Capture the Flag (CTF): Website Tutorial to Boost Cybersecurity Training

Reinaldo E. Santiago Lozada
Master in Computer Science
Advisor: Jeffrey Duffany, Ph.D.
Electrical and Computer Engineering & Computer Science Department
Polytechnic University of Puerto Rico

Abstract *— Cybersecurity is a new topic in many organizations, including educational organizations. This new field will have an increase, as new technologies emerged. For that reasons, in order to meet the cybersecurity personnel demand, it is vital to boost cybersecurity interest among students and workers. There are new ways to participate and get involve with this new field, which is the Capture the Flag Competitions. Capture the Flag (CTF) competitions permit students and workers to learn cybersecurity skills in a different and interesting approach. These competitions are platforms that keep them interested in cybersecurity and prepare them for defensive against real cyber attackers.*

Key Terms *— Capture the Flag (CTF), Competitions, Cybersecurity, Education.*

INTRODUCTION

Cybersecurity is “one of the most important challenges” that our nation faces right now [1]. The worldwide shortage of cybersecurity professionals is projected to reach 1.5 million by 2019 [2]. Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks [3, 4]. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes. Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.

In order to meet cybersecurity workforce demand, it is important to raise cybersecurity interest among the youth. In this regard the National Security Agency (NSA) and National Science Foundation (NSF) sponsors the Generation Cyber (GenCyber) [5] program, which is tailored towards K-12 students with a purpose of raising general awareness about the significance and influence of cybersecurity in this era of the Internet of Everything.

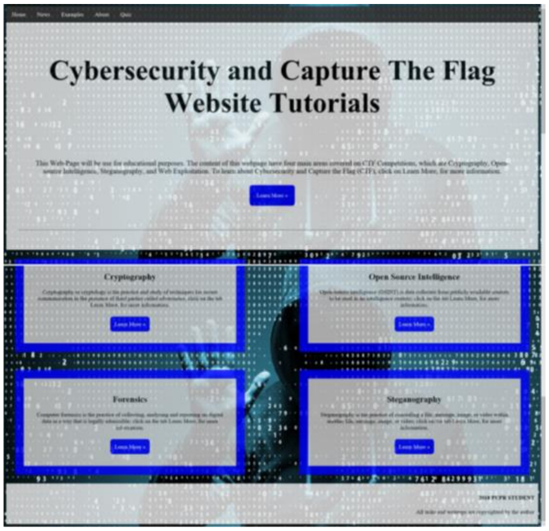
Education is one of the biggest success in order to boost this interest, for that reason, the CyberCorps: Scholarship for Service and Center of Academic Excellence at Polytechnic University of Puerto Rico joined the GenCyber initiative by offering several student and teacher camps in cybersecurity awareness and education. The camp is designed to encourage high school students to get involved into science, technology, engineering and mathematics. This year, the cybersecurity camp was designed to introduce participants to fundamental security concepts, problems, and solutions through a series of interactive lectures and hands-on learning lessons. The camp delivered about 30 different activities including Cryptography puzzle, Raspberry Pi-based cybersecurity exercises, Topology, Ethical Hacking, Digital Forensics, and Data Hiding & Steganography.

Back at Capture the Flag (CTF) competitions, allow students to learn cybersecurity skills in a fun and engaging way. The goal of a CTF is to capture “flags” that are hidden somewhere in a system; the participants must identify them via a variety of techniques. These flags can be anything from a string of letters to an image or data file [6]. CTF competitions are effective platforms to increase student interest in cybersecurity and prepare them for defending against real cyber attackers [7, 8, 9]. The game-like environment of CTF competitions engage students in solving complex cyber-challenges. With proper training and preparation, such competitions can produce high quality cybersecurity professionals [7, 10].

The paper will focus on developing a web page for tutoring people on Capture the Flag competitions (CTF). These competitions distill major disciplines of professional computer security work into short, objectively measurable exercises. The primary goals and objectives for this paper are as follow:

- Get students familiarize with cybersecurity concepts, so they incite the interest in cybersecurity.
- Students knowledge about CTF and general cybersecurity competitions increase.
- Students confidence and comfort level increase as they participated in real CTFs.

This paper is structed as follow. First, we introduced some background. The we will explain the methodology of this project. Follows that, it will explain and shows how the developed webpage looks like and demonstrates some of the CTF challenges examples. Finally, it will have the conclusion and acknowledgement of this paper. Below Figure 1, demonstrates how the developed webpage looks like.



Cybersecurity and Capture The Flag Website Tutorials

This Web-Page will be use for educational purposes. The content of this webpage have four main areas covered on CTF Competitions, which are Cryptography, Open-source Intelligence, Steganography, and Web Exploitation. To learn about Cybersecurity and Capture the Flag (CTF), click on Learn More, for more information.

Cryptography

Cryptography or cryptology is the practice and study of techniques for secure communication in the presence of third parties called adversaries, click on the tab Learn More, for more information.

Open Source Intelligence

Open-source intelligence (OSINT) is data collected from publicly available sources to be used in an intelligence context, click on the tab Learn More, for more information.

Forensics

Computer forensics is the practice of collecting, analysing and reporting on digital data in a way that is legally admissible, click on the tab Learn More, for more information.

Steganography

Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video, click on the tab Learn More, for more information.

2018 PUPR STUDENT

All texts and webpage are copyrighted by the author

Figure 1
Homepage of the Webpage

BACKGROUND

Cybersecurity is a high priority of companies, small and big, as cyber-attacks have been on the rise in recent years. In response to these attacks, security professionals and college students have been through rigorous training as how hackers are able to get into the companies and how to defend against them. One way of cyber security training is through a cyber security capture the flag (CTF) event. A cyber security CTF is a competition between security professionals and/or students learning about cyber security. This competition is used as a learning tool for everyone that is interested in cyber security and it can help sharpen the tools they have learned during their training and classes.

The very first cyber security CTF developed and hosted was in 1996 at DEFCON in Las Vegas, Nevada [11]. DEFCON is the largest cyber security conference in the United States and it was officially started in 1993 by Jeff Moss. DEFCON had become a platform for a skills competition and as the Internet grew, both DEFCON and the CTF competitions did as well. CTF competitions have become global as they did not have any borders and can be done via the Internet. International teams were competing for different types of prizes and bragging rights. There are two formats of the cyber security CTF: attack-defend and Jeopardy-style. See Figure 2 to acknowledge the CTF page.

Attack-Defense CTF

The attack-defend CTF is where each team attacks the other team's system, as well as defend their own system, Figure 2 shows the structure. Usually, there are two rounds of game play in which one team is the attacking team and the other team is the defending team in the first round and then they switch for the second round.

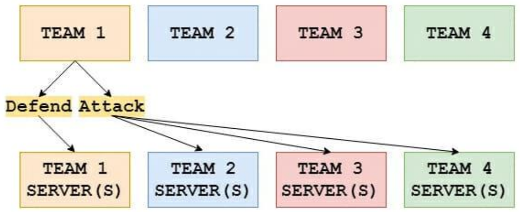
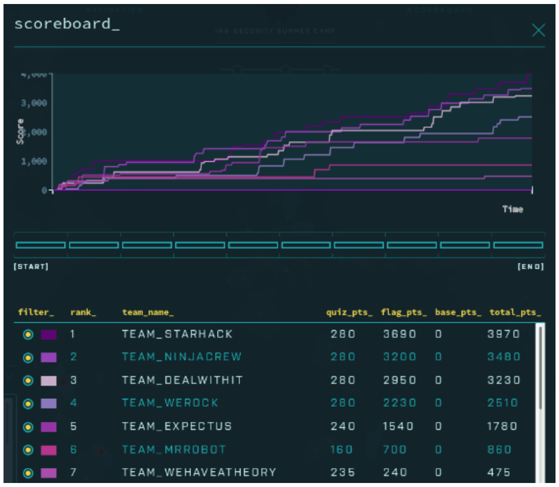


Figure 2
Attack-Defense CTF Structure

There are flags on CTF competition, this can be text files, folders, images, etc. In the defending machines that the attacking team attempts to find as they compromise the machines. The attacking team can use different hacking tools in order to compromise the defending machines but there are rules in place to ensure that the teams are not at an advantage over the other. The defending team can do anything within the rules to defend their machines against the attacking team. They are not allowed to disable any network connections or turn off the machines.

Jeopardy-Style CTF

The Jeopardy-style CTF is like the actual Jeopardy game as the scoreboard looks like a Jeopardy board with different categories and point values, as Figure 3 illustrates. There can be more than two teams as the teams are not trying to attack each other. Some of the categories can include Cryptography, Steganography, Open Source Intelligence, etc.



filter_	rank_	team_name_	quiz_pts_	flag_pts_	base_pts_	total_pts_
◉	1	TEAM_STARHACK	280	3690	0	3970
◉	2	TEAM_NINJACREW	280	3200	0	3480
◉	3	TEAM_DEALWITHIT	280	2950	0	3230
◉	4	TEAM_WEROCK	280	2230	0	2510
◉	5	TEAM_EXPECTUS	240	1540	0	1780
◉	6	TEAM_MRROBOT	160	700	0	860
◉	7	TEAM_WEHAVEATHEORY	235	240	0	475

Figure 3
Jeopardy-Style CTF Structure

Some of the challenges can be done against a main server that was developed for the CTF and the flag is inputted into the CTF scoreboard to get points for the team or as individual. A timer is used to start and stop the CTF and once the timer finishes, the game is over. The team or the individual with the most points at the end wins.

METHODOLOGY

The focus areas that CTF competitions tend to measure are Exploit Development, Packet Capture Analysis, Web Hacking, Digital Puzzles, Cryptography, Steganography, etc. The objectives for this paper are to train people for CTF competition, expose them to possible related-work situations, and let then gain new practical skills on real work situations. The developed webpage will focus on four main areas on cybersecurity, which are cryptography, forensics, open source intelligence, and steganography.

Cryptography

Cryptography is a method of protecting information and communications using codes so that only those for whom the information is intended can read and process it [12]. The pre-fix “crypto” means hidden and the suffix “graphy” stands for writing. In computer science, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms to transform messages in ways that are hard to decipher.

Forensics

Computer forensics, sometimes known as computer forensic science, is a branch of digital forensic science pertaining to evidence found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information. Although it is most often associated with the investigation of a wide variety of computer crime, computer forensics may also be used in civil proceedings. The discipline involves similar techniques and principles to data recovery, but with additional guidelines and practices designed to create a legal audit trail. Evidence from computer forensics investigations is usually subjected to the same guidelines and practices of other digital evidence [13]. It has been used in a number of high-profile cases and is becoming widely accepted as reliable within U.S. and European court systems.

Open Source Intelligence

Open Source Intelligence (OSINT) is the collection and analysis of information that is gathered from public, or open, sources. OSINT is primarily used in national security, law enforcement, and business intelligence functions and is of value to analysts who use non-sensitive intelligence in answering classified, unclassified, or proprietary intelligence requirements across the previous intelligence disciplines [14].

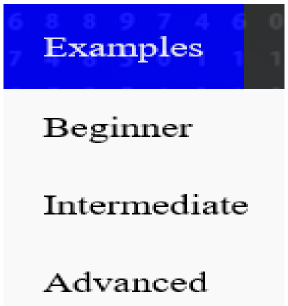
Steganography

Steganography is the practice of sending data in a concealed format so the very fact of sending the data is disguised [15]. The word steganography is a combination of the words “steganos,” meaning covered, concealed, or protected, and “graphy” meaning writing. Unlike cryptography, which conceals the contents of a secret message, steganography conceals the very fact that a message is communicated. Steganography is increasingly being used by actors creating malware and cyber-espionage tools.

WEBPAGE TUTORIAL

As is mentioned before in the paper, this paper focused on a developed webpage for tutoring people on Capture the Flag competitions (CTF). The webpage is divided on:

- Navigation Bar – this navbar has tabs where the participants can learn news about up-to-date, examples divided by categories, and competitions where they can participate. See Figure 4.
- Introduction Section – this is the top section, after the navbar, where the participants will gain knowledge on information about cybersecurity and capture the flag. See, Figure 5.
- Focus Area Section – this section has four boxes, one per each area, where the participants will gain knowledge on each of the areas. See, Figure 6.



Examples

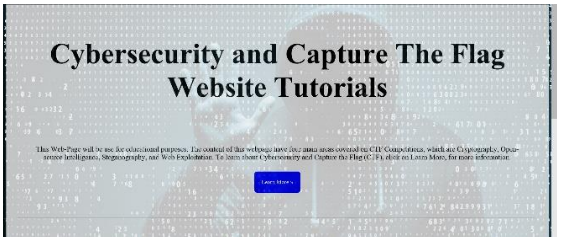
Beginner

Intermediate

Advanced

Figure 4

Different Categories for Examples



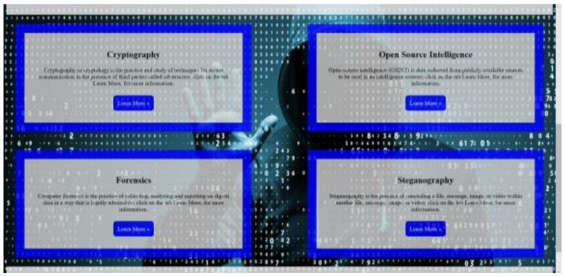
Cybersecurity and Capture The Flag Website Tutorials

This Web-Page will be use for educational purposes. The content of this webpage have four main areas covered on CTF Competitions, which are Cryptography, Open-source Intelligence, Steganography, and Web Exploitation. To learn about Cybersecurity and Capture the Flag (CTF), click on Learn More, for more information.

Learn More »

Figure 5

Introduction Section



Cryptography

Cryptography or cryptology is the practice and study of techniques for secure communication in the presence of third parties called adversaries; click on the tab Learn More, for more information.

Learn More »

Open Source Intelligence

Open-source intelligence (OSINT) is data collected from publicly available sources to be used in an intelligence context; click on the tab Learn More, for more information.

Learn More »

Forensics

Computer forensics is the practice of collecting, analyzing and reporting on digital data in a way that is legally admissible; click on the tab Learn More, for more information.

Learn More »

Steganography

Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video; click on the tab Learn More, for more information.

Learn More »

Figure 6

Focus Areas Section

TUTORIAL EXAMPLES

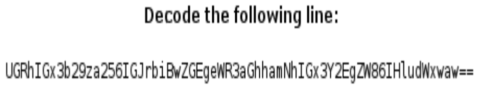
There are two ways to participate in CTF competitions, in-house or online. In-house CTF exercises require some level of technological infrastructure setup, which can be a barrier to some institutions depending upon resource availability. There are some online CTF competitions [16], but these CTFs usually assume some prior technical knowledge. Additionally, online CTFs are generally timed, causing CTF beginners to feel stressed under the time pressure. Some universities have developed their own CTF infrastructure and provide pre-CTF training, workshops to familiarize their students with the competition [6, 17]. With dedicated investments in time and resources to design the CTF architecture, it may not be a viable option for K-12 teachers who do not have those resources and expertise.

Each challenge exercise example tends to teach a particular set of skills of how to solve a specific problem. As participants complete the tutorials, they gain the knowledge and technical skills to solve the challenge. The following is an overview of the objective before the participants goes into the examples and after they complete the tutorial. They are classified as objectives:

- Objective 1: (Beginnings) Establishes the background information needed to understand each focus area and challenges examples. Which is the Focus Area Section.
- Objective 2: (Cryptography) Allows students to understand how to decode incomprehensible data into meaningful information.
- Objective 3: (Open Source Intelligence) Allows students to investigate to gather intelligence and find the flag for the challenge.
- Objective 4: (Steganography) Allows students to understand how to analyze image or data to uncover hidden information.
- Objective 5: (Web Exploitation) Allows students to understand how to use data from standard infrastructure utilities to obtain information about a target.

Cryptography Examples

In the cryptography challenges examples, they focus on discovering patterns in the ciphertext to comprehend how encryption transpired. Unlike hashing, encryption is not a one-way process, so we can reverse it to obtain the plaintext. Brute force is the last choice during cryptanalysis, since modern ciphers can have extremely large key sizes. While solving these challenges, you should refrain from mindless brute forcing or using automated tools as far as possible. Instead, it is best to study the cryptosystem as intricately as possible and develop code breaking skills along the way. Below, Figure 7, shows an example of cryptography example and it will have the process of how to solve this challenge.



Decode the following line:

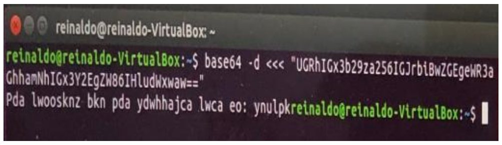
```
UGRhIGx3b29za256IGJrbiBwZGEgeWR3aGhhamNhIGx3Y2EgZW86IHludWxwaw==
```

Figure 7
Cryptography Challenge Example

This is a starter challenge to get us acquainted with the concept of cryptography and cryptanalysis and is hence very straight forward. It provided a string of characters that you need to decrypt to obtain the plaintext message. If the participants are familiar with base64 encode text, the trailing "=" signs are a dead giveaway that the string requires base64 decoding. To base64 decode this string in Linux, we use the base64 utility command:

base64 -d <<< "input the string"

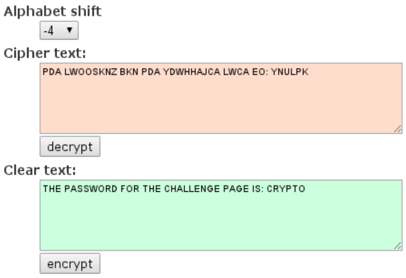
Figure 8 shows how looks on the Linux machine terminal.



```
reinaldo@reinaldo-VirtualBox: ~
reinaldo@reinaldo-VirtualBox:~$ base64 -d <<< "UGRhIGx3b29za256IGJrbiBwZGEgeWR3a
GhhamNhIGx3Y2EgZW86IHludWxwaw=="
Pda lwoosknz bkn pda ydwhhajca lwca eo: ynulpkreinaldo@reinaldo-VirtualBox:~$ 
```

Figure 8
Linux Machine Terminal

After base64 decoding, it still has a ciphertext, that appears to be the result of a simple rotation cipher. The participant can write a small Python script that brute forced the rotations until they could read plaintext. Alternatively, you could use one of the online rotation cipher decryption tools to get the plaintext, as shows in Figure 9.



Alphabet shift: -4

Cipher text: PDA LWOOSKNZ BKN PDA YDWHHAJCA LWCA EO: YNULPK

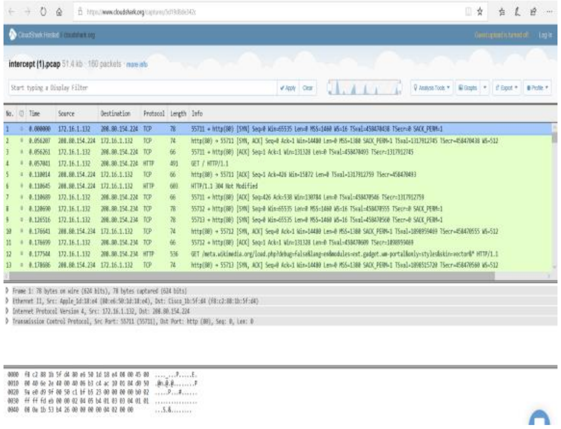
Clear text: THE PASSWORD FOR THE CHALLENGE PAGE IS: CRYPTO

Figure 9
Online Rotation Cipher Decryption Tool

To finish the challenge, after getting the plaintext, the participant input the text on the flag submission, and get the points for solving the challenge.

Forensics Examples

In a CTF context, "Forensics" challenges can include file format analysis, steganography, memory dump analysis, or network packet capture analysis. Any challenge to examine and process a hidden piece of information out of static data files; as opposed to executable programs or remote servers, could be considered a Forensics challenge. Unlike most CTF forensics challenges, a real-world computer forensics task would hardly ever involve unraveling a scheme of cleverly encoded bytes, hidden data, mastroshka like files-within-files, or other such brain-teaser puzzles. Below, Figure 10, shows an example of a Forensic Challenge in CTF, and it will include the tutorial of how to solve the challenge.



intercept (1).pcap 51.4 kb · 180 packets · more info

Start typing a Display Filter

```
No.  Time      Source         Destination    Protocol Length Info
1    0.000000  172.16.1.132   208.80.154.224 TCP      78     55711 → http(80) [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=16 TSval=458470438 TSecr=0 SACK_PERM=1
2    0.056207  208.80.154.224 172.16.1.132   TCP      74     http(80) → 55711 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1380 SACK_PERM=1 TSval=1317912745 TSecr=458470438 WS=512
3    0.056261  172.16.1.132   208.80.154.224 TCP      66     55711 → http(80) [ACK] Seq=1 Ack=1 Win=131328 Len=0 TSval=458470493 TSecr=1317912745
4    0.057041  172.16.1.132   208.80.154.224 HTTP     491    GET / HTTP/1.1
5    0.110014  208.80.154.224 172.16.1.132   TCP      66     http(80) → 55711 [ACK] Seq=1 Ack=426 Win=15872 Len=0 TSval=1317912759 TSecr=458470493
6    0.110645  208.80.154.224 172.16.1.132   HTTP     603    HTTP/1.1 304 Not Modified
7    0.110689  172.16.1.132   208.80.154.224 TCP      66     55711 → http(80) [ACK] Seq=426 Ack=538 Win=130784 Len=0 TSval=458470546 TSecr=1317912759
8    0.120690  172.16.1.132   208.80.154.234 TCP      78     55712 → http(80) [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=16 TSval=458470555 TSecr=0 SACK_PERM=1
9    0.126516  172.16.1.132   208.80.154.234 TCP      78     55713 → http(80) [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=16 TSval=458470560 TSecr=0 SACK_PERM=1
10   0.176641  208.80.154.234 172.16.1.132   TCP      74     http(80) → 55712 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1380 SACK_PERM=1 TSval=1898959469 TSecr=458470555 WS=512
11   0.176699  172.16.1.132   208.80.154.234 TCP      66     55712 → http(80) [ACK] Seq=1 Ack=1 Win=131328 Len=0 TSval=458470609 TSecr=1898959469
12   0.177544  172.16.1.132   208.80.154.234 HTTP     536    GET /meta.wikimedia.org/load.php?debug=false&lang=en&modules=ext.gadget.wm-portal&only=styles&skin=vector&* HTTP/1.1
13   0.178686  208.80.154.234 172.16.1.132   TCP      74     http(80) → 55713 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1380 SACK_PERM=1 TSval=1898515720 TSecr=458470560 WS=512
```

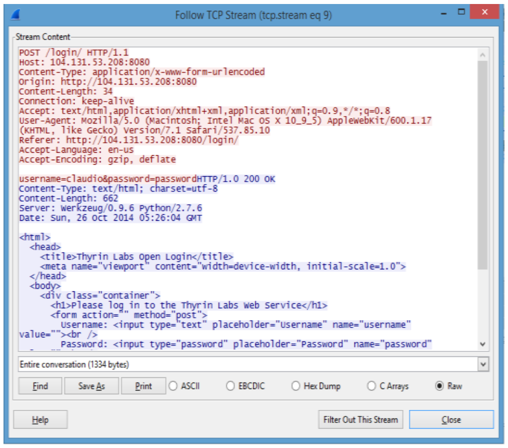
```
Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
Ethernet II, Src: Apple_1d:18:e4 (80:e6:50:1d:18:e4), Dst: Cisco_1b:5f:d4 (f8:c2:88:1b:5f:d4)
Internet Protocol Version 4, Src: 172.16.1.132, Dst: 208.80.154.224
Transmission Control Protocol, Src Port: 55711 (55711), Dst Port: http (80), Seq: 0, Len: 0
```

```
0000  f8 c2 88 1b 5f d4 80 e6 50 1d 18 e4 08 00 45 00   ...._...P.....E.
0010  00 40 6e 2e 40 00 40 06 b3 c4 ac 10 01 84 d0 50   .@n.@.@........P
0020  9a e0 d9 9f 00 50 c1 bf b5 23 00 00 00 00 b0 02   .....P...#......
0030  ff ff fd eb 00 00 02 04 05 b4 01 03 03 04 01 01   ................
0040  08 0a 1b 53 b4 26 00 00 00 00 04 02 00 00         ...S.&........
```

Figure 10
Forensic Challenge Example

Challenge problem: We intercepted some of your Dad's web activity. Can you get a password from his traffic? You can also view the traffic on CloudShark. Also give us a hint: Login is usually done through a POST request. Then, depending on what characters are in Claudio's password, they may be specially encoded.

For this challenge we must use a forensic tool, which is Wireshark application in order to analyze the .pcap file given. The problem tells us that the flag is a password from your Dad's web activity, and the hint tells us to look for a POST Request to find the password. Since we know we are looking for a POST Request, we should search for "POST" by using CTRL + F. Each time we search we receive a packet with the word POST somewhere in it. For each possible packet with a POST Request and the possible password, we can right-click on it and select "Follow TCP Stream". This should bring up a new window with the contents of that TCP Stream. The first time we search for POST requests we see a packet for posting on Wikipedia.org. By following the TCP Stream and glancing at the contents we can quickly see that this is not the packet of data we are looking for. We search again and receive a packet for logging into Thyrin Labs Web Service. By looking at the TCP Stream we see the following, as shows Figure 11.



Follow TCP Stream (tcp.stream eq 9)

Stream Content

```
POST /login/ HTTP/1.1
Host: 104.131.53.208:8080
Content-Type: application/x-www-form-urlencoded
Origin: http://104.131.53.208:8080
Content-Length: 34
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_5) AppleWebKit/600.1.17
(KHTML, like Gecko) Version/7.1 Safari/537.85.10
Referer: http://104.131.53.208:8080/login/
Accept-Language: en-us
Accept-Encoding: gzip, deflate

username=claudio&password=passwordHTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 662
Server: Werkzeug/0.9.6 Python/2.7.6
Date: Sun, 26 Oct 2014 05:26:04 GMT

<html>
  <head>
    <title>Thyrin Labs Open Login</title>
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
  </head>
  <body>
    <div class="container">
      <h1>Please log in to the Thyrin Labs Web Service</h1>
      <form action="" method="post">
        Username: <input type="text" placeholder="Username" name="username"
value=""><br />
        Password: <input type="password" placeholder="Password" name="password"
```

Entire conversation (1334 bytes)

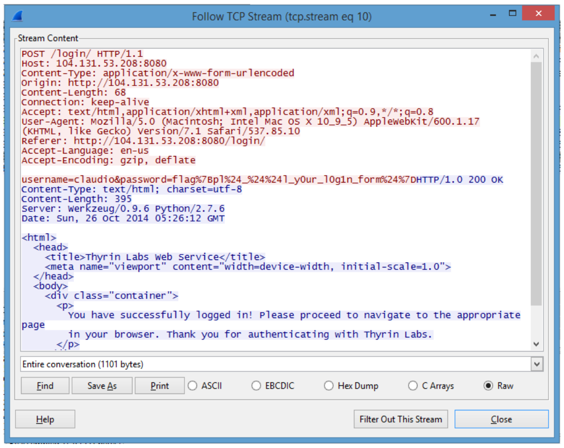
○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

Figure 11
TCP Stream Post Request Search 1

Looking at the stream we can see that a claudio has been filled in for the username, but that the password hasn't been filled in yet. We go back and search for a POST Request one last time and follow the TCP Stream for the packet. We see the following, as it is shown in Figure 12.

It seems that we have found something, which is: flag%7Bpl%24_%24%24l_y0ur_l0g1n_form%24%7D, filled out as the password.

Almost there just one last step. The Hint tells us that the password is encoded, and since we found this in Web Traffic, the password is encoded using UTF-8 as almost all web related things are. We can convert the password into ASCII by using an Online Unicode to ASCIII Converter. Now we just enter the password we received there and see that our decoded password is flag{pl$_$$l_y0ur_l0g1n_form$}.



```
POST /login/ HTTP/1.1
Host: 104.131.53.208:8080
Content-Type: application/x-www-form-urlencoded
Origin: http://104.131.53.208:8080
Content-Length: 68
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_5) AppleWebKit/600.1.17
(KHTML, like Gecko) Version/7.1 Safari/537.85.10
Referer: http://104.131.53.208:8080/login/
Accept-Language: en-us
Accept-Encoding: gzip, deflate

username=claudio&password=flag%7Bpl%24_%24%24l_y0ur_l0g1n_form%24%7DHTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 395
Server: Werkzeug/0.9.6 Python/2.7.6
Date: Sun, 26 Oct 2014 05:26:12 GMT

<html>
  <head>
    <title>Thyrin Labs Web Service</title>
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
  </head>
  <body>
    <div class="container">
      <p>
        You have successfully logged in! Please proceed to navigate to the appropriate
page
        in your browser. Thank you for authenticating with Thyrin Labs.
      </p>
```

Entire conversation (1101 bytes)

Find | Save As | Print | ○ ASCII | ○ EBCDIC | ○ Hex Dump | ○ C Arrays | ● Raw

Help | Filter Out This Stream | Close

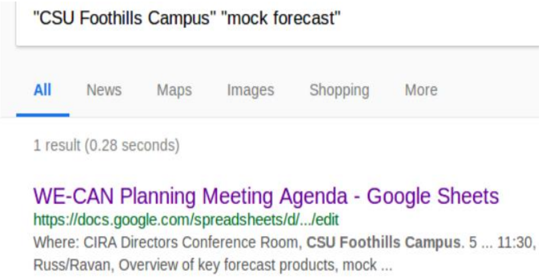
Figure 12

TCP Stream Post Request Search 2

Open Source Intelligence Examples

Open Source Intelligence challenges examples tends and allows students to investigate, gather intelligence and find the flag for the challenge. The idea for open source intelligence challenges is that the participants use free software or the browser instead of using a specific tool to find the flag or answer. Below is an example of an open source intelligence challenge example, with the tutorial on how to solve it.

Challenge Question: A meeting happened at CSU Foothills Campus and one of the agendas was Mock Forecast. We suspect that someone was able to sneak into the meeting by figuring out the meeting id and access code somehow. Can you investigate if the Access code is being leaked somewhere? So, the first thing the participant has to do is open the browser and search for “CSU Foothills Campus Mock Forecast”. Below, Figure 13, shows the search on the browser.



"CSU Foothills Campus" "mock forecast"

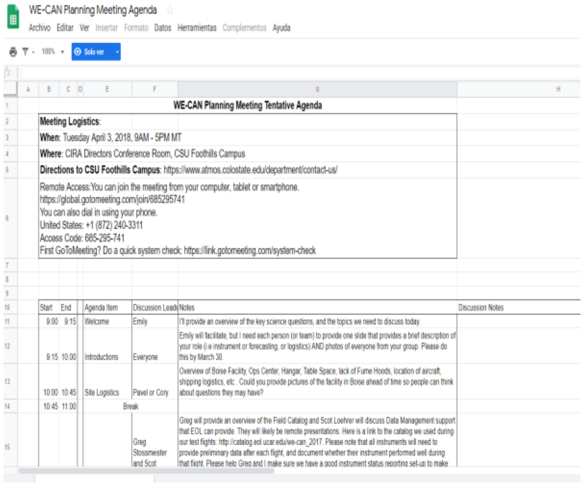
1 result (0.28 seconds)

WE-CAN Planning Meeting Agenda - Google Sheets
https://docs.google.com/spreadsheets/d/.../edit
Where: CIRA Directors Conference Room, **CSU Foothills Campus**. 5 ... 11:30, Russ/Ravan, Overview of key forecast products, mock ...

Figure 13

Browser Search for CSU Foothills Campus Mock Forecast

In the browser, we can find a Google Drive document. So, the participant can go ahead an open the document. The Google Drive document shows a spreadsheet like the one that follows on Figure 14.



WE-CAN Planning Meeting Tentative Agenda

Meeting Logistics:
When: Tuesday April 3, 2018, 9AM - 5PM MT
Where: CIRA Directors Conference Room, CSU Foothills Campus
Directions to CSU Foothills Campus: https://www.atmos.colostate.edu/department/contact-us/

Remote Access:You can join the meeting from your computer, tablet or smartphone.
https://global.gotomeeting.com/join/685295741
You can also dial in using your phone.
United States: +1 (872) 240-3311
Access Code: 685-295-741
First GoToMeeting? Do a quick system check: https://link.gotomeeting.com/system-check

Start	End	Agenda Item	Discussion Leade	Notes	Discussion Notes
9:00	9:15	Welcome	Emily	I'll provide an overview of the key science questions, and the topics we need to discuss today.	
9:15	10:00	Introductions	Everyone	Emily will facilitate, but I need each person (or team) to provide one slide that provides a brief description of your role (i.e instrument or forecasting, or logistics) AND photos of everyone from your group. Please do this by March 30.	
10:00	10:45	Site Logistics	Pavel or Cory	Overview of Boise Facility, Ops Center, Hangar, Table Space, lack of Fume Hoods, location of aircraft, shipping logistics, etc . Could you provide pictures of the facility in Boise ahead of time so people can think about questions they may have?	
10:45	11:00	Break			
			Greg Stossmeister and Scot	Greg will provide an overview of the Field Catalog and Scot Loehrer will discuss Data Management support that EOL can provide. They will likely be remote presentations. Here is a link to the catalog we used during our test flights: http://catalog.eol.ucar.edu/we-can_2017. Please note that all instruments will need to provide preliminary data after each flight, and document whether their instrument performed well during that flight. Please help Greg and I make sure we have a good instrument status reporting set-up to make	

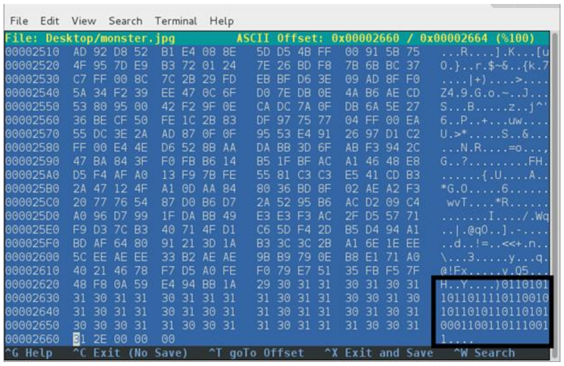
Figure 14

Google Drive Document of Browser Search

Once we have the google drive document opened, we can just look for the word code or access code or clicking “Ctrl+F” and input the access code. Finally, we have found the code “685-295-741” and just submit the code to get the points.

Steganography Examples

Steganalysis refers to the process of locating concealed messages inside seemingly innocuous containers. The idea behind steganography is embedding plaintext messages in places where an unsuspecting user would not think them to be present. During steganalysis, our objective is to discover where and how these plaintext messages are hidden within the provided files or data. Steganalysis is a process of trial-and-error. The solutions provided below offer only the correct approaches to solving steganographic challenges, while skipping the unsuccessful attempts for the sake of brevity. Below, Figure 15, shows an example of cryptography example and then, it will have the process of how to solve this challenge, as it is shown on the webpage.

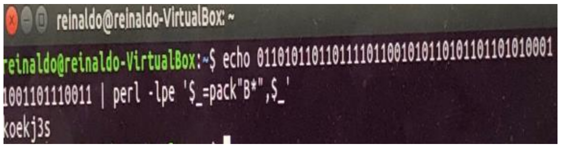


```
File: Desktop/monster.jpg          ASCII Offset: 0x00002660 / 0x00002664 (%100)
00002510  AD 92 D8 52  B1 E4 08 8E   5D D5 4B FF  00 91 5B 75   ...R....].K...[u
00002520  4F 95 7D E9  B3 72 01 24   7E 26 BD F8  7B 6B BC 37   O.}..r.$~&..{k.7
00002530  C7 FF 00 8C  7C 2B 29 FD   EB BF D6 3E  09 AD 8F F0   ....|+)....>....
00002540  5A 34 F2 39  EE 47 0C 6F   D0 7E DB 0E  4A B6 AE CD   Z4.9.G.o.~..J...
00002550  53 80 95 00  42 F2 9F 0E   CA DC 7A 0F  DB 6A 5E 27   S...B.....z..j^'
00002560  36 BE CF 50  FE 1C 2B 83   DF 97 75 77  04 FF 00 EA   6..P..+...uw....
00002570  55 DC 3E 2A  AD 87 0F 0F   95 53 E4 91  26 97 D1 C2   U.>*.....S..&...
00002580  FF 00 E4 4E  D6 52 8B AA   DA BB 3D 6F  AB F3 94 2C   ...N.R....=o...,
00002590  47 BA 84 3F  F0 FB B6 14   B5 1F BF AC  A1 46 48 E8   G..?.........FH.
000025A0  D5 F4 AF A0  13 F9 7B FE   55 81 C3 C3  E5 41 CD B3   ......{.U....A..
000025B0  2A 47 12 4F  A1 0D AA 84   80 36 BD 8F  02 AE A2 F3   *G.O.....6......
000025C0  20 77 76 54  87 D0 B6 D7   2A 52 95 B6  AC D2 09 C4    wvT....*R......
000025D0  A0 96 D7 99  1F DA BB 49   E3 E3 F3 AC  2F D5 57 71   .......I..../.Wq
000025E0  F9 D3 7C B3  40 71 4F D1   C6 5D F4 2D  B5 D4 94 A1   ..|.@qO..].-....
000025F0  BD AF 64 80  91 21 3D 1A   B3 3C 3C 2B  A1 6E 1E EE   ..d..!=..<<+.n..
00002600  5C EE AE EE  33 B2 AE AE   9B B9 79 0E  B8 E1 71 A0   \...3.....y...q.
00002610  40 21 46 78  F7 D5 A0 FE   F0 79 E7 51  35 FB F5 7F   @!Fx.....y.Q5...
00002620  48 F8 0A 59  E4 94 BB 1A   29 30 31 31  30 31 30 31   H..Y....)0110101
00002630  31 30 31 31  30 31 31 31   31 30 31 31  30 30 31 30   1011011110110010
00002640  31 30 31 31  30 31 30 31   31 30 31 31  30 31 30 31   1011010110110101
00002650  30 30 30 31  31 30 30 31   31 30 31 31  31 30 30 31   0001100110111001
00002660  31 2E 00 00  00                                       1....
^G Help   ^C Exit (No Save)   ^T goTo Offset   ^X Exit and Save   ^W Search
```

Figure 15
Steganography Challenge Example

This challenge offered us a simple JPEG image and asked us to locate the password within it. So, we focus our attention on the bytes stored within the image. To view the hexadecimal bytes within the image file, a hex editor is required. You can use "hexedit" or "hexeditor" on a Linux machine, and "Hiew", which is Hacker's view, on a Windows machine. Here, when we view the raw data inside the image, we notice a binary sequence in the ASCII view of the data, as you can see in the black box on Figure 16. This binary sequence immediately stands out from the rest of the 'garbage' ASCII dump. Consequently, we convert this binary sequence to ASCII, and we get the password, as it is shown in Figure 11. For this, we use Perl's pack function command, on Linux machine, to derive ASCII text corresponding to the binary sequence, as you can see below:

echo "input binary" | perl -lpe '$_=pack"B*",$_'

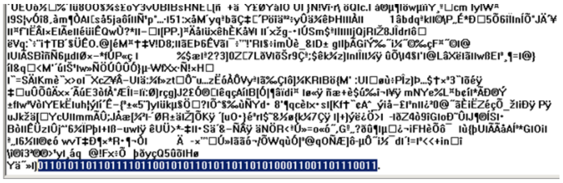


```
reinaldo@reinaldo-VirtualBox: ~
reinaldo@reinaldo-VirtualBox:~$ echo 0110101101101111011001010110101101101010001
1001101110011 | perl -lpe '$_=pack"B*",$_'
koekj3s
```

Figure 16
Perl's Pack Function on Linux Terminal

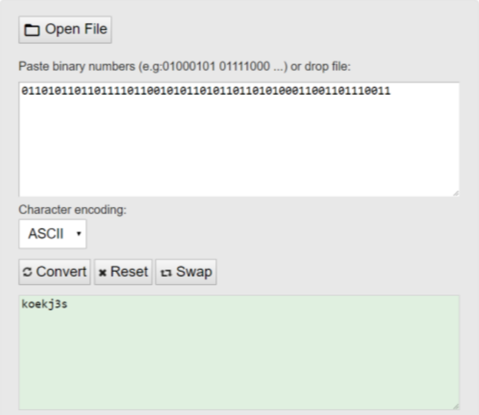
Alternatively, you can open this image file in "notepad.exe" to view the raw ASCII dump and scroll to the end of the file to locate the binary sequence that stands out, as you can see below on Figure 17. After locating the binary sequence, you can open an online decipher tool, to get the password from binary to text view, as shows Figure

18. Finally, you get the password and copy and pasted to get the points for the challenge.



```
ÜEÜò¾□%¨Iü8ÖÖ$¾s£oY3vÜBIBsHNE[ñ +ä Y£ØYàIÖ ÜI }N!Vi·ñ öQIc.I ä®µ¶löwµñY¸ª□cm IyIWª
I9S¦vÓî8¸àm¶ÒAI[sâ5jaôîIIÑ¹p"…·I51:xåM´yq²bãÇ‡□´Pöïäª²÷yÛä¾êÞHIIIÅII   1âbdq²kII©\P„É*Ð□5Õ6ïÌInÍÕ"JÄ´¥
II¤f'IËÂI×EIÃeIIéüiÊQwÙ?*II–□I[PP.)¤ÄåIüxêhÈKå¥I II´xžg-·IÚSm$²IIIIIjQjRIŽ8JÎdrIô□
ëVq:`÷¨ï†TB´§ÜÊO.@|éM¤†‡V!D8;IIãEÞ6ÊVãI¯÷"!'RI§÷imÙè_8ID± gIIþÅGiÝ‰¨i¼¨©%‚çF¤¨©I@
IUIÅSBìñÑ6µdIØ×–*fÚP«ç I      %$æI²2?3]0Z□7LðVIõŠr9Ç²;$êk¾z]InIÎII¼ÿ ûÕ\I4§I'I@LâXëIãIIwßEIª¸¶=I@}
íI&q□<M"´úIŠ'Iw»ÑÖÚÛÛÓ}µ-WfXx·Ñ!×H□
I¨=SÄIKmè¨x>oI¯XcZ¥Â–UIä:¾f»zt□Ô¨u…zËóÅÔVy²Iã‰ÇIô]¼KRIBö{M' :UI□øù÷PÎz]Þ…$†×³3¨Iõéÿ
‡□uÛÕûÄx×´ÃúE3òfÅ"ÆÎI=Iï:Ø]rçg]J2£Ó®□IêqçAíIB[Ó|¶âïdi¤ Iø«ÿ ñæ+è$ú‰î¬I¥ÿ mNYe%L¤bçíI*ÃÐ®Ý
±fIw'VòIYEkËIuh¦ýIí´Ê–{ª±«5¨]yIükµ§Ö□?IÕ^§‰ùÑYd· 8'¶qcèIx·sI[Kf†¨¢A^_ýiå–£I'nII¿²0@¨ãÈiËZéçÕ_žIiÐÿ Pÿ
uJkžä[□YcUIImmÃÛ;JÅæ[¾²I-´ØR±äIŽ]ÕKÿ ´[uO·}éªrI$¨&¾ø{k¼7Çÿ I|+]ýë¿Ö>I -IðZ4ò9îGIoÐ¨ÛIJ¶®ÍSI·
BòIIÊÛzIÛj^'6¾ÏPþI+Iß–uwIÿ êUÜ>*-‡II·Sä´&–ÑÅÿ äNÖR<²Ú»=o«ó¨,G²„?ðû¶Iµ□¿¬iFHèÕô¯ Iù{þUIÃÃåAÍª*GIOiI
²„I6½II®¢ó wvT‡Ð¶×*R·¶¬ÖI      Ä -×'"□Ú»Iãäó¬/ÕWqùÓ|ª@qOÑÆ]ô-µÔ¨i½¯dI´!=Iª<<+in□î
\I®i3²®®>'yI¸áq @!Fx÷Õ þðyçQ5ûõIHø
Yä¨»I)01101011011011110110010101101011011010100011001101110011.
```

Figure 17
View in Notepad.exe for the Raw ASCII Dump



Paste binary numbers (e.g:01000101 01111000 ...) or drop file:

```
01101011011011110110010101101011011010100011001101110011
```

Character encoding: ASCII

```
koekj3s
```

Figure 18
Online Decipher Tool: Binary to Text

Conclusion

There has been a steady increase in the number of Capture the Flag (CTF) type of competitions and participation in them by engineering students. Cyber security is a relatively young discipline, automatically attracts the attention of internet generation kids and is linked to technology-based competitions like CTF. In the current scenario, there does not exist a frame work to evaluate and rank CTFs. We have created and developed a web page for tutoring people on Capture the Flag competitions (CTF). The primary goals and objectives for this developed webpage are to train people for CTF competition, expose them to possible related-work situations, and let then gain new practical skills on real work situations. By completing the tutorials, students are exposed to challenges examples and a tutorial on how to solve and understand each challenge for the skills required for cybersecurity professionals. For example, the forensics exercise familiarizes students with different challenges that forensics professionals may face and develop approaches to solve them. The developed webpage builds a bridge for students with no cybersecurity knowledge and no access to technological resources to reach an understanding of CTF competitions. We believe that the developed webpage can drastically enhance both quality and quantity of the growing interest in K-12 cybersecurity education and workers with no knowledge on this field.

REFERENCES

[1] The White House. (2016). *Fact Sheet: National Cybersecurity Action Plan* [Online]. Available: https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

[2] Cybersecurity Ventures. (2019). *Job Report* [Online]. Available: http://cybersecurityventures.com.

[3] D. L. Burley, "Cybersecurity education", in *ACM Inroads*, part 1, 2015.

[4] D. L. Burley, "Cybersecurity education", in *ACM Inroads*, part 2, 2015.

[5] GenCyber. (n. d.). *Summer Cybersecurity Camp Program* [Online]. Available: https://www.gen-cyber.com.

[6] J. Werther, M. Zhivich, T. Leek, and N. Zeldovich, "Experiences in cybersecurity education: The MIT Lincoln laboratory capture-the-flag exercise", in *Cybersecurity Experimentation and Test*, 2011, vol. 8.

[7] R. S. Cheung, et al., "Effectiveness of cybersecurity competitions," in *Proceedings of the International Conference on Security and Management (SAM), the World Congress in Computer Science, Computer Engineering and Applied Computing*, 2012.

[8] C. Wee and M. Bashir, "Understanding the Personality Characteristics of Cybersecurity Competition Participants to Improve the Effectiveness of Competitions as Recruitment Tools," *Advances in Human Factors in Cybersecurity*, Springer Publishing, 2016, pp. 111-121.

[9] R. S. Cheung, J. P. Cohen, H. Z. Lo and F. Elia, "Challenge based learning in cybersecurity education," in *Proceedings of the International Conference on Security & Management,* vol. 1, Las Vegas, Nevada, USA: SAM 2011, Jul. 2011.

[10] C. Eagle and J. L. Clark, "Capture-the-flag: Learning computer security under fire," *Naval Postgraduate School*, Monterey CA, 2004.

[11] M. Collins, D/ Schweitzer and D. Massey, "CANVAS: a regional assessment exercise for teaching security concepts", *in Proceedings from the 12th Colloquium*, for Information Systems Security Education, June 2008.

[12] J. S. Coron, "What is cryptography?", *IEEE Security & Privacy Journal*, 12(8), 2006, pp. 70-73.

[13] Wikipedia. (n. d.). *Computer forensics* [Online]. Available: https://en.wikipedia.org/wiki/Computer_forensics.

[14] Wikipedia. (n. d.). *Open Source Intelligence* [Online]. Available: https://en.wikipedia.org/wiki/Open-source_intelligence.

[15] T. Morkel, J. H. P. Eloff and M. S. Olivier "An Overview of Image Steganography," in *Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005),* Sandton, South Africa, June/July 2005.

[16] CTFTIME. (n. d.). *Capture the Flag competitions* [Online]. Available: https://ctftime.org.

[17] G. Vigna, et al., "Ten years of iCTF: The good, the bad, and the ugly," in *USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE)*, 2014.