

Computer & Network Forensics

Week 8 (Lab5)

Steganography

Documentation

Tool 1. OpenPuff (GUI)

Data Embedding

Download: [from here](#), and run on Windows or with `wine` on UNIX (Linux/MacOS)

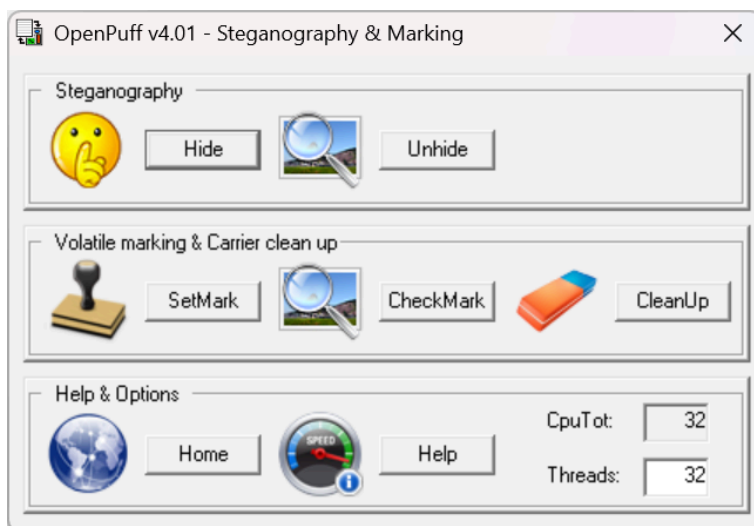
Embed:

- Open OpenPuff → choose “Hide”
- Add carrier (cover.wav), select data (secret.txt), set a password(s) and optional decoy carriers, click “Hide Data!”

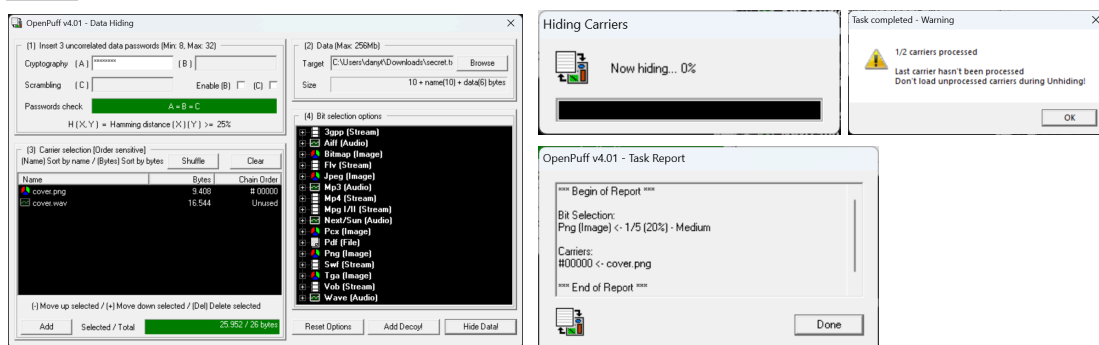
Extract:

- Open OpenPuff → choose “Unhide”
- Select stego carrier, enter keys/passwords, click “Unhide!”

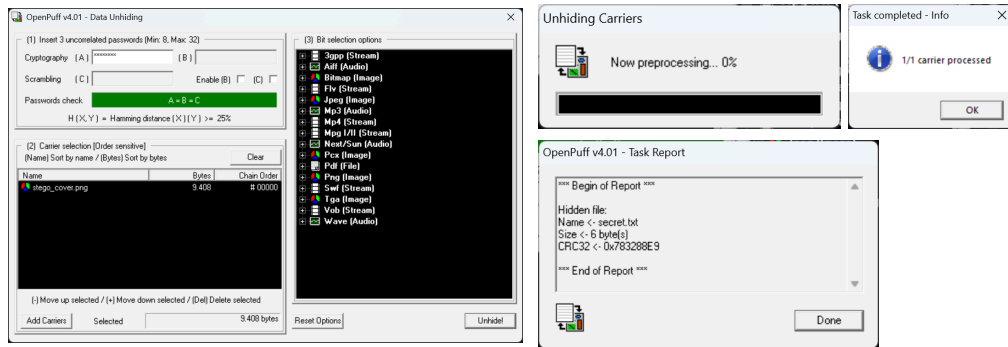
Windows (native)



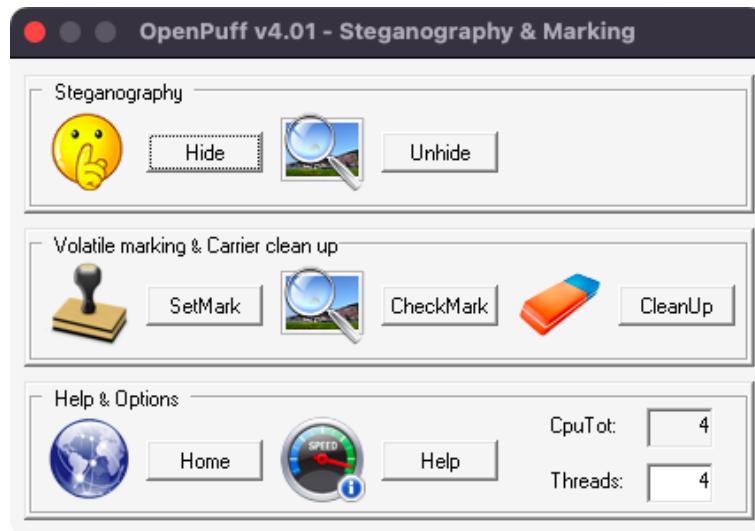
Hide:



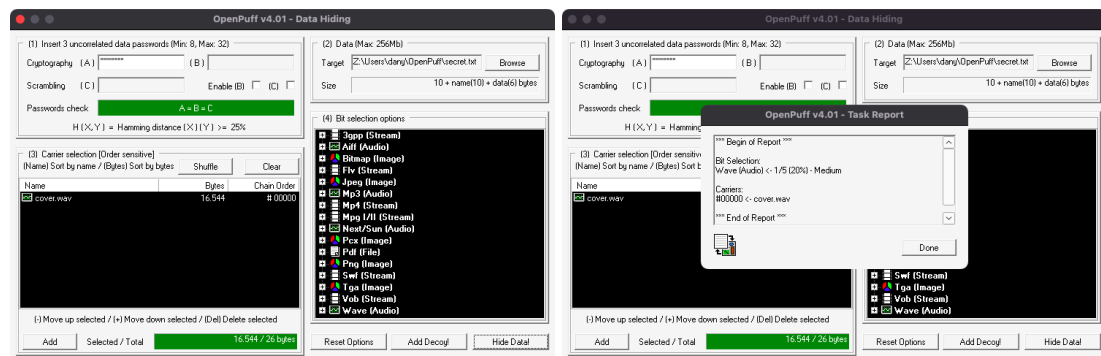
Unhide:



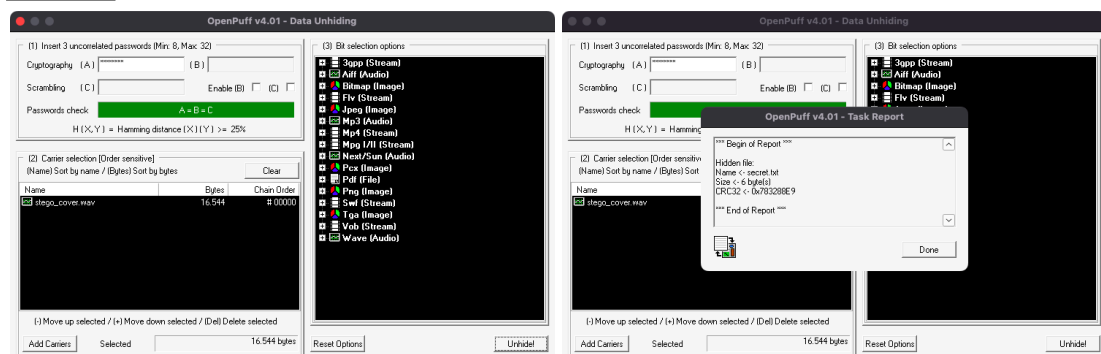
MacOS (with wine)



Hide:



Unhide:



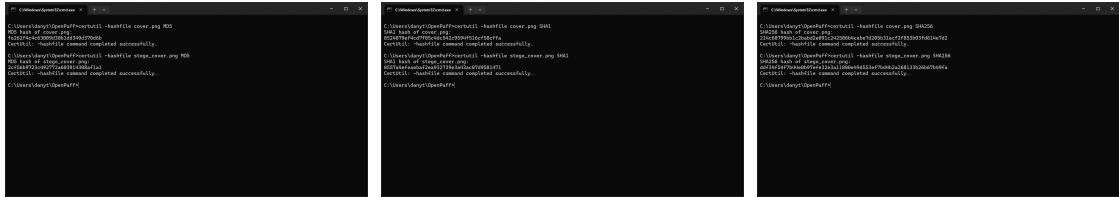
Hash Comparison

Windows (cmd - certutil)

→ MD5

→ **SHA1**

→ **SHA256**

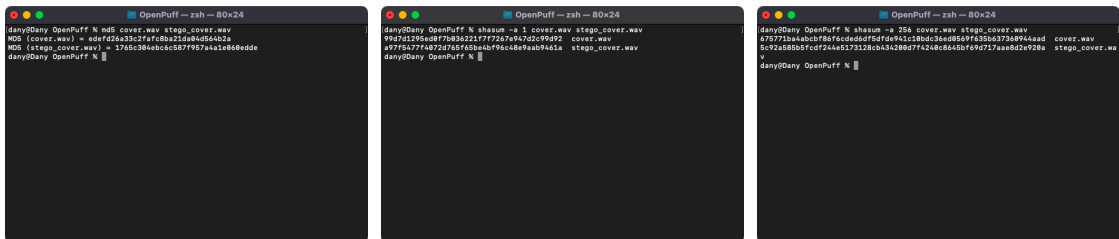


MacOS (zsh/bash - md5 & shasum)

→ **MD5**

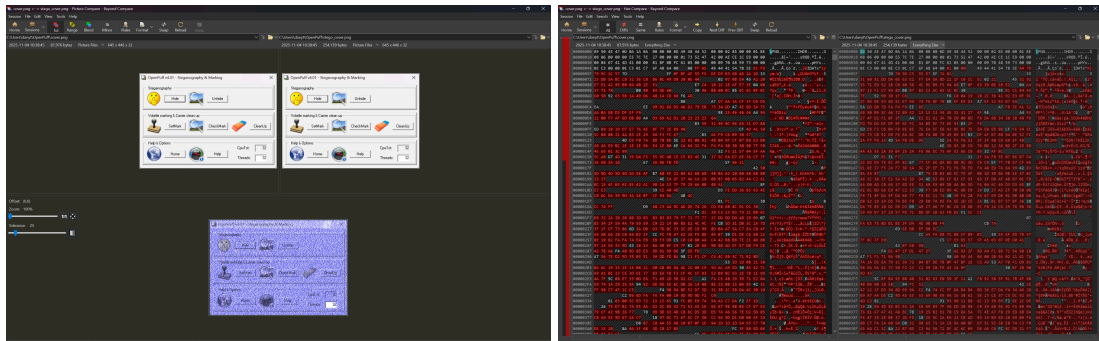
→ **SHA1**

→ **SHA256**



Binary/Hex Comparison

Beyond Compare ([ScooterSoftware](#)) – Windows



Tool 2.Steghide (CLI)

Data Embedding

Linux (kali, in my case)

Install: `sudo apt install steghide`

```
Embed: steghide embed -cf cover.jpg -ef secret.txt -sf stego_cover.jpg
```

Extract: `steghide extract -sf stego_cover.jpg`

```

1 [DAN670214@kali: ~]
2 # echo "secret" > secret.txt
3
4 [DAN670214@kali: ~]
5 # steghide embed -cf cover.jpg -af secret.txt -of steggy_cover.jpg
6 # mv steggy_cover.jpg
7 # cat steggy_cover.jpg
8 steghide "secret.txt" in "cover.jpg"... done
9 file size: 1048 "steggy_cover.jpg"... done
10
11 [DAN670214@kali: ~]
12 # rm secret.txt
13
14 [DAN670214@kali: ~]
15 # steghide extract -of steggy_cover.jpg
16 # mv steggy_cover.jpg
17 # cat steggy_cover.jpg
18 steghide extracted data to "secret.txt".
19
20 [DAN670214@kali: ~]
21 # cat secret.txt
22 secret
23
24 [DAN670214@kali: ~]
25 #

```

Hash Comparison

Linux (bash - md5sum & sha1sum, sha256sum)

```
md5sum → md5sum cover.jpg stego cover.jpg
```

```
sha1sum → sha1sum cover.jpg stego cover.jpg
```

```
sha256sum → sha256sum cover.jpg stego cover.jpg
```

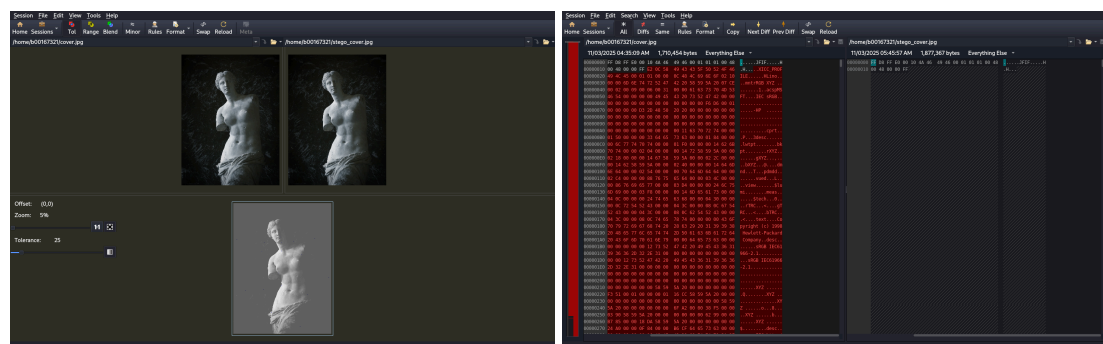
```

1 00007D24 RALL [7]
2 00007D25 RALL [7]
3 00007D26 RALL [7]
4 00007D27 RALL [7]
5 00007D28 RALL [7]
6 00007D29 RALL [7]
7 00007D2A RALL [7]
8 00007D2B RALL [7]
9 00007D2C RALL [7]
10 00007D2D RALL [7]
11 00007D2E RALL [7]
12 00007D2F RALL [7]
13 00007D30 RALL [7]
14 00007D31 RALL [7]
15 00007D32 RALL [7]
16 00007D33 RALL [7]
17 00007D34 RALL [7]
18 00007D35 RALL [7]
19 00007D36 RALL [7]
20 00007D37 RALL [7]
21 00007D38 RALL [7]
22 00007D39 RALL [7]
23 00007D3A RALL [7]
24 00007D3B RALL [7]
25 00007D3C RALL [7]
26 00007D3D RALL [7]
27 00007D3E RALL [7]
28 00007D3F RALL [7]
29 00007D40 RALL [7]
30 00007D41 RALL [7]
31 00007D42 RALL [7]
32 00007D43 RALL [7]
33 00007D44 RALL [7]
34 00007D45 RALL [7]
35 00007D46 RALL [7]
36 00007D47 RALL [7]
37 00007D48 RALL [7]
38 00007D49 RALL [7]
39 00007D4A RALL [7]
40 00007D4B RALL [7]
41 00007D4C RALL [7]
42 00007D4D RALL [7]
43 00007D4E RALL [7]
44 00007D4F RALL [7]
45 00007D50 RALL [7]
46 00007D51 RALL [7]
47 00007D52 RALL [7]
48 00007D53 RALL [7]
49 00007D54 RALL [7]
50 00007D55 RALL [7]
51 00007D56 RALL [7]
52 00007D57 RALL [7]
53 00007D58 RALL [7]
54 00007D59 RALL [7]
55 00007D5A RALL [7]
56 00007D5B RALL [7]
57 00007D5C RALL [7]
58 00007D5D RALL [7]
59 00007D5E RALL [7]
60 00007D5F RALL [7]
61 00007D60 RALL [7]
62 00007D61 RALL [7]
63 00007D62 RALL [7]
64 00007D63 RALL [7]
65 00007D64 RALL [7]
66 00007D65 RALL [7]
67 00007D66 RALL [7]
68 00007D67 RALL [7]
69 00007D68 RALL [7]
70 00007D69 RALL [7]
71 00007D6A RALL [7]
72 00007D6B RALL [7]
73 00007D6C RALL [7]
74 00007D6D RALL [7]
75 00007D6E RALL [7]
76 00007D6F RALL [7]
77 00007D70 RALL [7]
78 00007D71 RALL [7]
79 00007D72 RALL [7]
80 00007D73 RALL [7]
81 00007D74 RALL [7]
82 00007D75 RALL [7]
83 00007D76 RALL [7]
84 00007D77 RALL [7]
85 00007D78 RALL [7]
86 00007D79 RALL [7]
87 00007D7A RALL [7]
88 00007D7B RALL [7]
89 00007D7C RALL [7]
90 00007D7D RALL [7]
91 00007D7E RALL [7]
92 00007D7F RALL [7]
93 00007D80 RALL [7]
94 00007D81 RALL [7]
95 00007D82 RALL [7]
96 00007D83 RALL [7]
97 00007D84 RALL [7]
98 00007D85 RALL [7]
99 00007D86 RALL [7]
100 00007D87 RALL [7]
101 00007D88 RALL [7]
102 00007D89 RALL [7]
103 00007D8A RALL [7]
104 00007D8B RALL [7]
105 00007D8C RALL [7]
106 00007D8D RALL [7]
107 00007D8E RALL [7]
108 00007D8F RALL [7]
109 00007D90 RALL [7]
110 00007D91 RALL [7]
111 00007D92 RALL [7]
112 00007D93 RALL [7]
113 00007D94 RALL [7]
114 00007D95 RALL [7]
115 00007D96 RALL [7]
116 00007D97 RALL [7]
117 00007D98 RALL [7]
118 00007D99 RALL [7]
119 00007D9A RALL [7]
120 00007D9B RALL [7]
121 00007D9C RALL [7]
122 00007D9D RALL [7]
123 00007D9E RALL [7]
124 00007D9F RALL [7]
125 00007DA0 RALL [7]
126 00007DA1 RALL [7]
127 00007DA2 RALL [7]
128 00007DA3 RALL [7]
129 00007DA4 RALL [7]
130 00007DA5 RALL [7]
131 00007DA6 RALL [7]
132 00007DA7 RALL [7]
133 00007DA8 RALL [7]
134 00007DA9 RALL [7]
135 00007DAA RALL [7]
136 00007DAB RALL [7]
137 00007DAC RALL [7]
138 00007DAD RALL [7]
139 00007DAE RALL [7]
140 00007DAF RALL [7]
141 00007DB0 RALL [7]
142 00007DB1 RALL [7]
143 00007DB2 RALL [7]
144 00007DB3 RALL [7]
145 00007DB4 RALL [7]
146 00007DB5 RALL [7]
147 00007DB6 RALL [7]
148 00007DB7 RALL [7]
149 00007DB8 RALL [7]
150 00007DB9 RALL [7]
151 00007DBA RALL [7]
152 00007DBB RALL [7]
153 00007DBC RALL [7]
154 00007DBD RALL [7]
155 00007DBE RALL [7]
156 00007DBF RALL [7]
157 00007DC0 RALL [7]
158 00007DC1 RALL [7]
159 00007DC2 RALL [7]
160 00007DC3 RALL [7]
161 00007DC4 RALL [7]
162 00007DC5 RALL [7]
163 00007DC6 RALL [7]
164 00007DC7 RALL [7]
165 00007DC8 RALL [7]
166 00007DC9 RALL [7]
167 00007DCA RALL [7]
168 00007DCB RALL [7]
169 00007DCC RALL [7]
170 00007DCD RALL [7]
171 00007DCE RALL [7]
172 00007DCF RALL [7]
173 00007DD0 RALL [7]
174 00007DD1 RALL [7]
175 00007DD2 RALL [7]
176 00007DD3 RALL [7]
177 00007DD4 RALL [7]
178 00007DD5 RALL [7]
179 00007DD6 RALL [7]
180 00007DD7 RALL [7]
181 00007DD8 RALL [7]
182 00007DD9 RALL [7]
183 00007DDA RALL [7]
184 00007DDB RALL [7]
185 00007DDC RALL [7]
186 00007DD5 RALL [7]
187 00007DD6 RALL [7]
188 00007DD7 RALL [7]
189 00007DD8 RALL [7]
190 00007DD9 RALL [7]
191 00007DDA RALL [7]
192 00007DDB RALL [7]
193 00007DDC RALL [7]
194 00007DD5 RALL [7]
195 00007DD6 RALL [7]
196 00007DD7 RALL [7]
197 00007DD8 RALL [7]
198 00007DD9 RALL [7]
199 00007DDA RALL [7]
200 00007DDB RALL [7]
201 00007DDC RALL [7]
202 00007DD5 RALL [7]
203 00007DD6 RALL [7]
204 00007DD7 RALL [7]
205 00007DD8 RALL [7]
206 00007DD9 RALL [7]
207 00007DDA RALL [7]
208 00007DDB RALL [7]
209 00007DDC RALL [7]
210 00007DD5 RALL [7]
211 00007DD6 RALL [7]
212 00007DD7 RALL [7]
213 00007DD8 RALL [7]
214 00007DD9 RALL [7]
215 00007DDA RALL [7]
216 00007DDB RALL [7]
217 00007DDC RALL [7]
218 00007DD5 RALL [7]
219 00007DD6 RALL [7]
220 00007DD7 RALL [7]
221 00007DD8 RALL [7]
222 00007DD9 RALL [7]
223 00007DDA RALL [7]
224 00007DDB RALL [7]
225 00007DDC RALL [7]
226 00007DD5 RALL [7]
227 00007DD6 RALL [7]
228 00007DD7 RALL [7]
229 00007DD8 RALL [7]
230 00007DD9 RALL [7]
231 00007DDA RALL [7]
232 00007DDB RALL [7]
233 00007DDC RALL [7]
234 00007DD5 RALL [7]
235 00007DD6 RALL [7]
236 00007DD7 RALL [7]
237 00007DD8 RALL [7]
238 00007DD9 RALL [7]
239 00007DDA RALL [7]
240 00007DDB RALL [7]

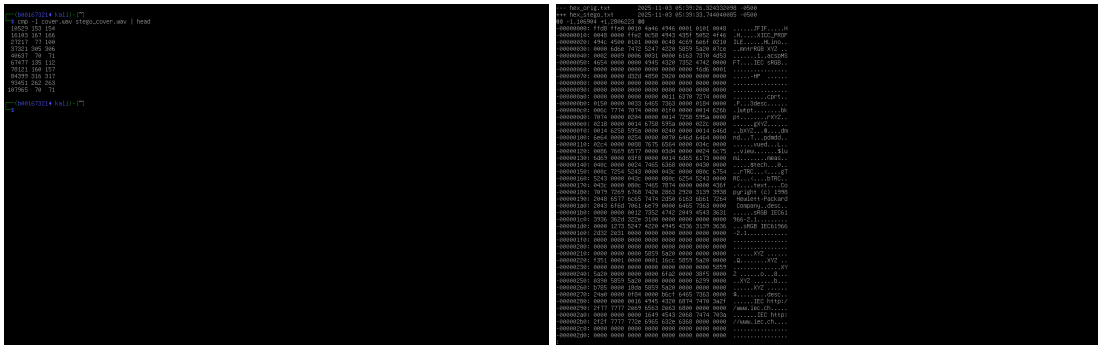
```

Binary/Hex Comparison

Beyond Compare ([ScooterSoftware](#)) – Linux



```
cmp -l (list differing bytes) | xxd & diff -u (hex comparison)
```



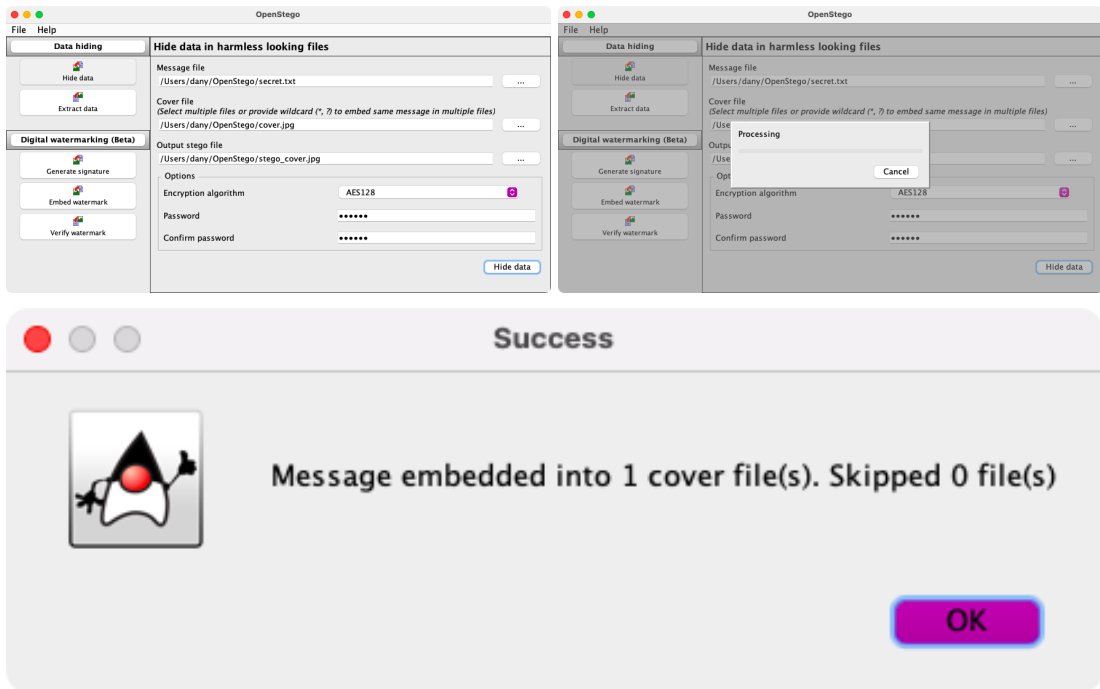
Tool 3. OpenStego (Java GUI)

Data Embedding

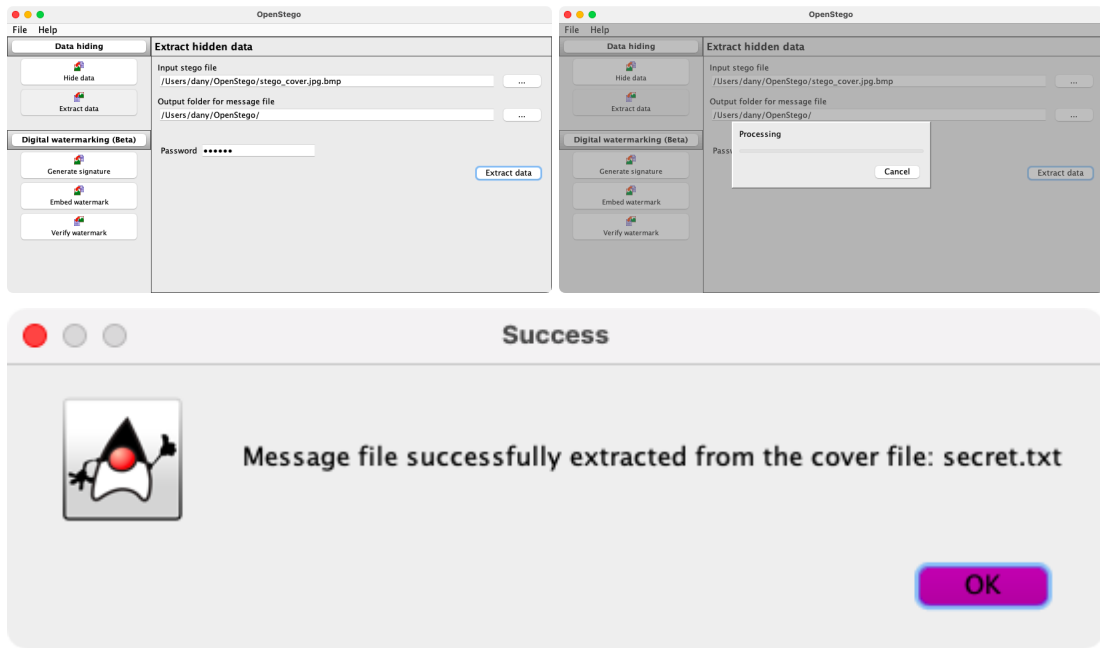
Download: [from here \(github – openstego/releases\)](https://github.com/openstego/releases), and run jar file (java need to be installed)

MacOS (jar file application – can be executed on any machine with java installed)

Hide data:



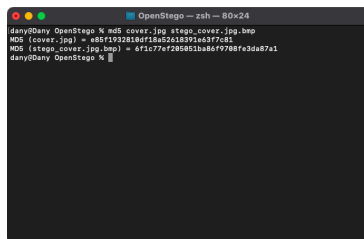
Extract data:



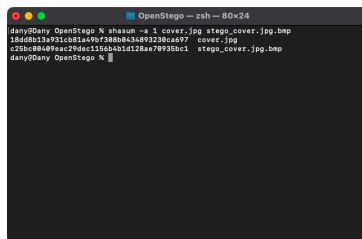
Hash Comparison

MacOS (*zsh/bash* - *md5* & *shasum*)

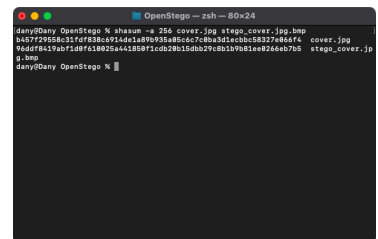
→ MD5



→ SHA1

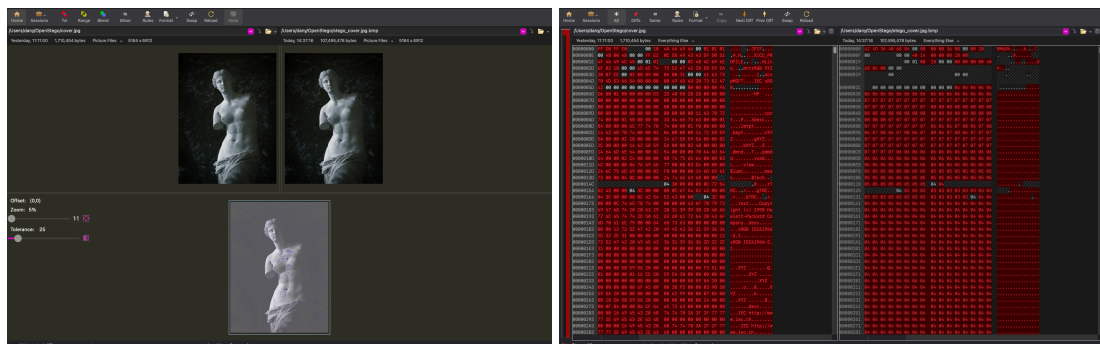


→ SHA256



Binary/Hex Comparison

Beyond Compare ([ScooterSoftware](#)) – MacOS

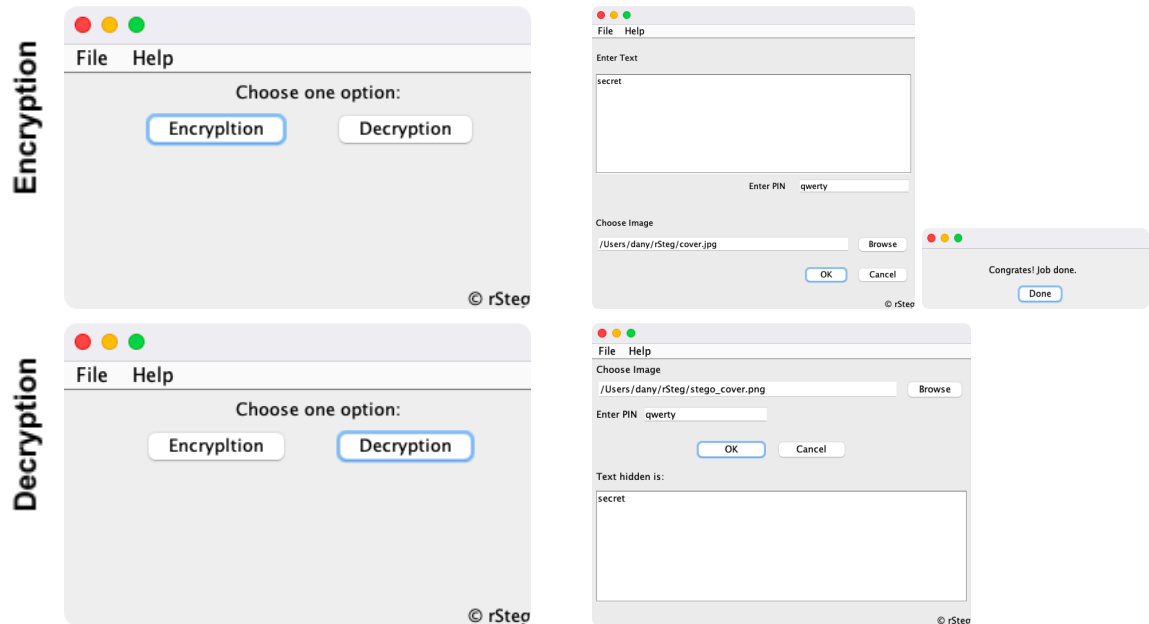


Tool 4.rSteg

Data Embedding

Download: [from here \(softpedia.com\)](https://softpedia.com), and run jar file (java need to be installed)

MacOS (jar file application – can be executed on any machine with java installed)



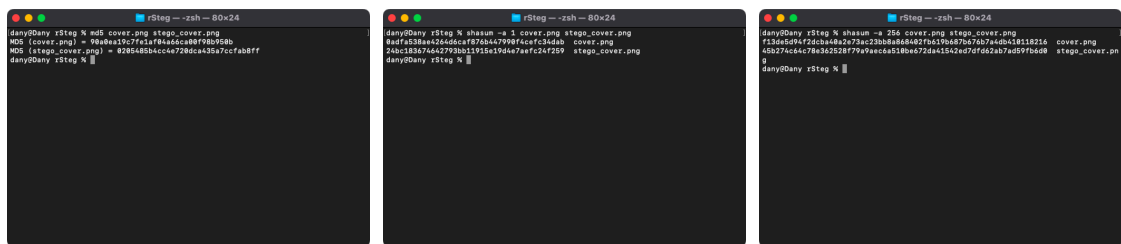
Hash Comparison

MacOS (zsh/bash – md5 & shasum)

→ MD5

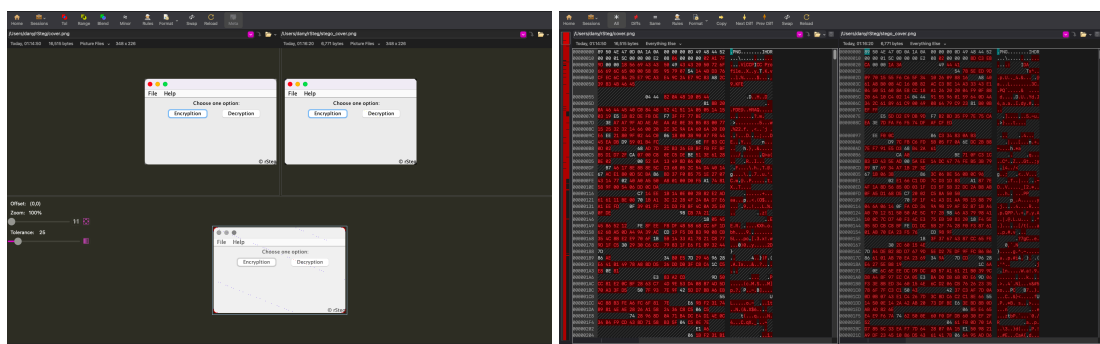
→ SHA1

→ SHA256



Binary/Hex Comparison

Beyond Compare (ScooterSoftware) – MacOS



Questions

1. How would you Investigate Hidden Information?

- Compute file hashes (MD5, SHA-1, SHA-256) and compare with known originals to detect any change.
- Use metadata tools (`exiftool`) to identify suspicious metadata.
- Use steganalysis tools such as `stegdetect`, `zsteg`, `stegseek`, and `binwalk` to check for signatures or anomalies.
- Perform entropy analysis to detect unnatural uniformity or noise bumps.
- Do a binary/hex comparison (`Beyond Compare` or `xxd + diff`) to identify changed byte offsets.
- Inspect image bitplanes and color channels (with `stegsolve`) and check LSB planes visually.
- Attempt extraction with known stego tools (`OpenPuff`, `Steghide`, `OpenStego`) using guessed passwords if necessary.

2. Compare and Contrast Steganography and Encryption:

- **Purpose:** Encryption hides content (makes it unreadable), steganography hides existence of a message.
- **Visibility:** Encrypted data is visible but unintelligible; steganographic data is concealed inside a carrier to avoid detection.
- **Use together:** Best practice often combines both — encrypt payload first, then hide it (defense-in-depth).
- **Detection:** Encrypted files usually show high entropy and are clearly different; steganography aims to minimize detectable changes so carriers look normal.
- **Legal/forensic implications:** Stego can bypass cursory inspections, while encryption draws attention (may trigger suspicion or legal obligations in some jurisdictions).

3. List Data Breaches Involving Steganography:

- **Stegoloader (Gatak) Malware (2015)** – Malware used steganography to conceal its code within PNG images downloaded from the web to evade antivirus detection.
- **Turla APT Campaign (2019)** – The Turla hacking group embedded encrypted commands in Instagram image comments to control malware remotely.
- **Vawtrak Banking Trojan (2016)** – Used steganography to hide configuration data inside favicons, making detection more difficult.

4. List 4 Authoritative Figures in Steganography:

- **Jessica Fridrich** – Leading researcher in digital image steganography and steganalysis, known for developing modern detection techniques.
- **Neil F. Johnson** – Early pioneer who co-authored foundational papers on steganography and steganalysis in the 1990s.
- **Niels Provos** – Creator of the OutGuess tool and researcher on statistical defenses against steganalysis.
- **Sushil Jajodia** – Academic expert in information hiding and computer security; co-authored seminal works on steganography theory.