CYBERSECURITY PEDAGOGY & PRACTICE JOURNAL

Volume 2, No. 2
September 2023
ISSN: 2832-1006

In this issue:

iscap
Information Systems & Computing Academic Professionals

The **Cybersecurity Pedagogy and Practice Journal** (**CPPJ**) is a double-blind peer-reviewed academic journal published by **ISCAP** (Information Systems and Computing Academic Professionals). Publishing frequency is two times per year. The first year of publication was 2022.

CPPJ is published online (https://cppj.info). Our sister publication, the proceedings of the ISCAP Conference (https://proc.iscap.info) features all papers, panels, workshops, and presentations from the conference.

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the ISCAP conference. At that point, papers are divided into award papers (top 15%), and other accepted proceedings papers. The other accepted proceedings papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the CPPJ journal.

While the primary path to journal publication is through the ISCAP conference, CPPJ does accept direct submissions at https://iscap.us/papers. Direct submissions are subjected to a double-blind peer review process, where reviewers do not know the names and affiliations of paper authors, and paper authors do not know the names and affiliations of reviewers. All submissions (articles, teaching tips, and teaching cases & notes) to the journal will be refereed by a rigorous evaluation process involving at least three blind reviews by qualified academic, industrial, or governmental computing professionals. Submissions will be judged not only on the suitability of the content but also on the readability and clarity of the prose.

Currently, the acceptance rate for the journal is under 35%.

Questions should be addressed to the editor at editorcppj@iscap.us or the publisher at publisher@iscap.us. Special thanks to members of ISCAP who perform the editorial and review processes for CPPJ.

2023 ISCAP Board of Directors

CYBERSECURITY PEDAGOGY AND PRACTICE JOURNAL

Teaching Case

Applied Steganography: An Interesting Case for Learners of all Ages

Johnathan Yerby
yerby_jm@mercer.edu
Computer Science
Mercer University
Macon, GA 31005, USA

Jennifer Breese
jzb545@psu.edu
Information Systems Technology
Penn State Greater Allegheny
McKeesport, PA 15132, USA

Abstract

There is a need for interesting demonstrations to capture the attention of learners in the fields of cybersecurity and cyber forensics. The number of new systems and amount of data grows constantly and needs to be secured using cybersecurity proactively and cyber forensics reactively. There is a large and growing gap between people aware, interested, and skilled enough to meet the needs. The United States is working to create a pipeline of learners that go into cyber related fields. This case study is an example of an exercise that gains the attention, interest, and positive feedback of students from middle school to college graduates. The exercise is a demonstration of steganography and only requires a computer and free software. The activity is tailorable for each audience with little preparation. The concept is simple, take a file, hide a message inside that is undetectable, then have the learners find the hidden information using software and passwords. Although the exercise is simple, it effectively gains students' attention and interest in the fields of cybersecurity and forensics and becomes the catalyst to have them imagine a new future. This case study discusses how to execute the exercise, the evolution of this exercise over the last decade, and how to use the case to allure new learners into the cyber field of study.

Keywords: forensics, cybersecurity, steganography, learning, case study

1. INTRODUCTION

There is an immense need for skilled cybersecurity professionals. Currently, K-12 teachers do not have exposure or skills to provide the inspiration and awareness for a career in cybersecurity. Time and funding are constraints that prevent cybersecurity from being introduced and practiced in K-12 and many workplaces. Students need to be introduced to, trained, and educated in the field of cybersecurity. There are barriers for K-12 teachers to be prepared to teach a field that is foreign to them as teachers, but also within the systems in which they are employed. Education is one of the least secure industries as a whole and a common target (Yerby & Floyd, 2018; Zimmerman, 2018). Practicing and teaching cybersecurity practices within educational institutions has not been the top priority for teachers and staff; instead they are focused on the roles that they are directly tasked with (Yerby & Floyd, 2018). From teaching to practicing principles, cybersecurity has not been a priority. Schools are looking for ways to fix the issues through training, awareness, education, and using modern technologies.

In the article *Children are the future of cybersecurity,* Webster (2017) described the paradox of high salary, secure jobs with great benefits, and a massive gap of skilled workers to fill the needs. Teenagers are not aware or confident that they could become a cybersecurity professional. Webster (2017) pointed out that the cybersecurity field needs more hands-on and fun activities for young audiences. There is an increasing emphasis on getting learners from K-12 to college interested in and skilled enough to meet the cyber needs of our nation. In 2015 the National Security Agency started a program called GenCyber, with eight prototype camps (Dark, Daugherty, Dark, Albright, Brown, Emry, & McCallen, 2021). Camps goals were to increase interest and diversity in the cybersecurity workforce of the nation, understand safe online behavior, and improve teaching methods for delivering cybersecurity content in K-12 curricula (Dark et al., 2021).

In the five years since the inception of GenCyber, 15,545 students attended cybersecurity camps at no cost. Another ongoing effort is Cyber.org, funded by the Department of Homeland Security (DHS) and the Cybersecurity Infrastructure and Security Agency (CISA)'s Cybersecurity Education Training Assistance Program (CETAP) grant (Noland, 2020). The group is working on preparing teachers, to prepare their K-12 students to meet the cybersecurity needs of the nation (Noland, 2020).

Cybersecurity is becoming more mainstream as represented in the plots of movies, television, and streaming service shows. Often media misrepresents reality of the field, which could help or hinder attaining a person's interest in the field, especially when reality falls short of dramatized expectations. A study examined numerous publications and found the literature to be mixed if there was a Tech-effect when reality and media representations mismatched (Paullet, Davis, McMillion, & Yerby, 2013). Educators should offer interesting and honest hands-on learning opportunities to reach deeper levels of learning and engagement. A 2013 (Paullet et al.) study examined how a potential tech-effect influenced jurors and found that an increased exposure to technology correlated with higher acquittal rates where digital evidence was used. Careful work must be done to introduce and positively present options in the broad field of cybersecurity. If reality is never presented to students from K-12 to college, they will not know if it is a field for which in which they may excel.

While students are being introduced to the concepts and ideas of what the field of cybersecurity entails, they need a realistic honest conceptual framework. Educators must be honest about the pros, cons, opportunities, and challenges of pursuing a life of learning and working in the field of cybersecurity. Cybersecurity is broad and ranging from technical to non-technical, frameworks, theoretical models, governance, physical security, sales, engineering, security architecture, forensics, to social engineering to name just some of the niches of the field. Again, how concepts or the field is introduced can influence the likelihood of sustained interest in becoming a cybersecurity professional. In a study with UK teachers of students 12–16 years-old, researchers found students feel more tech savvy than the teachers because they have grown up with technology, believe that hacking is glamorous, and are naive about how invincible they are online (Pencheva, Hallett, & Rashid, 2020).

The teachers point out that students are not technically aware of foundational cybersecurity concepts and that there is no adequate adult support network (Pencheva, et al., 2020). Using application-level learning has proven to engage students, especially when learning cybersecurity concepts (Nygard, Chowdhury, Kambhampaty, & Kotala, 2018). Using hands-on exercises following skills that would be used in real work is helpful. Deeply engaging students transfer knowledge, use it, and synthesize what they have learned (Nygard et al., 2018). Educators should strive to have engaged students and find the methods that reach their learners.

This case study explains how this unique exercise has been successfully used on learners from middle and high school through college students and parents. We began the study out of one exercise of over twenty in a cyber forensics course but noticed that there was something different about how this particular topic and technique resonated with learners. Future needs for recruiting events and building cyber related programs at multiple other schools led the authors and several colleagues to turn to this exercise.

The literature shows that Information Technology is a program that can be equally effectively delivered online or face-to-face (Yerby & Floyd, 2013). This is an exercise that is adaptable to in-person and online either synchronous, asynchronously, as an assignment, and as an interactive discussion. Overall, the entire exercise is very adaptable.

2. OVERVIEW

This exercise was created to meet several needs of a growing cybersecurity program, cyber forensics program, recruiting and outreach to students from middle school to college, and to increase interest and awareness of cybersecurity and cyber forensics as career opportunities. This is a simple lab to grab the attention of learners from middle school to adults and introduce them to something interesting and new. This steganography exercise uses a free website, a file, three passwords, and free software that can be run on a Windows PC.

The exercise began as one of many labs in an introduction to cyber forensics course. The reaction from the students was so overwhelmingly positive that the exercise went on to be demonstrated over 50 times in the intro to forensics class, cybersecurity classes, and a modified version in the intro to IT class as a preview of what students would learn if they decided to pursue the concentration in forensics or cybersecurity.

The exercise affords the demonstrator a large amount of flexibility on the inputs, outputs, and time that they wish to spend on the topic.

Before starting the assignments, the instructor should define and discuss the term steganography. Steganography is a technique to hide information in plain sight. In our case we will be using an image file to hide text, utilizing software.

Students of all ages are creative with thinking of nefarious and honest uses for hiding information within another file. Some examples that instructors may bring forth to discuss include:

1. Avoiding censorship
2. Watermarking to prove ownership or authenticity
3. Intellectual property protection or tracking
4. Store information on location
5. Terrorism
6. Exploitation

Students can begin with a prescribed set of inputs and outputs, detailed in Assignment 1 (Appendix B), then extend the exercise such as in Assignment 2 (Appendix C). After completing the exercise, the instructor has additional flexibility to introduce new related topics for the scenario of used in recruiting, capture-the-flag cyber competitions, in courses such as intro to IT, intro to forensics, or cybersecurity. The demonstration that has worked well over 50 times by one of the authors, and the second author over 20 times. Other instructors at other institutions have all reported positive findings and student interactions as well.

3. STEGANOGRAPHY

Steganography, the term translated from Greek means "covered writing" and is different from encryption which means "secret writing" in Greek (Khan, 1996). The introduction of this exercise was the first instance most students have ever heard of the term steganography, and commonly misheard it as stenography, which is recording spoken word, typically in a courtroom setting. Steganography is a technique to hide information in plain sight, it is a science of invisible communication (Singh & Singh, 2018). The term dates to the fifth century BC, where according to author Herodotus, messages would be tattooed onto shaved heads of a servant, and then once the hair grew back, the message would be sent (Khan, 1996). Steganography is a new fascinating topic to students and teachers. Diving into the possibilities of the ancient data hiding method inspires engaged discussions related to spy craft, invisible ink, criminal behavior, watermarking, and animal behavior before moving into anything related to technology.

In cyber related terms, steganography uses a cover, the hidden message, and sometimes also requires a key. The cover is an innocent looking file or set of files, which would be of no apparent value or danger if it were intercepted and viewed by an adversary. The cover file is intentionally designed to appear to have nothing suspicious. The hidden message can be text, cypher-text, other images, or anything that can be embedded into the cover file (Johnson & Jajodia, 1998; Hamid, 2018). The best files to use as covers are lossless files such as BMP and GIF, because there is information that can be replaced, compressed, or removed with less noticeable results to the image (Singh & Singh, 2018).

Students need the correct software to complete the process. There are many programs that perform steganography detailed in Table 1. Openpuff was used for this exercise; however, it can be adapted to use any of the software listed above. The interface of each program varies. The software typically has the cover file identified by the user first, then the hidden information is selected. Users complete the process by entering a key, which is a single or series of passwords. Then the software executes to create a stego-file. The stego-file looks remarkably like the cover file; however, it now has hidden information. The stego-file can be examined and usually the difference in imperceptible to the human eye. Some of the properties of the file may have changed and changes depending on several variables such as the software, size and format of the cover and hidden message.

Tool	Windows	Linux	Mac	Function
Camouflage	x			Data Hiding, Encryption
Crypture	x			Encrypt, Header modification, save as bmp
DeepSound	x			Data Hiding in Audio
Hide & Send	x			Data Hiding, Encryption
Image Steganography	x			Data Hiding, Encryption
iSteg			x	Data Hiding, Encryption
matroschka		x		Command line Data Hiding, Encryption
Openpuff	x			Data Hiding, Encryption
OpenStego	x	x	x	Data Hiding, Watermarking
OurSecret	x			Data Hiding, Encryption
Outguess			x	Data Hiding, Encryption
Rizzy built on Stepic		x		Data Hiding
SSuite Picsel Security	x			Data Hiding, Encryption
Steg		x		Data Hiding, Encryption
Steganograph XPlus	x			Data Hiding, Encryption
SteganPEG	x			Data Hiding multiple files
StegCloak	x	x	x	Web Interface, Data Hiding, Watermarking
Steghide	x	x		Data Hiding including audio files
Stegolego		x		Data Hiding in bmp only
S-tools	x			Data Hiding, Encryption
Xiao Steganography	X			Data Hiding in BMP and WAV, Encryption

TABLE 1: Free Steganography Tools by Platform and Functionality

Although the concept of steganography is ancient, it continues to be an effective method to covertly communicate or hide information. Just as there are dozens of software solutions dedicated to performing steganography (Table 1), there are also several programs designed to at least detect that a file has been subjected to steganography. At that point, it becomes a chore of trying to solve the type of encoding, which software, and version sometimes, and the keys. Steganography is often undetectable, and even when it is, the detection does not always result in uncovering the hidden message. For this exercise, students' imagination runs wild on the nefarious uses that they envision using this new skill to do good and harm in their world. The runaway conversations and freedom to use what they are beginning to understand hooks their attention.

4. EVOLUTION OF EXERCISE

The exercise began as a small piece of a greater lesson about data hiding techniques for a cyber forensics course in 2010. The instructor discussed several techniques during a lecture and then had multiple groups of students find a tool and perform the process as part of an in-class presentation. Something about this resonated more than most other topics. Students were captivated and continued discussing the lesson, tools, uses, and their genuine enjoyment. Soon students not even enrolled in the course were discussing steganography and using the method in other courses and created some online challenges for a capture-the-flag contest they were developing.

This simple exercise became a rite-of-passage when taking the intro to cyber forensics course. As time went on, there were some students in the class that already knew about the exercise and had practiced, because they found out from a friend. However, that did nothing to detract from the interest of other students and in fact created a more robust discussion and a drive for the students to push the technique further and challenge one another. Around the same time the instructor was working on creating something as a short demonstration for open house recruiting events and decided to use steganography.

Comments from students:

> Steganography -- It was interesting to see how the OpenPuff application worked and get some hands-on experience.
>
> When it came to the steganography module, I found it interesting how hidden information can be placed within low-quality images and other files. After watching the videos on how steganography works, I was able to determine that some organizations or criminals may use steganography to hide licensing information or secret files that will be concealed from the naked eye unless the individual has the software to find the hidden information. I enjoyed how we were able to use a hands-on tool to hide a document within a photo and also find hidden information in my classmates' files.
>
> I was a criminal justice major when I learned about how to do steganography, I had to switch majors to forensics this semester.

The authors have used this demonstration or exercise more than seventy times with remarkable success. It has been used in courses focused on cyber forensics, cybersecurity, and introduction to IT. The abbreviated lesson can be demonstrated as quickly as 5 minute “trick” and then discussion can ensue afterwards; the lesson worked. The activity has been performed for and by hundreds of people open house recruiting events, K-12 outreach, assignments, and sharing with colleagues as something clever that has students engaged.

In 2013, the instructor created a Weebly website with three videos and a hands-on portion for student to complete (Yerby, 2013). The first video (2-minutes) covered the background of steganography. The second video (9-minutes) was an instructor walk through of a similar exercise using a different, but analogous tool that students were expected to utilize in their hands-on portion. The exercise in the demonstration was based on a hands-on exercise from the textbook *Guide to Computer Forensics and Investigations* (Nelson, Phillips, & Steuart, 2009). The third and final video was a follow-up instructor led video providing additional steganography learning material.

The reason this method was used is because it is impactful yet simple to grasp. It is hands-on and does not require a lengthy period of planning or technology acquisition. This exercise adds time for critical thinking and creativity which allows learners to have fun with the topic and even think as an adversary. In the second portion of the assignment students have flexibility to turn the challenge into a game to see how difficult or how fast they can solve one another’s challenges.

The hands-on exercise on the website provides hints for completion but allows for free-thinking and problem solving by student participants. The exercise underwent peer review and was then reproduced with permission and shared multiple other channels including the Curriculum Standards series (National CyberWatch Center Curriculum, 2018). Educators have free access to utilize this activity.

Variations of the exercise included chapter readings in assigned course textbooks, instructor created capture-the-flag competition in class, and in class exercises (Nelson et. al., 2009 & 2018). Additionally, senior-level students were required to find their own cover image, hide a message, and provide the hints, including passwords, for peers to access the message with a response in a discussion post format with their Learning Management System. After posting the stegged images and enough hints to solve them, the students were expected to provide synopses about their thoughts on the pros and cons of using steganography. In-class or online discussions would ensue about the methods or tools each student chose to use. Sometimes the students would complain that there were not enough hints provided to decipher the stegged file. Students would discuss the challenges that they uncovered based on factors such as file size, file type, specific tool limitations, and the methods that each type of steganography tool was attempting to use. In some courses, the instructor gamified the submissions, to see which student could solve or uncover the most stegged files during a period of time. Although the method dates to the fifth century and this version of this exercise has been utilized for over a decade, there is something about it that remains fresh and engaging. Students are excited to win the challenge, to be first, or to make variations to make their version the best.

5. SET-UP

The straightforward implementation of the exercise involves reading, defining, and discussing what steganography is and additional applications of use. Students are encouraged to think about positive and negative utilization of the method. Students are asked if they believe they would be able to determine if there was hidden information in a file.

Students were directed to the Weebly page, http://yerby.weebly.com/forensics.html, as shown in Appendix A, or was embedded in the course Learning Management System (LMS). Then students use in-class time to try to be the first person to solve the challenge just using the limited information on the page. This gamification further creates a sense of interest and competitiveness.

After some students figured out the challenge, the instructor reviews the steps collectively. First, the students had to read carefully to download the correct software, which was Openpuff version 4. Some students may experience problems if they downloaded a different version or the wrong software altogether, such as S-tools, which was used in the demonstration video and is also available on the webpage. To solve the issue of the wrong version, simply guide the student to read the prompts more closely and use the correct version. Paying attention to details is a skill required to work in the fields of security and forensics. Once students run the correct version of the software, they need to provide the stego-file, which is a photo on the webpage. The photo is a German Shepherd dog, which came from an episode of *It's Always Sunny in Philadelphia* (Day, Howerton, & McElhenney, 2012). In the episode one of the characters used an old canvas to paint a new picture on, hence the nod to steganography. Students need to right-click on the webpage and save the image to their computer as secret.bmp, which is the existing name of the stego-file.

Next students execute the OpenPuff.exe file and select Unhide. They enter the three passwords which were given as "clues" on the webpage. If the passwords were copied incorrectly or an extra space is included, the uncovering does not work. To solve this issue, simply make sure that students are getting the passwords verbatim, with no additional spaces. Next students select Add carrier then select the previously downloaded secret.bmp file. At this point select Unhide on the Openpuff 4.0 interface, select a save location for the hidden message, and users are given a confirmation that "1/1 carrier processed." Clicking "OK" gives a summary of the process, including the name of the hidden data and the size. The file is saved, and the challenge is solved.

The entire process can be completed in multiple variations including having students use different software or creating their own stego-files.

6. CONCLUSION

While this exercise in its variations has been a small part of both intro and advanced courses it consistently ranked among the top experiences by students in their course feedback. Students can recall the discussions related to and hands-on use of this activity above others. The lesson can be as short or long as desired to provide an engaging introduction or as a leveling skill. Steganography does not stop with images, audio files can also be used, but the process and software are slightly different. Steganalysis is an interesting tangent related to this exercise. This short exercise is the opening to begin exposing students to the possibility of a future meeting the needs in cybersecurity and forensics work.

Steganography is a fantastic way to introduce the field and potential future of working in cybersecurity to learners from diverse ages, backgrounds, and educational interests. Image steganography is not the stopping point. You can extend this skill and conversation into documents, audio, and video. This activity is easy to turn into gamified learning, to further increase interest. Instructors can learn enough to feel confident in delivering the lesson and leading an in-class discussion. This small exercise is really something that works and is an interesting, quick set-up for learners of all ages.

7. REFERENCES

Dark, M., Daugherty, J., Dark, R., Albright, H., Brown, D., Emry, M., & McCallen, A. (2021) GenCyber 5-Year evaluation 2015-2019. https://tinyurl.com/gencyb

Day, C. (Writer), Howerton, G. (Writer), McElhenney, R. (Writer), & Shakman, M. (Director). (2012, October 11). Pop-Pop: The Final Solution (Season 8, Episode 1) [TV series episode]. *It's Always Sunny in Philadelphia*. 3 Arts Entertainment, FX Productions, & RCG Productions (II).

Johnson, N. F., & Jajodia, S. (1998). Exploring steganography: Seeing the unseen. *Computer*, *31*(2), 26-34. https://doi.org/10.1109/MC.1998.4655281

Kahn, D. (1996, May). The history of steganography. *International workshop on information hiding* (pp. 1-5). Springer, Berlin, Heidelberg.

National Cyberwatch Center Curriculum Standards Panel (2018). National Cyberwatch Center. https://www.nationalcyberwatch.org/csp/

Nelson, B., Phillips, A., & Steuart, C. (2009). *Guide to computer forensics and investigations*. Cengage Learning.

Nelson, B., Phillips, A., & Steuart, C. (2018). *Guide to computer forensics and investigations*. Cengage Learning.

Noland, H. (2020, June 25). *National Integrated Cyber Education Research Center Unveils Rebrand to CYBER.ORG*. Cyber.org. https://cyber.org/news/nicerc-unveils-rebrand-cyberorg

Nygard, K., Chowdhury, M., Kambhampaty, K., & Kotala, P. (2018, April). Cybersecurity materials for K-12 education. *The Midwest Instruction and Computing Symposium 2018*.

Paullet, K. L., Davis, G. A., McMillion, S. K., & Yerby, J. (2013). The new tech effect: A comparative analysis of two universities. *Issues in Information Systems*, *14*(2), 12-22.

Pencheva, D., Hallett, J., & Rashid, A. (2020). Bringing cyber to school: Integrating cybersecurity into secondary school education. *IEEE Security & Privacy*, *18*(2), 68-74.

Singh, H. & Singh, M. (2018). Color image steganography techniques - A review. *RA Journal of Applied Research, 4(1)*. https://doi.org/10.18535/rajar/v4i1.01

Webster, M. (2017, June 5). *Children Are the Future of Cybersecurity*. EDUCAUSE. https://er.educause.edu/blogs/2017/6/children-are-the-future-of-cybersecurity

Yerby, J., & Floyd, K. (2018, August). Faculty and staff information security awareness and behaviors. *Journal of The Colloquium for Information Systems Security Education, 6(1),* 1-23. https://cisse.info/journal/index.php/cisse/article/view/90

Yerby (2013). Forensics - Steganography. http://yerby.weebly.com/forensics.html

Yerby, J., & Floyd, K. (2013). An investigation of traditional education vs. fully online education in information technology. SAIS 2013 Proceedings. http://aisel.aisnet.org/sais2013/40

Zimmerman, E. (2018, December 14). *Three cybersecurity focus areas for education institutions in 2019.* EdTech. https://edtechmagazine.com/higher/article/2018/12/3-cybersecurity-focus-areas-education-institutions-2019

APPENDIX A
Website containing instructions, file, hints, and tools

Steganography

To begin to understand what steganography is, watch the three short videos below. You will likely want to watch them in full screen mode to see them at the best resolution.

The first video will give you an understanding of what steganography is, the second video will give you a demonstration of using S-tools to complete the challenge below, and the final video gives a review that will help you understand the process in more detail.

Find the hidden information in the attached file...

There is a hidden message hidden within the image below using steganography.
Please do not share the solution to keep it fair to everyone.

<u>Here are your only clues:</u>

- forensics techniques hidedata
- I used this software - version 4.0
  - http://embeddedsw.net/OpenPuff_Steganography_Home.html

openpuff.zip
Download File

s-tools4.zip
Download File

Source: http://yerby.weebly.com/forensics.html

APPENDIX B
ASSIGNMENT ONE

ASSIGNMENT ONE is prescribed, and the instructor will be able to determine what the secret message is. Every student who completes the challenge will get the same message.

1. Students begin by going to http://yerby.weebly.com/forensics.html
2. Students should use their imagination for the uses of steganography. Both with and without involving computers. Write two responses.
3. On the webpage above there is a 9-minute video demonstration of how to use steganography.
   a. Download steganography software.
   b. Select a cover file (an image file)
   c. Drag the .bmp file into the software.
   d. Select a .txt file.
   e. Drop it on top of the .bmp file.
   f. Enter a passphrase.
   g. Select the encryption algorithm.
   h. Select OK
   i. A new identical looking image will appear with a window titled “hidden data”
   j. Right-click the file and save the file as Steg.bmp
   k. Examine the file with an image viewer.
4. After viewing the demonstration, students will attempt to unhide data in another file that is displayed.
5. They will need to right-click the large image of a dog on the webpage, and save it as “secret.bmp”
6. Then they will download OpenPuff version 4.0. They must get the correct version for the exercise to work.
7. OpenPuff 4.0 is an executable that does not need to be installed – just run it.
8. Once you run the software you will see the menu displayed in Figure 1. Select “Unhide.”

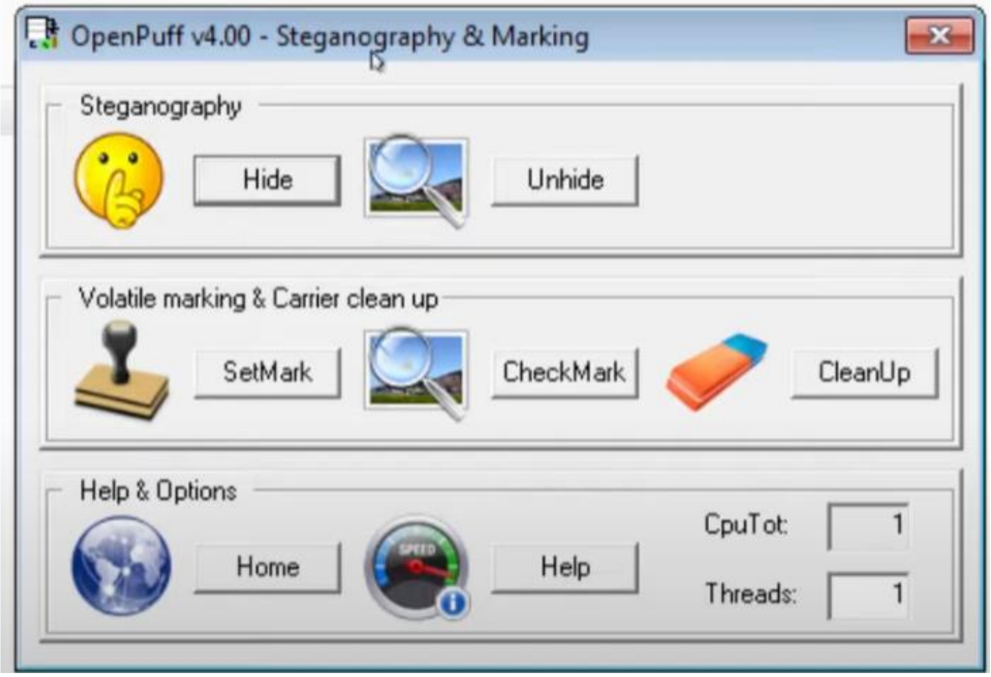
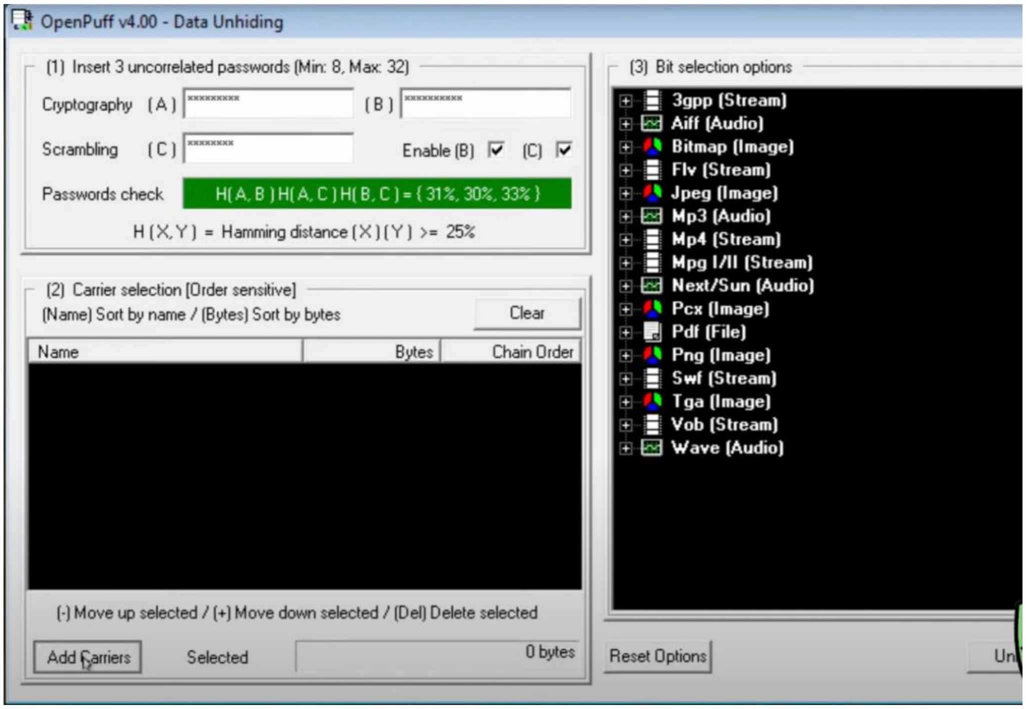


Figure 1. OpenPuff 4.0 select Unhide

9. Students should navigate back to the webpage to copy the three passwords precisely. If they add an extra space or misspell any of the words or put them in the wrong order the Unhiding will not succeed.

10. Next select "Add Carriers" as shown in Figure 2.



OpenPuff v4.00 - Data Unhiding

(1) Insert 3 uncorrelated passwords (Min: 8, Max: 32)

Cryptography (A) ********** (B) ***********

Scrambling (C) ********* Enable (B) ☑ (C) ☑

Passwords check H(A, B) H(A, C) H(B, C) = { 31%, 30%, 33% }

H (X, Y) = Hamming distance (X) (Y) >= 25%

(2) Carrier selection [Order sensitive]

(Name) Sort by name / (Bytes) Sort by bytes

Name	Bytes	Chain Order

(-) Move up selected / (+) Move down selected / (Del) Delete selected

Selected 0 bytes

(3) Bit selection options

Figure 2. After inserting passwords, Add carriers in OpenPuff 4.0

11. Next select the secret.bmp file that was previously downloaded from the website.
12. Click "Unhide"
13. Save the file to the desktop. Students will get a success message and task report indicating that a new file secret.txt was created.
14. Students open the secret.txt file, view the secret message and submit it as evidence that they solved the challenge.

APPENDIX C
ASSIGNMENT TWO

ASSIGNMENT TWO allows students to branch out and create their own version using this skill. Every student that completes the challenge will get the message that was added by another student.

For ASSIGNMENT TWO, students can create and solve their own steganography puzzle using software detailed in Table 1 in this paper. The instructions have less structure for this second portion of the assignment to grant additional opportunity for students to be creative and employ the skill using a different method and software.

1. Run a new steganography tool. The students will need to examine what is available and compatible with the computer that they are using. A few on the list are Linux utilities and many others run in modern Windows operating systems. Students may start with a tool that does not work for them. They are allowed to choose a different tool.
2. Choose a low-resolution image that is in a file format supported by the tool selected by the student. Then add a (short) .txt sentence/message using the tool/program.
3. Choose a low-resolution image that is in a file format supported by the tool selected by the student. Then add a (short) .txt sentence/message using the tool/program.
4. Visually inspect the two images and describe the differences before and after hiding information in the image. Describe any differences you see in 2-3 sentences. Submit your images for comparison and your comparison.
5. Students will usually see no difference in the high resolution and will sometimes see degraded image detail in the low-resolution images.