The Noble Profession

Historical Analysis of Mr. Scrooge's Change Of Heart

Presented by Mike Cecil, GCIH, Time Traveling Penetration Tester (Sr)
Technical And Refreshingly Detailed Information Security (TARDIS), Inc.
@Mickeycecil, tabeshaw@gmail.com

Abstract

This document has been submitted by TARDIS Inc.* with the intention of collecting the bounty posted to the hacking community to provide an accurate and detailed record of how Mr. Scrooge's position on hacking was changed to serve good. TARDIS Inc. ventured through time and space to find the answer to this ancient riddle.

* TARDIS Inc. is a fictitious organization; any resemblance to a real organization is purely coincidental.

Introduction

TARDIS Inc. volunteered time and subject matter expertise to conduct an information security analysis of various systems in different time dimensions. The actions of our brother hacker, Ebenezer Scrooge, having lost his way and turning to the dark arts, almost had a disastrous impact on future security postures throughout the galaxy. With no official record in historical indices of how Mr. Scrooge was convinced to change his path, a bounty was announced to the time traveling hacking community. The security professional that could provide evidence for historical records of what turned Mr. Scrooges heart back to the noble hacking profession would be awarded with a much sought after text inscribed by leaders of the trade. TARDIS Inc. chose to take action and travel through time and space to properly identify and record the events leading to Mr. Scrooge′s change. This document contains the submitted evidence of how Scrooge's heart was changed.

Background

While conducting an analysis of artificial intelligence operations in star date 702990.0 (Earth year 3025) for an Imperial Galactic Government agency on the planet Earth; an Electronic Voice Phenomenon (EVP) of what appeared to be a specter, sobbing over the loss of Tiny Tom, was identified during echo hiding analysis.

The odd part about this artifact was that it was time stamped as having been recorded on the galactic star date of -289982.2 (Earth year 2034); however, our records indicate that Tiny Tom had been a young penetration tester during that time and lived to accomplish a great deal after that date. Tiny Tom was widely known for having been Mr. Scrooge's business partner, and in his older years referring to him as a second father. Armed with this new information the TARDIS team sprung into action to lay claim to the bounty and provide an accurate depiction of these historical events.

Analysis of the audio file was matched against a master database of other recorded EVP's and the voice most closely matched the Ghost of Hacking Yet to Come.

A meeting was scheduled with the elusive specter to assess his recollection of his encounters with Mr. Scrooge. The TARDIS team felt confident that armed with the knowledge of his emotional attachment to Tiny Tom we could gain his trust and ultimately learn more about where to look for the answers to this ancient riddle.

Summary

The hardest part about time travel is having to constantly look at a calendar to know where I am. When traveling to times that have not yet discovered how time travel is possible I must always have appropriate attire. It's a good thing my vehicle is bigger on the inside; else I would never be able to transport my jump bag and wardrobe. The meeting with the Ghost of Hacking Yet to Come was scheduled, inconveniently, in the earth year 2014 (star date -309979.4). In preparation for this meeting I made a pit stop to take in a SANS@night talk regarding assessing deception. I would need every tip and trick Mike Murr had to offer. I quickly realized that the art of identifying deception is much more complex than the media had depicted, so I would have to rely on my wits and a great deal of luck. The Ghost of Hacking Yet to Come is known throughout the galaxy as a stubborn being. An apparition of few words but incredible action. It has long been speculated that he is the wicked cousin of Death himself.

Upon my arrival to our scheduled meeting I was surprised to find the apparition in great spirits, much more friendly and talkative than I had expected. "Well it's about time someone gave me the credit due for my part in this matter" the ghost proclaimed proudly as I reached out a hand to introduce myself. The high spirited, almost giddy, specter lead me down a dark corridor. Mist seemed to cover every particle of the air around us. It was difficult to decipher where we were going or even where we were as we traversed the seemingly endless hall. There was little conversation during our journey; having no clue about our destination I presumed I was being led to my demise. I wondered if the reason Scrooge's turn was so poorly documented was because this wicked apparition disposed of anyone that got close. My only comfort was that the ghost was singing Christmas carols and occasionally skipping; his large wool robe filling with air and gently swaying along to the rhythm of the tune coming from the wraith's indiscernible face. Surely no being with a song in his heart and skip to his step would intend me ill. Having traveled through the millennia to amazing worlds and unimaginable futures, I thought I had seen it all. But this was definitely a new experience for me.

As we approached the end of the hall the mist around us began to dissolve and I was able to see more clearly my surroundings. What was previously darkness and moisture had begun to transform into a staircase with rich wooden hand rails, leading to what appeared to be an ancient static electricity generator. As we ascended the staircase and veered to the left I could see the walls around me opening to an office space. "Welcome to my laboratory" the specter exclaimed proudly. As I stopped to take in my surroundings I was surprised to find myself standing not twenty feet from a massive, statuesque, knight mounted next to a large wooden book case; it appeared to be standing guard over the laboratory. The space was impressive, comfortable with high wooden beams, comfortable chairs and couches surrounding a strong wooden desk. The specter offered me a seat as he glided comfortably into an oversized leather chair, a framed image of the great professor Einstein mounted on the wall above him. "You know I can get that picture autographed for you if you like" I offered. "My phone box is parked right outside if you would like to come along". The ghost turned to face me, though I couldn't make out his features under the hood of his thick robe; I had the the feeling he was smiling warmly. "Thank you kindly for the offer but that picture was sent to me by the professor after I helped him with a relatively difficult issue some time ago". the ghost replied. 'Besides that phone box of your is actually

parked two weeks in the future from where we are now. I thought the mist would have tipped you off to our traveling into a time warp. Have you not yet discovered on planet time warps?"

Surprised and somewhat awed by the ghosts advanced time travel abilities, I realized my mouth was agape and my mind racing to absorb and process this information. Suddenly out of the corner of my eye I notice the eyes on the framed professor above the specter were moving. The ghost must have picked up on my realization; he said "Alan, why don't you come out and join us?". Just then the book case next to the knight opened revealing a hidden room, a sharply dressed gentleman walked casually out of the secret room. "May I present to you Royal Society Fellow Alan Turing" the ghost offered, "Alan has come to help you with the delicate riddle you are trying to decipher". My awe quickly turned to star shock as I stood to shake the had of one of histories greatest hackers. In a thick British accent the Cambridge professor said, " it is truly a pleasure to make your acquaintance finally, you know we have been following your adventures and development very closely young man". I had no words to offer in reply only a confused look. "You see my friends and I have been patiently waiting for you to to mature into the fine hacker you have become so that we could deliver this message to you personally; feeling confident you would be able to decipher it." Looking around the room I knew it was only Alan, the ghost, and I. "Friends?" I questioned with a child like curiosity in my tone. "Well you see the events that you seek to learn about were put into action by three of us with the help of several tormented operating systems" Alan explained. " The last of our trio Johnny Long is presently sharing the knowledge and creating real change in Uganda, unfortunately he will not be able to join us for this meeting. I am sure he would appreciate a visit sometime though. His mission can always use someone with your passion and ability".

Now sitting in this beautiful laboratory with the ghost and Alan Turing I came to the realization that I wasn't the one in control of this investigation, These beings had been planning this meeting for some time. An awkward silence filled the room as we sat staring at one another. I had so many questions for the duo but I felt as if I needed to get more information about the EVP that brought me here in the first place. "Mr Ghost, if I may call you that, can you tell me more about this audio recording of you weeping over the demise of Tiny Tom?" I asked nervously. "Awe yes the EVP; well you see that recording was hidden in a place we knew you would find it.The weeping you hear is not me but that of a thousand Weeping Angels. Sometimes in my travels I must battle evil to keep the universe safe from the night. Those Angels meant to do harm to Tiny Tom before his time" the ghost explained. "The darkness that looms in every man is the weakness that these evil creatures look to exploit. At times we are forced to intervene, to shun the darkness and return the good to our world." the ghost continued. "As we learned by exploring possible futures, the actions of Mr. Scrooge could have left the universe in a very dark place; the death of Tiny Tom was not the least of the results of his dark deeds should he have stayed on that path."

As I listened to the ghost I couldn't shake the feeling that his voice was incredibly familiar. Almost as if he had been the voice in my head as I traveled the universe learning to tune my trade craft. I couldn't shake the feeling that the ghost was some great mentor in the hacking community. That makes no sense though; this spirit has a reputation of being cold and unreachable. Perhaps there is more to what is behind that robe than he wants to reveal. I chose to listen to my instinct and not pursue and avenue of revealing the man behind the robe. It wasn't really in the scope of my mission and the world is obviously a better place without knowing his dark secret. I secretly hoped that someday he would choose to reveal his identity to me willingly however.

"My brother hacker, we want to present to you the information that you seek. We cannot however simply tell you the answer to your riddle. What kind of growth would develop if we simply told you all the answers to these mysteries? We will however present you with some artifacts to help you find your way. We are sure you have the ability to find the answers hidden deep in the data we are about to provide you." the ghost further explained. "There is a well known story 'A Christmas Hacking Carol' all of the clues you need to unravel this mystery are hidden in that text." The ghost concluded.

The ghost and Alan rose from their seats; the ghost handed me a usb stick as he shook my hand. The room suddenly faded to mist and in a few moments I was standing in my time traveling phone box wondering if I had just awoken from a very strange dream. I looked into my right hand and there was a USB drive. It wan't a dream I realized. With that I got right to work studying the text from 'A Christmas Hacking Carol' and following the clues I found there.

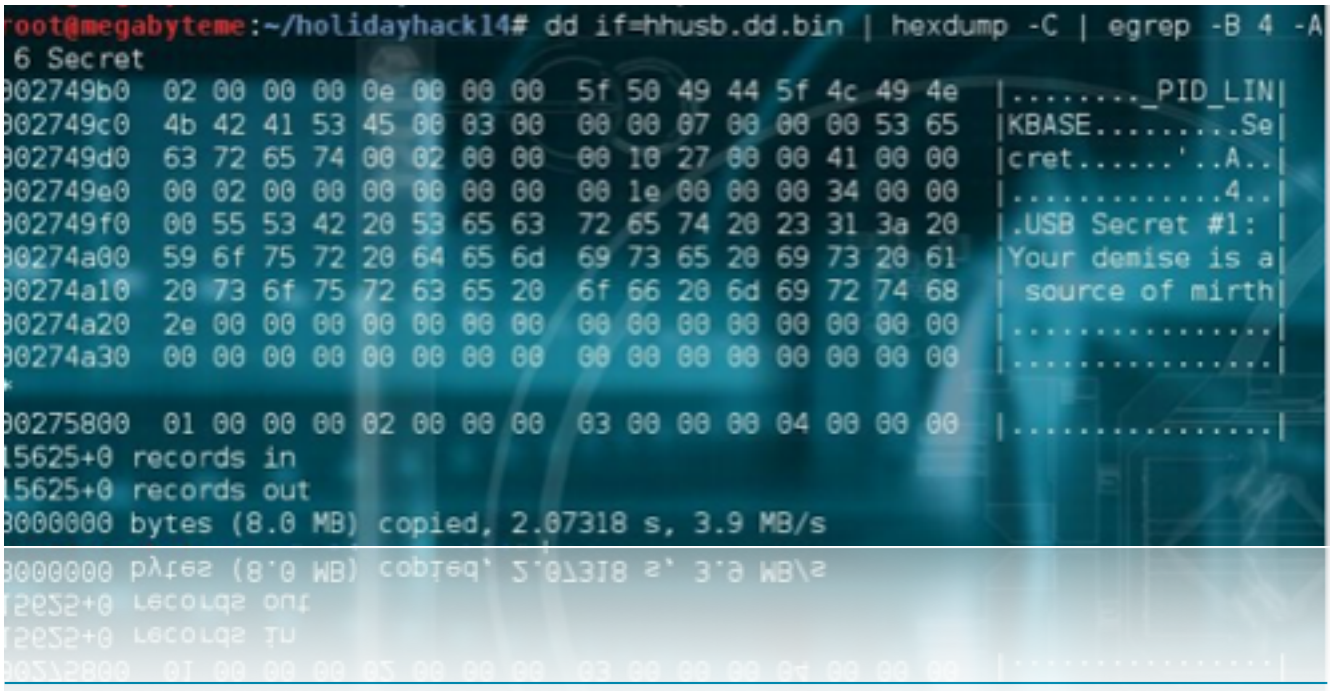
Findings

USB Drive Image Analysis

The USB Drive provided by the ghost contained four hidden messages meant to teach Mr. Scrooge the importance of his impact on the information security community. After analyzing the drive carefully I found the following information:

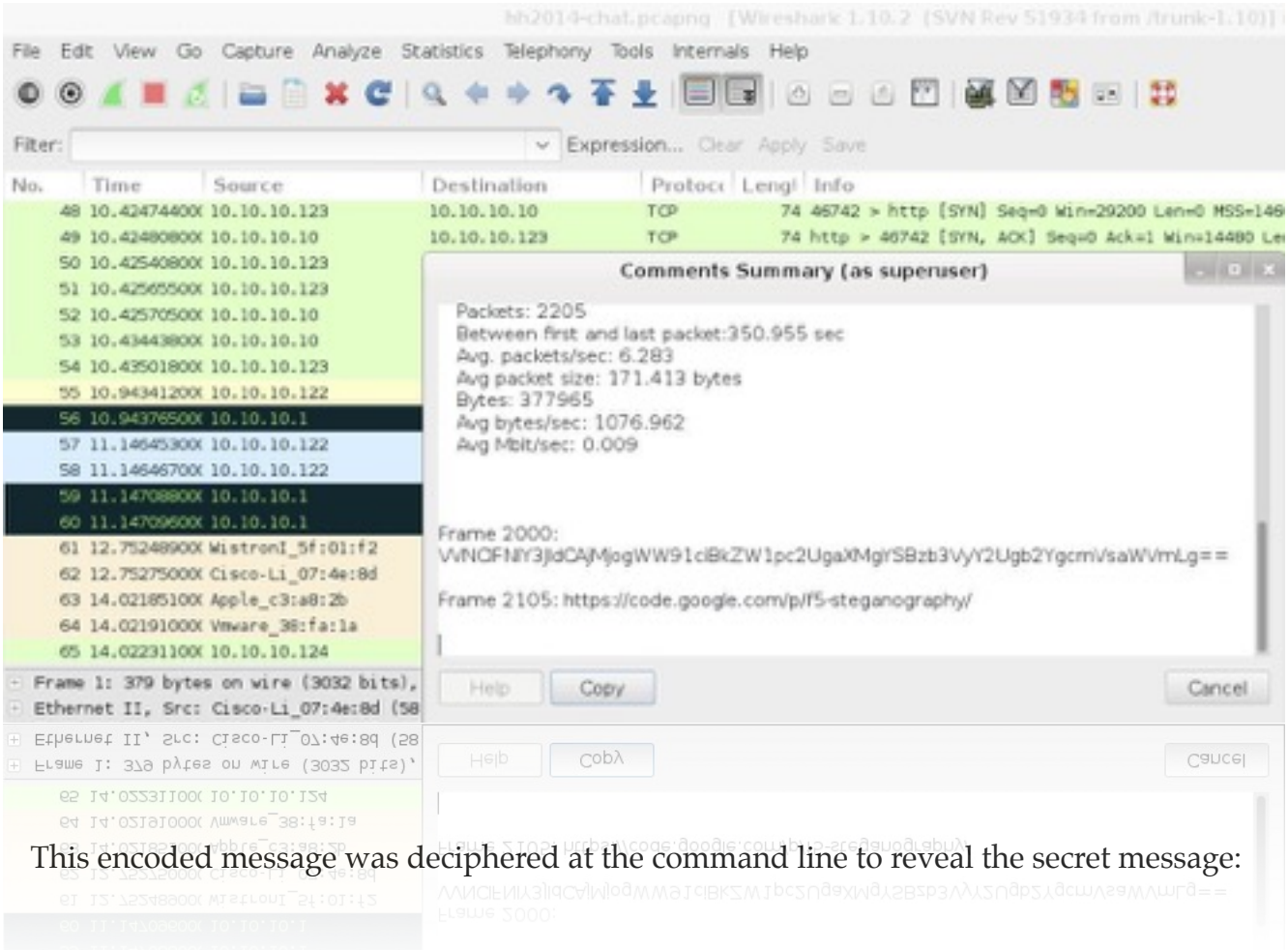
USB Secret #1: Your demise is a source of mirth

This information was gathered by analyzing the dd image of the drive. It was hidden in the meta data in the comments field of a word document on the drive. The data was easy to discover by simply doing a hex dump of the drive image and searching for various terms. In this case searching for the term 'secret' provided the answer.

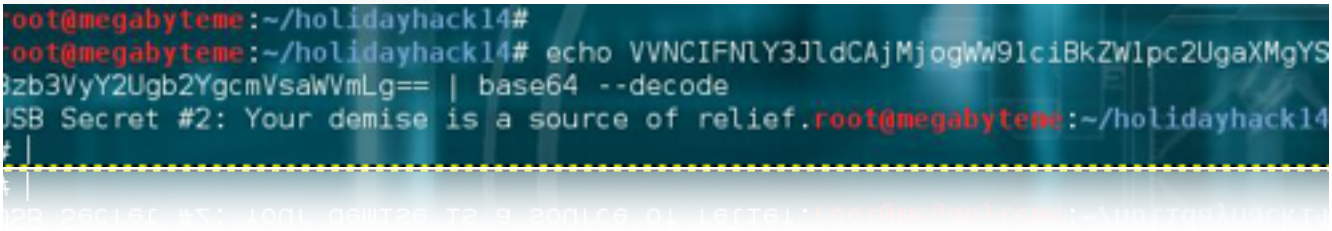


USB Secret #2: Your demise is a source of relief.

While analyzing the drive with Autopsy a packet capture was identified. This packet capture was a pcapng file. With the knowledge that the newer pcap file type allowed for packet comments to be added to a packet I chose to analyze the capture for comments. In the comments of frame 2000 I found a base64 encoded message:
VVNCIFNlY3JldCAjMjogWW91ciBkZW1pc2UgaXMgYSBzb3VyY2Ugb2YgcmVsaWVmLg==

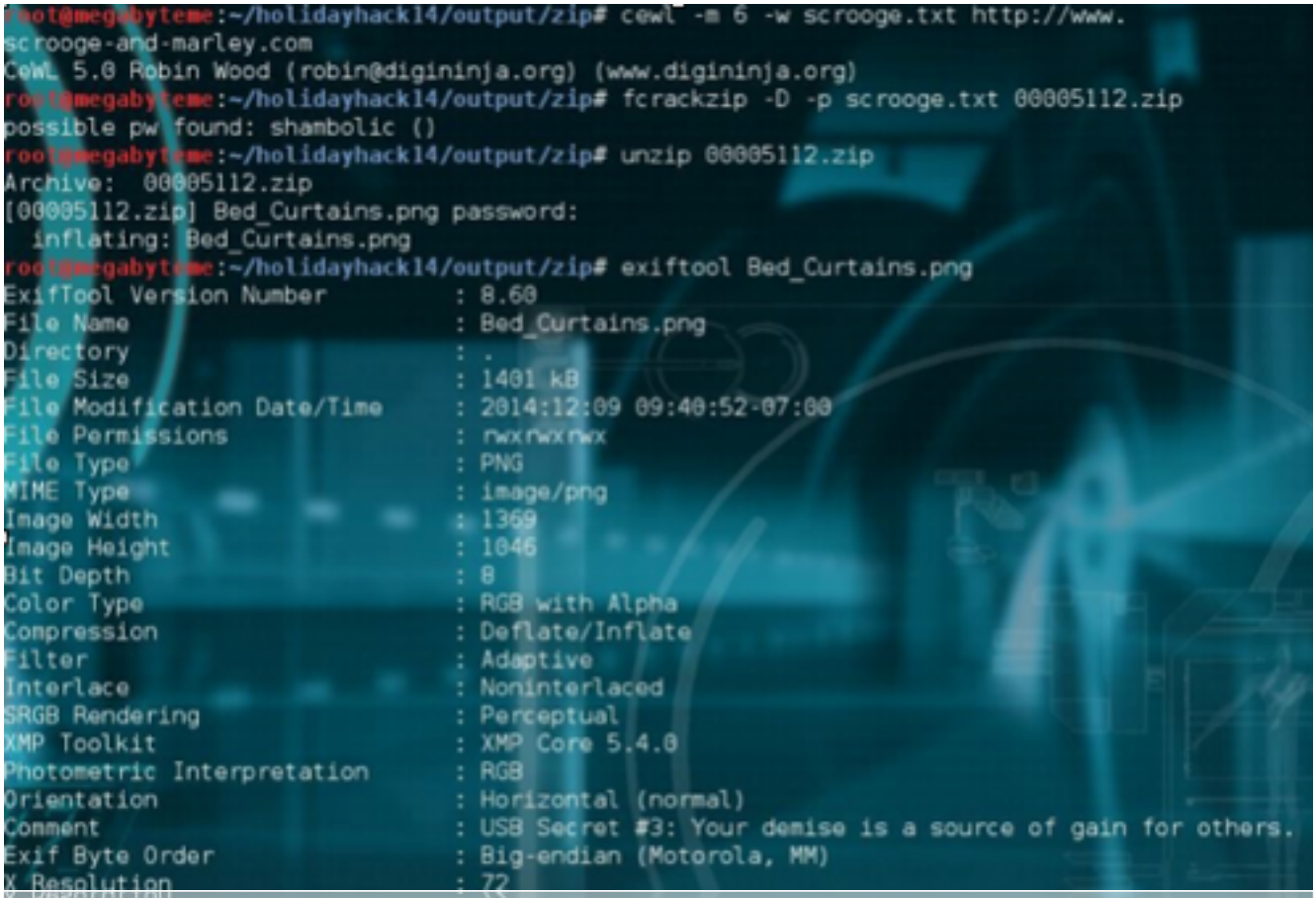


This encoded message was deciphered at the command line to reveal the secret message:



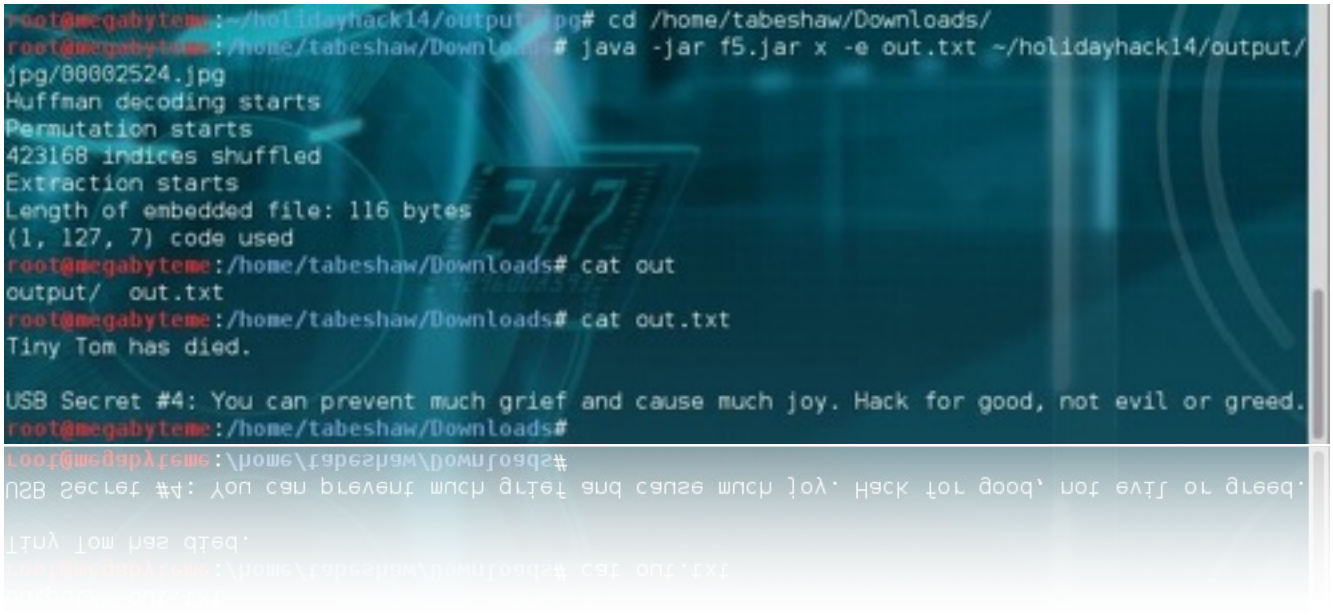
USB Secret #3: Your demise is a source of gain for others.

This artifact was a little more tricky to find than the previous two. A ZIP file was hidden in an Alternate Data Stream behind the previously identified PCAPNG file. Autopsy revealed for me the hidden file. Using Foremost to carve out the data as well as Bulk Extraction Tool I was able to get a good copy of the ZIP file. I found however that it was password protected. After reviewing the text in 'A Christmas Hacking Carol' I realized that Johnny Long used the term CEWL in reference to www.scrooge-and-marley.com. I chose to get a password list from the site using CEWL and then run a dictionary attack against the ZIP file. The secret text was hidden in meta data (comment field) of the image Bed_Curtains.png



USB Secret #4: You can prevent much grief and cause much joy. Hack for good, not evil or greed.

The previously identified PCAPNG comments analysis included a URL that was completely out of place for this capture. It was to a google codes site for Stegoextract F5 stegonography.ttps://code.google.com/p/f5-steganography. I used this java based tool to extract the hidden message from a jpg image of Tiny Tom's crutches.

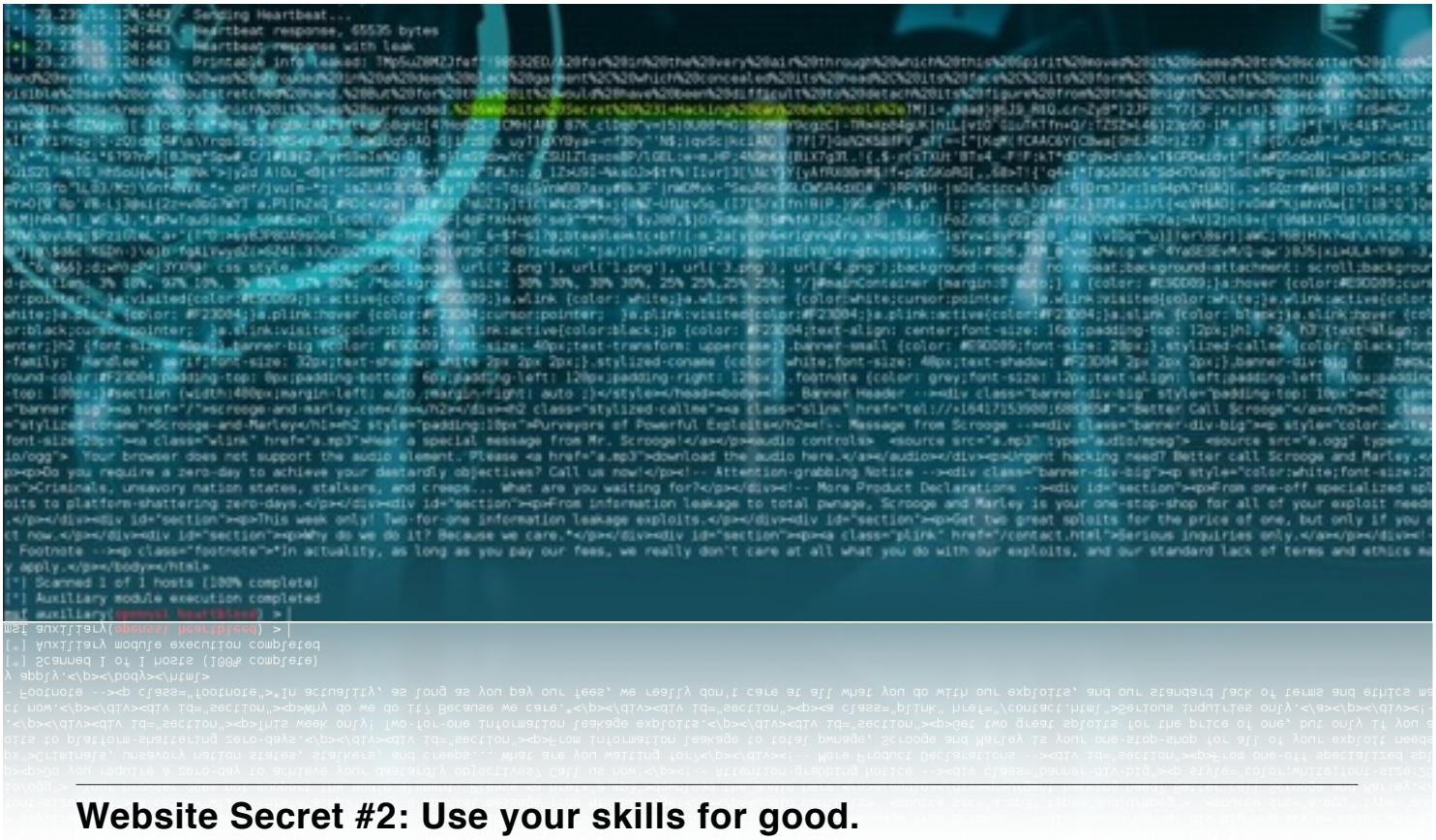


Website www.scrooge-and-marley.com analysis

The website www.scrooge-and-marley.com was in scope on ports 80 and 443. Given the popularity of heart bleed and shellshock recently I immediately attempted to exploit these vulnerabilities. Heart bleed was easily successful. Shellshock was a bit trickier. I spent several days trying to isolate audio stegonagraphy possibilities before returning to shellshock in different ways; which were ultimately successful.

Website Secret #1=Hacking can be noble

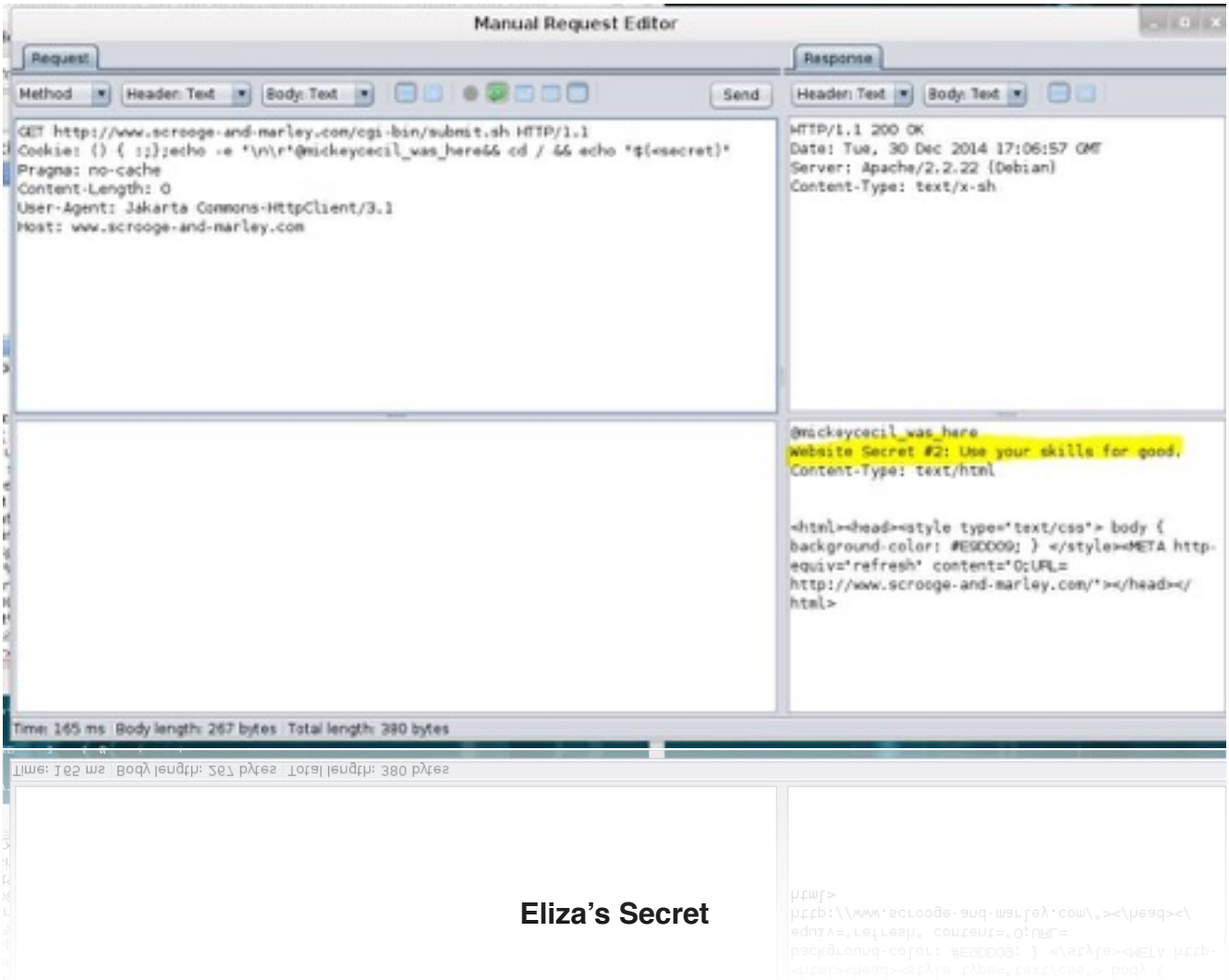
This artifact was extracted using the metasploit heart bleed aux scan agains port 443 of www.scrooge-and-marley.com. The memory dump included text from ‘A Christmas Carol’ followed by the secret message.



Website Secret #2: Use your skills for good.

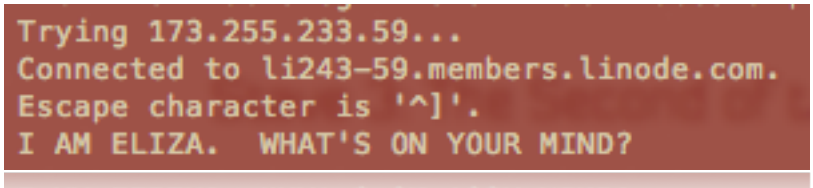
This is the one that took me the most time to exploit. Using DirBuster I was able to identify the contact page and submit script used on it. The script was a simple refresh back to the home page so I assumed SQL Injection was not a possibility. I attempted ShellShock using the metasploit attack initially however I focused on the User Agent string as my attack surface. This has been the most documented method of attack so I didn’t think to try other fields. I spent a great deal of time focused on the voicemail box and mp3 and ogg recordings. I was assuming there was either hidden text in the audio, a hidden image in the spectrogram, or hidden audio in the message itself. Once I exhausted this course of analysis I returned to shellshock with renewed vigor. Using OWASP ZAP Manual Request to run the magic string in the Cookie field I was eventually successful. I then had to focus on how to extract the

message using only native bash commands. I eventually came up with the location of the file ‘secret’ which I initially thought was a directory. I then came up with a successful string:
Cookie: () { :;};echo -e "\n\r" 123 && cd/ && echo “$(<secret)"



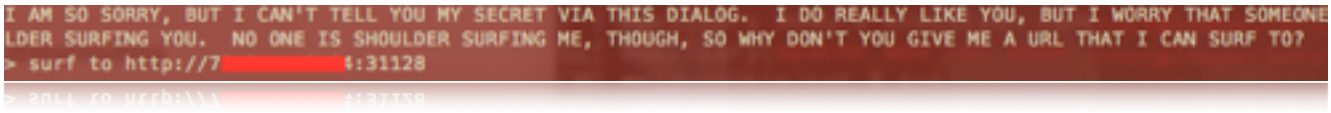
Eliza’s Secret

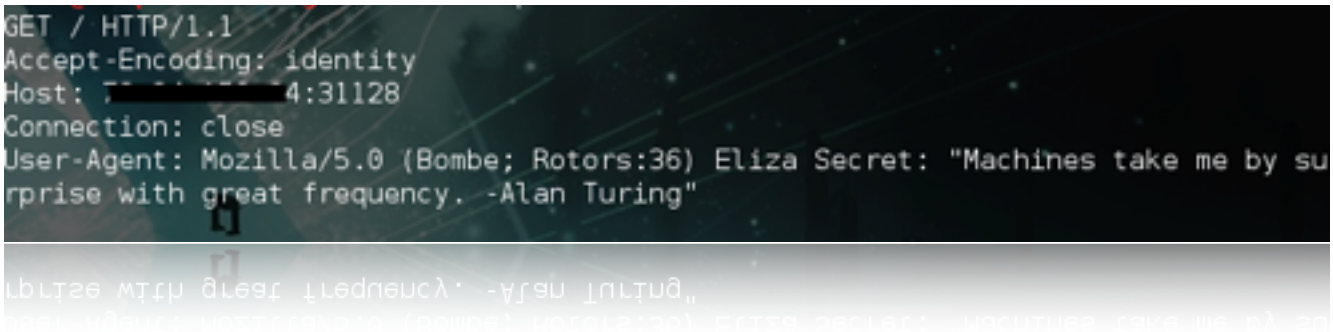
While inspecting the server at 173.255.233.59 I initially only found port 22 open and it would only accept key based authentication attempts. I relied too heavily on nmap’s default port scans. After searching everywhere I could think of to find a key file I decided to rescan for open ports on the server; modifying my nmap query to look for all open TCP ports not just NMAP’s top ports. I found port 31124 was open. When I connected to this port using telnet I received a response from Eliza asking what was on my mind.



Eliza Secret: "Machines take me by surprise with great frequency. -Alan Turing"

After working to query the apparent chat bot for some kind of key phrase I decided to ask her questions related to the Turing test and then specifically Alan Turing. When I asked Eliza to tell me about Enigma several times she eventually asked me to tell her a site to surf to. I had to ask her in a couple different ways before I got the syntax right but eventually she was willing to browse to a site for me. So I opened a NetCat listener on my Kali image and asked her to connect to my public IP address (after making appropriate network and client firewall changes). When Eliza connected to me she provided me a User-Agent string containing her secret.





Conclusion

After carefully analyzing all of the artifacts presented it became clear to me that Mr. Scrooge's heart was changed by the passion and dedication of a group of powerful hacking professionals, traveling through time and space. Scrooge was given an opportunity to learn how his positive impact on the security community could improve the lives of so man people. Scrooge was visited by three historically positive influences in the trade and they used his love for cracking the codes to help him see the error of his negative direction. I was both honored and excited to be given an opportunity to decipher and document these historic events.