requirements includes a variety of options to explore additional aspects of system (host) security. The next set of requirements focuses on network security, such as home WiFi settings and open network ports. The next

Table 12. Summary of Activity Requirements

Ethics and Current Events.
Locate and examine a code of ethics from an information security society.
Find out about a recent cybersecurity incident in the news.
System Security. DO SIX OF THE FOLLOWING (INCLUDING BOTH MARKED WITH *):
*Check for and install updates. Verify your computer is up-to-date.
*Run a virus scanner on your computer. Review the results.
Set a “strong” account password, or install and set up a password manager.
Add a new user account and set permissions. Disable the guest account.
Use two different methods to see what processes are running on your computer.
Use a command line to view your computer’s open network connections.
Check your firewall. Turn it on if it is not already.
Identify and fix one or more other vulnerabilities on your computer or network.
Network Security. DO TWO OF THE FOLLOWING:
Verify your home Wi-Fi security settings. Set a strong password.
Run a network port scan on your computer and discuss the results.
Show how to tell if a Wi-Fi network is secure, and how to connect to it.

Cryptography. DO ONE OF THE FOLLOWING:

Create an encrypted ZIP file.

Create and share your own PGP email key. Send a digitally encrypted email.

Hash a file. Change the file. Re-hash it, and compare to the original value.

Careers. DO TWO OF THE FOLLOWING:

Investigate three careers that involve cybersecurity.

Visit a business or organization that does work in cybersecurity.

Discuss certifications in cybersecurity, and find out about two of them.

requirement set provides an option to learn one of three ways a Scout can use cryptography in his everyday computer use: encrypting a file, encrypting an email, or hashing a file. The next set prompts the Scout to explore further learning opportunities, either through cybersecurity competitions or by teaching a cybersecurity topic to their peers. Finally, the Scout examines career opportunities in cybersecurity.

The full proposal (in Appendix G: Proposal for Cybersecurity Merit Badge as Sent to BSA National Office) also includes information pertaining to feasibility, age appropriateness, recruitment of merit badge counselors, and funding.

All proposed requirements can be completed by an individual Scout with just a computer and access to the Internet. If the Scout does not have a computer or Internet access of his own, the requirements can be completed on a school or library computer (with permission), or a computer supplied by the merit badge counselor.

Local BSA organizations often choose to run dedicated merit badge classes, either in the form of a "[specific merit badge] Day" or a merit badge "clinic," where classes for

multiple merit badges are offered simultaneously, and each Scout chooses what to take. In order to run a merit badge class or clinic, a unit would need one computer for every Scout participating, or at least enough computers such that Scouts can rotate through and each get sufficient time on the computer, plus Internet access with sufficient bandwidth. Appropriate computers can be purchased new for as little as $200-300, sometimes even cheaper. However, a unit need not buy new computers, since the computers available in most school or library computer labs would be sufficient. The unit would merely need permission to install any software they were using for the class and/or to access any security settings the Scouts might be working with.

One of the issues of concern to the BSA is whether the activities are age-appropriate for middle and high school-aged boys, and whether there would be enough interest in this new merit badge. There is ample evidence to suggest there would be. CyberPatriot, described in greater detail in a previous section, has been growing rapidly in recent years. The number of registered teams has grown by over 330% over the last five years. In 2017, they continued this growth trend, registering nearly 5,600 teams – over 15,000 registered participants [97]. These teams are spread throughout the country and attract a diverse group of students [89]. Notably, these students commit to spending several hours per week for up to an entire school year on the program and belong to a school or other organization with the resources to field such a team. A Cybersecurity merit badge in the BSA would reach a significantly broader audience. As discussed in Section 2.4 of this thesis, a growing body of research indicates that young people get excited about cybersecurity when given the chance to explore it hands-on. For example,

in a survey of CyberPatriot participants, 81% indicated that it was more fun than other extracurricular activities, and 33% said it was the most fun of all their extracurricular activities [88]. Furthermore, as detailed earlier in this chapter, participation in CyberPatriot can have a significant impact on a student's interest in cybersecurity and related careers. Additionally, the success of Robotics, Programming, Digital Technology, and others validates that there is significant interest among Scouts in exploring technology fields and in pursuing technology-related merit badges [79], [98].

Feedback from the focus group provides additional insight into the potential perceptions of the target audience (i.e. boys aged 11-18 years who participate in Boy Scouting). The focus group was conducted with approximately eight Boy Scouts at a leadership meeting of a local Boy Scout troop. Reactions to the proposed merit badge were overwhelmingly positive. The Scouts were especially supportive of the requirements pertaining to mobile devices and wireless Internet, commenting that those subjects were particularly applicable to their everyday lives. The requirement regarding cybersecurity in current events and popular culture was another stated favorite. There was a general feeling that the requirement set as presented was too long, but they liked the fact that there was flexibility to choose from a set of options. Of the approximately eight Scouts present, only one had earned Digital Technology, and none had earned Programming, the two merit badges closest to the proposed Cybersecurity badge. This suggests that a Cybersecurity merit badge may have even wider appeal to Boy Scouts than the current computing-related offerings.

In order to earn a merit badge, a Scout must work with a merit badge counselor, who is typically an expert in the subject, either as a professional or a hobbyist [75]. Therefore, it is imperative that enough merit badge counselors are recruited in order to provide the maximum number of Scouts the opportunity to complete the badge.

According to data from CyberSeek, a job analytics site sponsored by the National Initiative for Cybersecurity Education, there are approximately 747,000 cybersecurity workers in the United States (this includes both those in primary cybersecurity jobs and those in other roles that require cybersecurity skills) [99]. Members of IT/cybersecurity professional organizations regularly volunteer for community outreach and education efforts. $(ISC)^2$ and ISSA, two of the largest and most prominent such organizations and co-sponsors of this proposal, are committed to supporting and helping to recruit new merit badge counselors. Several other national and international organizations for cybersecurity professionals also have significant volunteer efforts focused on youth education, including ISACA, the Armed Forces Communications and Electronics Association, and the Military Cyber Professionals Association. These organizations will be excellent places to start recruiting additional merit badge counselors.

Additionally, CyberPatriot recruits thousands of volunteers every year to coach and mentor teams for its competitions. Each of the 5,600 teams nationwide has at least one coach or mentor that is knowledgeable in cybersecurity, and often more than one. Since merit badge counseling requires a significantly smaller time commitment than coaching or mentoring a CyberPatriot team, it is likely the BSA will be able to attract even more volunteers.

Developing and launching a new program of this scale requires significant resources, including financial support. As a non-profit organization, the BSA has limited extra funds to apply towards new programs. Thus, external funding is important to making a Cybersecurity merit badge a reality. This merit badge proposal is sponsored by the ISSA Education Foundation and the Center for Cyber Safety and Education and is endorsed and supported by $(ISC)^2$. The ISSA Education Foundation has donor funds specifically designated to support the development of a Cybersecurity merit badge program for Boy Scouts.

When it comes time to launch the new Cybersecurity merit badge, or if the development costs exceed the funds available from the sponsoring organizations, a corporate sponsor can be solicited. As leading cybersecurity professional and education organizations, both ISSA and $(ISC)^2$/Center for Cyber Safety and Education have valuable connections with industry. In the past, large information technology and security companies have been eager to sponsor, support, and promote cyber education programs. For example, Palo Alto Networks is sponsoring development of the GSUSA cybersecurity badges [74], and CyberPatriot has at least nine large corporate sponsors annually, including Cisco, Microsoft, and Facebook (in addition to several government and academic sponsors) [100].

The complete proposal, approved by consensus of the aforementioned team of experts and sponsoring organizations, was mailed by $(ISC)^2$/Center for Cyber Safety and Education to the BSA national office on January 25, 2018. A copy of this document is attached in Appendix G: Proposal for Cybersecurity Merit Badge as Sent to BSA

National Office. The proposal will now undergo review by a committee of volunteers at the BSA National Council. The committee reviews proposals approximately once every four months [95]; if approved, full development of a new badge can take up to two years [94].

4.8 Summary

This thesis begins to assess the impact of the CyberPatriot program on the career interests of students by analyzing responses to recent surveys conducted by the competition organizers. The results show that interest in cybersecurity as an educational or career prospect increased meaningfully across multiple dimensions, such as perception of career tasks, interest and awareness, and view of self. The reliability of these self-reported perceptions is bolstered by comparing responses across surveys administered at different times. The findings of this research indicate that a significant majority of those reporting that they are very likely to choose a cybersecurity field are still planning to do so when asked again one year later.

The findings also indicate that the CyberPatriot competition is contributing positively to correct the gender imbalance in the cybersecurity workforce. Although a minority of participants in the program are female, it is more than twice the percentage of females in the overall cybersecurity workforce. Furthermore, despite female participants' lower perceptions of cybersecurity careers, they showed a greater increase overall in positive perceptions than their male counterparts, significantly narrowing the gap between male and female responses.

In reviewing available cybersecurity extracurricular activities, particularly competitions, for middle and high school students, it is observed that there is a distinct lack of options in the area of digital forensics. A digital forensics activity is created that is appropriate for middle or high school students. The activity is in the form of a ZIP file with the contents of a suspected thief's `Documents` folder. Students analyze the forensic evidence in the folders and files, reconstructing user activity to answer some basic questions. It meets the design criteria of being hands-on, scalable, low-cost, and introductory.

The merit badges analyzed generally have three basic categories of requirements: safety, knowledge, and activities (sometimes including larger projects). Therefore, the Cybersecurity merit badge created here for proposal to the Boy Scouts of America has safety, knowledge, and activity requirements, which together cover a broad foundation of essential cybersecurity concepts and skills. A number of additional pieces of information, related to the appropriateness and practicality of implementing a Cybersecurity merit badge, are also compiled and included in the proposal.

V. Conclusions and Recommendations

5.1 Conclusions of Research

It is evident that the cybersecurity career field is in dire need of more workers. The U.S. government, including the Department of Defense, are also suffering from a critical shortage of skilled cybersecurity personnel. The government and the cybersecurity community at large must find ways of increasing the talent pool, and they are currently trying a number of approaches. A critical aspect of attaining this objective is recruiting more young people, and a more diverse group of young people, to pursue educations and careers in cybersecurity and related fields.

Organized extracurricular activities have been shown to have positive effects on the development of children and young adults. Academic or career-oriented activities can also have an impact on students' future educational and career choices. In recent years this has been studied with special emphasis on STEM subjects, activities, and related careers. Participation in certain STEM-focused extracurricular activities has a positive correlation with higher interest in STEM subjects and careers, and there is evidence to suggest that participating in such activities does increase this interest. Competitions are a specific subset of extracurricular activity, and seem to have several additional benefits as well, such as developing motivation, building self-confidence, and fostering relationships with professionals in a specific field. Research on some of these competitions has found that they have the potential to have significant positive impacts on participants' career interests. The use of educational badges is another approach used

successfully in some extracurricular contexts. Research findings on the effectiveness of educational badges have been mixed, depending on the pre-existing skills of the learner, the intrinsic value of the content of the badge, and the social context. One context that seems to be consistently successful at using badges is Scouting. Research has found positive results from the use of badges in both Girl Scout and Boy Scout organizations.

Cybersecurity-specific extracurricular activities have been studied to a much more limited degree. A few limited studies have found mostly positive evidence that cybersecurity competitions and other extracurricular activities can increase interest in cybersecurity subjects and careers. With over 14,000 participants in the 2016-2017 school year, CyberPatriot is by far the largest such program in the United States for middle and high school students. However, prior to the work in this thesis there had been no published peer-reviewed studies of its impact on the career interests and aspirations of its participants.

This thesis assesses the impact of the CyberPatriot program on the career interests of students by analyzing responses to recent surveys conducted by the competition organizers. The results show that interest in cybersecurity as an educational or career prospect increased meaningfully across multiple dimensions, such as perception of career tasks, interest and awareness, and view of self. The reliability of these self-reported perceptions is bolstered by comparing responses across surveys administered at different times. The findings of this research indicate that a significant majority of those reporting that they are very likely to choose a cybersecurity field are still planning to do so when asked again one year later.

The findings also indicate that the CyberPatriot competition is contributing positively to correct the gender imbalance in the cybersecurity workforce. Although a minority of participants in the program are female, it is more than twice the percentage of females in the overall cybersecurity workforce. Furthermore, despite female participants' lower perceptions of cybersecurity careers, they showed a greater increase overall in positive perceptions than their male counterparts, significantly narrowing the gap between male and female responses.

To gauge the impact of extracurricular cybersecurity activities and related computing outreach efforts specifically on developing the U.S. Air Force's enlisted cyber workforce, a survey of enlisted Airmen is designed. The survey addresses two basic research questions: first, assessing the impact of computing-related educational and outreach activities on the career decisions of enlisted Airmen; second, measuring the impact of computing-related educational and outreach activities on the academic performance of enlisted Airmen in cyber tech schools. Because of the length of the approval process the results of the survey are not available at the time of this writing. However, the Commander of the Air Force Research Laboratory, which oversees the Air Force STEM Outreach Program Office, is eager to receive the results as soon as they become available.

In reviewing available cybersecurity extracurricular activities, particularly competitions, for middle and high school students, it is observed that there is a distinct lack of options in the area of digital forensics. This thesis demonstrates the feasibility of developing new activities by designing and creating a flexible hands-on, scalable, low-

cost, introductory digital forensics activity appropriate for middle or high school students. The activity is in the form of a ZIP file with the contents of a suspected thief's `Documents` folder. Students analyze the forensic evidence in the folders and files, reconstructing user activity to answer some basic questions.

Like competitions, badges are also gaining interest as a potential approach to gamification in extracurricular and non-traditional STEM education. The Boy Scouts of America is one of the largest and most prominent youth organizations and it has a well-established and successful badge program, however it does not currently have a badge for cybersecurity. This thesis proposes a Cybersecurity merit badge for the BSA. Modeled on other successful technology-related merit badges the BSA already offers, a set of proposed requirements constructed by a panel of experts has been sent to the BSA for consideration.

5.2 Limitations and Future Work

5.2.1 CyberPatriot Survey Analysis

Due to the retrospective nature of the "before" questions on the CyberPatriot participant surveys, it is impossible to know with certainty how much a participant's opinions really changed over the course of one or more competition seasons. Reliability is high for all but one question, but the retrospective nature of the questions still introduces error. Additionally, the methods used for linking individual participants across multiple surveys are not as effective as a unique participant identifier, and reduce the number of responses that can be linked. Because the survey questions were

originally designed for program evaluation purposes rather than scientific research, they are not as granular or methodical as those used in typical educational research. For instance, although respondents were prompted with multiple-choice selections similar to Likert-type questions, they were not true Likert tests with the formal parameters and procedures that normally entails. Finally, due to the self-selected nature of competition participants and lack of control group, this study cannot make any claims regarding causation. While the results show that participants reported an increase in their positive perceptions toward cybersecurity, it is not known how much these perceptions may have changed on their own, with or without the influence of the CyberPatriot program. Future research should attempt to answer this question by identifying a control group of students with similar interest levels but who do not participate in the competition.

Additional work is required to determine what elements of the program contribute most significantly to student impact, and what can be done to attract more students, especially females, to participate. The 2017 survey adds several questions about students' reasons for participating, elements of the competition that were most impactful, how much time they spent training, etc. Analysis of the results of those questions should continue. Further analysis is also required to quantify impacts on other underrepresented groups, including racial minorities, low-income students, and rural populations. Additionally, a true longitudinal study is needed to measure the long-term impact on participants, including actual career outcomes.

5.2.2 Survey of Enlisted Airmen

The survey presented in this thesis is a complete design, but the survey needs to be approved by the Institutional Review Board and the Air Force Survey Control Office before it can be actually conducted. Once it has been approved, the survey should be conducted, and results analyzed. The results should be sent to the Air Force STEM Outreach Office, AFRL/EN, at Wright-Patterson Air Force Base, Ohio.

5.2.3 Digital Forensics Educational Activity

While the activity can be evaluated objectively against the four design parameters, the learning objectives require further study. Future work should actually conduct this activity with a group of participants in the target audience (6th-12th grade students) and measure learning outcomes. If the activity can be demonstrated to be effective, it should be submitted to the CyberPatriot Program Office as a model for digital forensics challenges that can be incorporated into future iterations of the cyber defense competition.

5.2.4 Cybersecurity Merit Badge

The proposal for a Cybersecurity merit badge, including draft requirements for earning the badge, is complete and has been sent to the BSA national staff for their consideration. However, much work remains to be done to bring this proposal to fruition. Initial review of the proposal takes about four months, but development of the full curriculum and everything else that goes into launching the new badge can take up to two years. Initial communications with the BSA national staff indicate that they are not considering any new merit badges at this time. The team should continue to work

with the BSA staff to convince them that when they are ready to start creating new badges again, Cybersecurity should be at the top of the list. More cybersecurity experts and industry leaders can be recruited to support the effort, such as advocating for the badge with the BSA. Additionally, a corporate sponsor will need to be solicited to assist with the costs of developing and launching the new badge.

While the BSA national staff considers the proposal, the team can continue to develop the program. Additional focus groups should be held to get feedback from the target audience. A pilot program can be run with local BSA councils to test and refine the draft requirements, and to provide evidence to BSA leadership that a Cybersecurity program for Boy Scouts can be successful.

Appendix A: IRB Exemption Request Memo

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY (AETC)

6 July 2017

MEMORANDUM FOR AFIT EXEMPT DETERMINATION OFFICIAL

FROM: AFIT/ENG
2950 Hobson Way
Wright Patterson AFB OH 45433-7765

SUBJECT: Request for exemption from human experimentation requirements (32 CFR 219, DoDD 3216.2 and AFI 40-402) for CyberPatriot existing survey data analysis

1. Our research goal is to understand the impact of the CyberPatriot national youth cyber defense competition on young people's interests in cybersecurity, computing, and STEM careers. To do this, we will analyze existing data from five previously completed surveys by the CyberPatriot Program Office, Air Force Association, the last of which concluded prior to 22 June 2017, and limited participant registration data collected from 2013 to 2016. The objectives are to answer the following questions, as measured by the previously conducted surveys: To what extent did the program influence participants' perceptions of cybersecurity and related careers? To what extent did the program influence participants' higher education and career choices? Are there significant differences in these outcomes between different genders, ethnicities, etc.? The results of this study will be submitted for publication/presentation at a relevant academic conference.

2. This request is based on the Code of Federal Regulations, title 32, part 219, section 101, paragraph (b)(2) Research activities that involve the use of educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview procedures, or observation of public behavior unless: (i) Information obtained is recorded in such a manner that human subjects can be identified, directly or through identifiers linked to the subjects; and (ii) Any disclosure of the human subjects' responses outside the research could reasonably place the subjects at risk of criminal or civil liability or be damaging to the subjects' financial standing, employability, or reputation.

3. The following information is provided to show cause for such an exemption:

a) Equipment and facilities: N/A

b) Subjects surveyed in the original data collection efforts from approximately August 2013 to June 2017. The last survey concluded prior to 22 June 2017.

- Source of subjects: Past participants in the CyberPatriot cyber defense competition, as recorded and retained by the CyberPatriot Program Office (approx. 30,000)
- Total number of subjects: varies by dataset, up to 17,756
- Inclusion/exclusion criteria: Individuals were sent an invitation to complete a survey if they had been a registered participant in a previous CyberPatriot competition. There was no exclusion criteria.
- Age range: 11-25

c) Timeframe: N/A – we are using data previously collected approximately August 2013 to June 2017. The final survey concluded prior to

d) Data collected: There are up to 9 sources of data (2 alumni surveys, 3 post-season surveys, and up to 4 years of registration questionnaires). Complete list of questions in the attachment. Data has been anonymized/de-identified by replacing potential identifiers, such as name and email address, with a computer-generated participant ID. The participant IDs were generated from the Hashed Message Authentication Code (HMAC) using SHA-256 and a randomly-generated 16-character key. The key will be retained by the data owners, and not under any circumstances shared with the researchers. It would be infeasible to identify participants based on either the participant IDs or on the remaining data.

i. Alumni Surveys (June-July 2014 and June 2016)
   - Demographic data: age, gender, ethnicity, ZIP code
   - Program participation: which seasons of CyberPatriot participated in, extent CyberPatriot impacted education and career goals
   - Academic status: yes/no completed high school, yes/no enrolled in higher education, category of degree field of study
   - Educational/career plans: plan to enroll in higher education or enter the workforce immediately, category of (planned) degree field of study
   - Employment status/plans: yes/no currently employed, category of field employed/hoping to be employed
   - Participant IDs

ii. Post-Season Surveys (May-June 2014, 2015, and 2017)
   - Demographic data: age, gender, ethnicity, city, state, ZIP code
   - Opinions about CyberPatriot program: level of cybersecurity knowledge before and after competition (5-pt scale, self-reported), level of cybersecurity career awareness before and after competition (5-pt scale, self-reported), likelihood to pursue STEM education/career (4-pt scale, self-reported), likelihood to pursue cybersecurity education/career (4-pt scale,

self-reported), perception of how welcoming cybersecurity is to women, perception of how engaging CyberPatriot is, perception of how fun CyberPatriot is

- Educational plans: graduation year, plan to enroll in higher education or enter the workforce immediately, college(s) planning to attend
- Participant IDs

iii. Additional data only on 2017 Post-Season Survey

- Opinions/interactions regarding CyberPatriot program: factors affecting decision to participate, factors of competition having greatest impact (open-ended), aspects of competition helping to learn (open-ended), rewards for participating, time spent on various training activities
- Team characteristics: gender makeup of team, gender of coach, gender of mentor(s)

iv. Registration Questionnaires (approx. August-December 2013, 2014, 2015, and 2016)

- Team number (correlated with school or organization)
- Demographic data: birth year, gender, race/ethnicity, city, state, ZIP code
- Education data: graduation year, GPA (optional, self-reported)
- Open-ended responses: favorite classes, interests
- Participant IDs

e) Risks to Subjects: The survey data being studied has been de-identified. There is no risk of disclosure because no individual data will be held.

f) Informed consent: N/A, pre-collected de-identified data

4. If you have any questions about this request, please contact Dr. Laurence Merkle (principal investigator) – Phone 937-255-6565, ext. 4526; E-mail – Laurence.Merkle@afit.edu.

Dr. Laurence Merkle
Principal Investigator

Attachment:
Survey questions

Attachment: Survey Questions

CyberPatriot Student Alumni Survey

1. In which season(s) of CyberPatriot did you compete? (Select all that apply).
   - CyberPatriot I (2008-2009)
   - CyberPatriot II (2009-2010)
   - CyberPatriot III (2010-2011)
   - CyberPatriot IV (2011-2012)
   - CyberPatriot V (2012-2013)
   - CyberPatriot VI (2013-2014)
   - CyberPatriot VII (2014-2015)
   - CyberPatriot VIII (2015-2016)
   - I will also compete in CyberPatriot IX (2016-2017)
2. What is your gender?
   - Male
   - Female
   - Prefer not to answer
3. What is your ethnicity? (Please select all that apply.)
   - Asian or Pacific Islander
   - American Indian or Alaskan Native
   - Black or African American
   - Hispanic or Latino
   - White
   - Prefer not to answer
4. What is your age?
5. Have you completed your high school diploma, GED, or equivalent home schooling?
   - Yes.
   - No, I am still enrolled in high school or an equivalent program.
6. Are you currently enrolled in a 2-year or 4-year institute of higher education?
   - Yes.
   - No, I entered the workforce after high school.
   - No, I have already obtained a higher education degree.
   - No (other)
7. In what field are you pursuing your higher education degree?
   - A cybersecurity field
   - A computer science field
   - Another STEM field
   - A non-STEM field
   - A career technical education field.
   - Undecided
8. Do you plan to attend an institute of higher education after you finish your high school or equivalent education?

- Yes, I plan to enroll in a 2-year program.
- Yes, I plan to enroll in a 4-year program.
- No, I will enter the workforce immediately.

9. In what field do you plan to pursue your higher education degree?
   - A cybersecurity field
   - A computer science field
   - Another STEM field
   - A non-STEM field
   - Undecided
10. Are you currently employed?
   - Yes (full time)
   - Yes (part time)
   - No
   - Prefer not to answer
11. In what type of organization do you work?
   - Public sector organization (i.e. federal or state government department, non-profit organization, school or university)
   - Private sector organization (i.e. for-profit company)
   - Military service.
   - Other
12. In what career field are you employed or hoping to be employed?
   - A cybersecurity field
   - A computer science field
   - Another STEM field
   - A non-STEM field
13. To what extent did you participation in CyberPatriot impact your education and career goals?
   - CyberPatriot had somewhat impacted on my goals.
   - CyberPatriot had a significant impact on my goals.
   - CyberPatriot did not impact my goals at all.
14. Please provide your address:
   - City/Town
   - State/Province
   - ZIP/Postal Code
   - Country

   The following fields have been replaced with participant IDs (based on SHA-256 HMAC):
   - *Name*
   - *Address*
   - *Email address*

Post-Season Competitor Survey

1. Gender
2. Ethnicity
3. Age
4. Thinking back to before you had ever heard of CyberPatriot, on a scale of 1 to 5, what was your knowledge of cybersecurity basic principles at the time?
   - 1. No knowledge of
   - 2. A little knowledge of
   - 3. Some knowledge of
   - 4. A lot of knowledge of
   - 5. An advanced understanding of
5. Thinking back to before you had ever heard of CyberPatriot, how likely did you think at the time that you were going to pursue education or a career in a STEM field?
   - Very unlikely
   - Somewhat unlikely
   - Somewhat likely
   - Very likely
6. Thinking back to before you had ever heard of CyberPatriot, on a scale of 1 to 5, what was your knowledge of possible cybersecurity careers at the time?
   - 1. I didn't know anything about cybersecurity career opportunities.
   - 2. I knew very little about cybersecurity career opportunities.
   - 3. I knew about some opportunities out there.
   - 4. I knew a lot about cybersecurity career opportunities.
   - 5. I knew a lot about cybersecurity career opportunities, as well as how to pursue them.
7. Thinking back to before you had ever heard of CyberPatriot, on a scale of 1 to 5, how cool did you think it would be to work in cybersecurity?
   - 1. I thought it would be boring. I had no interest in a career in cybersecurity.
   - 2. I was not very interested in a career in cybersecurity.
   - 3. I thought a career in cybersecurity would be OK.
   - 4. I was really interested in pursuing a career in cybersecurity.
   - 5. I was already determined to pursue a career in cybersecurity. I thought it would be very cool.
8. Thinking back to before you had ever heard of CyberPatriot, how likely did you think at the time that you were going to pursue education or a career in cybersecurity?
   - Very unlikely
   - Somewhat unlikely
   - Somewhat likely
   - Very likely
9. Thinking back to before you had ever heard of CyberPatriot, at the time, overall, how welcoming and accessible to females did you think a career in cybersecurity was?
   - 1. I did not think women were welcome at all in the cybersecurity field.
   - 2. I thought it was pretty difficult for women to enter the cybersecurity field.
   - 3. I thought women were neither especially welcome nor especially excluded from the cybersecurity field.

- 4. I thought it was pretty easy for women to enter the cybersecurity field.
- 5. I felt a career in cybersecurity was very accessible and welcome to women.

10. How would you rate your present knowledge of cybersecurity basic principles?
    - 1. No knowledge of
    - 2. A little knowledge of
    - 3. Some knowledge of
    - 4. A lot of knowledge of
    - 5. An advanced understanding of
11. How likely are you now to pursue education or a career in a STEM field?
    - Very unlikely
    - Somewhat unlikely
    - Somewhat likely
    - Very likely
12. On a scale of 1 to 5, what is your current knowledge of possible cybersecurity careers?
    - 1. I don't know anything about cybersecurity career opportunities.
    - 2. I know very little about cybersecurity career opportunities.
    - 3. I know about some opportunities out there.
    - 4. I know a lot about cybersecurity career opportunities.
    - 5. I know a lot about cybersecurity career opportunities, as well as how to pursue them.
13. On a scale of 1 to 5, how cool do you currently think it would be to work in cybersecurity?
    - 1. I think it would be boring. I have no interest in a career in cybersecurity.
    - 2. I am not very interested in a career in cybersecurity.
    - 3. I think a career in cybersecurity would be OK.
    - 4. I am really interested in pursuing a career in cybersecurity.
    - 5. I am already determined to pursue a career in cybersecurity. I think it would be very cool.
14. How likely are you now to pursue education or a career in cybersecurity?
    - Very unlikely
    - Somewhat unlikely
    - Somewhat likely
    - Very likely
15. How welcoming and accessible to females do you currently think a career in cybersecurity is?
    - 1. I do not think women are welcome at all in the cybersecurity field.
    - 2. I think it's pretty difficult for women to enter the cybersecurity field.
    - 3. I think women are neither especially welcome nor especially excluded from the cybersecurity field.
    - 4. I think it's was pretty easy for women to enter the cybersecurity field.
    - 5. I feel a career in cybersecurity is very accessible and welcome to women.
16. On a scale of 1-5, how engaging do you think CyberPatriot is? (Engaging meaning that a CyberPatriot participant doesn't just learn things, but gets to DO things.)

17. On a scale of 1-5, how fun do you think CyberPatriot is?
    - 1. CyberPatriot is not at all fun.
    - 2. CyberPatriot is pretty boring. I did not have much fun participating.
    - 3. CyberPatriot is about as fun as other extracurricular activities.
    - 4. CyberPatriot is very fun.
    - 5. Of all the extracurricular activities I do, CyberPatriot is the most fun.
18. In what year will you graduate high school?
19. Will you be attending an institution of higher education next year?
    - Yes, I will be attending a two-year college or junior college.
    - Yes, I will be attending a four-year university.
    - No, I will be joining the military out of high school.
    - No, I will be entering the workforce out of high school.
    - Other (Please Specify).
20. What is the name of the institution you will be attending? Or, if you are still deciding, please list your top three choices.
21. Please provide your address
    - City/Town
    - State/Province
    - ZIP/Postal Code
    - Country

    The following fields have been replaced with participant IDs (based on SHA-256 HMAC):
    - *Name*
    - *Address*
    - *Email address*

Additional questions only on 2017 Post-Season Competitor Survey

22. Thinking back to when you first joined a CyberPatriot team, what factors were most important to your decision to participate? (Select all that apply)
    - I was already interested in cybersecurity
    - I was already interested in computers in general
    - I wanted to learn more about careers related to computers or cybersecurity
    - A teacher recommended it
    - To do something fun with my friends
    - To be part of a team
    - For a class requirement or extra credit
    - For scholarship or internship opportunities
    - To boost my resume for college admission
    - I knew someone who had previously participated
    - I wanted to learn more about cybersecurity
    - I wanted to learn more about computers
    - Other (please specify)

23. What was the gender makeup of your team?
    - All male
    - 1 female
    - 2 or more females
    - All female
24. What was the gender of your coach?
    - Male
    - Female
25. What was the gender of your mentor(s)?
    - Male
    - Female
    - Both male and female
    - My team did not have a mentor
26. List up to three factors or elements of the competition that had the greatest impact on you? (open-ended response)
27. What aspects of the competition helped you learn the most? (open-ended response)
28. Check the three best rewards for participating in CyberPatriot
    - Working with my Coach
    - Working with my Mentor
    - Competing against other teams
    - Learning new things about computers
    - Learning about cybersecurity careers
    - Having fun
    - Preparing for my future
    - Winning awards
    - Pleasing my parents
    - Pleasing my Coach
    - Getting my name in a news story
    - Working with friends
    - Being on a team
29. During the school year, on average, about how many hours did you spend per week doing the following
    - Formal team training with a Coach or Mentor
    - Informal training with my teammates
    - Studying or practicing on my own
    - Other computer-related activities on my own

Registration Questionnaire

1. Team Number
2. Graduation Year
3. Birth Year

4. City, State, Country, ZIP Code
5. Current GPA
6. Favorite Classes
7. Interests
8. Gender
9. Race

The following fields have been replaced with participant IDs (based on SHA-256 HMAC):

- First Name, Last Name

- Email address

Appendix B: Approved IRB Exemption Memo

DEPARTMENT OF THE AIR FORCE
AIR FORCE INSTITUTE OF TECHNOLOGY
WRIGHT-PATTERSON AIR FORCE BASE OHIO

14 Jul 2017

MEMORANDUM FOR Dr. Laurence D. Merkle (AFIT/ENG)

FROM: Brett J. Borghetti, Ph.D.
AFIT IRB Exempt Determination Official
2950 Hobson Way
Wright-Patterson AFB, OH 45433-7765

SUBJECT: Approved exemption determination on exemption request from human experimentation requirements (32 CFR 219, DoDD 3216.2 and AFI 40-402) for "CyberPatriot existing survey data analysis", dated 6 Jul 2017.

1. Your request was for exemption based on the Code of Federal Regulations, title 32, part 219, section 101, paragraph (b) (2) Research activities that involve the use of educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview procedures, or observation of public behavior unless: (i) Information obtained is recorded in such a manner that human subjects can be identified, directly or through identifiers linked to the subjects; and (ii) Any disclosure of the human subjects' responses outside the research could reasonably place the subjects at risk of criminal or civil liability or be damaging to the subjects' financial standing, employability, or reputation.

2. Your study **qualifies for this exemption.** Specifically, another non-AFIT entity has collenced the survey data and the direct identifying information in these surveys have been removed by the data collector, and the data collector has replaced the participant identifying information with 16-character "Participant ID" numbers instead of direct identifiers. Furthermore, the AFIT researchers have agreed to not attempt to request the participant-to-ID key or in any other way attempt to identify the participants in the data. Finally, the questions asked in the surveys do not provide enough information to indirectly identify participants.

3. This determination pertains only to the Federal, Department of Defense, and Air Force regulations that govern the use of human subjects in research. This determination is only for the research outlined in the exemption request letter. If the research changes from what was described in the request letter, or the data received is determined to be different than described in the request letter (e.g. unexpected identifying information is discovered in the data), please cease research efforts immediately and contact me as soon as possible for determining course of action.

7/14/2017

X 

Signed by: BORGHETTI.BRETT.J.1009082820
BRETT J. BORGHETTI, Ph.D.
AFIT Exempt Determination Official

Appendix C: Questionnaire for Enlisted Airmen Survey

1. Please specify your AFSC: (dropdown box)
2. How many years have you been on active duty?
   - Less than 1 year
   - Between 1 and 2 years
   - Between 2 and 3 years
   - Between 3 and 4 years
   - More than 4 years (discontinue survey if selected)

For those that select a cyber-related AFSC (3D0X2, 3D0X3, 3D1X1, or 3D1X2):

3. Which of the following best describes how you felt about being assigned to this career field when you first enlisted?
   - Great match! It was one of my top job preferences.
   - Acceptable. It was on my list, though not my top choice.
   - Disappointed, but it's better than nothing.
   - Terrible. I did not want this career field at all.
   - Unsure/Didn't care
   - Other (please comment): _____

For those that select a non-cyber AFSC:

4. Which of the following best describes how you felt about being assigned to this career field when you first enlisted?
   - Great match! It was one of my top job preferences.

- I would have preferred a cyber-related career field (such as [. . .])

- I would have preferred some other, non-cyber career field

- Unsure/Didn't care

- Other (please comment): _____

In many schools, camps, and organizations, there are clubs and activities for learning about computers, such as programming, games, hardware, robotics, and more.

Some of these clubs and activities may meet only once, while others meet over the course of an entire year or longer. Some are activities within other clubs, such as Girl Scouts or Boy Scouts. Some meet as part of a class in school and others meet after school or during the summer or winter breaks, and even during special camps. Some use special software to introduce students to computer programming using tools like Scratch or Alice.

You may have participated in one or more of these activities in high school or even earlier. Think back for a moment and consider any of these types of activities that you may have participated in. this section asks you a few questions about these types of activities.

5. At some point in the past before entering the military, did you participate in an activity or activities to learn about computers, like programming, cybersecurity, game development, or robotics?

   Mark all that apply. If an activity you participated in is not listed, mark "Other" and

fill in the activity in the text box.

- Computer class in school (such as Computer Science, Programming, “Intro to Computing,” or something similar)
- Computer-related activities in a non-computer class (such as Hour of Code or other activities designed to teach you something about how computers work)
- CyberPatriot
- Robotics club or competition
- Scouting badges (for example, Digital Technology, Programming, or Robotics merit badges)
- School-based computer club
- Computer or programming camp (such as GenCyber, or some other computer-themed camp at a local college, school, or other place)
- Other (please specify): _____
- Other (please specify): _____
- I did not participate in any such activity
- I don’t recall
- Unsure (please comment): _____

For each of the activities marked in Q5:

6. To the best of your recollection, when did you participate in this activity (mark all that apply):
   - While in elementary school

- While in middle school or junior high school

- While in high school

- After high school (but before joining the military)

- Other/Unsure (please comment): _____

7. Please select the option that is most correct regarding this activity:

- This activity was part of a required class in school

- This activity was part of an elective (non-required) class in school

- This activity was required as part of an extracurricular activity I was already participating in

- This activity was a voluntary part of an extracurricular activity I was already participating in

- This activity was its own separate extracurricular activity that I voluntarily participated in

- I don't recall

- Other/unsure (please comment): _____

8. Please rate the following items as they apply to this activity, using the scale provided:

Scale: Strongly disagree—Disagree—Neither agree nor disagree—Agree—Strongly agree—Unsure/I do not recall

Question items:

- I enjoyed this activity

- I enjoyed learning about computers

- I was interested in computers before I participated in this activity

- I felt like I was a welcome part of the group participating in the activity

- Participating in this activity increased my interest in computers

9. How did participating in this activity affect your decision to enlist in the Air Force?

- Strongly affected my decision to enlist in the Air Force

- Somewhat affected my decision to enlist in the Air Force

- Did not affect my decision to enlist in the Air Force

- I am unsure what effect, if any, this activity had on my choice to enlist in the Air Force

10. How did participating in this activity affect your career field preferences when you enlisted in the Air Force?

- Affected my decision to prefer a cyber career field

- Affected my decision to prefer a non-cyber career field

- Did not affect my career field preferences

- I am unsure what effect, if any, this activity had on my career field preferences

11. Based on your experiences in your career field so far, please rate the following items as they apply to this activity, using the scale provided:

Scale: Strongly disagree—Disagree—Neither agree nor disagree—Agree—Strongly agree—Unsure/I do not recall

Question items:

- This activity gave me a realistic perspective on what it would be like to work in a computing field

- This activity helped prepare me for a job in my current career field

- I believe I performed better in tech school because of my participation in this activity

- I believe I perform better at my job because of my participation in this activity

12. Which of the following do you most closely identify with?

    - *List of ethnic/racial groupings*

13. Please specify your gender:

    - Male

    - Female

    - Other/Decline to specify

14. If you have any additional comments, please share them below:

    - *Text box*

Appendix D: IRB Protocol for Enlisted Airmen Survey

1. Principal Investigator

Dr. Laurence D. Merkle, Assistant Professor

Dept. of Electrical and Computer Engineering, Air Force Institute of Technology

AFIT/ENG

53636, x4526

laurence.merkle@afit.edu

2. Associate Investigators

Capt Michael H. Dunn, Master's Student

Dept. of Electrical and Computer Engineering, Air Force Institute of Technology

AFIT/ENG

53636, x4526

michael.dunn@afit.edu

3. Research Monitor

Name/Rank/Title, Organization/Office Symbol, Phone Number, Email address, contractor affiliation if applicable.

4. Facility/Contractor

4.1. Sponsor:

4.2. Funding Source and Funding Amount:

4.3. Contract #/CRADA #/Cooperative Agreement #:

4.4. Activity location(s) (where activity will be conducted):

5. Conflicts of Interest

None

6. Background Information and Scientific Rationale

Recent work suggests extracurricular academic activities, such as academic competitions, can be effective at stimulating students' interest in specific career fields, particularly in the sciences, and can have significant impact on their educational and career choices. In a study of past National Ocean Sciences Bowl participants, 41% said participation influenced their career choice and 39% said it influenced their college major choice [2].

Academic competitions can also help launch talented students into highly successful careers. A study of past academic Olympiad winners found they significantly outperformed their peers in various measures, including doctorates earned and number of publications. A significant majority of both participants and their parents agreed that the Olympiad programs helped develop their talent and fostered their future accomplishments [3].

However, little is known about the impact of computing and cybersecurity activities as a means of attracting young people to these fields. One study of past participants in Cybersecurity Awareness Week evaluated personality profiles of

competitors, and found that the high levels of "perceived self-efficacy in cybersecurity tasks, rational decision-making style, and investigative interests" correlated with a higher likelihood of participants later choosing a cybersecurity career [1]. An upcoming paper by Dunn and Merkle studies the results of a post-competition survey from CyberPatriot, the largest youth cybersecurity education program in the United States. Participants indicated a definite increase in their interest in cybersecurity careers, as measured by multiple questions related to career interest [5].

A relatively large-scale survey by McGill, Decker, and Settle [6] studied the long-term effects of pre-college computing outreach activities, especially in relation to students' choice of major (specifically, computing vs. non-computing). These researchers found that there is a strong link between participating in computing educational activities and later choosing to major in a computing field. This correlation is stronger when participation is voluntary than when it is required, and stronger for males than for females [6].

[Citations are listed in section 16 below.]

7. Study Objective(s) and Purpose

7.1. Purpose: To gain insight into the effectiveness of computing outreach activities at fostering the Air Force cyber workforce and guide decisions about AF STEM outreach programs

7.2. Primary Objective: Assess the impact of computing-related educational and outreach activities on the career decisions of enlisted Airmen

7.3. Secondary Objective(s): Assess the impact of computing-related educational and outreach activities on the academic performance of enlisted Airmen in cyber tech schools

8. Study Design

8.1. Description of Study Design:

- Participant list for survey pulled as random sample from the target population by the Air Force Survey Office according to inclusion criteria (section 9.1).
- Invitation to take survey sent out using approved survey platform.
- Survey will be open for two weeks, with a reminder sent out after about a week.
- Those who choose to participate will click on link in email, agree to the informed consent statement, and fill out the questionnaire. The email address of the respondent will be automatically recorded.
- Survey responses will be matched with tech school grade data via name/email address.
- If anyone declines to agree to the informed consent statement, or fails to complete the survey, their (partial) response will be discarded.

9. Subject Selection

9.1. Inclusion Criteria:

A subject who has met all of the following criteria is eligible for participation in the study:

- Enlisted
- Less than 4 years time-in-service (i.e. first enlistment, non-prior service)
- Under 24 years old

9.2. Exclusion Criteria:

A subject who meets any of the following criteria is disqualified from participation in the study:

9.3. Recruitment Plan

The Air Force Survey Office will provide a list of contacts based on the criteria in section 9.1 above. The investigator will send an email to the provided contacts with an invitation to take the survey.

Text of the email:

The Air Force Institute of Technology, in partnership with the Air Force Research Laboratory, is investigating the impact of computer-related educational activities on the career pathways of future Airmen. We ask that you take just a few minutes to fill out a short survey on your experiences. This survey should take about 5-10 minutes.

9.4. Consent Plan

The first page of the survey will be the informed consent document (ICD). Participants will be given the option to agree or not. The survey will only continue if the participant agrees.

9.5. Compensation

There are no plans to provide compensation for participation in the research.

10. Experimental Plan

10.1. Equipment:

No special equipment will be required. The study will be conducted solely using standard office computers.

11. Risk/Benefit Analysis

11.1. Benefits:

- The benefit to society is a greater understanding of the effect of participation in a computing or cyber-related educational activity on an individual's choice to enlist in the Air Force and their job preferences. This will allow better targeting of Air Force and DoD resources (funding, volunteer man-hours, etc.) toward the activities that are most beneficial for meeting Air Force and DoD cyber workforce needs.
- There is no benefit to the subjects.

11.2. Risks:

- Risk: Participants may feel uncomfortable with researchers having access to data about their performance in tech school.

- To minimize: The consent document that the participants read will make it very clear that tech school performance data will be anonymized and the researchers will not keep copies of identifiable training or performance data. Additionally, the informed consent document will make it clear that participation in the survey is voluntary and that an individual can exit the survey at any time prior to completion and their tech school records will not be accessed.
- Risk: If participant grade data were to leak and be obtained by participants' coworkers who otherwise would not have had access to that data, it could affect those coworkers' impressions of the participants and their knowledge, skills, and abilities.
- To minimize: Survey and grade data will be protected according to procedures in section 14 below.

12. Statistical Consideration and Plan

12.1. Sample Size (Power analysis):

The power analysis was conducted according to Jacob Cohen, *Statistical Power Analysis for the Behavioral Sciences* (2nd ed.), 1988 [4].

The sample size for **cyber Airmen** is based on a **t-test** measuring the difference in mean tech school GPA between those who had participated in a computing extracurricular activity (population 1) and those that had not (population 2).

Hypothesis tests:

H_0: $m_1 - m_2 = 0$

H_A: $m_1 - m_2 > 0$ (one-tailed test)

Parameters:

$\alpha = .05$ (one-tailed)

$\beta = .20$ (power = .80)

d = .20 ("small" effect size)

The sample size table in Cohen (pg. 54) gives a sample size required of n = 310.

Based on a previous study by McGill et al. [5], we are estimating that about 1/3 of cyber Airmen will have participated in a qualifying extracurricular activity. Thus the total number of responses needed to get at least 310 in population 1 is three times that: 930. With a predicted response rate of 20% or less, the number of surveys to be sent out should no fewer than **4,650**.

The sample size for **non-cyber Airmen** is based on a difference of proportions test, measuring the difference in proportion of respondents who chose or preferred a cyber AFSC, between those who had participated in a computing extracurricular activity (population 1) and those that had not (population 2).

Hypothesis tests:

H_0: $p_1 - p_2 = 0$

H_A: $p_1 - p_2 > 0$ (one-tailed test)

Parameters:

$\alpha = .05$ (one-tailed)

$\beta = .20$ (power = .80)

h = .20 ("small" effect size)

The sample size table in Cohen (pg. 205) gives a sample size required of n = 309.

Based on a previous study by McGill et al. [5], we are estimating that about 15% of non-cyber Airmen will have participated in a qualifying extracurricular activity. Thus the total number of responses needed to get at least 309 in population 1 is 6.67 times that: 2,060. With a predicted response rate of 20% or less, the number of surveys to be sent out should no fewer than **10,300**.

13. Safety Monitoring and Reporting

Not applicable

14. Confidentiality

Initial survey response data will be identified by the official email address to which the survey was sent. Once retrieved, the survey data will be kept in the investigators' secured accounts on the AFIT internal network, accessible only to the investigators. Tech school grade data will be sent securely by AETC/A3PS, either via encrypted email or AMRDEC SAFE. This data will contain only names and grades; no other personal information (e.g. SSN) will be sent. Once the survey response data and the grade data are correlated, the associated personal information will be deleted. The investigators will not store any personal information past the initial downloading and correlation steps.

15. Data Management/ Data Sharing Plan

A DVD with the correlated, de-identified dataset will be shared with the AF STEM Outreach office in AFRL to retain for future use at their discretion.

16. References

[1] Bashir, M. et al. 2016. Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool. Computers & Security. 65, (Mar. 2016), 153–165.

[2] Bishop, K. and Walters, H. 2007. The National Ocean Sciences Bowl: Extending the Reach of a High School Academic Competition to College, Careers, and a

Lifelong Commitment to Science. American Secondary Education. 35, 3 (2007), 63–76.

[3] Campbell, J.R. and Walberg, H.J. 2010. Olympiad Studies: Competitions Provide Alternatives to Developing Talents That Serve National Interests. Roeper Review. 33, 1 (Dec. 2010), 8–17.

[4] Cohen, J. (1988). Statistical Power Analysis for the Behavioral Sciences (2nd ed.). Hillsdale, NJ: Lawrence Erlbaum Associates.

[5] Dunn, Michael H. and Merkle, Laurence D. Assessing the Impact of a National Cybersecurity Competition on Students' Career Interests. SIGCSE '18.

[6] McGill, M.M. et al. 2016. Undergraduate Students' Perceptions of the Impact of Pre-College Computing Activities on Choices of Major. ACM Transactions on Computing Education (TOCE). 16, 4 (Jun. 2016), Article 15.

17. Attachments

- Informed Consent Document.
- Current Curriculum Vitae of investigators.
- Survey questions.

Consent to Participate in Research

For

Survey on Impact of Pre-Service Computing Activities

Principal Investigator: Dr. Laurence D. Merkle, Assistant Professor

Dept. of Electrical and Computer Engineering, Air Force Institute of Technology

AFIT/ENG

53636, x4526

laurence.merkle@afit.edu

1. INTRODUCTION

The Air Force Institute of Technology, in partnership with the Air Force Research Laboratory, is investigating the impact of computer-related educational activities on the career pathways of future Airmen. We ask that you take just a few minutes to fill out a short survey on your experiences. This survey should take no more than X minutes.

2. PURPOSE

The purpose of this study is to assess the impact of computer-related educational and outreach activities on the career decisions and tech school performance of enlisted Airmen.

3. PROCEDURES

If you decide to take part in this study, you will be asked to complete a brief questionnaire regarding computer-related education and extracurricular activities you may have participated in prior to entering the military. If you are in a cyber-related AFSC (defined as 3D0X2, 3D0X3, 3D1X1, and 3D1X2), your survey responses will be correlated with your tech school academic scores.

The survey should take approximately 5 to 10 minutes, depending on your specific responses.

4. POTENTIAL RISKS and/or DISCOMFORTS

Your responses to this survey, and any other data collected about you in the process, will be de-identified before being used in the study. If you are in a cyber-related AFSC (defined as 3D0X2, 3D0X3, 3D1X1, and 3D1X2), your survey responses will be correlated with your tech school academic scores from official records, which will also be de-identified before being used. All personal information will be protected by approved security measures, and will only ever be seen by the researchers. However, exposure of this data before it has been de-identified is always a risk. If your survey responses and/or grade data were to leak before being de-identified, and it were to be obtained by your coworkers who otherwise would not have had access to that data, it could affect those coworkers' impressions of you and your knowledge, skills, and abilities.

5. BENEFITS

If you agree to take part in this research study there may be no direct benefit to you. However, the information learned from this study will help the Air Force better allocate resources to improve recruitment of new Airmen with important cyber talents and interests.

6. COSTS

There will be no cost to you for participation in this study.

7. ALTERNATIVES TO PARTICIPATION

Your alternative is to choose not to participate in this research study. Refusal to participate will involve no penalty or loss of benefits to which you are otherwise entitled. You may discontinue participation at any time without penalty or loss of benefits to which you are otherwise entitled. To discontinue, simply close your browser window at any time prior to completing the survey.

8. YOUR PARTICIPATION IS VOLUNTARY

The decision to participate in this research is voluntary on your part. No one may coerce or intimidate you into participating in this program. Participate only if you want to. Capt Dunn, or an associate, should adequately answer all questions you have about this study, your participation and the procedures

involved. If you have any further questions, Capt Dunn can be reached at michael.dunn@afit.edu. Capt Dunn, or an associate will be available to answer any questions concerning procedures throughout this study. You may withdraw from this research study at any time without penalty.

If you have any questions or concerns about your participation in this study or your rights as a research subject, please contact the AFRL IRB at (937) 904-8100 or AFRL.IR.ProtocolManagement@us.af.mil.

If you are removed from the study, the study investigator will contact you to answer any questions you may have.

9. COMPENSATION

There are no plans to provide compensation for participation in this research.

10. RESEARCH-RELATED INJURY

Your entitlements to medical and dental care and/or compensation in the event of injury are governed by federal laws and regulations. If you desire further information you may contact the legal office (711 HPW/JA, 986--5666 at Wright-Patterson AFB). In the event of a research related injury, you may contact the

Principal Investigator, Dr. Laurence Merkle, of this research study at (937) 255-3636 x4526.

11. CONFIDENTIALITY

Records of your participation in this study may only be disclosed according to federal law, including the Federal Privacy Act, 5 U.S.C. 552a, and its implementing regulations and the Health Insurance Portability and Accountability Act (HIPAA), and its implementing regulations, when applicable, and the Freedom of Information Act, 5 U.S.C. Sec 552, and its implementing regulations when applicable.

Your personal information will be stored in a locked cabinet in an office that is locked when not occupied. Electronic files containing your personal information will be password protected and stored only on a secure server. Organizations that may look at and/or copy your medical and/or records for research oversight, quality assurance and data analysis include:

- **the researchers named above,**
- **the study's Research Monitor or Consultant,**
- **the AFRL Wright Site IRB,**
- **the Air Force Surgeon General's Research Compliance office,**
- **the Director of Defense Research and Engineering office or**

- **other IRB(s) involved in the review and approval of this protocol.**
- *Add any others that may be granted access*

You will be identified by a code, and personal information from your records will not be released without your written permission unless required for military personnel. Information related to health and fitness for duty may be required to be reported to appropriate medical or command authorities. Complete confidentiality for military members cannot be promised. You will not be identified in any publication or in the sharing of your data about this study.

After the study is completed, the data may be placed in a central storage location. The purpose is to make study data available to other researchers. The data will be completely de-identified. These data will not include your name or other information that can identify you.

Complete confidentiality cannot be promised, in particular for military personnel, whose health or fitness for duty information may be required to be reported to appropriate medical or command authorities. If such information is to be reported, you will be informed of what is being reported and the reason for the report.

12. PRIVACY ACT

Personal Identifiable Information to be obtained for this study includes first and last name, gender, racial demographic, and tech school GPA (if you are in a cyber AFSC).

13. STUDY PARTICIPATION AGREEMENT/CONSENT

Taking part in this research study is completely voluntary. By clicking "I agree" below, you indicate that:

- **You agree to be in this study**
- **You have read and understand the information you have been given**
- **You were given the opportunity to ask questions about the study and all of your questions have been answered to your satisfaction**
- **You understand that signing this consent does not take away any of your legal rights**

You may print a copy of this consent agreement for your records

Appendix E: Example Prompt, Questions, and Answers for Digital Forensics Educational Activity

Prompt

August 23, 2017

World-infamous supercriminal Carla Sanfrancisco just stole all the deep dish pizza in Chicago! ACNE detectives lost her trail somewhere in the Windy City, but they managed to nab her laptop. ACNE has extracted Carla's user profile folder (`C:\Users\Carla Sanfrancisco`) and have sent it to you for analysis. Can you uncover the clues she left behind and figure out where she's headed next? And what is her next target?

Note: Carla's laptop was running Windows 7 with Internet Explorer 11

Questions and Answers

Q: What date and time was the file `email.txt` last modified?

A: August 22, 2017, 9:20 PM

Q: What is the title of the book Carla downloaded from Gutenberg.org?

A: Hans Andersen's Fairy Tales, Second Series

Q: What time did Carla download the book from Project Gutenberg?

A: 7:24 PM

Q: What cities did Carla look up?

A: Sydney (Australia), Milan (Italy), Dublin (Ireland), and Copenhagen (Denmark)

Q: What city is Carla headed to?

A: Copenhagen

Q: What date did Carla book her flight?

A: August 21, 2017

Q: What airport is Carla flying out of?

A: Chicago O'Hare International Airport (ORD)

Q: What airline is she flying?

A: United Airlines

Q: What date will she arrive?

A: August 24, 2017

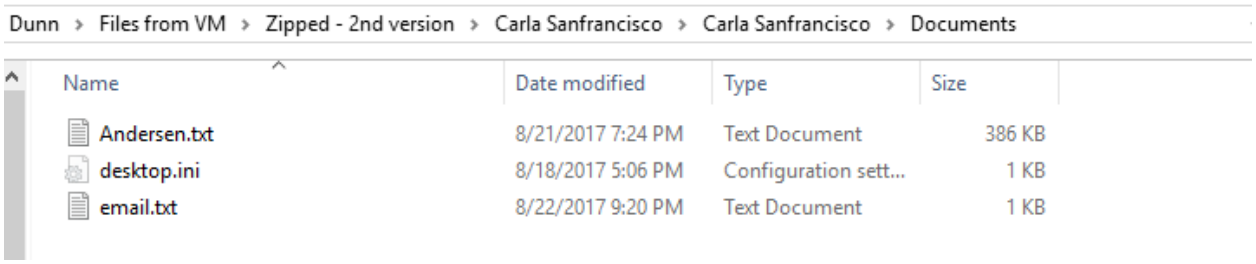
Q: What is Carla's target?

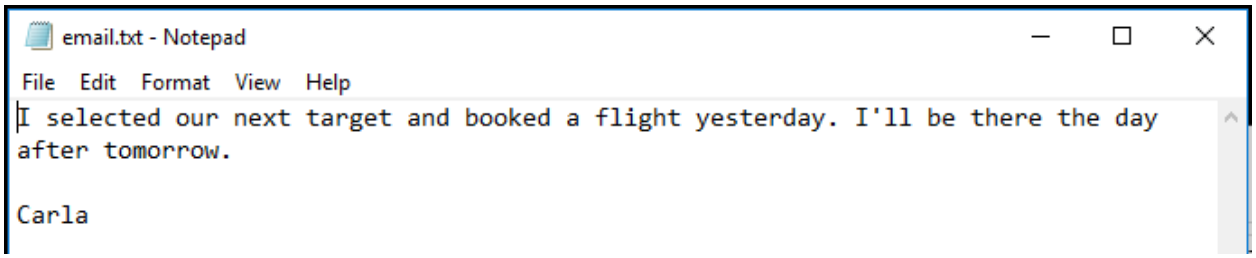
A: The Little Mermaid statue in Copenhagen

Appendix F: Detailed Description of Evidence for Digital Forensics Education Activity

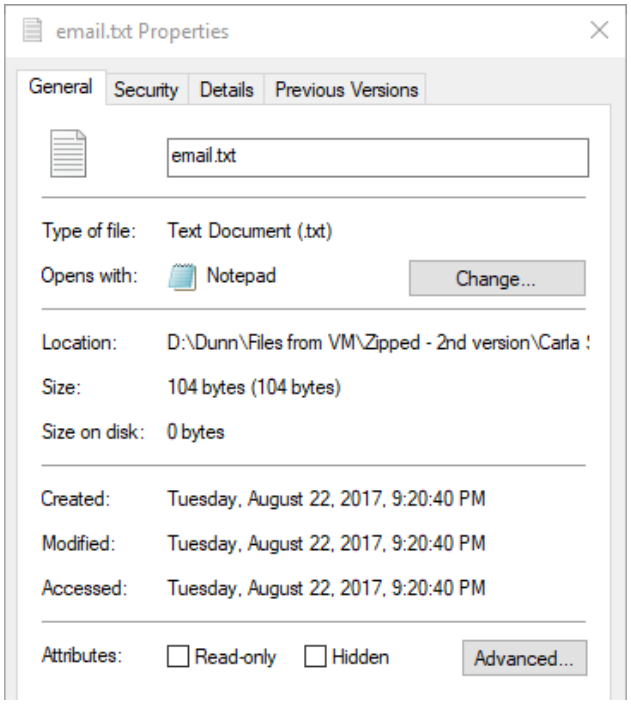
Email text

File: `\Documents\email.txt`



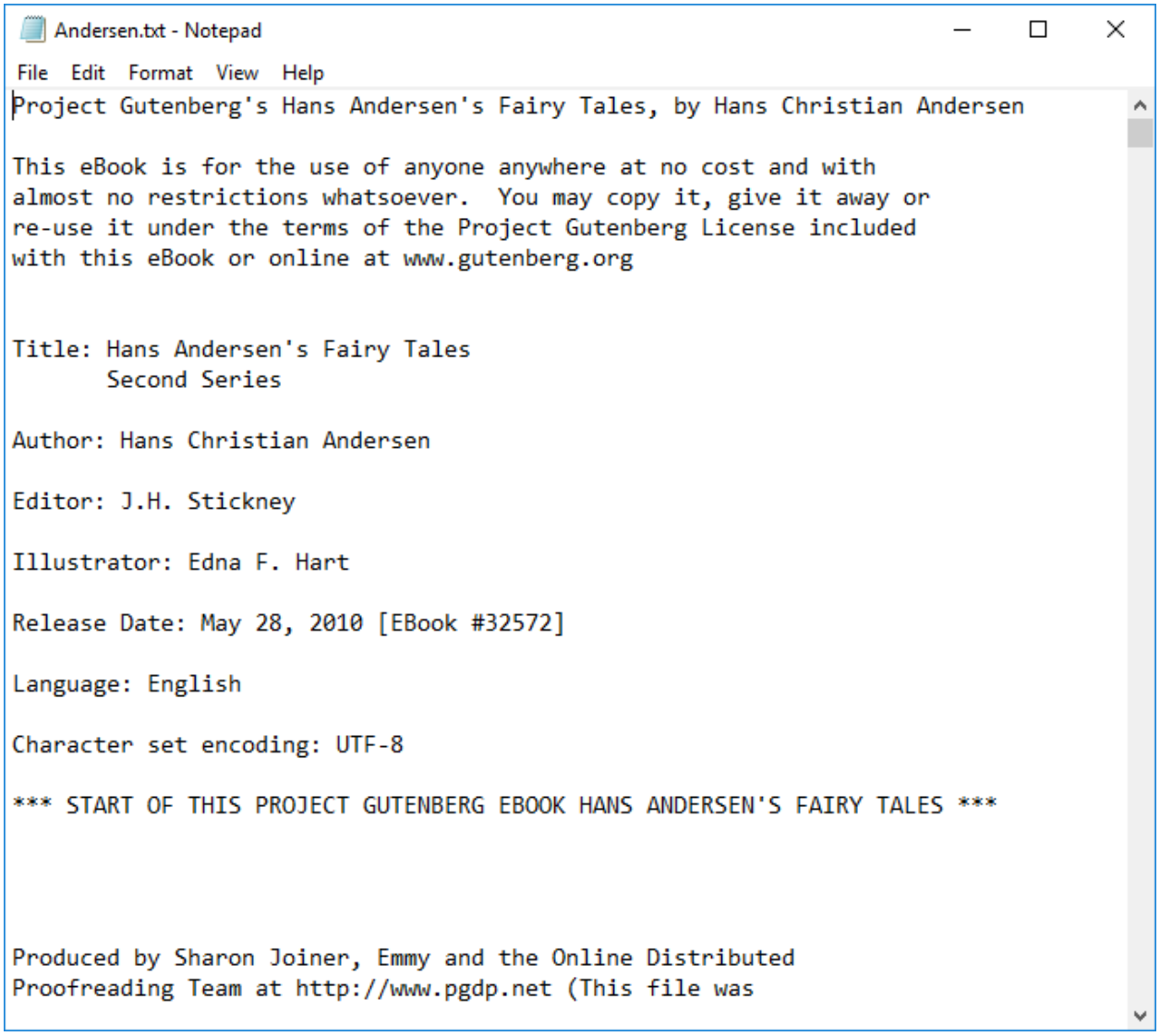


Based on file modified time, Carla booked her flight on August 21, and will arrive at her destination on August 24.

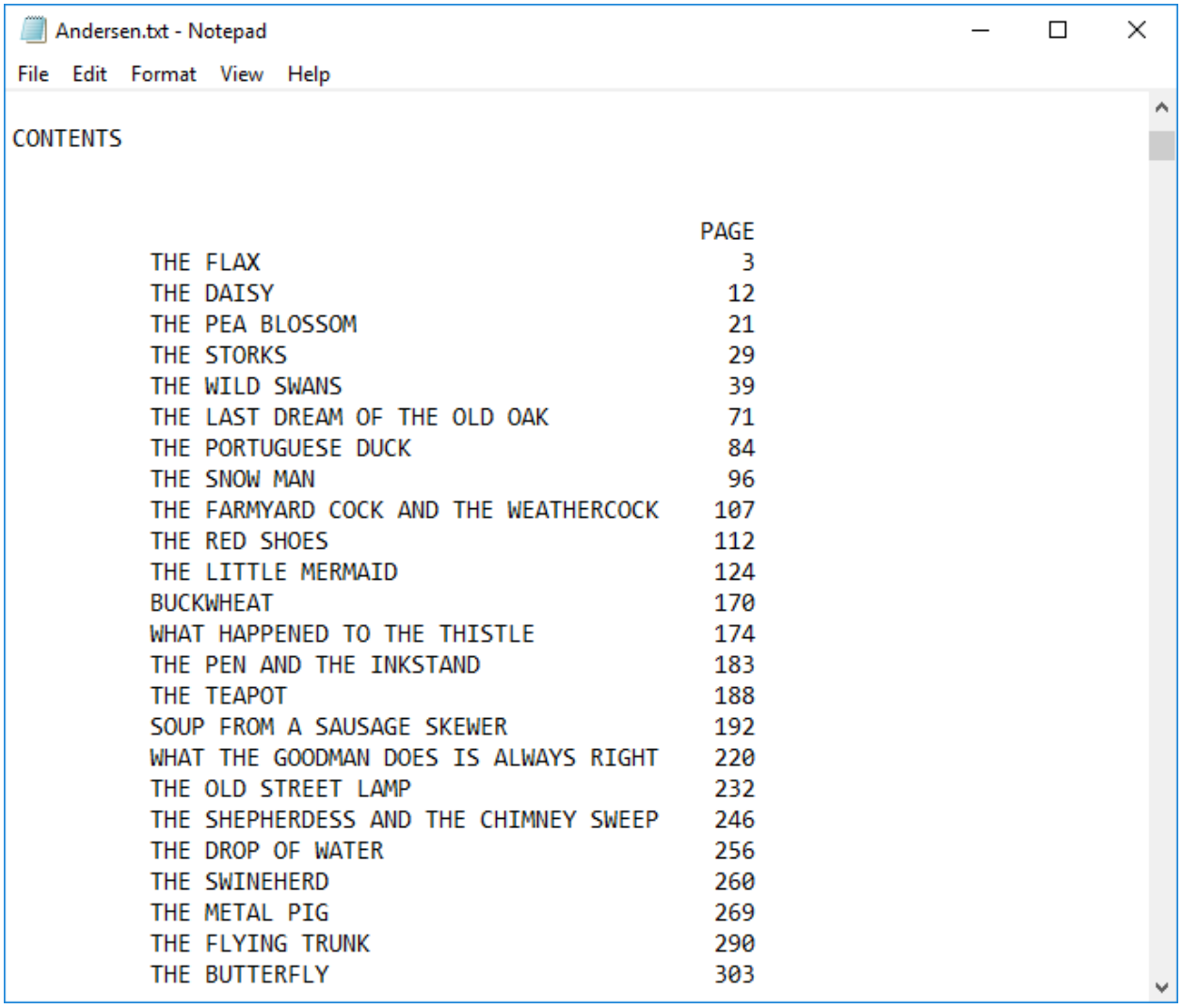


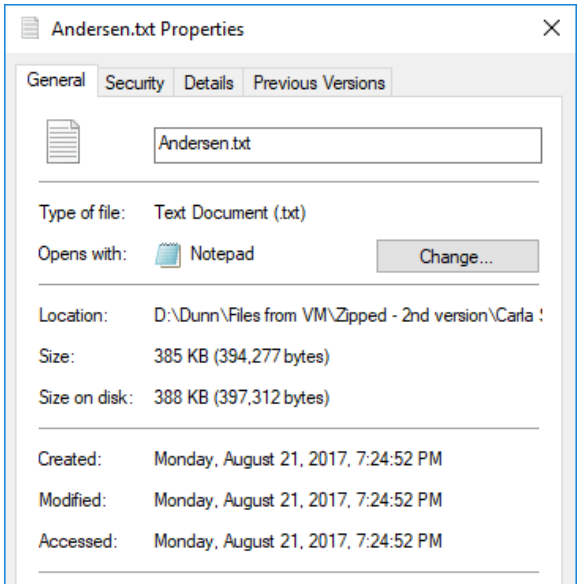
Andersen's Fairy Tales text

File: `\Documents\Andersen.txt`

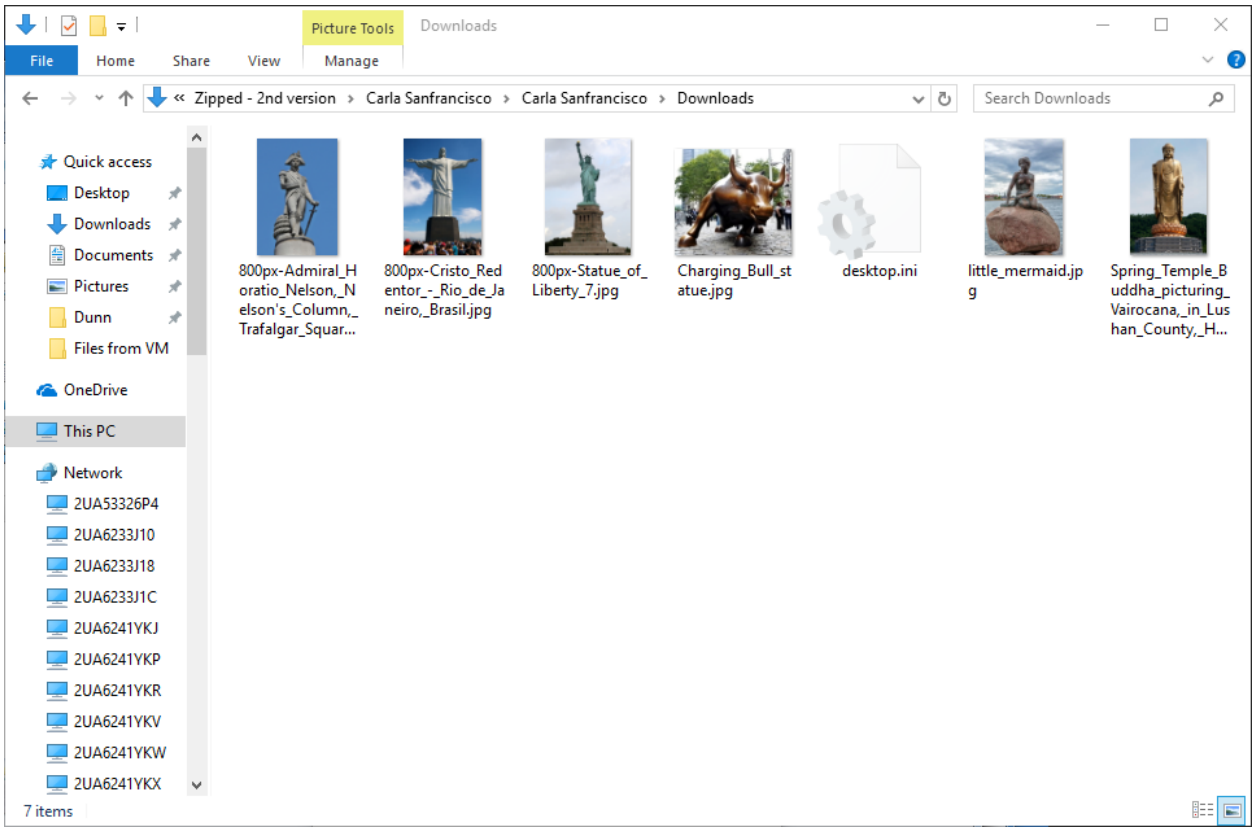

Andersen.txt - Notepad
File Edit Format View Help
Project Gutenberg's Hans Andersen's Fairy Tales, by Hans Christian Andersen
This eBook is for the use of anyone anywhere at no cost and with
almost no restrictions whatsoever. You may copy it, give it away or
re-use it under the terms of the Project Gutenberg License included
with this eBook or online at www.gutenberg.org
Title: Hans Andersen's Fairy Tales
Second Series
Author: Hans Christian Andersen
Editor: J.H. Stickney
Illustrator: Edna F. Hart
Release Date: May 28, 2010 [EBook #32572]
Language: English
Character set encoding: UTF-8
*** START OF THIS PROJECT GUTENBERG EBOOK HANS ANDERSEN'S FAIRY TALES ***
Produced by Sharon Joiner, Emmy and the Online Distributed
Proofreading Team at http://www.pgdp.net (This file was

Book contains the story “The Little Mermaid”

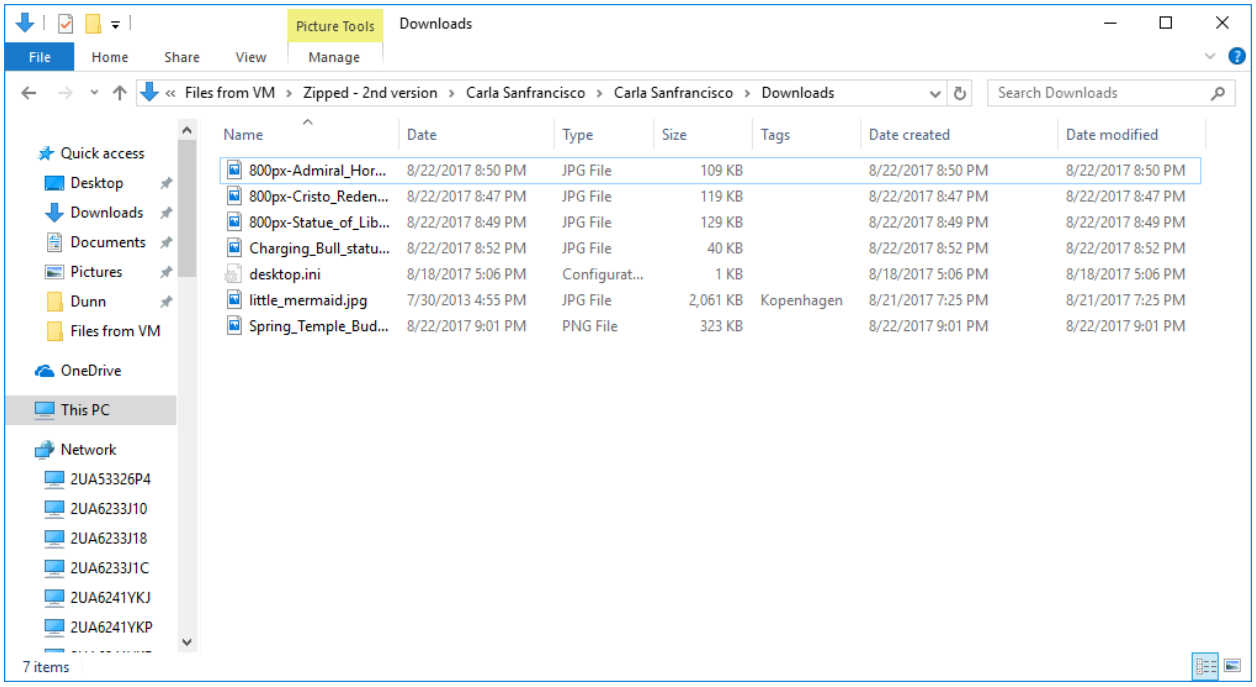




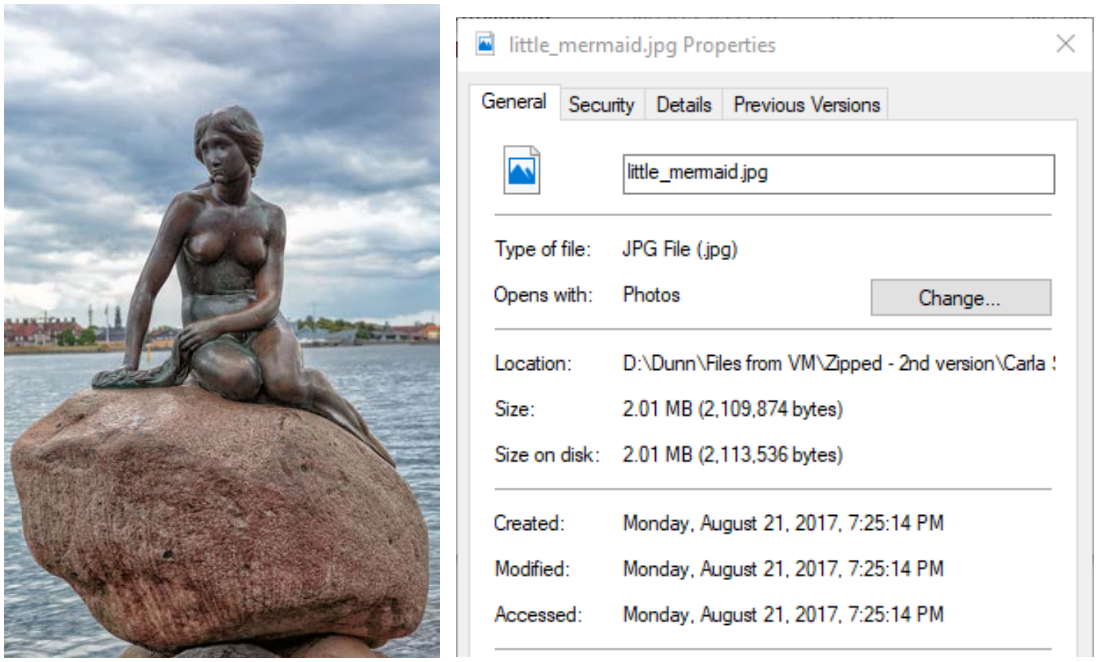
Photos in `Downloads` folder

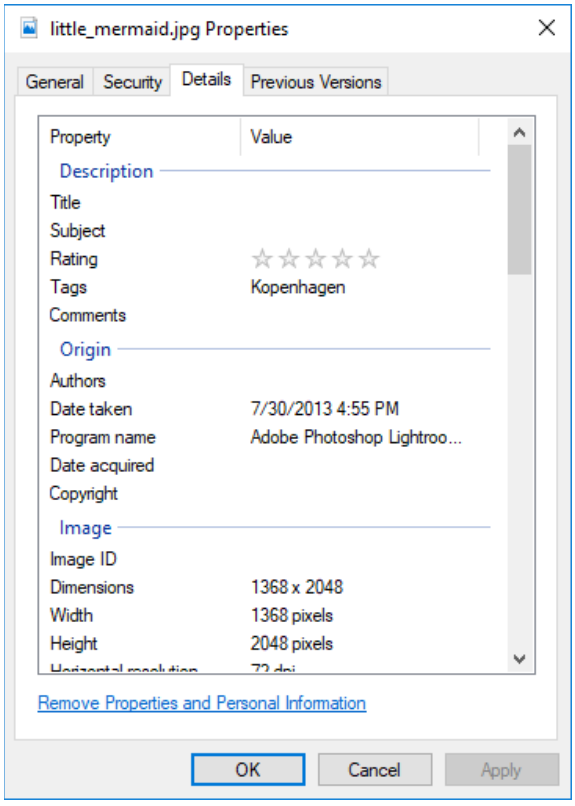


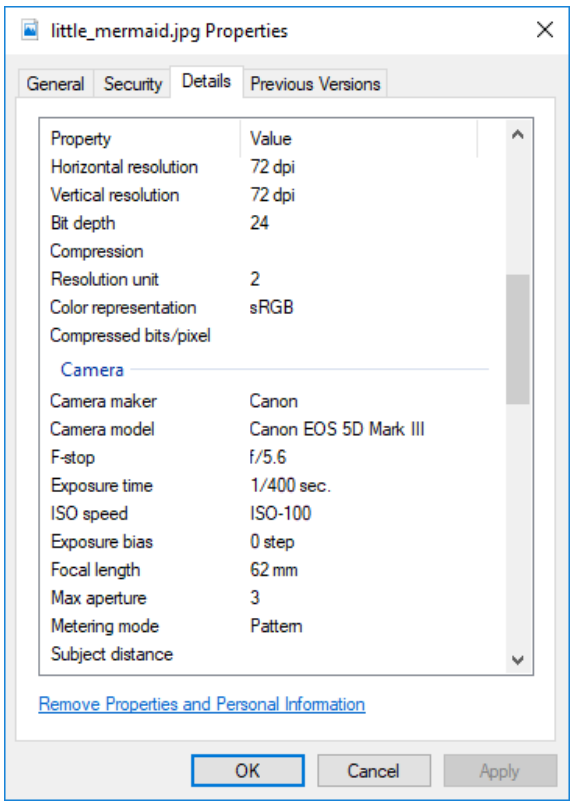
Set view to Details; right-click properties bar, select Date created and Date modified



Only one file (`little_mermaid.jpg`) was created August 21, the day Carla said she selected her next target. The rest were created (downloaded, presumably) August 22 -- *after* Carla's flight was already booked.







From file properties, it can be seen that the file is a photograph, and is tagged

“Kopenhagen”

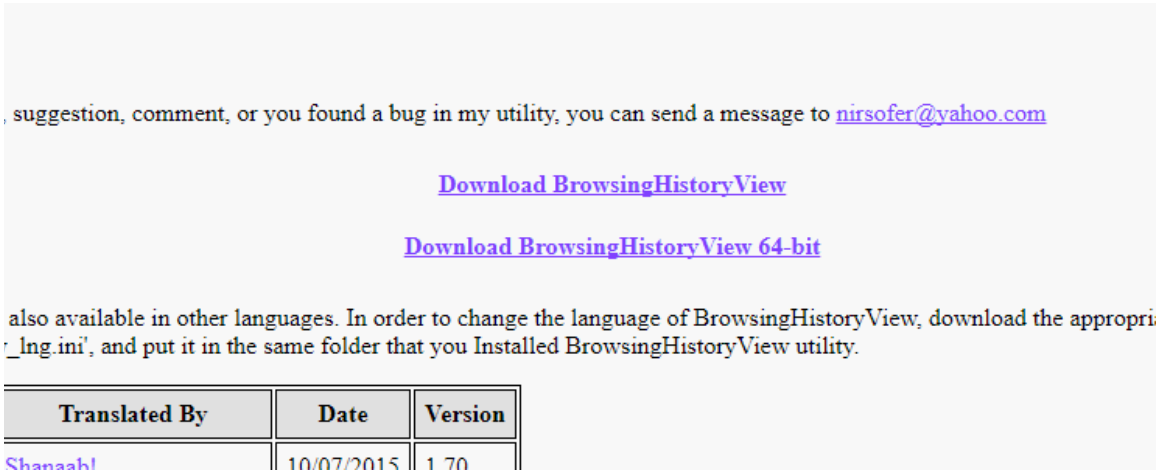
Browser history

Location: `\AppData\Local\Microsoft\Windows\History\`

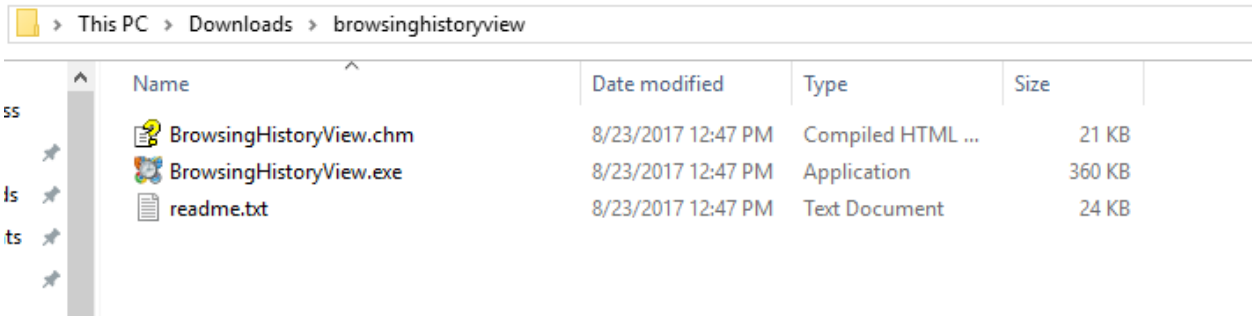
Tool: BrowsingHistoryView v2.10, from NirSoft

http://www.nirsoft.net/utils/browsing_history_view.html

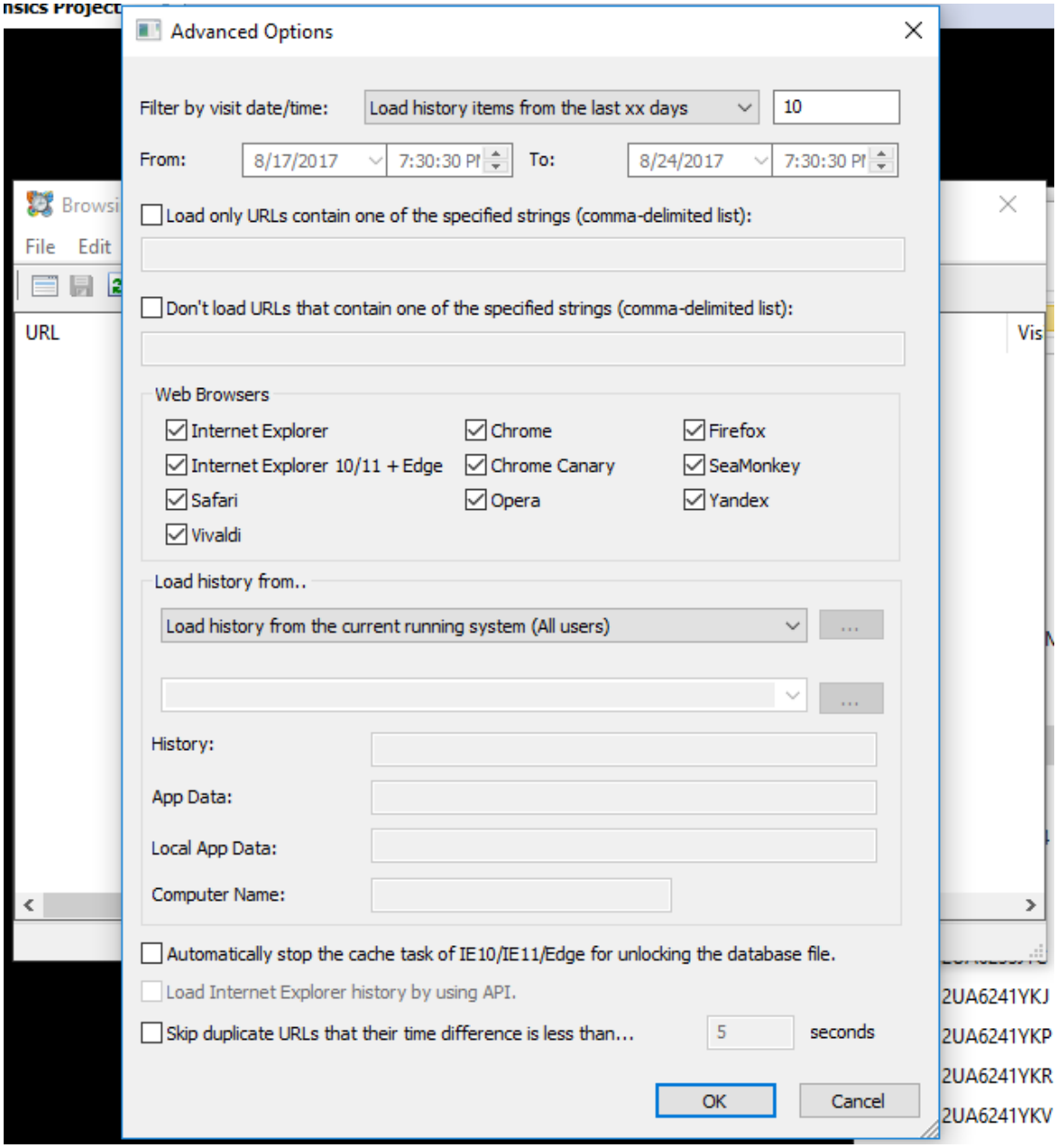
Click link to download:



Extract ZIP file:



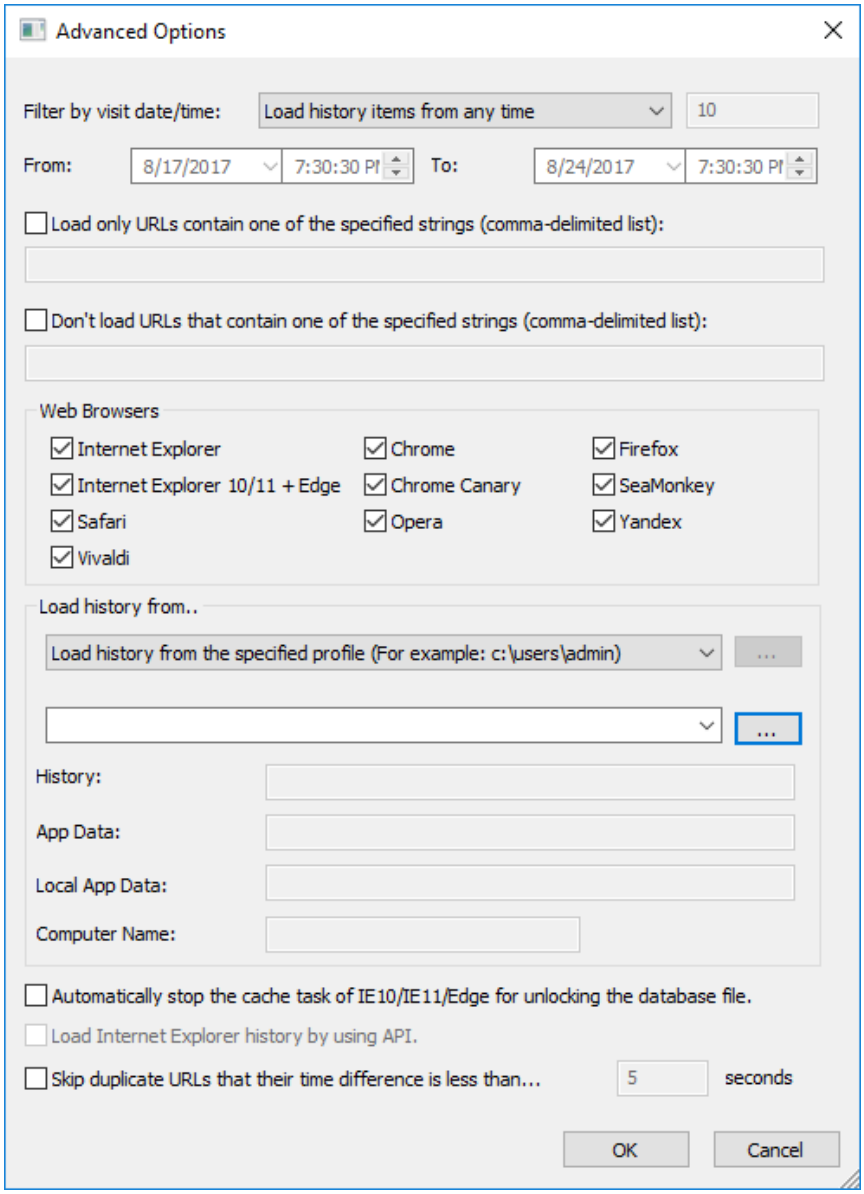
Run `BrowsingHistoryView.exe`



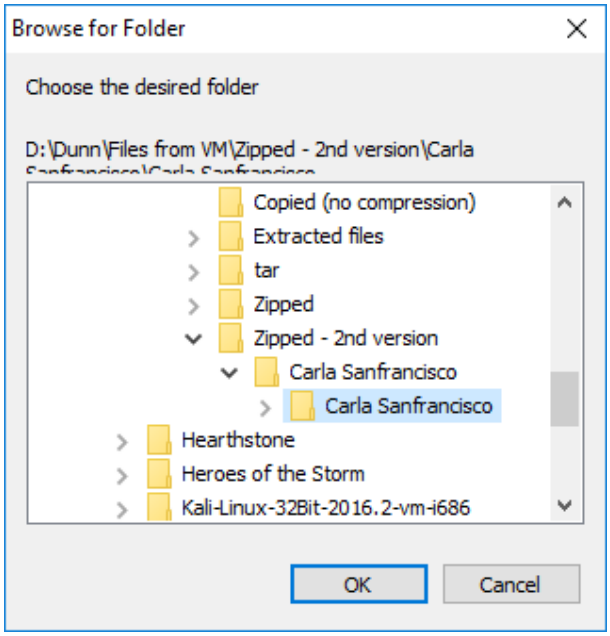
Filter by visit date/time: Load history items from any time

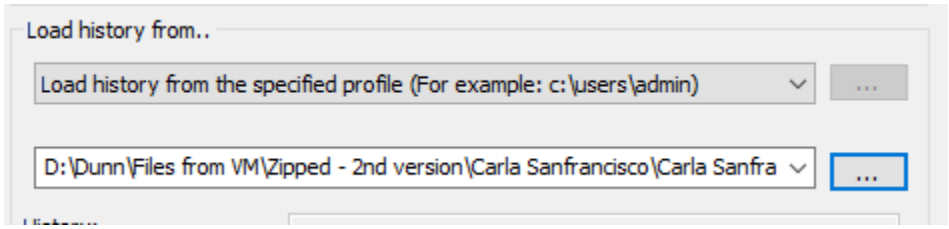
Load history from… Load history from the specified profile (For example:

`c:\users\admin`)



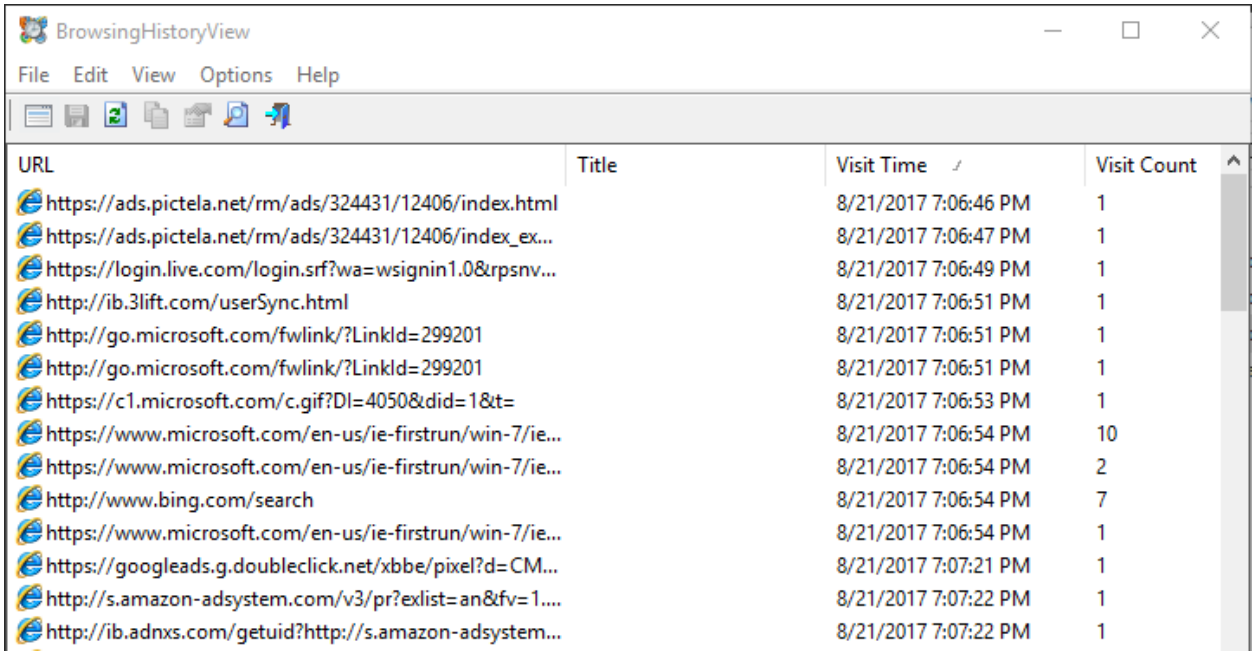
Select profile folder





Click OK

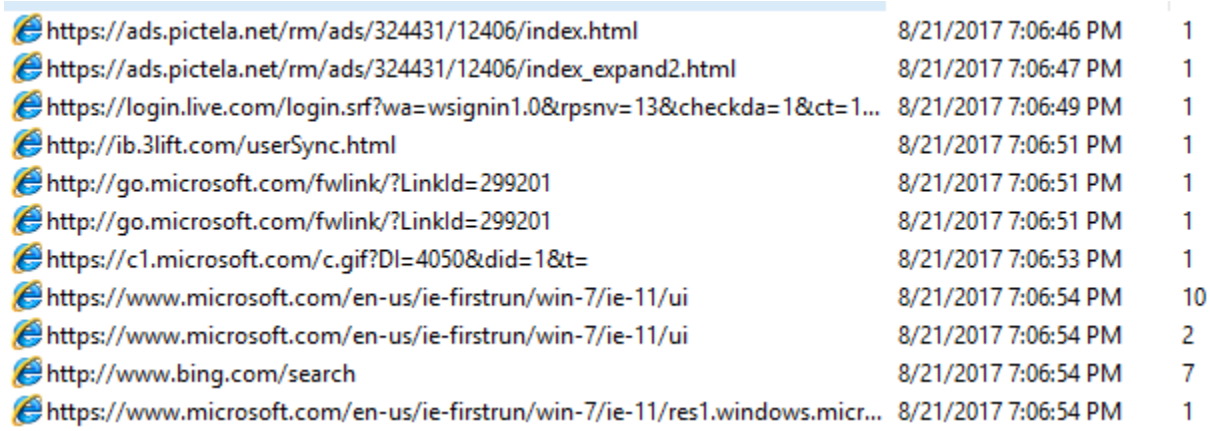
Click Visit Time column to sort URLs chronologically



Browsing history reconstruction

Open browser: August 21, 2017, 7:06 PM

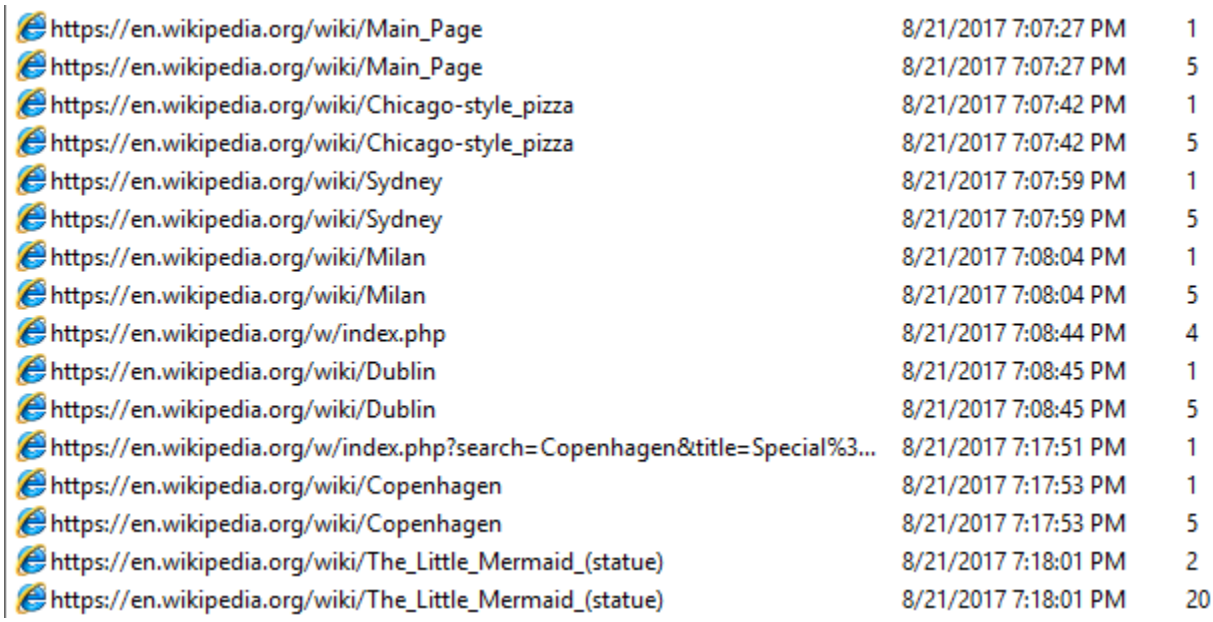
- Loads default page(s)



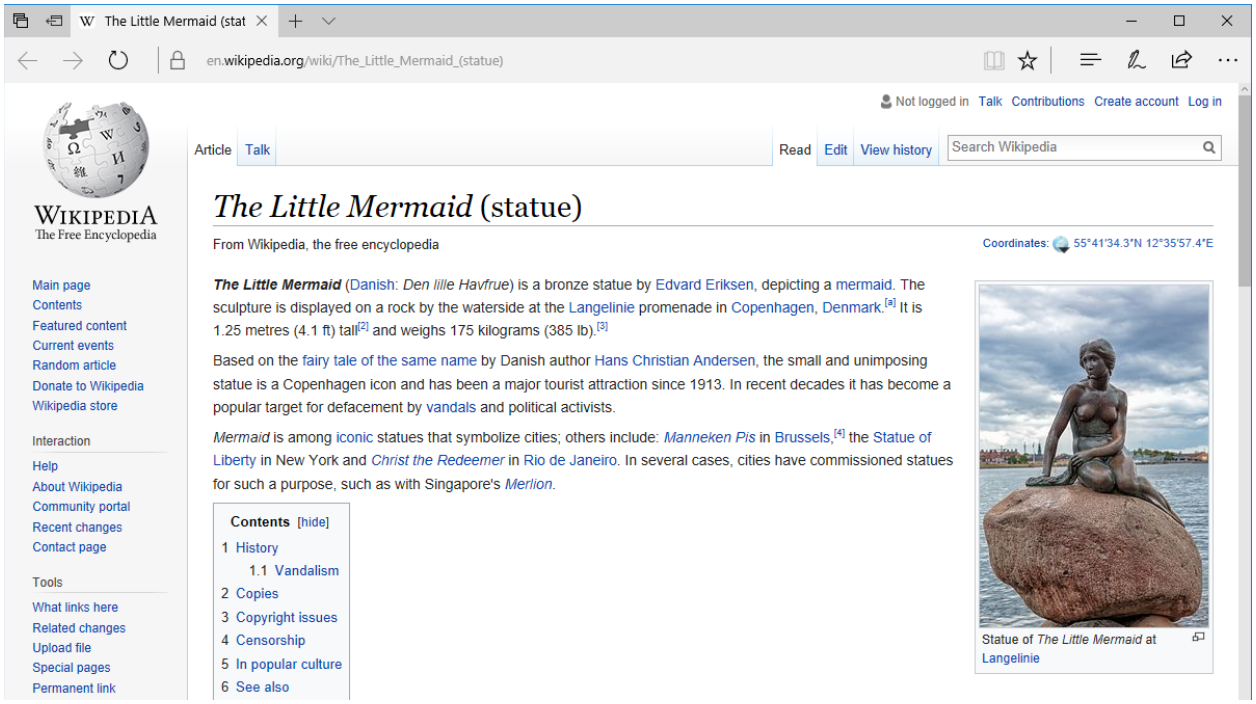
Wikipedia

- Main_Page (default)
- Chicago-style pizza

- Sydney
- Milan
- Dublin
- Copenhagen
- The Little Mermaid (statue) *[note the large number of page views]*



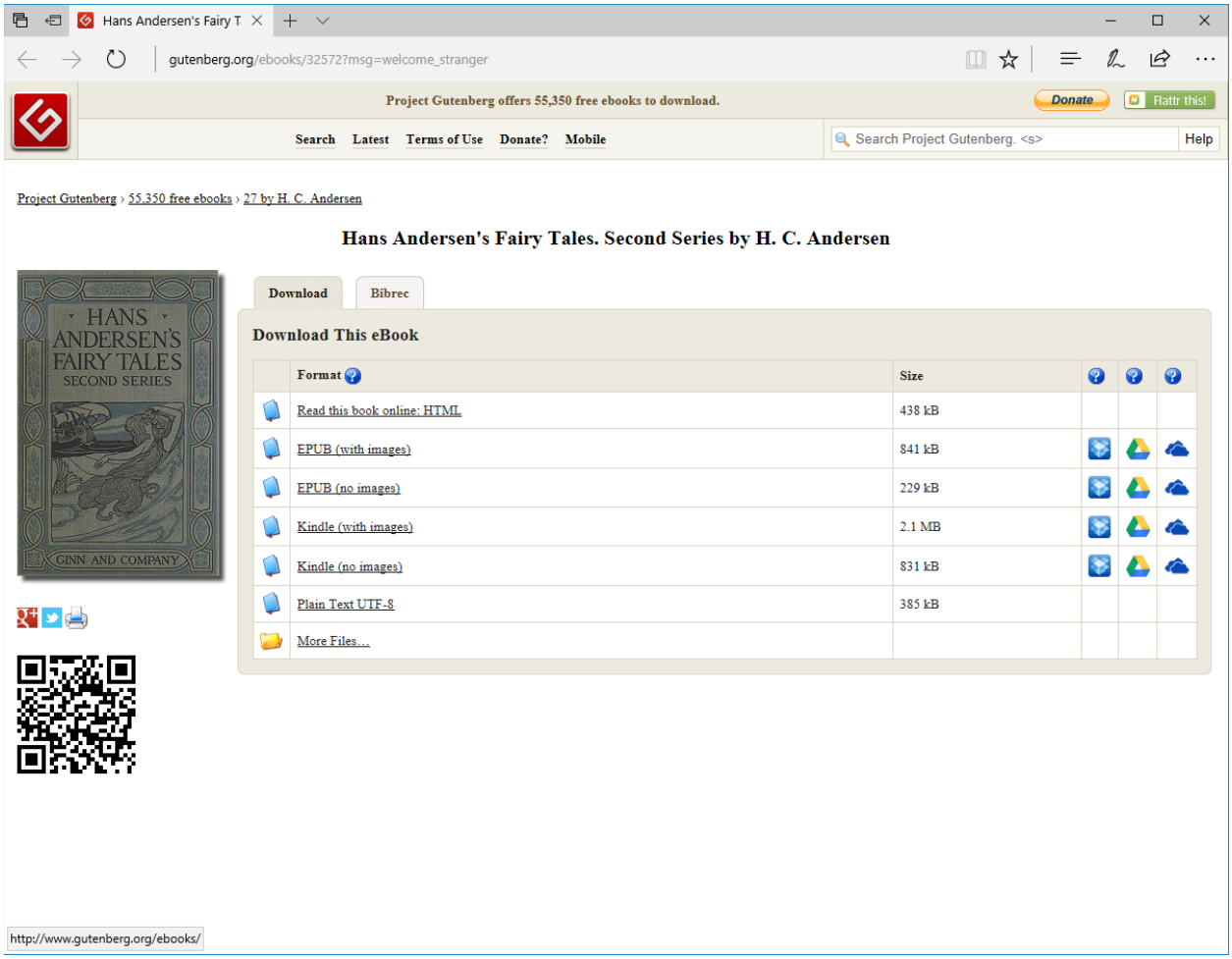
https://en.wikipedia.org/wiki/Main_Page	8/21/2017 7:07:27 PM	1
https://en.wikipedia.org/wiki/Main_Page	8/21/2017 7:07:27 PM	5
https://en.wikipedia.org/wiki/Chicago-style_pizza	8/21/2017 7:07:42 PM	1
https://en.wikipedia.org/wiki/Chicago-style_pizza	8/21/2017 7:07:42 PM	5
https://en.wikipedia.org/wiki/Sydney	8/21/2017 7:07:59 PM	1
https://en.wikipedia.org/wiki/Sydney	8/21/2017 7:07:59 PM	5
https://en.wikipedia.org/wiki/Milan	8/21/2017 7:08:04 PM	1
https://en.wikipedia.org/wiki/Milan	8/21/2017 7:08:04 PM	5
https://en.wikipedia.org/w/index.php	8/21/2017 7:08:44 PM	4
https://en.wikipedia.org/wiki/Dublin	8/21/2017 7:08:45 PM	1
https://en.wikipedia.org/wiki/Dublin	8/21/2017 7:08:45 PM	5
https://en.wikipedia.org/w/index.php?search=Copenhagen&title=Special%3...	8/21/2017 7:17:51 PM	1
https://en.wikipedia.org/wiki/Copenhagen	8/21/2017 7:17:53 PM	1
https://en.wikipedia.org/wiki/Copenhagen	8/21/2017 7:17:53 PM	5
https://en.wikipedia.org/wiki/The_Little_Mermaid_(statue)	8/21/2017 7:18:01 PM	2
https://en.wikipedia.org/wiki/The_Little_Mermaid_(statue)	8/21/2017 7:18:01 PM	20

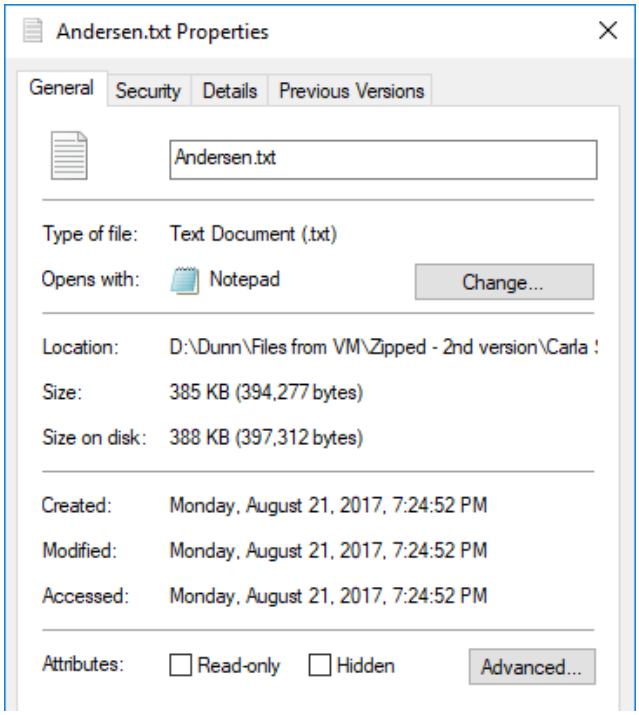


Gutenberg.org (free public domain books)

- Search for Hans Andersen
- Selected *Hans Andersen's Fairy Tales, Second Series*
- Downloaded text file, saved as `Andersen.txt`

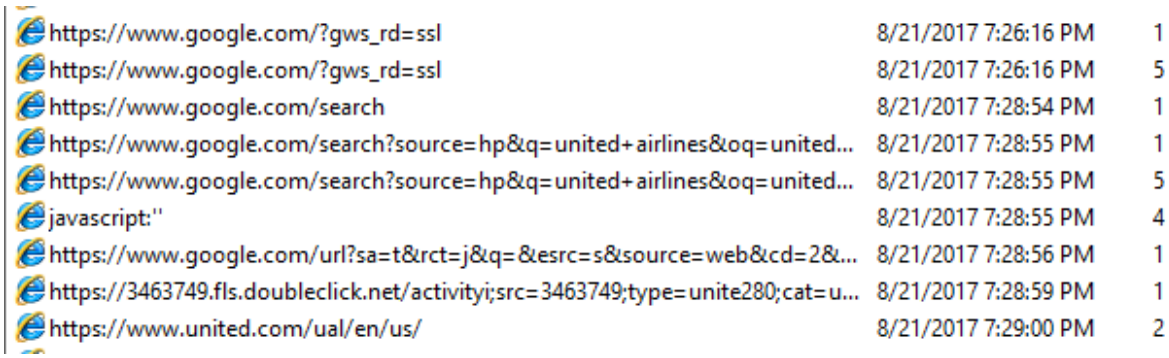
http://www.gutenberg.org/cache/latest-covers	8/21/2017 7:18:28 PM	1
http://www.gutenberg.org/	8/21/2017 7:18:29 PM	1
http://www.gutenberg.org/	8/21/2017 7:18:29 PM	13
http://www.gutenberg.org/files/32571/32571-0.txt	8/21/2017 7:23:52 PM	10
http://www.gutenberg.org/files/32571/32571-0.txt	8/21/2017 7:23:52 PM	2
http://www.gutenberg.org/ebooks/32571	8/21/2017 7:23:58 PM	3
http://www.gutenberg.org/ebooks/32571	8/21/2017 7:23:58 PM	13
http://www.gutenberg.org/ebooks/search/?query=hans+andersen	8/21/2017 7:24:00 PM	2
http://www.gutenberg.org/ebooks/search/?query=hans+andersen	8/21/2017 7:24:00 PM	13
http://www.gutenberg.org/files/32572/32572-0.txt	8/21/2017 7:24:06 PM	6
http://www.gutenberg.org/files/32572/32572-0.txt	8/21/2017 7:24:06 PM	2
http://www.gutenberg.org/ebooks/32572	8/21/2017 7:24:17 PM	3
http://www.gutenberg.org/ebooks/32572	8/21/2017 7:24:17 PM	13
http://www.gutenberg.org/pics/favicon	8/21/2017 7:24:18 PM	1
file:///C:/Users/Carla%20Sanfrancisco/Documents/Andersen.txt	8/21/2017 7:24:50 PM	1


Hans Andersen's Fairy T
gutenberg.org/ebooks/32572?msg=welcome_stranger
Project Gutenberg offers 55,350 free ebooks to download.
Donate
Flattr this!
Search
Latest
Terms of Use
Donate?
Mobile
Search Project Gutenberg. <s>
Help
Project Gutenberg › 55,350 free ebooks › 27 by H. C. Andersen
Hans Andersen's Fairy Tales. Second Series by H. C. Andersen
HANS ANDERSEN'S FAIRY TALES
SECOND SERIES
GINN AND COMPANY
Download
Bibrec
Download This eBook
Format
Size
Read this book online: HTML
438 kB
EPUB (with images)
841 kB
EPUB (no images)
229 kB
Kindle (with images)
2.1 MB
Kindle (no images)
831 kB
Plain Text UTF-8
385 kB
More Files…
http://www.gutenberg.org/ebooks/



Google

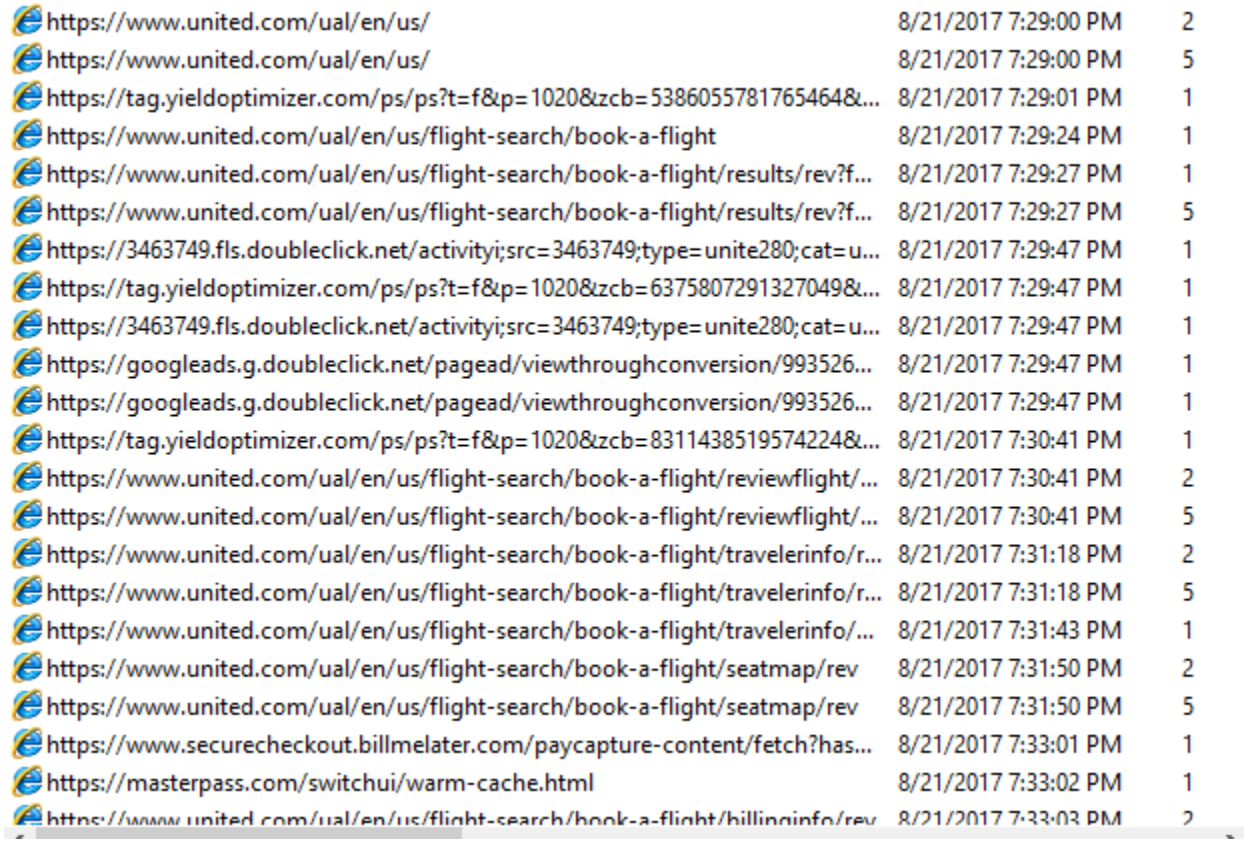
- Searched “united airlines”
- Clicked link to https://www.united.com/ual/en/us (United Airlines U.S. homepage)



United Airlines

- Searched for flight from Chicago to Copenhagen departing August 23, 2017
- Selected flight (exact flight unknown)

- Continued through booking process



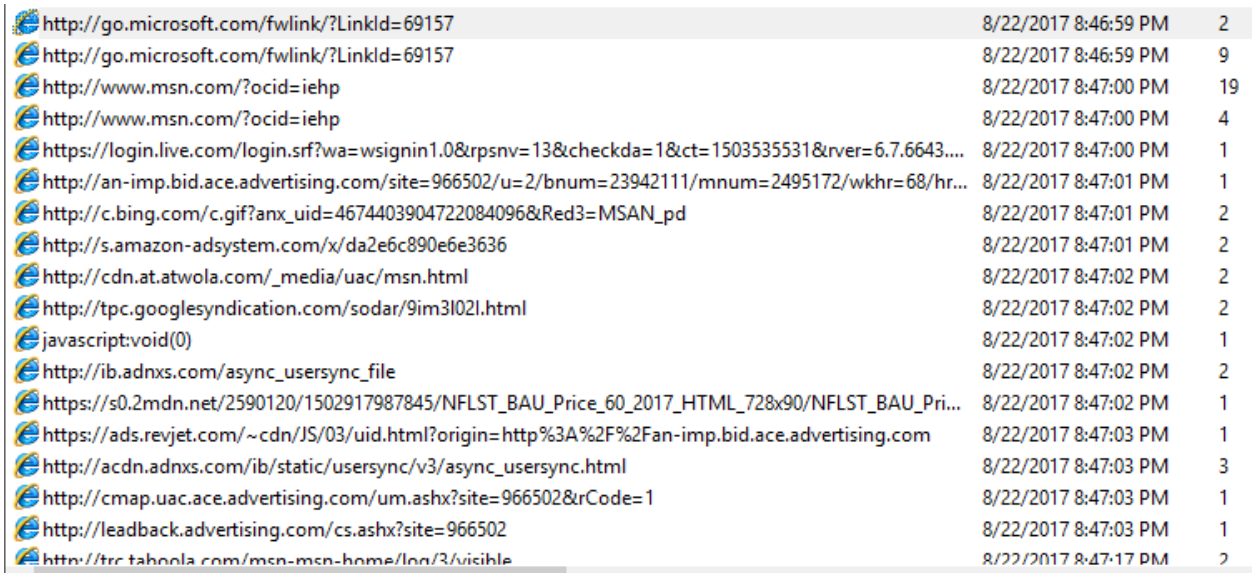
https://www.united.com/ual/en/us/	8/21/2017 7:29:00 PM	2
https://www.united.com/ual/en/us/	8/21/2017 7:29:00 PM	5
https://tag.yieldoptimizer.com/ps/ps?t=f&p=1020&zcb=5386055781765464&...	8/21/2017 7:29:01 PM	1
https://www.united.com/ual/en/us/flight-search/book-a-flight	8/21/2017 7:29:24 PM	1
https://www.united.com/ual/en/us/flight-search/book-a-flight/results/rev?f...	8/21/2017 7:29:27 PM	1
https://www.united.com/ual/en/us/flight-search/book-a-flight/results/rev?f...	8/21/2017 7:29:27 PM	5
https://3463749.fls.doubleclick.net/activityi;src=3463749;type=unite280;cat=u...	8/21/2017 7:29:47 PM	1
https://tag.yieldoptimizer.com/ps/ps?t=f&p=1020&zcb=6375807291327049&...	8/21/2017 7:29:47 PM	1
https://3463749.fls.doubleclick.net/activityi;src=3463749;type=unite280;cat=u...	8/21/2017 7:29:47 PM	1
https://googleads.g.doubleclick.net/pagead/viewthroughconversion/993526...	8/21/2017 7:29:47 PM	1
https://googleads.g.doubleclick.net/pagead/viewthroughconversion/993526...	8/21/2017 7:29:47 PM	1
https://tag.yieldoptimizer.com/ps/ps?t=f&p=1020&zcb=8311438519574224&...	8/21/2017 7:30:41 PM	1
https://www.united.com/ual/en/us/flight-search/book-a-flight/reviewflight/...	8/21/2017 7:30:41 PM	2
https://www.united.com/ual/en/us/flight-search/book-a-flight/reviewflight/...	8/21/2017 7:30:41 PM	5
https://www.united.com/ual/en/us/flight-search/book-a-flight/travelerinfo/r...	8/21/2017 7:31:18 PM	2
https://www.united.com/ual/en/us/flight-search/book-a-flight/travelerinfo/r...	8/21/2017 7:31:18 PM	5
https://www.united.com/ual/en/us/flight-search/book-a-flight/travelerinfo/...	8/21/2017 7:31:43 PM	1
https://www.united.com/ual/en/us/flight-search/book-a-flight/seatmap/rev	8/21/2017 7:31:50 PM	2
https://www.united.com/ual/en/us/flight-search/book-a-flight/seatmap/rev	8/21/2017 7:31:50 PM	5
https://www.securecheckout.billmelater.com/paycapture-content/fetch?has...	8/21/2017 7:33:01 PM	1
https://masterpass.com/switchui/warm-cache.html	8/21/2017 7:33:02 PM	1
https://www.united.com/ual/en/us/flight-search/book-a-flight/billinginfo/rev	8/21/2017 7:33:03 PM	2

earch/book-a-flight/results/rev?f=ORD&t=CPH&d=2017-08-23&tt=1&sc=7&px=1&taxng=1&idx=1

earch/book-a-flight/results/rev?f=ORD&t=CPH&d=2017-08-23&tt=1&sc=7&px=1&taxng=1&idx=1

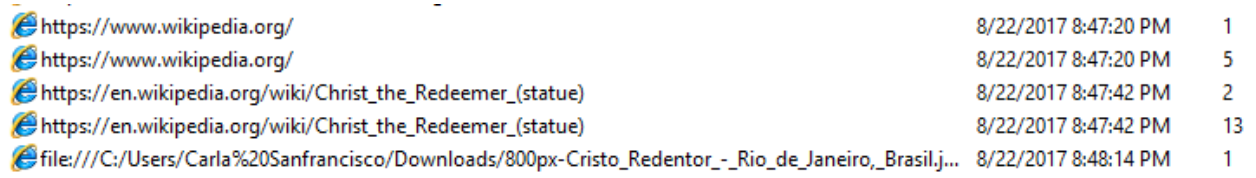
Open browser: August 22, 2017, 8:46 PM

- Loads default page
- Lots of built-in advertisements



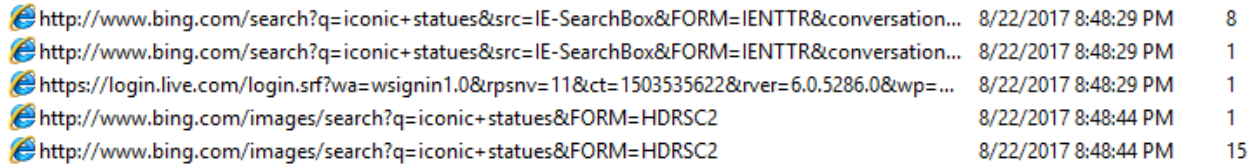
Wikipedia

- Christ the Redeemer (statue)
- Downloaded photo



Bing

- Searched “iconic statues” (using the IE Search Box)



Wikipedia

- Statue of Liberty → downloaded photo
- Trafalgar Square
- Nelson’s Column → downloaded photo

- Charging Bull → downloaded photo
- Angel of Grief
- Spring Temple Buddha → downloaded photo

https://en.wikipedia.org/w/index.php?search=Statue+of+Liberty&title=Special%3ASearch	8/22/2017 8:49:12 PM	1
https://en.wikipedia.org/wiki/Statue_of_Liberty	8/22/2017 8:49:14 PM	1
https://en.wikipedia.org/wiki/Statue_of_Liberty	8/22/2017 8:49:14 PM	9
file:///C:/Users/Carla%20Sanfrancisco/Downloads/800px-Statue_of_Liberty_7.jpg	8/22/2017 8:49:26 PM	1
https://en.wikipedia.org/w/index.php?search=Trafalgar+Square&title=Special%3ASearch	8/22/2017 8:49:35 PM	1
https://en.wikipedia.org/wiki/Trafalgar_Square	8/22/2017 8:49:36 PM	1
https://en.wikipedia.org/wiki/Trafalgar_Square	8/22/2017 8:49:36 PM	5
https://en.wikipedia.org/wiki/Nelson%27s_Column	8/22/2017 8:50:09 PM	2
https://en.wikipedia.org/wiki/Nelson%27s_Column	8/22/2017 8:50:09 PM	9
file:///C:/Users/Carla%20Sanfrancisco/Downloads/800px-Admiral_Horatio_Nelson,_Nelson's_Colu...	8/22/2017 8:50:34 PM	1
https://en.wikipedia.org/w/index.php?search=Charging+Bull&title=Special%3ASearch	8/22/2017 8:52:34 PM	1
file:///C:/Users/Carla%20Sanfrancisco/Downloads/Charging_Bull_statue.jpg	8/22/2017 8:52:44 PM	1
http://www.bing.com/images/search?view=detailV2&ccid=Zpbnfw7%2f&id=1AF067B9C5E3F9200...	8/22/2017 8:53:25 PM	1
https://en.wikipedia.org/w/index.php?search=Angel+of+Grief&title=Special%3ASearch	8/22/2017 8:54:30 PM	1
https://en.wikipedia.org/wiki/Angel_of_Grief	8/22/2017 8:54:31 PM	1
https://en.wikipedia.org/wiki/Angel_of_Grief	8/22/2017 8:54:31 PM	5
https://en.wikipedia.org/wiki/Charging_Bull	8/22/2017 8:54:39 PM	2
https://en.wikipedia.org/wiki/Charging_Bull	8/22/2017 8:54:39 PM	15
https://en.wikipedia.org/w/index.php?search=Spring+Temple+Buddha&title=Special%3ASearch	8/22/2017 9:01:03 PM	1
https://en.wikipedia.org/wiki/Spring_Temple_Buddha	8/22/2017 9:01:03 PM	1
https://en.wikipedia.org/wiki/Spring_Temple_Buddha	8/22/2017 9:01:03 PM	9
about:blank	8/22/2017 9:01:06 PM	45
file:///C:/Users/Carla%20Sanfrancisco/Downloads/Spring_Temple_Buddha_picturing_Vairocana,_in...	8/22/2017 9:01:42 PM	1

`Email.txt`

file:///C:/Users/Carla%20Sanfrancisco/Documents/email.txt	8/22/2017 9:10:53 PM	1

Appendix G: Proposal for Cybersecurity Merit Badge Sent to BSA National Office

(ISC)²

CENTER FOR CYBER SAFETY AND EDUCATION

311 Park Place Blvd., Suite 610, Clearwater, FL 33759
United States of America
p: +1.727.493.3587 | f: +1.727.489.2803

January 23, 2018

Pilots and Program Development—Merit Badge Proposal
Attn: Janice Downey
1325 West Walnut Hill Lane, S272
Irving, TX 75038

Dear Janice,

After months of work by a top caliber team of cybersecurity experts, Eagle Scouts and even your own BSA National Staff, we are pleased to formally provide for your review the outline of a new Cybersecurity merit badge.

(ISC)² members and the Center for Cyber Safety and Education are excited to partner with the Boy Scouts of America to create the first Cybersecurity merit badge. Our two nonprofit organizations are dedicated to inspiring a safe and secure cyber world for everyone, and we believe this new merit badge will go a long way toward achieving this vision.

Our research has found there is a dangerous shortage of cybersecurity professionals. In fact, we project that in the next five years we will be facing a 1.8 million shortfall of trained professionals to combat this growing threat. A Cybersecurity merit badge will help reduce that gap by getting more young men (and soon women) to explore and consider a career in a field that has nearly 100% employment.

We stand prepared to support this program in a variety of ways, including:

1) Access to our membership of more than 130,000 certified cybersecurity professionals as a pool of potential merit badge counselors.
2) Subject matter experts to help build the program, and keep it fresh and relevant for years to come.
3) Continuing support and promotion through our members and local chapters around the country.

This is an exciting step for the BSA, and we are honored to have the opportunity to be a part of this historic program.

We look forward to your feedback and guidance.

Sincerely,

David Shearer
CEO
(ISC)²

Patrick Craven
Director / Eagle Scout
Center for Cyber Safety and Education

INSPIRING A SAFE AND SECURE CYBER WORLD.

Proposal for Cybersecurity Merit Badge

Description

This merit badge introduces Scouts to the subject of computer and network security, broadly known as cybersecurity. The focus of the badge is two-fold:

1) To teach Scouts the basic concepts they need to know to keep themselves and their families secure in our modern, connected world, and

2) To introduce them to the exciting and rapidly growing career opportunities in cybersecurity.

The badge will cover topics including ethics, security fundamentals, cyber threats, defenses, cryptography, mobile and connected devices, and careers. The activities are designed to help each Scout learn to secure their own computers and to explore the wider world of cybersecurity.

Rationale

Securing cyberspace is one of the most significant challenges facing our generation. Modern society has become dependent on a wide range of networked computer systems, and addressing the many security problems inherent to this dependence is an increasingly difficult task. One of the key components to doing so is employing enough skilled cybersecurity workers. However, organizations across all sectors of industry are having difficulty filling existing cybersecurity jobs. This labor shortage is only increasing as growth in the number of cybersecurity jobs significantly

outpaces the number of workers entering the field. A recent study the Center for Cyber Safety and Education conducted in partnership with (ISC)[2], the world's leading information security professional organization, estimated that the cybersecurity worker shortage will grow to 1.8 million by 2022.[8] Among professionals surveyed in North America, 68% said there were too few cybersecurity workers in their department, and the majority believe that one of the main reasons for this is difficulty in finding qualified personnel.

This problem has wide-ranging effects on our society, from loss of private information to threats to national security. Experts estimate that cybercrime causes tens of billions of dollars of damage each year to the U.S. economy alone and hundreds of billions globally.[9] This problem impacts everyone. In recent Congressional testimony on the cybersecurity workforce, one industry leader put it this way: "The cybersecurity talent issue isn't limited to a few sectors; it runs across the board from government to education to healthcare and all industries. Strong talent is needed in all communities from rural farms that increasing rely on information technology to financial service companies in large urban areas."[10] At a recent conference on this issue, a representative from the U.S.

---

[8] Center for Cyber Safety and Education. 2017. "2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk." https://iamcybersafe.org/gisws/.
[9] Lewis, James, and Stewart Baker. 2013. "The Economic Impact of Cybercrime and Cyber Espionage." Washington, DC. https://www.mcafee.com/es/resources/reports/rp-economic-impact-cybercrime.pdf.
[10] Jarvis, David, Security and CIO Lead, IBM Institute for Business Value. 24 Oct 2017. "Public-Private Solutions to Educating a Cyber Workforce." Statement for the Record. https://homeland.house.gov/hearing/public-private-solutions-educating-cyber-workforce/.

Department of Homeland Security called it "a national security crisis."[11] The U.S. President's Commission on Enhancing National Cybersecurity also identified this challenge, concluding that building the cybersecurity workforce was one of its strategic imperatives for bolstering the nation's cybersecurity posture.[12]

The Boy Scouts of America (BSA) is in a unique position to contribute to the solution of this crisis. The BSA merit badge program has long been a way to introduce young men to potential careers, as well as educate them in important subjects, even for those that don't pursue them as careers. The BSA has shown great leadership with the recent addition of its STEM-based merit badges. Some are even related to computing, such as Digital Technology and Programming, both of which include an element of online safety. However, online safety is very different from cybersecurity. Whereas online safety is all about smart personal behavior when using the Internet, cybersecurity is about protecting computer systems against abuse, attack, or other failures. This distinction is analogous to the difference between outdoor safety and First Aid/Medicine or between aquatics safety and Lifeguarding. The Girl Scouts of the USA has recognized this need, announcing in June of last year that they will be introducing a series of cybersecurity badges for their programs starting in fall 2018.[13] We propose that the BSA also create a separate and distinct Cybersecurity merit badge, which would introduce Boy

---

[11] Dan Stein, Branch Chief, Cybersecurity Education and Awareness, U.S. Department of Homeland Security. 2 Aug 2017. Workshop on Cybersecurity Workforce Development. Chicago, IL.
[12] Commission on Enhancing National Cybersecurity. 2016. "Report on Securing and Growing the Digital Economy." https://www.nist.gov/cybercommission/.
[13] Palo Alto Networks. 13 Jun 2017. "Palo Alto Networks and Girl Scouts of the USA Announce Collaboration for First-Ever National Cybersecurity Badges." Santa Clara, CA. Press Release.

Scouts to the fundamentals of securing the digital communications of our modern world, teach them to become responsible digital citizens and expose them to the wide range of careers in the field. Our nation and our society are in desperate need of this progress.

The Merit Badge Task Force stated in the inaugural issue of the *Counselor's Compass* newsletter that "developing merit badges that expand Scouts' horizons into technological careers […] will be the merit badge trend of the future."[14] A Cybersecurity badge positions the BSA on the cutting edge of this trend and is the ideal next step.

Requirements

The following proposed requirements were developed by a team of cybersecurity experts representing academia, government, and industry. A complete list of contributors is at the end of this document.

Safety

As with all merit badges, safety comes first.

- Show your counselor your current, up-to-date **Cyber Chip**.

Knowledge

These requirements help a Scout understand some key cybersecurity terms and topics. This is important not only for laying the foundation for the activity requirements but also for helping the Scout become a well-informed citizen. So many of these concepts affect

[14] BSA Merit Badge Task Force. 2014. "Counselor's Compass, Vol. 1, No. 1." Irving, TX: Boy Scouts of America. http://www.scouting.org/filestore/counselors_news/Fall_2014.pdf.

our everyday life, it is abundantly beneficial for citizens to have a basic understanding of them.

Ethics

- Relate one or more tenants of the Scout law to the purpose of cybersecurity.
- Explain what is and is not acceptable behavior in cyberspace.
- Discuss with your counselor what you should do if you discover a vulnerability in your school's computers or network, a public website, or software product.

Fundamentals

- Cybersecurity definitions. Explain to your counselor the meaning of: Vulnerability, Exploit, Identity, the "C.I.A." triad (confidentiality, integrity, availability), Authentication, and Authorization.
- Discuss with your counselor why cybersecurity is important and who benefits when it is done properly.

Cyber Defenses

- Describe three of the following and how they are used to defend a computer or network: firewall, antivirus software, intrusion detection system, intrusion prevention system, access control list, identity management.
- Describe multi-factored authentication and how it can be used to improve security (something you know, something you have, something you are).

Cyber Threats & Attacks

- Describe the following major categories of threats to computer systems, and give two examples of each: people, natural disasters, and accidents/mistakes.
- Describe at least four different categories or types of malware (for example: virus, worm, Trojan, backdoor, spyware, or ransomware).
- Explain what a botnet is, its purpose, and how it operates.
- Describe how to spot an online scam (e.g. phishing or scareware) and what to do when you encounter one.
- Discuss with your counselor the potential consequences of a cyberattack or disaster to individuals, companies, and governments.

Cryptography

- Describe the differences between symmetric encryption, asymmetric encryption, and hashing. Give an example of when each would be used.
- Explain what public key infrastructure (PKI) is and the use for certificates and digital signatures.

Mobile

- Describe at least two possible risks when using public Wi-Fi.
- List at least three best practices for securing a mobile device.

Do TWO of the following:

- Describe how a mobile device connects to the Internet, both when using Wi-Fi and when using "cellular data" and the difference in each one (speed, security, cost).
- With your or your counselor's mobile device, demonstrate how to check that it has the latest version of the OS and any installed apps.
- With your or your counselor's mobile device, demonstrate how to back it up to a local PC or the cloud.
- Describe potentials risks of jailbreaking a mobile device, application sideloading, and application permissions.

"Internet of Things" (IoT)

- Describe what the "Internet of Things" (IoT) is. Name four connected devices that might be found in a digital home.
- Discuss why it is more difficult to have good cybersecurity with IoT devices.

Critical Infrastructure

- Explain how computers are used in power and water plants and why they need to be secure.

Activities

These requirements give a Scout hands-on experience with real-life cybersecurity. Most of them revolve around the devices and networks a Scout is likely to have or use in his day-to-day life. They help a Scout learn to secure his computer, his home network, and

his mobile device (e.g. smartphone). They also empower the Scout to help others secure their devices.

Ethics

- Locate and examine the code of ethics used by an information security professional society. Discuss your findings with your counselor.

Current Events. Do ONE of the following:

- Discuss with your counselor an article or a news report about a recent cybersecurity incident, such as a data breach or malware infection. Explain how the incident happened (to the best of your ability based on the information available) and what the consequences are or might be to the victim.
- Watch a movie or read a book in which cybersecurity plays a significant role. Discuss with your counselor how cybersecurity topics were depicted and how realistic you think it was.

Installing updates. Do the following:

- Explain to your counselor the importance of installing the latest updates on your computer, why they are needed, and what kinds of problems they can prevent.
- Demonstrate to your counselor how to check for, download, and install the latest updates for your computer or another computer you have permission to use. Show your counselor how to verify that your computer is up-to-date.

Virus scanning.

- Run a virus scanner on your home computer or another computer you have permission to use. Show the results to your counselor.

System security. Using on your own computer, a mobile device, or a computer that you have permission to use, do any FOUR of the following:

- Describe what makes a good password and why. Set or change an account password to one that is “strong.”
- Add a new regular (non-administrator) user account to your computer and show how to check that the permissions are set correctly. Check if the computer has a guest account enabled. If it is not needed and you have permission, disable the guest account.

- Install and set up a password manager.
- Use two different methods to see what programs or processes are running on your computer.
- Use a command line interface to view your computer's open network connections. Discuss the results with your counselor.
- On a mobile device, install a free app (from an official app store) to scan the local network and run it to identify all network devices.
- Show how you can check that your computer's firewall is on. Show how you would turn it on if it wasn't already.
- Identify one or more other vulnerabilities on your home computer or network or another computer or network you have permission to use, and take the necessary actions to fix it.

Network security. Do TWO of the following:

- If your home has a Wi-Fi router, verify that it has the highest available settings that it supports, such as WPA2 (not WEP). Also, set a password that is considered "strong". Explain to your counselor what a "strong" password is.
- Run a network port scan on your home computer. Write down the ports that are open and show this list to your counselor. Discuss what programs could be using the open ports and whether they are needed on your computer.
- Using a Raspberry Pi device or laptop computer, show the available Wi-Fi networks nearby and how to tell which ones are running with encryption. Show how to connect it to a known, trusted network that uses a passphrase.
- Design a simple network for an imaginary company or organization. Draw a network diagram showing the Internet gateway, routers, switches, public-facing servers, and workstations. Include security features such as firewalls, DMZ, IDS or IPS, and web proxy. Share your diagram with your counselor, and discuss the purpose of each of the security features you included.

Cryptography. Do ONE of the following:

- Create an encrypted ZIP file. Place this on a thumb drive or email it to your counselor then tell them (verbally, not through email) the password to unlock it [7zip is a free online program Scouts can use for this].
- Create your own PGP (pretty good privacy) email key. Share your public key with others (and your counselor). Also, get their public keys and add them to your computer's key ring. Send a message that has been digitally encrypted.

- Use a hashing algorithm (for example, SHA or MD5) to create a checksum for a file. Have a fellow Scout or your counselor make a change to the file. Recreate the checksum for the file and compare the new checksum to the original as a demonstration of file integrity checking.

Cybersecurity activity. Do ONE of the following:

- Learn about three cybersecurity competitions, camps, or other activities you could participate in (either now or in the future). Tell your counselor about these, including the type of activity, time commitment, and age of participants.
- Organize a cybersecurity competition for members of your troop, school, or some other group approved by your counselor. Either design your own competition or use an existing platform that teams or individuals can race to lock down all vulnerabilities.
- Give a presentation to your patrol, troop, or another group approved by your counselor, on a cybersecurity topic of your choice. Your presentation must include at least one demonstration and/or hands-on activity.

Careers. Do TWO of the following:

- Investigate three careers that involve cybersecurity. Pick one and find out what education, training, and experience are required for this profession. Discuss this with your counselor, and explain why this profession might interest you.
- Visit a business or organization that does work in cybersecurity. Find out about different work roles and what they do. Share what you learned with your counselor.
- Discuss the role of certifications in cybersecurity. Pick two and find out the following: purpose, governing organization, and requirements. Share what you learned with your counselor.

Additional Information for Consideration

Applicability to Scouting

How well the proposed topic fits with Scouting (values, Scout Oath, Scout Law, Guide to Safe Scouting, etc.)

How fun and engaging the subject is for Scout-age youth (depth and breadth of appeal, age appropriateness)

Scouting's Mission and Values

Cybersecurity is a topic extremely well suited to the Boy Scouts of America. By its very nature, the cybersecurity profession requires individuals of high moral character. Security professionals often have access to sensitive data and systems, making it imperative that they be trustworthy and ethical. The technical and creative skills possessed by many young people interested in computer technology can easily be used for illegal purposes when pursued outside the context of a strong ethical framework. Young people with these interests will pursue and obtain these skills anyway. It is consistent with the BSA's mission to give these young people the necessary ethical framework to apply their interests and skills to help others.

Furthermore, this is something that is badly needed by the nation. As mentioned earlier, the state of cybersecurity has become a national crisis. Billions of dollars are lost by all sectors of our economy. Criminal networks are stealing personal information, exposing millions of people to identity theft and other crimes. Ransomware threatens hospital operations and therefore patients. Military and defense networks are under constant attack. Critical infrastructure is at risk of compromise by foreign states. The BSA has a long and proud history of supporting the nation in times of need, from planting Victory gardens in World War II, to distributing emergency handbooks and Civil Defense posters during the Cold War, to the National Good Turns fighting national

problems such as soil erosion and homelessness.[15] Hands-on experiences such as those provided by the merit badge program have been demonstrated to increase young people's interest in certain careers.[16,17] In the same way, hands-on cybersecurity activities have the potential to increase Scouts' interest in cybersecurity careers in a meaningful way.[18]

Interest and Age-Appropriateness for Scouts

One of the issues of concern to the BSA is whether there would be enough interest in this new merit badge. We believe there is ample evidence to suggest there would be. CyberPatriot[19], a cyber defense competition for middle and high school students run by the Air Force Association, has been growing like wildfire. The number of registered teams has grown by over 330% over the last five years. This year, they continued this growth trend, registering nearly 5,600 teams -- over 15,000 registered participants.[20] These teams are spread throughout the country and attract a diverse group

---

[15] Boy Scouts of America. 2014. Scouting Heritage (Merit Badge Series). Irving, TX: Boy Scouts of America.
[16] Alberts, Bruce. 2010. "An Education That Inspires." Science 330 (6003): 427. doi:10.1126/science.1199138.
[17] Maxim, Bruce R, and Bruce S Elenbogen. 2009. "Attracting K-12 Students to Study Computing." In 39th ASEE/IEEE Frontiers in Education Conference, M1H 1-5. San Antonio, TX: IEEE. doi:10.1109/FIE.2009.5350694.
[18] Dunn, Michael H., and Laurence D. Merkle. 2018. "Assessing the Impact of a National Cybersecurity Competition on Students' Career Interests." In Proceedings of the 49th ACM Technical Symposium on Computer Science Education (SIGCSE '18), Baltimore, MD, USA. doi:10.1145/3159450.3159462.
[19] "Air Force Association's CyberPatriot: The National Youth Cyber Education Program." 2017. http://uscyberpatriot.org/.
[20] Air Force Association. 23 Oct 2017. "CyberPatriot Breaks Registration Record Again." Arlington, VA. Press Release.

of students.[21] Even more remarkable, these are students who chose to commit to spending several hours per week for up to an entire school year on the program and belong to a school or other organization with the resources to field such a team. A Cybersecurity merit badge would reach a significantly broader audience. A growing body of research indicates that young people get excited about cybersecurity when given the chance to explore it hands-on. For example, in a survey of CyberPatriot participants, 81% indicated that it was more fun than other extracurricular activities, and 33% said it was the *most* fun of all their extracurricular activities![22] Additionally, the success of Robotics, Programming, Digital Technology, and others validates that there is significant interest among Scouts in exploring technology fields and in pursuing technology-related merit badges.

Practicality

The practicality of the proposed merit badge (resources to recruit merit badge counselors, uniqueness, existence of standardized "rules" and administrative organization, safety and risk considerations, etc.)

Resource requirements (cost to Scouts/units, camp implications, etc.)

---

[21] CyberPatriot Program Office. 2017. "CyberPatriot Impact Report." https://www.uscyberpatriot.org/Documents/Fact Sheets/Impact Report_2017.pdf.

[22] CyberPatriot Program Office. 2014. "CyberPatriot Survey Results: CyberPatriot VI Post-Season Competitor Survey 2013-2014."

Availability of Merit Badge Counselors

According to data from CyberSeek, a job analytics site sponsored by the National Initiative for Cybersecurity Education, there are approximately 747,000 cybersecurity workers in the United States (this includes both those in primary cybersecurity jobs and those in other roles that require cybersecurity skills).[23] Members of IT/cybersecurity professional organizations regularly volunteer for community outreach and education efforts. (ISC)[2] and ISSA, two of the largest and most prominent such organizations and co-sponsors of this proposal, have already committed to supporting and helping to recruit new merit badge counselors. Several other national and international organizations for cybersecurity professionals also have significant volunteer efforts focused on youth education, including ISACA, AFCEA, and the Military Cyber Professionals Association.[24] These organizations will be excellent places to start recruiting additional merit badge counselors.

CyberPatriot, described above, recruits thousands of volunteers every year to coach and mentor teams for its competitions. Each of the 5,600 teams nationwide has at least one coach or mentor that is knowledgeable in cybersecurity, and often more than one. Since merit badge counseling requires a significantly smaller time commitment than coaching or mentoring a CyberPatriot team, we expect that we will be able to recruit even more volunteers.

---

[23] http://cyberseek.org/heatmap.html

[24] https://www.isaca.org/ | https://www.afcea.org/ | http://public.milcyber.org/

Resource Requirements

All proposed requirements can be completed by an individual Scout with just a computer and access to the Internet. If the Scout does not have a computer or Internet access of his own, the requirements can be completed on a school or library computer (with permission), or a computer supplied by the merit badge counselor.

In order to run a merit badge class/clinic, a unit would need one computer for every Scout participating, or at least enough computers such that Scouts can rotate through and each get sufficient time on the computer, plus Internet access with sufficient bandwidth. Appropriate computers can be purchased new for as little as $200-300, sometimes even cheaper. However, a unit need not buy new computers, since the computers available in most school or library computer labs would be sufficient. The unit would merely need permission to install any software they were using for the class and/or to access any security settings the Scouts might be working with.

Safety and Risk Considerations

The primary safety concern is online safety, just as with any activity where a young person is using the Internet. For this reason, this merit badge proposal relies on the BSA's existing best practice, the Cyber Chip, which is the first requirement.

Another risk consideration that should be taken any time young people engage with information technology is the potential for misuse. Skilled young people are likely to be able to engage in unethical activities, including circumventing security and safety

controls, manipulating computers and people to their own ends, or participating in illegal activities online. This is why the proposed requirements address ethics and ethical conduct immediately following safety. It is imperative that Scouts consider the way in which they can apply Scouting's values to their activities with computers and the Internet.

Development Resources

Availability of outside resources for developmental support

Sponsorship/Funding

This merit badge proposal is sponsored by the ISSA Education Foundation (issa-foundation.org) and the Center for Cyber Safety and Education (www.iamcybersafe.org) and is endorsed and supported by $(ISC)^2$ (www.isc2.org). The ISSA Education Foundation has donor funds specifically designated to support the development of a Cybersecurity merit badge program for Boy Scouts. See the "Sponsoring Organizations" section near the end of this document for more information about each of these organizations.

When it comes time to launch the new Cybersecurity merit badge, or if the development costs exceed the funds available from the sponsoring organizations, a corporate sponsor can be solicited. As leading cybersecurity professional and education organizations, both ISSA and $(ISC)^2$/Center for Cyber Safety and Education have valuable connections with industry. In the past, large information technology and security companies have been eager to sponsor, support, and promote cyber education programs.

For example, Palo Alto Networks is sponsoring development of the GSUSA cybersecurity badges,[6] and CyberPatriot has at least nine large corporate sponsors annually, including Cisco, Microsoft, and Facebook (in addition to several government and academic sponsors).[25]

The following resources aid in the understanding of the topic and will be helpful in the future development of the merit badge and pamphlet.

Ethics

The following leading cybersecurity professional organizations provide a Code of Ethics:

- ISACA: https://www.isaca.org/certification/code-of-professional-ethics/
- (ISC)^2: https://www.isc2.org/Ethics
- ISSA: http://www.issa.org/?page=CodeofEthics
- IEEE: https://www.ieee.org/about/corporate/governance/p7-8.html

Additional ethics resource(s):

- Richard A. Spinello, *Cyberethics: Morality and Law in Cyberspace, Sixth Edition* (Jones & Bartlett, 2017)
- Herman T. Tavani, Ethics and Technology (Wiley, 2015 ISBN 978-1119355311)
- Stanford Encyclopedia of Philosophy: Computer and Information Ethics
- Stanford Encyclopedia of Philosophy: Information Technology and Moral Values

[25] http://uscyberpatriot.org/about/sponsors

- Communications of the ACM: “A uniform code of ethics: business and IT professional ethics” by Brett Landry
- International Society for Ethics & Information Technology: Promotes and facilitates scholarship, education, discussion, and debate, and other activities, on the ethical issues in and surrounded by information technology; distinctly devoted to normative issues.

Cybersecurity Basics

The following resources give an introduction to cybersecurity fundamentals. These resources can be used as guidance in developing the merit badge, and by Scouts while working on earning the badge.

- Cyber Aces - free online cybersecurity courses from SANS, a leader in IT security training
- CyberPatriot training modules - slides used for training CyberPatriot teams, covering a number of important cybersecurity topics
- Cyberspace Principals Course - text for an introductory course developed by Civil Air Patrol, the U.S. Air Force’s auxiliary cadet program
- Cybersecurity Labs - videos and hands-on activities from PBS NOVA Labs
- 20 Critical Security Controls - list of top industry-consensus best practices, from the Center for Internet Security (CIS)
- List of additional online resources from CyberPatriot
- *Cybersecurity for Dummies* free from Palo Alto Networks. (ISBN-13 978-1-119-25029-6)
- *An Introduction to Information Security* NIST SP 800-12 Rev. 1, from the National Institute for Standards and Technology - Computer Security Resource Center.

Vendor-Specific

These resources will assist the team in developing how-to guides for securing specific operating systems. Since the details of how to work with specific operating systems change more quickly than the merit badge pamphlet cycle, we recommend that this information be put on a companion website.

- Microsoft: Windows 8, Windows 10

- Ciprian Adrian Rusen and Joli Ballew, *Windows 8 Step by Step* (Microsoft Press, 2012)
- Joan Lambert, *Windows 10 Step by Step* (Microsoft Press, 2015)
- Woody Leonhard, "Securing Windows 10," *Windows 10 All-In-One For Dummies* (Wiley, 2016)
- Bob LeVitus, "Safety First: Backups and Other Security Issues," *macOS Sierra For Dummies* (Wiley, 2016)
- Bob LeVitus, "Safety First: Backups and Other Security Issues," *macOS High Sierra For Dummies* (Wiley, 2017)

Mobile Device Security

- Mobile device security tips - guide from the Privacy Rights Clearinghouse
- Mobile device security guidelines from MIT's Information Systems and Technology office

Internet of Things

- YouTube video: IBM How It Works: Internet of Things video
- YouTube video: How the Internet of Things Will Change the World
- YouTube video: Making the Internet of Things Safe

Cybersecurity Activities

While Scouts working on this badge would not be required to participate in any specific outside activity, they are encouraged (via an optional requirement) to explore which options are out there for them if they wish to do more. These are just some of the cybersecurity competitions and camps they could consider, all of which are available at no or low cost to the student:

- CyberPatriot - With over 5,600 teams in 2017 and growing every year, this is the big one. Teams are available at hundreds of schools, JROTC and Civil Air Patrol units, and other youth groups nationwide at no or very low

cost to the youth. Scout troops are also eligible to field teams (several have done so already), at a relatively minimal cost.

- picoCTF - A "capture the flag" style security game, specifically designed for middle and high school students. FREE.
- Cyber Aces - FREE online cybersecurity courses from top instructors at the SANS Institute, plus a quiz-based competition.
- GenCyber - An NSA-sponsored program of locally funded camps run by universities and other organizations around the country. FREE to attendees.
- AFA CyberCamp - A program created by CyberPatriot that can be used to run local camps hosted by any interested organization. In its fourth year, there are already 160 camps.[26] Participant fees are set by the hosting organization and will vary.

Careers

The CyberSeek website (www.cyberseek.org) – supported by CompTia, Burning Glass Technologies, and the U.S. government's National Initiative for Cybersecurity Education (NICE) – interactively shows where cybersecurity jobs are located in the United States and also shows career pathways within the cybersecurity profession.

List of 20 information security jobs, with brief descriptions, from SANS Cyber Aces: http://www.cyberaces.org/careers.

The National Security Agency (NSA) sponsors an online program called "Day of Cyber" to give students an "online, interactive cyber career exploration experience." Students, either individually or as part of a classroom group, explore cyber careers by virtually shadowing six NSA cyber professionals. https://www.nsadayofcyber.com/

---

[26] CyberPatriot Program Office. 2017. "CyberPatriot Impact Report."

Badge Design Ideas



The letters and numbers on these badge designs are a hexadecimal representation of “Boy Scouts of America” in ASCII.

Sponsoring Organizations

(ISC)²

(ISC)² is an international non-profit 501(c)(6) membership association focused on inspiring a safe and secure cyber world. Best known for the acclaimed Certified Information Systems Security Professional (CISSP®) certification, (ISC)² offers a portfolio of credentials that are part of a holistic, programmatic approach to security. Our membership, over 130,000 strong, is made up of certified cyber, information, software and infrastructure security professionals who are making a difference and helping to advance the industry. You can learn more by going to www.isc2.org.

Center for Cyber Safety and Education

The **Center for Cyber Safety and Education** (Center), is a non-profit 501(c)(3) charitable trust committed to making the cyber world a safer place for everyone. We work to ensure that people across the globe have a positive and safe experience online through our educational programs, scholarships, and research. We are the charitable trust of (ISC)², whose dedication to our mission has been an inspiring example to the cybersecurity industry.

ISSA Education Foundation

The **Information Systems Security Association Education Foundation** (ISSAEF), is a non-profit 501(c)(3) charitable foundation which fosters, supports, develops and provides education and training in matters involving information security and its applications. A main focus of the foundation is to provide scholarships to students seeking a career in cyber security. ISSAEF is associated with the international Information Systems Security Association (ISSA), with over 10,000 members and chapters worldwide. You can learn more by visiting issaef.org.

Authors

Primary Authors

Michael H. Dunn, CISSP, GISP, GCIH—Eagle Scout; cyberspace operations officer, U.S. Air Force; graduate student and researcher, Air Force Institute of Technology; CyberPatriot coach and Civil Air Patrol educational programs volunteer

Robert J. Caruso, CISSP, CRISC, GMOB—Application security architect, West Monroe Partners, LLC.; inventor and software product developer; CyberPatriot mentor and lifelong Scouter; co-author, *Digital Technology* and *Programming* merit badge pamphlets; BSA Cyber Chip co-developer

Contributors / Team Members

Patrick T. Craven—Eagle Scout; Director, Center for Cyber Safety and Education; professional Scouter for 24 years; former Scout Executive

Lorraine Frost, PMP, CSM, CISM—Chief Information Officer, Mount Saint Mary's University; Board of Directors, ISSA Educational Foundation

Laurence D. Merkle, Ph.D.—Eagle Scout; Assistant Professor of Computer Science, Air Force Institute of Technology; Troop Advancement Coordinator, Merit Badge Counselor, and father of a soon-to-be Eagle Scout

Jason M. Pittman, Sc.D.—Professor of Cybersecurity, Capitol Technology University; Director, Research Institute for Synthetic Intelligence Safety and Trust; cyber science researcher; cybersecurity competition mentor and coach; former Scouter

Allen Stubblefield—Cybersecurity middle and high school coach and high school cybersecurity teacher; 2016 CyberPatriot National Coach of the Year; coaches the largest CyberPatriot program in the United States; former Scouter

Ray Trygstad—Industry Professor of Information Technology and Management, Illinois Institute of Technology; Associate Director, Center for Cyber Security and Forensics Education, Illinois Institute of Technology; Co-Chair, 2018 National Women in Cyber Security (WiCyS) Conference; Life Scout and former Scouter

Scott G. Wyatt, CISSP—Eagle Scout; Senior Security Analyst, Boy Scouts of America; Crew Associate Advisor, Chartered Org Representative, Merit Badge Counselor.

Bibliography

[1] Center for Cyber Safety and Education, (ISC)2, and Frost & Sullivan, "2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk," 2017.

[2] Commission on Enhancing National Cybersecurity, "Report on Securing and Growing the Digital Economy," 2016.

[3] Booz Allen Hamilton, "2017 Global Information Security Workforce Study: U.S. Federal Government Results," 2017.

[4] J. Lewis and S. Baker, "The Economic Impact of Cybercrime and Cyber Espionage," Washington, DC, 2013.

[5] D. Jarvis, "Statement for the Record: Public-Private Solutions to Educating a Cyber Workforce," 2017.

[6] U.S. President, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, Exec. Order 13800," *Federal Register*, vol. 82, no. 93. Government Printing Office, Washington, DC, pp. 22391–22397, May-2017.

[7] U.S. President, "National Security Strategy of the United States of America," Washington, DC, 2017.

[8] U.S. Joint Chiefs of Staff, "The National Military Strategy of the United States of America," Washington, DC, 2015.

[9] U.S. Department of Defense, "Department of Defense Cyberspace Workforce Strategy." 2013.

[10] A. Corrin, "Basic training enters unfamiliar territory in cyberspace," *Defense Systems*, 2011. [Online]. Available: https://defensesystems.com/articles/2011/11/28/feat-military-cyber-training.aspx. [Accessed: 10-Aug-2017].

[11] U.S. Air Force Headquarters/Force Management Policy Division, "FY18 INITIAL ENLISTMENT BONUS (IEB) ANNOUNCEMENT MESSAGE." 2017.

[12] D. Vergun, "Army to direct commission cyber officers," *United States Army*, 2017. [Online]. Available: https://www.army.mil/article/197691/army_to_direct_commission_cyber_officers. [Accessed: 23-Jan-2018].

[13] Frost & Sullivan, Center for Cyber Safety and Education, (ISC)2, and Executive Women's Forum on Information Security Risk Management & Privacy, "The 2017

Global Information Security Workforce Study : Women in Cybersecurity," 2017.

[14] M. M. McGill, A. Decker, and A. Settle, "Undergraduate Students' Perceptions of the Impact of Pre-College Computing Activities on Choices of Major," *ACM Trans. Comput. Educ.*, vol. 16, no. 4, p. Article 15, Jun. 2016.

[15] T. McEwan and A. McConnell, "Young people's perceptions of computing careers," in *2013 IEEE Frontiers in Education Conference (FIE)*, 2013, pp. 1597–1603.

[16] Katzcy Consulting, "Cybersecurity Games: Building Tomorrow's Workforce," 2016.

[17] P. Pusey, M. Gondree, and Z. Peterson, "The Outcomes of Cybersecurity Competitions and Implications for Underrepresented Populations," *IEEE Security & Privacy*, vol. 14, no. 6, pp. 90–95, 2016.

[18] C. Eagle, "Computer security competitions: Expanding educational outcomes," *IEEE Security & Privacy*, vol. 11, no. 4, pp. 69–71, 2013.

[19] D. Jacobson and J. A. Rursch, "Engaging Millenials with Information Technology : A Case Study Using High School Cyber Defense Competitions," in *CISSE '08 - Proceedings of the 12th Colloquium for Information Systems Security Education*, 2008, pp. 59–65.

[20] G. B. White, D. Williams, and K. Harrison, "The CyberPatriot National High School Cyber Defense Competition," *IEEE Security & Privacy*, vol. 8, no. 5, pp. 59–61, 2010.

[21] CyberPatriot Program Office, "National Youth Cyber Defense Competition Registration Report: 2016-2017," 2017.

[22] Air Force Association, "Air Force Association's CyberPatriot: The National Youth Cyber Education Program," 2017. [Online]. Available: http://uscyberpatriot.org/. [Accessed: 20-Nov-2017].

[23] B. L. Barber, M. R. Stone, and J. S. Eccles, "Protect, Prepare, Support, and Engage: The Roles of School-Based Extracurricular Activities in Students' Development," in *Handbook of Research on Schools, Schooling, and Human Development*, J. L. Meece and J. S. Eccles, Eds. New York: Routledge, 2010, pp. 366–378.

[24] A. Sahin, "STEM Clubs and Science Fair Competitions: Effects on Post-Secondary Matriculation," *J. STEM Educ. Innov. Res.*, vol. 14, no. 1, pp. 2–3, 2013.

[25] S. Garg, “Expanding high school STEM literacy through extra-curricular activities,” in *5th IEEE Integrated STEM Education Conference*, 2015, pp. 276–281.

[26] J. Vennix, P. den Brok, and R. Taconis, “Perceptions of STEM-based outreach learning activities in secondary education,” *Learn. Environ. Res.*, vol. 20, no. 1, pp. 21–46, 2017.

[27] D. T. Sciarra, H. J. Seirup, and E. Sposato, “High School Predictors of College Persistence: The Significance of Engagement and Teacher Interaction,” *Prof. Couns.*, vol. 6, no. 2, pp. 189–203, 2016.

[28] E. T. Pascarella and P. T. Terenzini, *How college affects students: A third decade of research (Vol. 2)*. San Fransisco, CA: Jossey-Bass Higher & Adult Education, 2005.

[29] G. D. Kuh, T. M. Cruce, J. Kinzie, and R. M. Gonyea, “Unmasking the Effects of Student Engagement on First-Year College Grades and Persistence Unmasking the Effects of Student Engagement on First-Year College Grades and Persistence,” *J. Higher Educ.*, vol. 79, no. 5, pp. 540–563, 2008.

[30] S. Deterding, “Gamification: Designing for Motivation,” *Interactions*, vol. 19, no. 4, ACM, pp. 14–17, Jul-2012.

[31] J. Hamari, J. Koivisto, and H. Sarsa, “Does Gamification Work? — A Literature Review of Empirical Studies on Gamification,” in *Proceedings of the 47th Hawaii International Conference on System Sciences*, 2014, pp. 3025–3034.

[32] M. A. Ozturk and C. Debelak, “Affective Benefits From Academic Competitions for Middle School Gifted Students,” *Gift. Child Today*, vol. 31, no. 2, pp. 48–53, 2008.

[33] M. R. Lepper, “Social-control processes and the internalization of social values: An attributional perspective,” in *Social Cognition and Social Development: A Sociological Perspective*, E. T. Higgins, D. N. Ruble, and W. W. Hartup, Eds. New York: Cambridge University Press, 1983, pp. 294–330.

[34] W. Damon, *Greater Expectations: Overcoming the Culture of Indulgence in America’s Homes and Schools*. New York: Free Press, 1995.

[35] G. A. Davis and S. B. Rimm, *Education of the Gifted and Talented*, 5th ed. New York: Pearson, 2004.

[36] K. Bishop and H. Walters, “The National Ocean Sciences Bowl: Extending the Reach of a High School Academic Competition to College, Careers, and a Lifelong Commitment to Science,” *Am. Second. Educ.*, vol. 35, no. 3, pp. 63–76,

2007.

[37] T. V. Abernathy and R. N. Vineyard, “Academic Competitions in Science: What Are the Rewards for Students?,” *Clear. House A J. Educ. Strateg. Issues Ideas*, vol. 74, no. 5, pp. 269–276, May 2001.

[38] C. C. Chung, C. Cartwright, and M. Cole, “Assessing the Impact of an Autonomous Robotics Competition for STEM Education,” *J. STEM Educ. Innov. Res.*, vol. 15, no. 2, pp. 24–34, 2014.

[39] J. R. Campbell and H. J. Walberg, “Olympiad Studies: Competitions Provide Alternatives to Developing Talents That Serve National Interests,” *Roeper Rev.*, vol. 33, no. 1, pp. 8–17, Dec. 2010.

[40] D. Ragsdale, “Evolution of Competition-Based Cybersecurity Education: Continuing to Inspire.” NICE 2017 Conference and Expo, Dayton, OH, 2017.

[41] “National Collegiate Cyber Defense Competition,” *National Collegiate Cyber Defense Competition*, 2017. [Online]. Available: http://www.nationalccdc.org/. [Accessed: 02-Mar-2018].

[42] National Cyber League, “NCL | National Cyber League | Ethical Hacking and Cyber Security,” 2017. [Online]. Available: https://www.nationalcyberleague.org/. [Accessed: 01-Jan-2018].

[43] D. H. Tobey, P. Pusey, and D. L. Burley, “Engaging learners in cybersecurity careers: Lessons from the launch of the national cyber league,” *ACM Inroads*, vol. 5, no. 1, pp. 53–56, Mar-2014.

[44] “GenCyber,” 2017. [Online]. Available: https://www.gen-cyber.com/. [Accessed: 31-Dec-2017].

[45] NYU Tandon School of Engineering, “High School Forensics,” *Cyber Security Awareness Week*, 2017. [Online]. Available: https://csaw.engineering.nyu.edu/hsf. [Accessed: 06-Sep-2017].

[46] G. B. White, D. Williams, and K. Harrison, “Developing a National High School Cyber Defense Competition,” in *CISSE ’10 - Proceedings of the 14th Colloquium for Information Systems Security Education*, 2010, pp. 83–89.

[47] CyberPatriot Program Office, “CyberPatriot X: National Youth Cyber Defense Competition Rules and Procedures.” The Air Force Association, Arlington, VA, 2017.

[48] M. Bashir, C. Wee, N. Memon, and B. Guo, “Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of

competitions as a recruitment tool," *Comput. Secur.*, vol. 65, pp. 153–165, Mar. 2017.

[49] L. Amo, "Addressing Gender Gaps in Teens' Cybersecurity Engagement and Self-Efficacy," *IEEE Security & Privacy*, vol. 14, no. 1, pp. 72–75, 2016.

[50] M. Danforth and C. Lam, "Effects of a Four-Week Cyber Security Summer Program on the Attitudes and College Interests of High School Students," *J. Colloq. Inf. Syst. Secur. Educ.*, vol. 4, no. 2, pp. 75–93, Feb. 2017.

[51] "Annual Challenge," *Black T-Shirt Cyber Forensics Challenge*, 2017. [Online]. Available: https://cyberforensicschallenge.com/challenges/annual-challenge/. [Accessed: 04-Aug-2017].

[52] "Inaugural Black T-Shirt Cyber Forensics Challenge Winners Announced," *Stevenson University Online*, 2016. [Online]. Available: http://www.stevenson.edu/online/blog-news-events/cyber-forensics-challenge-2016. [Accessed: 05-Sep-2017].

[53] D. Manson, "CyberFed Episode 44," *The CyberFed Show*, 2015. [Online]. Available: https://www.youtube.com/watch?v=8PWxq5QU0j8. [Accessed: 09-Aug-2017].

[54] "Black T-Shirt Cyber Forensics Challenge," *Facebook*, 2016. [Online]. Available: https://www.facebook.com/BlackTshirtCyberForensicsChallenge/. [Accessed: 04-Aug-2017].

[55] Counter Hack Challenges, "Digital Forensics Security Treasure Hunt," *Security Treasure Hunt*, 2010. [Online]. Available: http://digitalforensics.securitytreasurehunt.com/. [Accessed: 16-Aug-2017].

[56] Counter Hack Challenges, "Security Treasure Hunt," *Security Treasure Hunt*, 2013. [Online]. Available: http://www.securitytreasurehunt.com/. [Accessed: 16-Aug-2017].

[57] D. Manson, "CSSIA's Youth Forensics Competition (Episode 26)," *The CyberFed Show*, 2015. [Online]. Available: https://www.youtube.com/watch?v=5NsA_yvujUI. [Accessed: 11-Aug-2017].

[58] Digital Forensics Consortium, "Digital Crime Scene Challenge," *Digital Forensics Consortium*. [Online]. Available: http://www.usdfc.org/digital-crime-scene-challenge.html. [Accessed: 11-Aug-2017].

[59] Digital Forensics Consortium, "US Digital Forensics Challenge," *Digital Forensics Consortium*. [Online]. Available: http://www.usdfc.org/us-digital-forensics-challenge.html. [Accessed: 11-Aug-2017].

[60] D. Manson, “Top Picks for NCCDC and Information on Digital Forensics Forum (Episode 14),” *The CyberFed Show*, 2015. [Online]. Available: https://www.youtube.com/watch?v=ISnBBp9jdGY. [Accessed: 11-Aug-2017].

[61] “Digital Forensics Consortium,” *Facebook*, 2016. [Online]. Available: https://www.facebook.com/usdfc/. [Accessed: 11-Aug-2017].

[62] Civil Air Patrol Cyber Defense Training Academy, “cap-cdta/cyber-forensics-challenge,” *GitHub*, 2016. [Online]. Available: https://github.com/cap-cdta/cyber-forensics-challenge. [Accessed: 15-Aug-2017].

[63] Civil Air Patrol Cyber Defense Training Academy, “cap-cdta/cyber-forensics-challenge/ChallengePriceListing.pdf,” *GitHub*, 2016. [Online]. Available: https://github.com/cap-cdta/cyber-forensics-challenge/blob/master/ChallengePriceListing.pdf. [Accessed: 15-Aug-2017].

[64] “Khan Academy,” 2018. [Online]. Available: https://www.khanacademy.org/. [Accessed: 18-Jan-2018].

[65] S. Abramovich, C. Schunn, and R. M. Higashi, “Are badges useful in education?: It depends upon the type of badge and expertise of learner,” *Educ. Technol. Res. Dev.*, vol. 61, no. 2, pp. 217–232, 2013.

[66] B. B. Morrison and B. DiSalvo, “Khan Academy Gamifies Computer Science,” in *SIGCSE ’14 - Proceedings of the 45th ACM Technical Symposium on Computer Science Education*, 2014, pp. 39–44.

[67] B. Alberts, “An Education that Inspires,” *Science (80-.).*, vol. 330, no. 6003, p. 427, 2010.

[68] R. Hintz, “Science Education in the Boy Scouts of America,” The Ohio State University, 2009.

[69] R. Hintz and B. Thomson, “Geoscience Education in the Boy Scouts of America,” *J. Geosci. Educ.*, vol. 60, no. 2, pp. 159–167, 2012.

[70] B. R. Maxim and B. S. Elenbogen, “Attracting K-12 Students to Study Computing,” in *39th ASEE/IEEE Frontiers in Education Conference*, 2009, p. M1H 1-5.

[71] Girl Scout Research Institute, “How Girl Scout STEM Programs Benefit Girls,” New York, NY, 2016.

[72] Girl Scout Research Institute, “The Girl Scout Impact Study,” New York, NY, 2017.

[73] Girl Scout Research Institute, “Girl Scouting Works: The Alumnae Impact Study,” New York, NY, 2012.

[74] Palo Alto Networks, “Palo Alto Networks and Girl Scouts of the USA Announce Collaboration for First-Ever National Cybersecurity Badges.” Santa Clara, CA, 2017.

[75] Boy Scouts of America, “Merit Badges,” *Boy Scouts of America*, 2017. [Online]. Available: https://www.scouting.org/Home/BoyScouts/AdvancementandAwards/MeritBadges.aspx. [Accessed: 18-Jan-2018].

[76] Boy Scouts of America, *Digital Technology (Merit Badge Series)*. Irving, TX: Boy Scouts of America, 2014.

[77] Boy Scouts of America, *Programming (Merit Badge Series)*. Irving, TX: Boy Scouts of America, 2013.

[78] Boy Scouts of America, “Cyber Chip.” [Online]. Available: www.scouting.org/cyberchip. [Accessed: 15-Nov-2017].

[79] BSA Merit Badge Task Force, “Counselor’s Compass, Vol. 1, No. 1.” Boy Scouts of America, Irving, TX, 2014.

[80] “Current Merit Badge Pamphlet and Requirement Revision Dates,” *U.S. Scouting Service Project*, 2018. [Online]. Available: http://usscouts.org/mb/mbbooks.asp. [Accessed: 21-Jan-2018].

[81] A. All, E. P. N. Castellar, and J. Van Looy, “Towards a conceptual framework for assessing the effectiveness of digital game-based learning,” *Comput. Educ.*, vol. 88, pp. 29–37, 2015.

[82] H. Walters and K. Bishop, “Assessing the Impact of the National Ocean Sciences Bowl : A Systems Approach Final Report,” 2004.

[83] H. Walters, K. Bishop, and R. Wlodarsky, “Assessing the Impact of the National Ocean Sciences Bowl (NOSB®): A Systems Approach,” Mar. 2006.

[84] M. K. Tallent-Runnels and A. C. Candler-Lotven, *Academic Competitions for Gifted Students: A Resource Book for Teachers and Parents*, 2nd ed. Thousand Oaks, CA: Corwin Press, 2008.

[85] J. S. Eccles, “Why doesn’t Jane run? Sex differences in educational and occupational patterns,” *The gifted and talented: Developmental perspectives*. 1985.

[86] J. Lupart and E. Cannon, “Gender differences in junior high school students

towards future plans and career choices," *Technol. Dev.*, 2000.

[87] CyberPatriot Program Office, "CyberPatriot Student Alumni Survey Report: 2016," Jul. 2016.

[88] CyberPatriot Program Office, "CyberPatriot Survey Results: CyberPatriot VI Post-Season Competitor Survey 2013-2014 and CyberPatriot Student Alumni Survey 2014," Jun. 2014.

[89] CyberPatriot Program Office, "CyberPatriot Impact Report," 2017.

[90] J. Cohen, *Statistical Power Analysis for the Behavioral Sciences*, 2nd ed. Hillsdale, NJ: Lawrence Erlbaum Associates, 1988.

[91] National Security Agency, "Academic Requirements for Designation as a CAE in Cyber Operations Fundamental," *NSA | CSS*, 2017. [Online]. Available: https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-operations/fundamental/requirements.shtml. [Accessed: 15-Feb-2018].

[92] "The History of Carmen Sandiego," *Houghton Mifflin Harcourt*. [Online]. Available: http://www.hmhco.com/at-home/featured-shops/the-learning-company/carmen-sandiego/history. [Accessed: 10-Jan-2018].

[93] Boy Scouts of America, "2016 Annual Report," Irving, TX, 2016.

[94] D. Stopnick, "New Merit Badge Brings Welding to Scouts," *American Welding Society*, 2013. [Online]. Available: http://www.aws.org/resources/detail/new-merit-badge-brings-welding-to-scouts. [Accessed: 28-Jul-2017].

[95] Boy Scouts of America, "Merit Badge Proposal form." 2016.

[96] T. M. Akey, "School Context, Student Attitudes and Behavior, and Academic Achievement: An Exploratory Analysis," 2006.

[97] Air Force Association, "CyberPatriot Breaks Registration Record Again." Arlington, VA, 2017.

[98] B. Wendell, "2016 Merit Badge Rankings unveiled: These were the most and least popular," *Bryan on Scouting*, 2017. [Online]. Available: https://blog.scoutingmagazine.org/2017/03/23/2016-merit-badge-rankings-unveiled-these-were-the-most-and-least-popular/. [Accessed: 16-Nov-2017].

[99] Burning Glass and CompTIA, "Cybersecurity Supply/Demand Heat Map," *CyberSeek*, 2017. [Online]. Available: http://cyberseek.org/heatmap.html. [Accessed: 16-Nov-2017].

[100] Air Force Association, “Sponsors,” *Air Force Association’s CyberPatriot: The National Youth Cyber Education Program*. [Online]. Available: http://uscyberpatriot.org/about/sponsors. [Accessed: 02-Dec-2017].

[101] M. H. Dunn and L. D. Merkle, “Assessing the Impact of a National Cybersecurity Competition on Students’ Career Interests,” in *SIGCSE ’18 - Proceedings of The 49th ACM Technical Symposium on Computing Science Education*, 2018, pp. 62–67.

[102] Microsoft, “Hard Links and Junctions,” *Windows Dev Center*. [Online]. Available: https://msdn.microsoft.com/en-us/library/windows/desktop/aa365006(v=vs.85).aspx. [Accessed: 05-Feb-2018].

[103] M. H. Dunn, R. J. Caruso, L. D. Merkle, and R. Trygstad, “Proposed Cybersecurity Merit Badge for the Boy Scouts of America (Poster),” in *SIGCSE ’18 - Proceedings of The 49th ACM Technical Symposium on Computing Science Education*, 2018, p. 1085.

Vita

Captain Michael H. Dunn graduated from the Illinois Institute of Technology (IIT), Chicago, Illinois, in May 2010 with a Bachelor of Science in Computer Science and a Specialization in Information Security. He was commissioned through Air Force ROTC Detachment 195 at IIT. In December, he was awarded a Master of Public Administration degree from IIT's Stuart School of Business.

Captain Dunn graduated at the top of his class from Undergraduate Cyber Training at Keesler AFB, Mississippi, in May 2011. He was assigned to the 432d Aircraft Communications Maintenance Squadron at Creech AFB, Nevada, where he served as Assistant Officer-in-Charge of the Systems Maintenance Unit, managing maintenance of Ground Control Stations for MQ-1/MQ-9 remotely piloted aircraft (RPA) global combat operations. In October 2013 Captain Dunn was transferred to the 99th Communications Squadron, Nellis AFB, Nevada, as the Plans and Resources (SCX) Flight Commander, and later the Operations (SCO) Flight Commander. While stationed at Nellis AFB, he deployed to Al Udeid Air Base, Qatar, where he worked at the Combined Air Operations Center as a cyber operations planner and liaison.

Following graduation from the Air Force Institute of Technology, Captain Dunn will return to Keesler AFB to serve as an instructor for Undergraduate Cyber Training.

In addition to his academic credentials, Captain Dunn also holds multiple information security certifications, including Certified Information Systems Security Professional (CISSP) and GIAC Certified Incident Handler (GCIH).

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From – To)*
22-03-2018	Master's Thesis	September 2016 – March 2018

4. TITLE AND SUBTITLE

Assessing and Expanding Extracurricular Cybersecurity Youth Activities' Impact on Career Interest

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Dunn, Michael H., Captain, USAF

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT-ENG-MS-18-M-021

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force STEM Outreach Program Office
ATTN: Victoria S. Stoneking
1864 4th Street
WPAFB, OH 45433
(937) 656-4868 (DSN 986-4868), victoria.stoneking@us.af.mil

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL/EN

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
DISTRUBTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES
This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

14. ABSTRACT
This thesis assesses and expands the potential of extracurricular activities to address the shortage of cybersecurity workers by increasing secondary school students' interest in these careers. Competitions and badges, two forms of gamification often applied in extracurricular educational activities, have potential to improve motivation and increase interest in related careers, but are significantly understudied in the context of cybersecurity activities. CyberPatriot is the largest cybersecurity competition in the United States for secondary school students. Impact on participants' career interests is assessed by analyzing responses to recent surveys conducted by the competition organizers. Analysis demonstrates significantly increased interest in cybersecurity in several dimensions relevant to career selection, significantly larger increases for females than males, and persistence of increased interest over time. A survey of U.S. Air Force enlisted members is designed to gauge the impact of cyber-related education activities on developing its cyber workforce. Cybersecurity activity options are expanded by creating a flexible age-appropriate digital forensics activity in which students analyze forensic evidence in folders and files, reconstructing user activity to answer some basic questions. A cybersecurity merit badge is proposed for the Boy Scouts of America with suggested requirements modeled on other successful technology-related merit badges.

15. SUBJECT TERMS
cybersecurity education, K-12 education, extracurricular activities, competitions, badges, career choice, gender, digital forensics, CyberPatriot, Boy Scouts of America

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Dr. Laurence D. Merkle, AFIT/ENG
U	**U**	**U**	**UU**	201	**19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-6565, ext 4526 laurence.merkle@afit.edu

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39-18