

# SIT282/SIT703 Computer Forensics and Investigations

## Workshop Session 8

In the previous session, you learned how to encrypt/decrypt data using automated software tools. During this session, we will practice three forensic software tools – stegbreak, S-Tools and jpseek. You will be able to use these steganography tools to solve forensic tasks. Ubuntu VM is used in this session.

## Learning Objectives

1. Describe the challenges faced by digital forensic investigators when having to identify and deal with steganographic content in files.
2. Practice embedding and detecting steganographic content in different types of files using forensic tools and techniques to recover digital evidence.
3. Understand the limitations of using automated tools to detect steganography.
4. Compare the steganography tools used by defining the purpose and function of each tool.

### 1. Introducing Stegbreak

Stegbreak is a well-known program included in the Stegdetect package and an automated tool for detecting steganographic content in images. Stegdetect is capable of detecting several different steganographic methods that embed hidden information in JPEG images. It is used to launch dictionary attacks against JSteg-Shell, JPHide and OutGuess 0.13b.

Remember that Stegbreak needs a dictionary to execute.

Launch a Terminal and change directory to “Desktop/Data-files/week08”. In the folder, you will see a few image files, a rule file “rules.ini” and a dictionary file “words”. Because Stegbreak is a Windows tool, we will use the “wine” emulator to execute it by typing “**wine ~/Desktop/win-tools/jphide\ and\ Stegbreak\stegdetect\stegbreak.exe -r rules.ini -f words boys.jpg**”. As shown in the following screenshot, we can obtain the password “donkey” for image “boys.jpg”.

```
user@Ubuntu1804: ~/Desktop/Data-files/week08
File Edit View Search Terminal Tabs Help
user@Ubuntu1804: ~/Des... x user@Ubuntu1804: ~/Des... x user@Ubuntu1804: ~/Des... x
user@Ubuntu1804:~/Desktop/Data-files/week08$ ls -l
total 1092
-rw----- 1 user user 231317 Mar 25 2007 boys.jpg
-rw----- 1 user user 25395 May 8 2008 butterfly.jpg
-rw----- 1 user user 184786 Mar 25 2007 girl.jpg
-rw----- 1 user user 129456 Mar 25 2007 man.jpg
-rwxr-xr-x 1 user user 1912 Jun 25 11:28 rules.ini
-rw----- 1 user user 529097 Mar 25 2007 words
user@Ubuntu1804:~/Desktop/Data-files/week08$ wine ~/Desktop/win-tools/jphide\ and
d\ Stegbreak/stegdetect/stegbreak.exe -r rules.ini -f words boys.jpg
001c:err:module:import_dll Library MSVCR100_CLR0400.dll (which is needed by L"C:
\\windows\\Microsoft.NET\\Framework64\\v4.0.30319\\mscorlib.exe") not found
001c:err:module:import_dll Library mscorlib.dll (which is needed by L"C:\\windows
\\Microsoft.NET\\Framework64\\v4.0.30319\\mscorlib.exe") not found
001c:err:module:attach_dlls Importing dlls for L"C:\\windows\\Microsoft.NET\\Fra
mework64\\v4.0.30319\\mscorlib.exe" failed, status c0000135
000f:err:service:process_send_command service protocol error - failed to write p
ipe!
Loaded 1 files...boys.jpg : jphide[v5](donkey)Processed 1 files, found 1 embeddi
ngs.Time: 2 seconds: Cracks: 15588, 7794.0 c/suser@Ubuntu1804:~/Desktop/Data-f
iles/week08$
```

But steganographic pictures cannot be detected by current detection programs. For instance, after using the above Stegbreak command, you can try Stegdetect by typing the following command **"wine ~/Desktop/win-tools/jphide\ and\ Stegbreak/stegdetect/stegdetect.exe boys.jpg"**. The result shows a negative detection as shown in the following:

```
user@Ubuntu1804: ~/Desktop/Data-files/week08
File Edit View Search Terminal Tabs Help
user@Ubuntu1804: ~/Des... x user@Ubuntu1804: ~/Des... x user@Ubuntu1804: ~/Des... x
-rwxr-xr-x 1 user user 1912 Jun 25 11:28 rules.ini
-rw----- 1 user user 529097 Mar 25 2007 words
user@Ubuntu1804:~/Desktop/Data-files/week08$ wine ~/Desktop/win-tools/jphide\ and
d\ Stegbreak/stegdetect/stegdetect.exe boys.jpg
001c:err:module:import_dll Library MSVCR100_CLR0400.dll (which is needed by L"C:
\\windows\\Microsoft.NET\\Framework64\\v4.0.30319\\mscorlib.exe") not found
001c:err:module:import_dll Library mscorlib.dll (which is needed by L"C:\\windows
\\Microsoft.NET\\Framework64\\v4.0.30319\\mscorlib.exe") not found
001c:err:module:attach_dlls Importing dlls for L"C:\\windows\\Microsoft.NET\\Fra
mework64\\v4.0.30319\\mscorlib.exe" failed, status c0000135
000f:err:service:process_send_command service protocol error - failed to write p
ipe!
Loaded 1 files...boys.jpg : jphide[v5](donkey)Processed 1 files, found 1 embeddi
ngs.Time: 2 seconds: Cracks: 15588, 7794.0 c/suser@Ubuntu1804:~/Desktop/Data-f
iles/week08$
d\ Stegbreak/stegdetect/stegdetect.exe boys.jpg
001c:err:module:import_dll Library MSVCR100_CLR0400.dll (which is needed by L"C:
\\windows\\Microsoft.NET\\Framework64\\v4.0.30319\\mscorlib.exe") not found
001c:err:module:import_dll Library mscorlib.dll (which is needed by L"C:\\windows
\\Microsoft.NET\\Framework64\\v4.0.30319\\mscorlib.exe") not found
001c:err:module:attach_dlls Importing dlls for L"C:\\windows\\Microsoft.NET\\Fra
mework64\\v4.0.30319\\mscorlib.exe" failed, status c0000135
000f:err:service:process_send_command service protocol error - failed to write p
ipe!
boys.jpg : negativeuser@Ubuntu1804:~/Desktop/Data-files/week08$
```

Note: Ignore the error messages generated by wine, the result is in the bottom line.

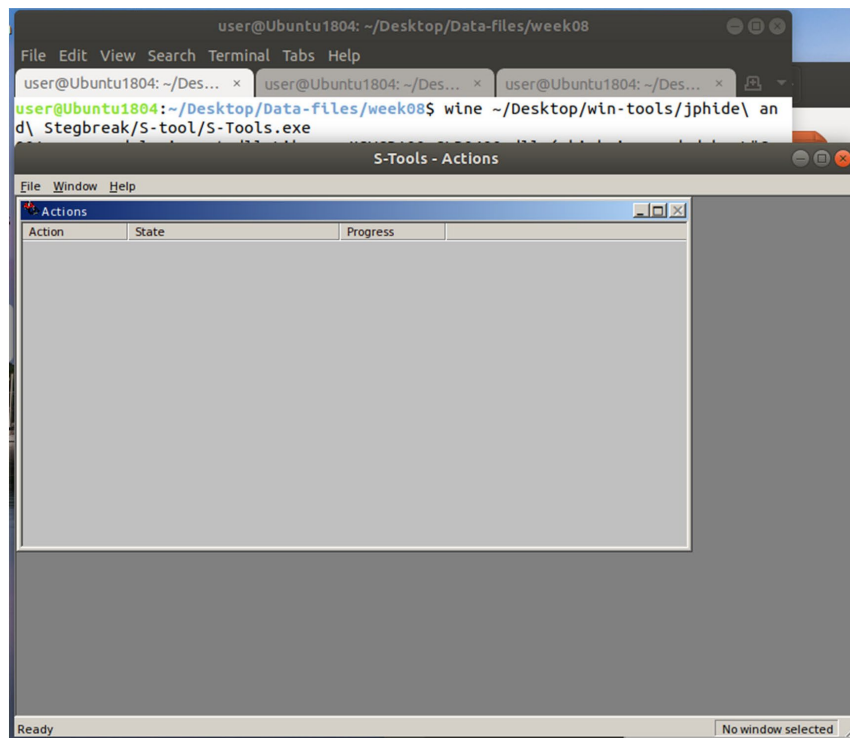
Therefore, *remember not to completely rely on the automated tools to detect steganography.*

Spend 10 mins or so to get used to the Stegbreak tool. Use it to break the other jpg images. After you have finished, open the words file and study what words are included in this file. Explain how this file is used by the Stegbreak tool.

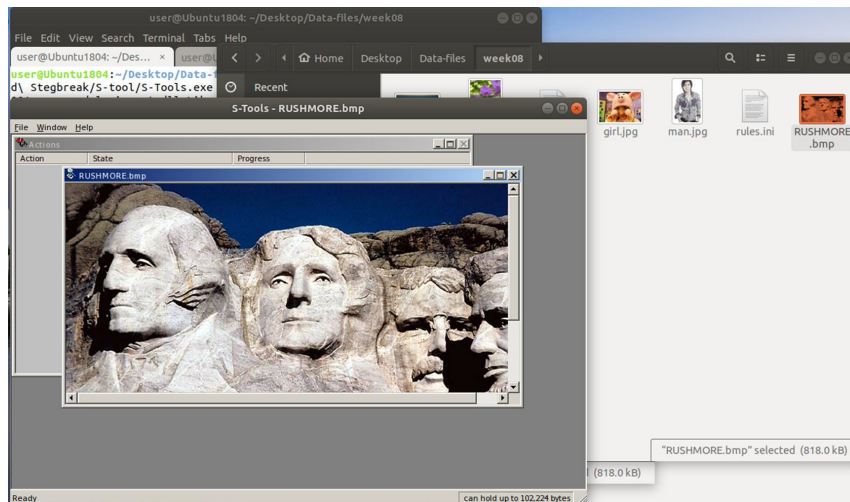
## 2. Introducing S-Tools

S-Tools is a GUI-based steganography tool which allows user to hide and reveal contents in a graphic file.

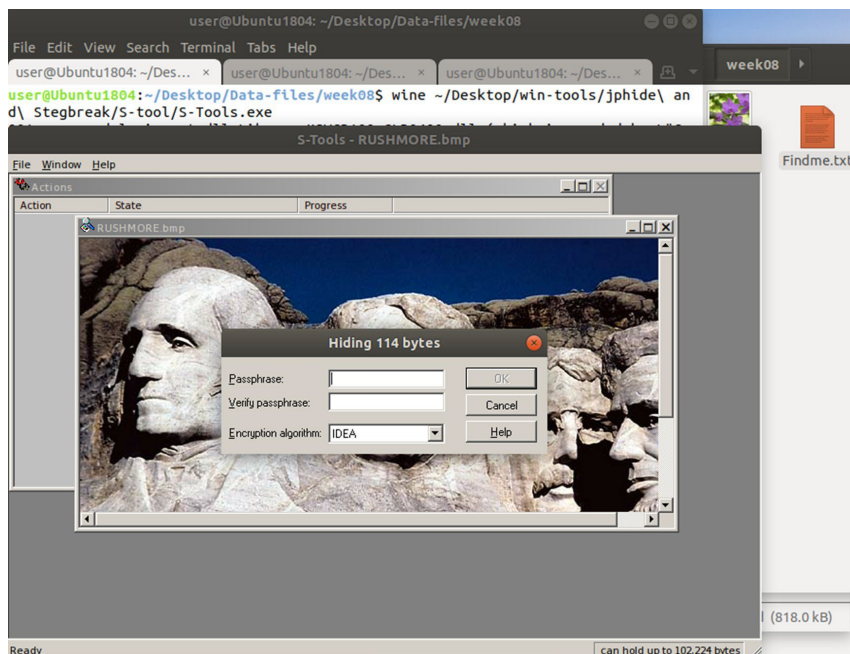
Launch the program through the wine emulator by typing the command “**wine ~/Desktop/win-tools/jphide\ and\ Stegbreak/S-tool/S-Tools.exe**”. You will see the following screen:



From the Desktop navigate to the directory “~/Desktop/Data-files/week08”, drag **RUSHMORE.bmp** to the S-Tools window. It shows



Drag **findme.txt** from the same directory to the S-Tools window, then you will see



Type **FREEDOM** in the Passphrase and Verify passphrase text boxes, and then click OK. The password dialog box will disappear. Now, right click the newly generated picture and **Save** the new image as **Steg.bmp** (overwrite the previous Steg.bmp file, if it already exists).



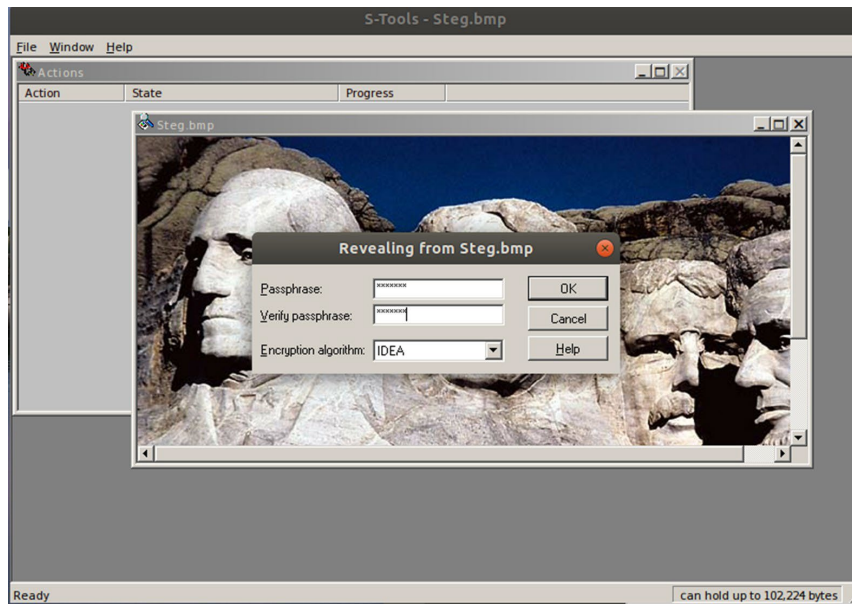


Now close the files opened in the S-Tools. In order to reveal the hidden text, you need to use the Reveal function provided in the S-Tools.

Open the Steg.bmp in S-Tools, right click the picture and select **Reveal**



Type in the passphrase **FREEDOM** and make sure you use IDEA encryption.



If the passphrase is correct, the hidden data will be revealed. Right click **Findme.txt** and select **Save As** to save the file.



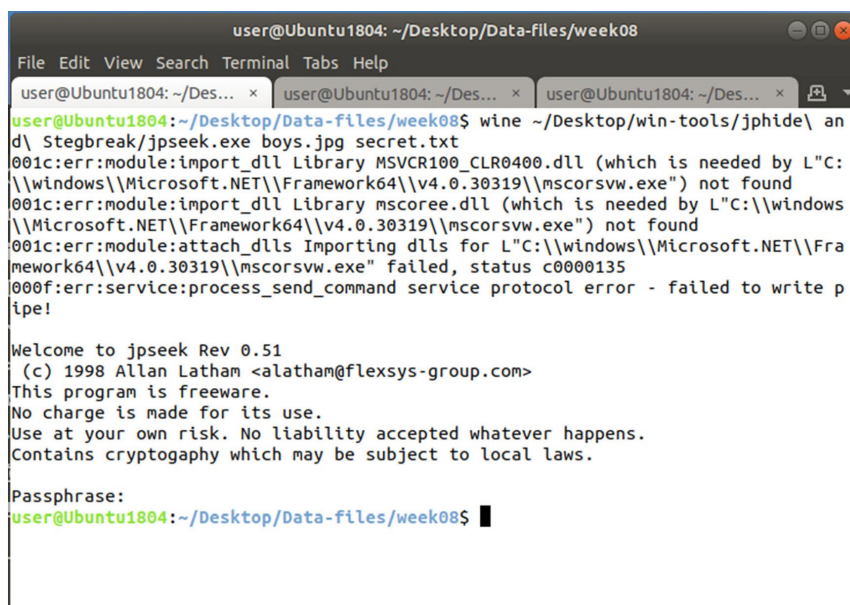
After you recovered the Findme.txt, close S-Tools.

Spend 10 minutes or so to get used to S-Tools and try different encryption schemes. Use your own passphrase and 3-DES encryption to hide the same text file in the same picture.

### 3. Using jpseek to Recover Steganography Images

We have recovered the password “donkey” for file “boys.jpg”. We will use the tool “jpseek” to reveal the hidden contents. Because jpseek is a Windows executable, we will use the wine emulator to launch the tool. Type in the

command “**wine ~/Desktop/win-tools/jphide\ and\ Stegbreak/jpseek.exe boys.jpg secret.txt**” and the program will prompt you for the password. Type in “donkey” and you will see that the program terminates. The output is saved in secret.txt.

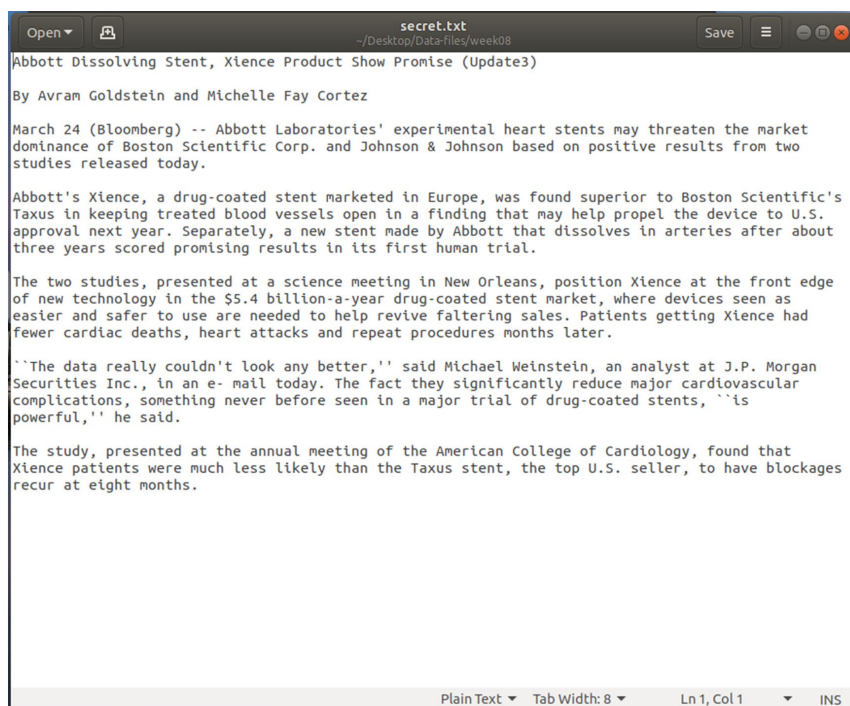


```
user@Ubuntu1804: ~/Desktop/Data-files/week08
File Edit View Search Terminal Tabs Help
user@Ubuntu1804: ~/Des... x user@Ubuntu1804: ~/Des... x user@Ubuntu1804: ~/Des... x
user@Ubuntu1804:~/Desktop/Data-files/week08$ wine ~/Desktop/win-tools/jphide\ and\
Stegbreak/jpseek.exe boys.jpg secret.txt
001c:err:module:import_dll Library MSVCR100_CLR0400.dll (which is needed by L"C:
\\windows\\Microsoft.NET\\Framework64\\v4.0.30319\\mscorlib.exe") not found
001c:err:module:import_dll Library mscorlib.dll (which is needed by L"C:\\windows
\\Microsoft.NET\\Framework64\\v4.0.30319\\mscorlib.exe") not found
001c:err:module:attach_dlls Importing dlls for L"C:\\windows\\Microsoft.NET\\Fra
mework64\\v4.0.30319\\mscorlib.exe" failed, status c0000135
000f:err:service:process_send_command service protocol error - failed to write p
ipe!

Welcome to jpseek Rev 0.51
(c) 1998 Allan Latham <alatham@flexsys-group.com>
This program is freeware.
No charge is made for its use.
Use at your own risk. No liability accepted whatever happens.
Contains cryptography which may be subject to local laws.

Passphrase:
user@Ubuntu1804:~/Desktop/Data-files/week08$ █
```

The contents of the file secret.txt are as following:



```
secret.txt
~/Desktop/Data-files/week08
Open Save
Abbott Dissolving Stent, Xience Product Show Promise (Update3)
By Avram Goldstein and Michelle Fay Cortez
March 24 (Bloomberg) -- Abbott Laboratories' experimental heart stents may threaten the market
dominance of Boston Scientific Corp. and Johnson & Johnson based on positive results from two
studies released today.
Abbott's Xience, a drug-coated stent marketed in Europe, was found superior to Boston Scientific's
Taxus in keeping treated blood vessels open in a finding that may help propel the device to U.S.
approval next year. Separately, a new stent made by Abbott that dissolves in arteries after about
three years scored promising results in its first human trial.
The two studies, presented at a science meeting in New Orleans, position Xience at the front edge
of new technology in the $5.4 billion-a-year drug-coated stent market, where devices seen as
easier and safer to use are needed to help revive faltering sales. Patients getting Xience had
fewer cardiac deaths, heart attacks and repeat procedures months later.
''The data really couldn't look any better,'' said Michael Weinstein, an analyst at J.P. Morgan
Securities Inc., in an e-mail today. The fact they significantly reduce major cardiovascular
complications, something never before seen in a major trial of drug-coated stents, ''is
powerful,'' he said.
The study, presented at the annual meeting of the American College of Cardiology, found that
Xience patients were much less likely than the Taxus stent, the top U.S. seller, to have blockages
recur at eight months.
Plain Text Tab Width: 8 Ln 1, Col 1 INS
```

## 4. Forensic Tasks

Try to use Stegbreak to crack Steg.bmp which you made in Section 2. Explain why it does/doesn't work. We will discuss this in our session.