

An abstract network diagram composed of various sized grey circles (nodes) connected by thin grey lines. Some nodes are highlighted with blue outlines or solid blue dots. The diagram is positioned in the top-left and bottom-right corners of the slide.

DISCLOSE Project

Final Presentation - Studio 2

Introduction

Digital Forensics Students - Year II

Elisabeth Øvensen

Lorena Carthy

Elisabeth Schanke



Agenda

- ◎ Project Overview
- ◎ Achievements
- ◎ Teamwork
- ◎ Challenges
- ◎ Main lessons learned

Project Overview:

Aim & Objectives

The project objective is to create practical challenges for educational purposes in the Digital Forensics field, with three difficulty levels.

Our project aim is to better our understanding in our field and get more practical experience.

Subjects covered:

- ⊙ Steganography
- ⊙ Cryptography
- ⊙ Photo Forensics

Steganography: Example 1



```

Hex Editor Neo
File Edit View Select Operations Bookmarks NTFS Streams Tools History Window Help

krista-mangulsone-53122-unsplash.jpg x
00073174 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
00072f10 8f a5 72 56 db 53 a2 9a f7 cf 2d bd fb 34 4b 3b 8vV0Se&+I~4K;
00072f20 4c 0c 9b 46 d3 83 d0 9a d4 79 b1 a7 18 54 91 b5 L.v0fD00ys.5.T p
00072f30 55 f1 ea aa 30 3f 9d 67 5f 6a d7 1b a2 8f ec 91 UR&*0? g_j..e i'
00072f40 48 d3 15 de 08 c7 24 ff 00 41 54 db 5c b6 ba 62 H0.P.Çsy.AT0\T*b
00072f50 56 d6 36 cb 08 b0 09 53 84 e3 15 c6 9a e8 77 72 V04E".S.a.E&éwr
00072f60 c8 a7 63 2b 4e 19 58 fc 85 81 1b 97 a1 15 13 da 2Sc=N.Xu_..j..0
00072f70 3c ca e9 6e 44 ae 79 d8 3e f3 7d 3d 6b 69 ae f4 <E&nD0ys>0]=ki00
00072f80 c4 90 ab 41 22 92 0a fe 87 38 fe eb 92 d4 a7 d0 Å aA""..u80e'0S0
00072f90 a3 05 93 55 9a d6 40 57 6b 3a 6e c1 ed ca 9c 8a s."U&0QWk:nA&E&s
00072fa0 e7 a9 15 63 68 4e 57 38 4d 66 fc a4 c6 17 43 1c q0.chN0M0fUR&.C.
00072fb0 8b 90 db f7 02 3d b1 5c 4c fa a8 05 20 85 cc 71 < 0+.="a\0&"._iq
00072fc0 8e a3 fb ec df de af 57 be 51 af a4 69 79 a8 58 2&01B"WQ"riy"X
00072fd0 5e 48 a3 11 5d 23 f9 73 27 a0 70 df 7c 0f ce bc "HE.j#as' pB(.I&
00072fe0 8f 5d 46 4c 41 47 20 53 54 41 52 54 c6 43 14 b8 ]FLAG STARTEC..
00072ff0 89 77 c6 57 ea bd 0f b1 ac 15 0e a8 ec 85 64 d7 2u&N0&.a-..i.d+
00073000 bc 73 d7 5a c5 54 48 45 20 44 45 41 4c 45 52 4e 4s+Z&THE DEALERN
00073010 05 9b 37 10 2c a5 d7 77 1f ec fc bf 35 71 f7 be .>7.,Ww.iü;5q÷4
00073020 49 53 20 41 20 46 55 52 52 59 6b 98 b1 d5 ad ae IS A FURRYk~±0-0
00073030 19 61 28 e8 f1 46 4c 55 46 46 59 34 65 b9 94 49 .a(èñFLUFFY4e1"I
00073040 74 4b 00 da 46 b1 25 43 41 54 cb 6f 9a 17 0d d9 tKEÚF&CATËoš..Û
00073050 95 b8 3c f1 5f 44 e8 7a 3e 8d e3 5b b3 69 79 a5 *.<ñ_Dèz> ã[³iyW
00073060 8d 3b 51 92 02 e6 ee d3 9b 69 15 46 49 78 fb 71 ;Q'.æi0>i.FIXûq
00073070 e9 5f 07 c3 30 7b 29 48 dc c6 dd 98 é_Ã0()HÜ&Ý~û²ip
00073080 0 45 4e 44 2e .jæ³ñ0AFLAG END.
00073090 f 00 68 93 c0 u+?)c..5u8fy.h"A
000730a0 2 3d 4b c1 4e "F 5m0:5&A&=KAN
000730b0 c 30 0e a5 a5 *Wv.-H&0&A10.WW
000730c0 c 9b 56 d4 be A0.).Å&xZ.0&v0&
  
```



Cryptography: Example 2

Secret Key:

M4rg4r3TAtw00d

```
1 EnCt290235f18df140f649eefc66f258499e2e92fe91990235f1
2 216II5lqeXemx5dv9IP16ReTkji/4I9MWI/dzKL9qUt1vYPhZUqP
3 Si3GGWs9KSwgMjVZEshDCN4TMGPwszpLok3qsaBkj6bQ7vV0m8E
4 SDrM7RkR/i8NMxbTl/h1xJh1We9Mo8wGox+aXuC350ZH9ufpeJw
5 DXCxVwZFph3BGsC1boVmZpYMPaEhX8wGox+aXuC350ZH9ufpe%FG
6 DXCxVwZFph3BGsC1boVmZpYMPaEhXDoIgkH9CQeMo=EbyYLiJeLe
7 CPvKpASq2wNVC+dM0ETqMSk66KOToScn3RsoT1GcHE2CuVRGWVS5
8 awdjdOP09GVjHNJfDFSRRop940Vv'8wy8bfMM4dZfEMVtScid8M5
9 vR161A6lMMRSk=ILWg28NdU3D32zeLCeV/BlpZm4z0LsOQYLxGpR
10 UEe1hG7GtHMSmnQYJNbSSuqLMLd7iLn/B9NMw+bqQkCZXcKvZlBF
```

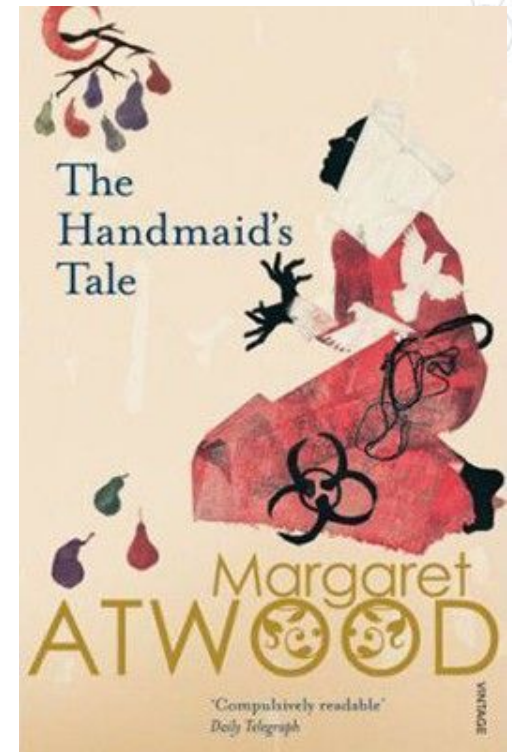
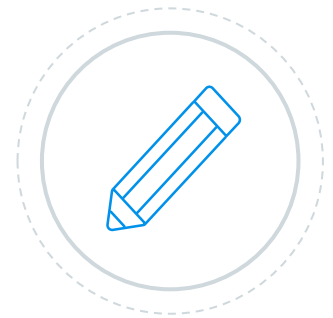


Photo Forensics: Example 3



Guided Solutions for Educators



Answer Sheet Level 2 - Photo Forensics

The Challenge

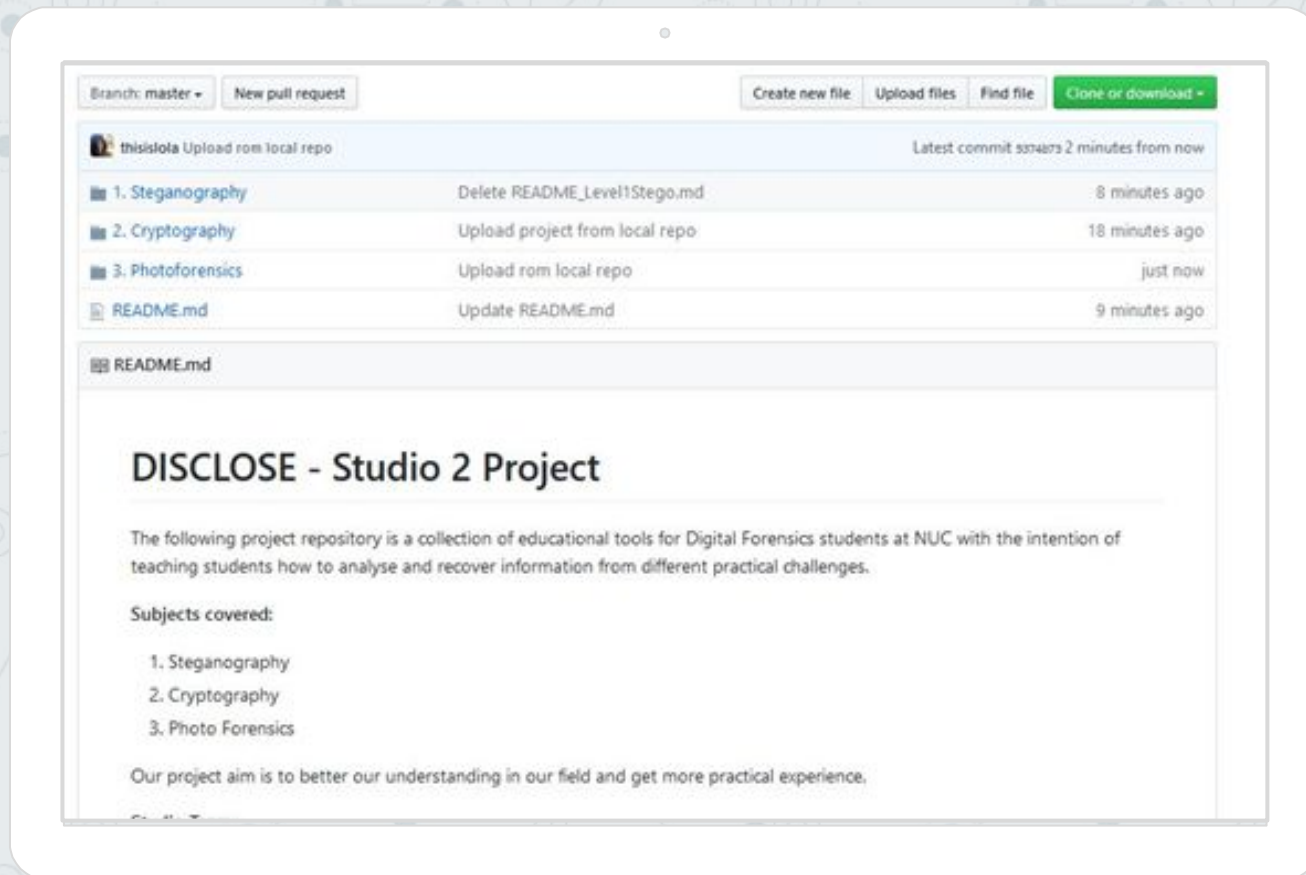
A suspect's alibi puts them in [REDACTED] (location) at the time of the crime. Pictures were found in the suspect's seized phone. Determine if the pictures in question create a timeline supporting the alibi or otherwise.

How To: Creation of the challenge

The pictures include location coordinates in the [REDACTED] (location). The pictures match the seized phone and...

These are the correct GPS locations:

Original GPS	Location	Device	EXIF Data
45678903	Mi Casa 123, Tucasa	iPhone 9	Yes
454545454	Mi Casa 123, Tucasa	iPhone 9	Yes
45612121203	Mi Casa 123, Tucasa	iPhone 9	Yes
45232303	Mi Casa 123, Tucasa	iPhone 9	Yes
45678903	Mi Casa 123, Tucasa	iPhone 9	Yes



Github

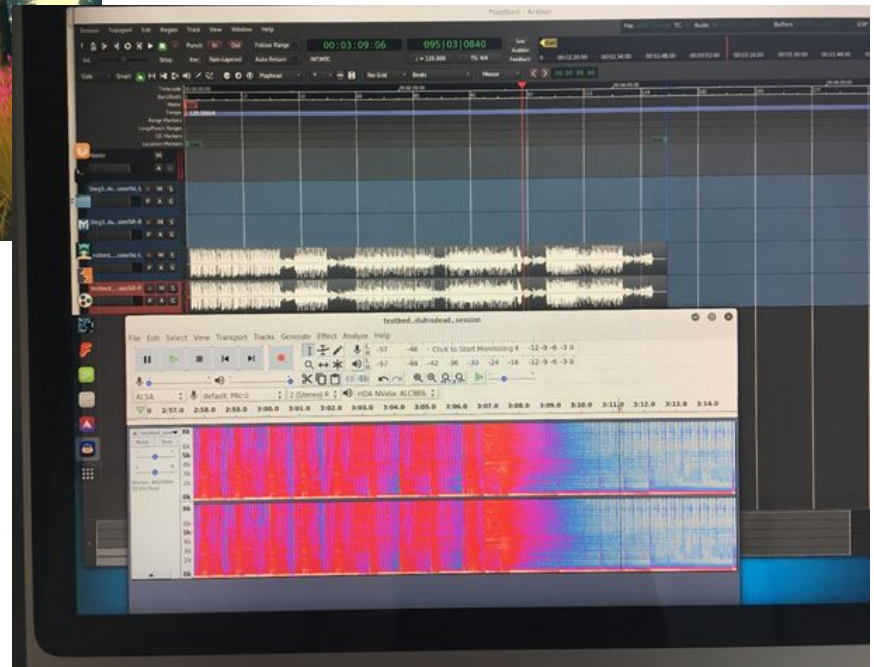
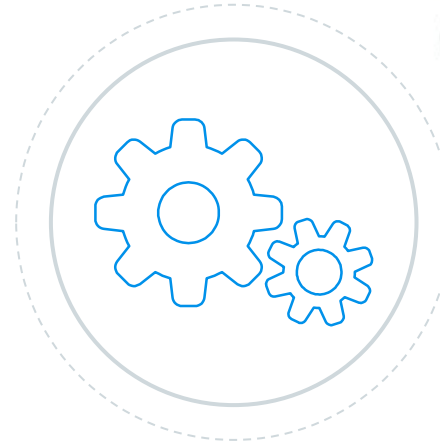
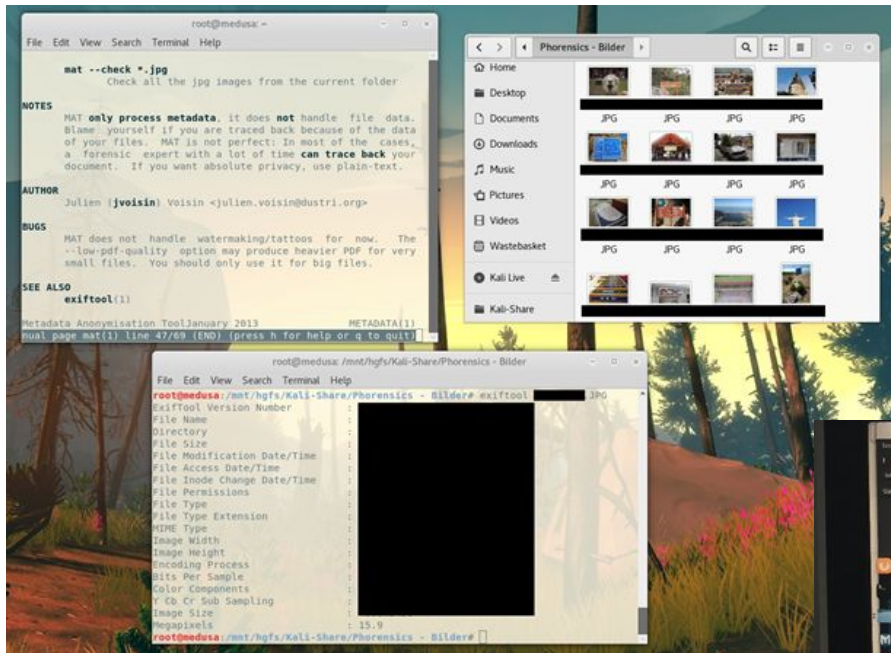
<https://github.com/thisislola/DISCLOSE>

Achievements

- ◎ We managed to reach our goal in creating the challenges.
- ◎ We tested the quality of our challenges with an external tester.
- ◎ We learned how to use the tools to cover (Anti-forensics) and uncover the challenges (Forensics).
- ◎ We learned how to better plan a project and work together as a team.

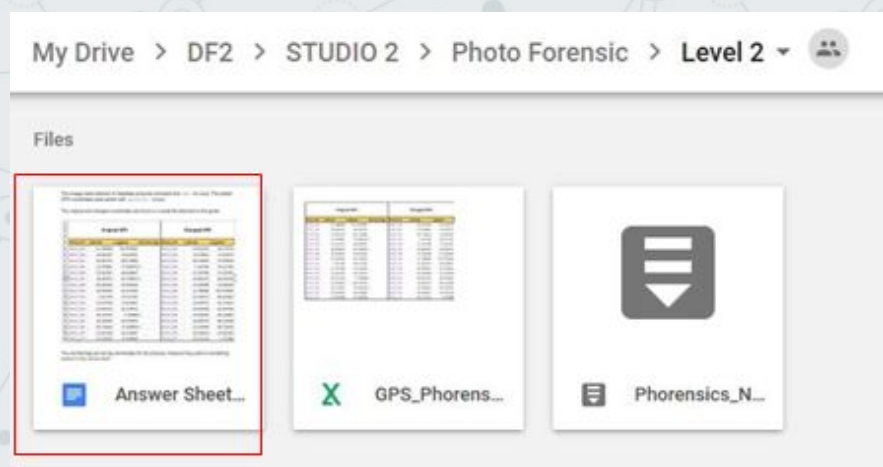
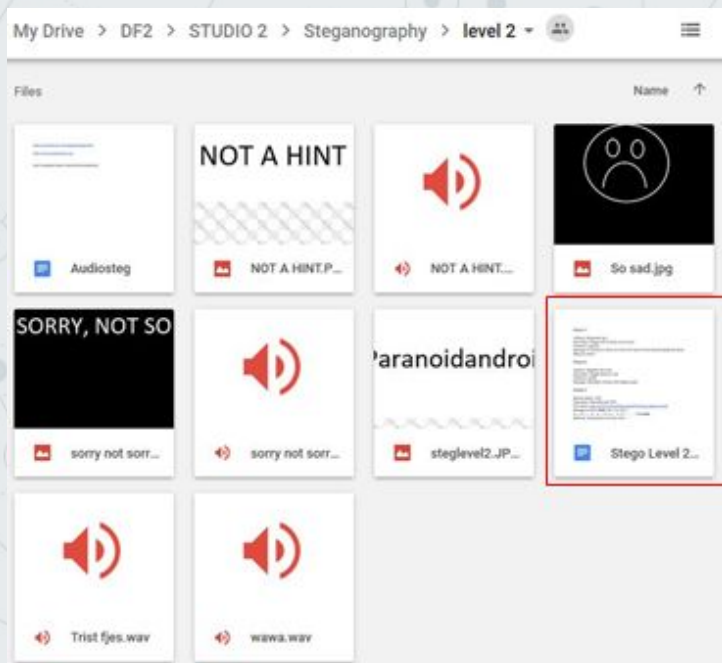
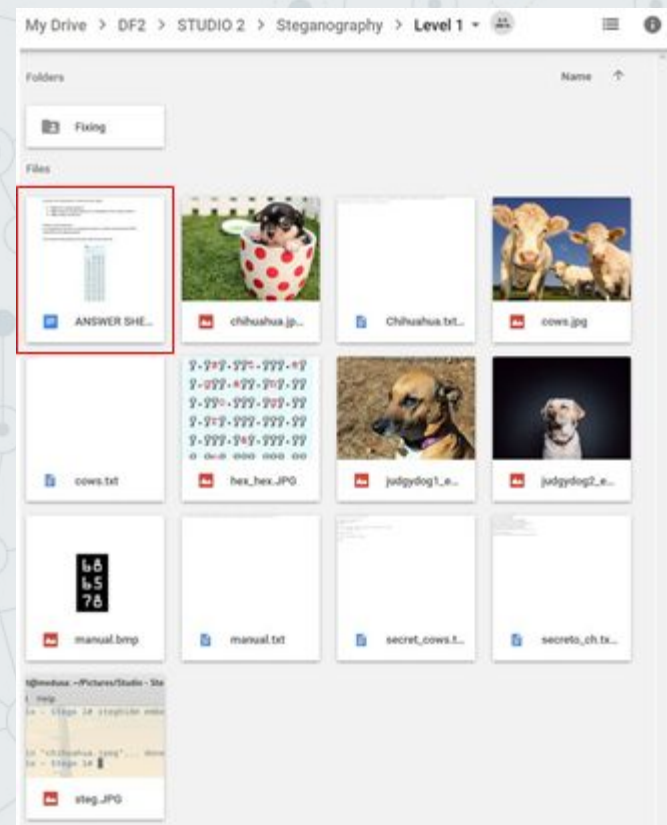
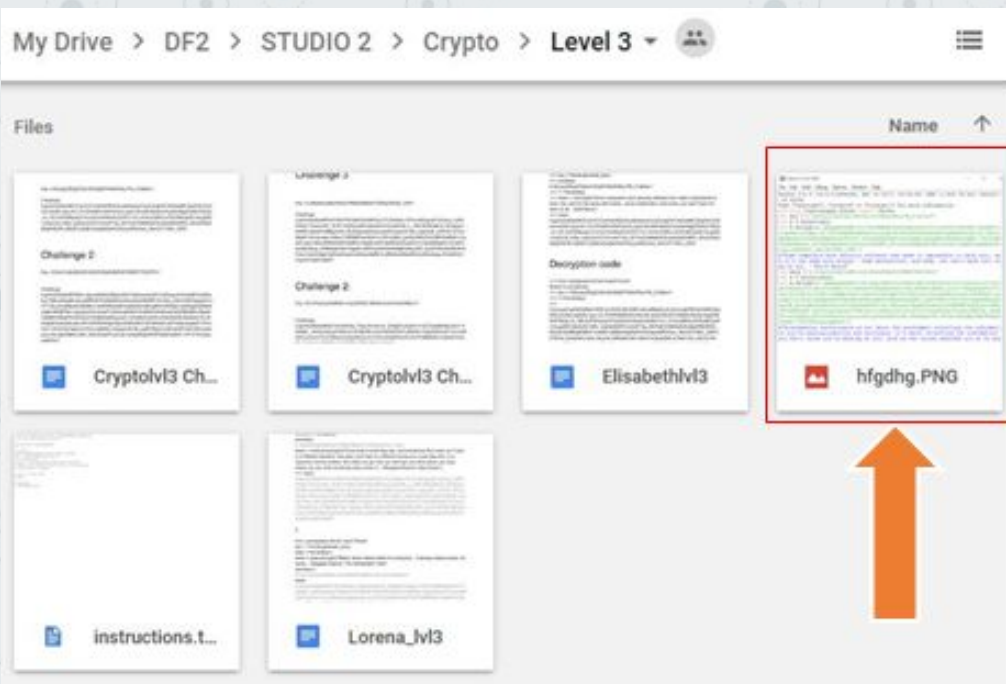


Achievement Example



Teamwork

- ◎ New team member in January
- ◎ Great group dynamics
- ◎ We divided some tasks, while the others were performed as a team
- ◎ We met both on Skype and on campus regularly, weekly at a minimum
- ◎ We gave each other feedback
- ◎ Tools used for project planning were Skype, Github, and Google Drive



Challenges



- ⦿ Testing revealed issues that were fixed
- ⦿ Too much work initially. Feedback from course leader led to changes in the project
- ⦿ The difficulty levels were hard to estimate



Main Lessons Learned

- ◎ We developed an understanding of project planning and how to work together in a group as well as progressing in our field.
- ◎ We learned how to reflect on our work and give each other constructive feedback.
- ◎ We learned about the professional issues in a project like ours.
- ◎ Learned more about Linux and associated tools.



Thanks!

Any questions?

Our project on Github:

<https://github.com/thisislola/DISCLOSE>