Sri Lanka Institute of Information Technology

Escort The Tourists

ISP Project Report

Information Security Project 2021

Project ID: ISP-21-GRP-43

Submitted by:

IT Number	Name
IT19184104	B.G.R.D.Samarathunga
IT19048260	N.A.W.D.V.Nanayakkara

13/11/2021

Abstract

Capture the flag (CTF) activities are becoming increasingly popular in the world of computer security for recruiting, training, assessment, and entertainment. There is a wide range of CTF software available today; this software may be separated into game engines and challenge components. Game engines such as TryHackMe that allow dynamic challenges and those that support static challenges can be used to decide the overall style of the competition. A limited number of game engines are open and available for anybody to use to create their own challenges, however the most majority are proprietary solutions.

Over the previous years, the Cyber Security group at Sri Lanka Institute of Information Technology has organized annual CTF event for its undergraduates, testing various CTF kinds and engines and ultimately producing statistics on the state-of-the-art in this sector. While these events were largely successful in terms of the above-mentioned aims, a rigorous examination of the software utilized by the Cyber Security group and more broadly throughout the field highlighted significant flaws in existing CTF techniques. Current software, in particular, should be enhanced in terms of challenge realism, affordability and accessibility, educational uses, and research possibilities

Acknowledgement

We would like to offer our heartfelt gratitude to Mr. Lakmal Rupasinghe, as well as Ms. Chathuri Udagedara, Ms. Menaka Moonamaldeniya and Ms. Laneesha Ruggahakotuwa, who assisted and directed us in successfully completing the CTF project.

A project serves as a link between theoretical and practical learning, and it was with this mindset that we worked on the project and were able to complete it thanks to timely assistance and the efforts of those who assisted us.

Once again, we'd want to express our gratitude to our colleagues and seniors for their support and encouragement in developing and executing our project. All of them owe us a duty of gratitude. We were only able to build the project and make it a positive and pleasurable experience because of them.

Declaration

We declare that this project report or part of it was not a copy of a document done by any organization, university any other institute or a previous student project group at SLIIT and was not copied from the Internet or other sources.

Project Details

Project Title	Escort The Tourist
Project ID	ISP-21GRP-43

Group Members

Reg. No	Name	Signature
IT19184104	B.G.R.D.Samarathunga	Rashmika
IT19048260	N.A.W.D.V.Nanayakkara	Dilith

Table of Contents

List of Figures

List of Tables

List of Acronyms and Abbreviations

Abbreviations	Definitions
CTF	Capture The Flag
Flag	Secrets hidden in purposefully-vulnerable programs or websites
Jeopardy-style	Competitors with a set of questions that reveal clues that guide them in solving complex tasks in a specific order
Gamification	Adding game mechanics into nongame environments
Exploit	A software tool designed to take advantage of a flaw in a computer system, typically for malicious purposes such as installing malware.
Forensics	Collect, process, preserve, and analyze computer-related evidence
Tradecraft	Allows security professionals to position each improvement in attackers' capabilities

Table 1

1. Introduction

1.1 Problem Statement

Capture The Flag (CTF) is a sort of Information/Cyber security event or competition that challenges to get or find a specific text that might be hidden on a server. This specific text is called the flag. Attackers should be capable of performing some hacking skills like reverse engineering, cryptography, forensics to find the flag. There are two main common types of CTFs; namely, Jeopardy-style CTFs and Attack & Defense CTFs.

Computer security represents a challenge to education due to its interdisciplinary nature. Topics in computer security are drawn from areas ranging from theoretical aspects of computer science to applied aspects of information technology management. This makes it difficult to encapsulate the spirit of what constitutes a computer security professional.

One approximation for this measure has emerged the capture the flag competition. Attack-oriented CTF competitions try to distill the essence of many aspects of professional computer security work into a single short exercise that is objectively measurable. The focus areas that CTF competitions tend to measure are vulnerability discovery, exploit creation, toolkit creation, and operational tradecraft.

A modern computer security professional should be an expert in at least one of these areas and ideally in all of them. Success in CTF competitions demands that participants be an expert in at least one and ideally all these areas. Therefore, preparing for and competing in CTF represents a way to efficiently merge discrete disciplines in computer science into a focus on computer security.

1.2 Product Scope

TryHackMe has been used to host the project and allow individuals and groups worldwide to attempt the CTF. TryHackMe is a website that teaches cyber security through short, gamified realworld laboratories. We include information for both total beginners and experienced hackers, with instructions and challenges to accommodate different learning methods.

1.3 Project Report Structure

This project report is structured and multiple main topics and multiple subtopics. This includes, Methodology, which consists of Requirements and Analysis, Design, Implementation and Testing. Secondly, Walkthrough is there to explain how to complete the CTF. Then the Evaluation, which includes Project Results and Future work. Finally, the report includes the Conclusion of the project.

2. Methodology

2.1 Requirements and Analysis

The main requirement of this project is to create a competitive environment which can be used for tournaments, and it can be a lot of fun tackling challenges with friends. And also, this project is used as a learning tool for everyone that is interested in cyber security, and it can help sharpen the tools they have learned. Jeopardy CTF's are the most common kind of CTF.

2.2 Design

The design in TryHackMe platform is premade design which is not customizable but there are all the essential features to host any level of CTF within a great UI/UX. It has been tested for more than 10 years and optimized accordingly.

2.3 Implementation

TryHackMe implementation is straightforward. It gives few options to add tasks into the CTF and allow to determine the answer and allow to add hint to the answer. It allows to either upload Virtual

Machines or Downloadable files to add into each task. UI/UX is great, and implementation is easy to handle.

Task	Responsible Person	Duration
Information Gathering	Dilith & Rashmika	5 days
Planning and Scheduling	Dilith & Rashmika	5 days
Web site creation for First Evaluation	Dilith	14 days
Level (1, 2,)	Dilith & Rashmika	6 days
Level (3, 4, 5)	Dilith	5 days
Level (6, 7, 8)	Rashmika	7 days
Level (9, 10)	Dilith & Rashmika	3 days
Tryhackme Implementation	Dilith & Rashmika	2 days
Testing	Rashmika	2 days
Documentation	Dilith & Rashmika	5 days

Table 2

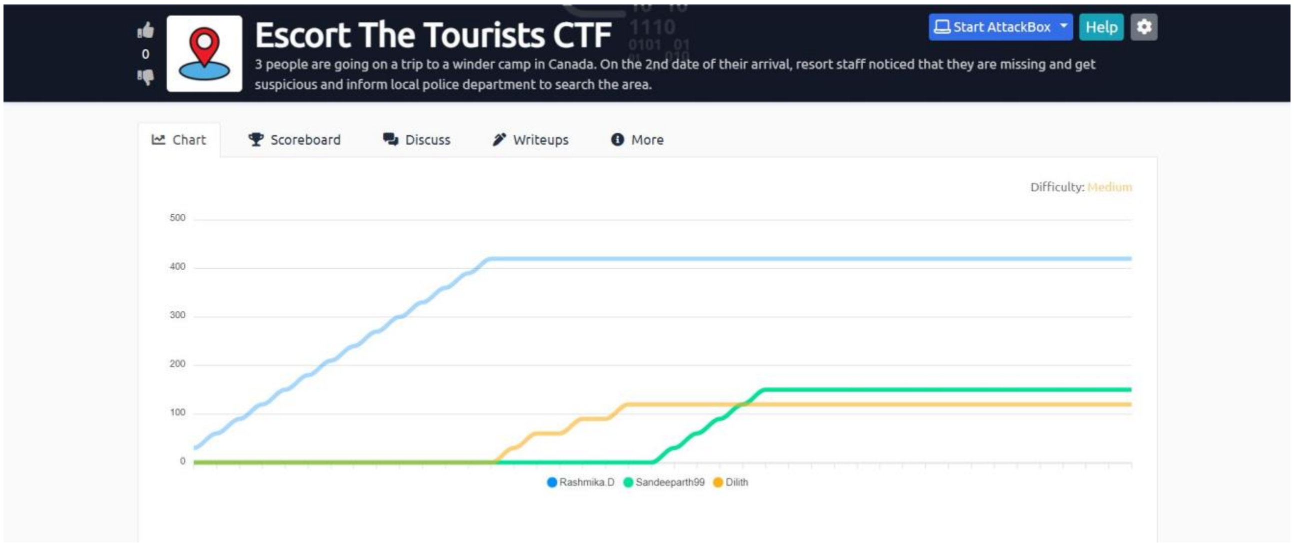
2.4 Testing

In order to analyze the project for testing, it was handed over to some colleagues to perform the tasks. Thereafter, it gave a better understanding about the project and overall difficulty of it. Then, it also helped to get an idea about time management. Also, it helped in identifying what areas needs to be improved and what areas where hints should be added in order to successfully complete the project and find the FLAG. There was no need to test server capacity and server security as it has already been tested for more than 10 years by TryHackMe itself.

3. Evaluation

3.1 Assessment of the Project results

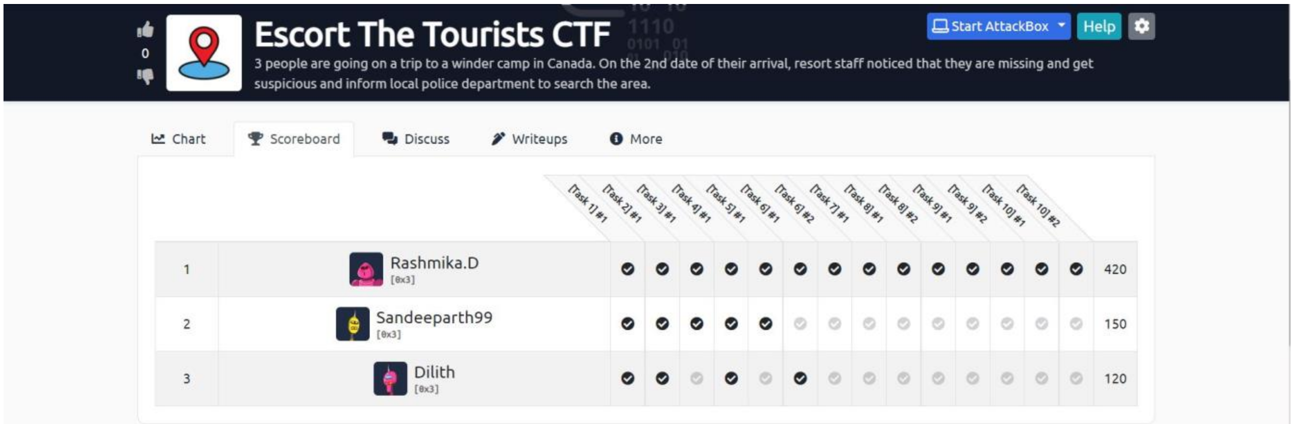
In the admin dashboard on TryHackMe, creators can see the statistics of their CTF and it shows user performance in task wise as well. Since it’s newly developed CTF, only some colleagues have attempted them for now.



Escort The Tourists CTF

3 people are going on a trip to a winder camp in Canada. On the 2nd date of their arrival, resort staff noticed that they are missing and get suspicious and inform local police department to search the area.

Figure 1



Escort The Tourists CTF

3 people are going on a trip to a winder camp in Canada. On the 2nd date of their arrival, resort staff noticed that they are missing and get suspicious and inform local police department to search the area.

		[Task 1] #1	[Task 2] #1	[Task 3] #1	[Task 4] #1	[Task 5] #1	[Task 6] #1	[Task 6] #2	[Task 7] #1	[Task 8] #1	[Task 8] #2	[Task 9] #1	[Task 9] #2	[Task 10] #1	[Task 10] #2	
1	Rashmika.D [0x3]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	420
2	Sandeeparth99 [0x3]	✓	✓	✓	✓	✓	○	○	○	○	○	○	○	○	○	150
3	Dilith [0x3]	✓	✓	○	✓	○	✓	○	○	○	○	○	○	○	○	120

Figure 2

3.2 Lessons Learned

It’s important have better understanding of how TryHackMe works and to have the general knowledge in implementing the CTF. Moreover, when creating challenges, they should be relative to the storyline. Also the answers should be straightforward as if even a single letter is missed, answer would not be valid. When creating tasks and completing them, creators’ knowledge of common sense and mostly cryptography will be increased as it is mostly used here to create challenges.

3.3 Future Work

CTFs are helping to keep security professionals and students up to date with their skills in the cyber security industry. As we are undergraduates which developing this CTF box we might have lack of knowledge up to some extent. We target the people interested in the cybersecurity, may be students or security professionals. Since we are students to develop this CTF box we will be spending only a low cost to implement the final CTF box.

There is a higher market value in Sri Lanka for CTF games. As well there is less potential local competitors in Sri Lanka. The target audience for the product is a little difficult for the CTF box. Our customers will be the companies that take CTF competitions, while the consumer of our product will be the younger generation. Since the younger generation is constantly looking for more knowledge about cybersecurity, they tend to participate in these competitions in search of new knowledge.

As this is the startup of our project, we can promote our project by Facebook advertisements, Instagram advertisements, and website advertisements

4. Conclusion

Gamification in computer security education often results in positive learning outcomes; the Cyber Security group's experience over last years of CTF competition supports this view. It was a great experience working on CTFs like this and completing fellow colleagues CTFs. However, current

CTF software frameworks can be improved in a variety of ways to make CTFs more extensible to support novel challenges, easier thus available to more groups, more flexible to be a valuable teaching tool in a variety of contexts, and more valuable as a research tool through improved data collection

5. References

[1] "TryHackMe," *Tryhackme.com*. [Online]. Available: https://tryhackme.com/about. [Accessed: 12-Nov-2021].

[2] "About picoCTF," *Picoctf.org*. [Online]. Available: https://picoctf.org/about. [Accessed: 12-Nov-2021].

[3] "CODEGATE," *Codegate.org*. [Online]. Available: https://www.codegate.org/en/hacking/general. [Accessed: 14-Nov-2021].

[4] "Insomni'Hack," *Insomnihack.ch*, 15-Dec-2015. [Online]. Available: https://insomnihack.ch/. [Accessed: 13-Nov-2021].

[5] "What is digital forensics in cyber security: Is this a good career for me?," *Ecpi.edu*. [Online]. Available: https://www.ecpi.edu/blog/what-is-digital-forensics-in-cybersecurity-is-this-a-good-career-for-me. [Accessed: 13-Nov-2021].

[6] B. Lutkevich, "What is Computer Forensics (Cyber Forensics)?," *Techtarget.com*, 05-May-2021. [Online]. Available: https://searchsecurity.techtarget.com/definition/computer-forensics. [Accessed: 12-Nov-2021].

[7] Gamify, "Gamify.Com - how to make a video game," *Gamify.com*. [Online]. Available: https://www.gamify.com/. [Accessed: 12-Nov-2021].

[8] "The Hackers Meetup – Medium," *Medium.com*. [Online]. Available: https://thehackersmeetup.medium.com/. [Accessed: 12-Nov-2021].

[9] Wikipedia contributors, "Capture the flag," *Wikipedia, The Free Encyclopedia*, 09-Nov-2021. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Capture_the_flag&oldid=1054396186. [Accessed: 12-Nov-2021].

[10] *Europa.eu*. [Online]. Available: https://www.enisa.europa.eu/news/enisa-news/capture-the-flag-competitions-all-you-ever-wanted-to-know. [Accessed: 14-Nov-2021].

[11] O. Lab and L. L. C. CTFd, "CTF 101," *Ctf101.org*. [Online]. Available: https://ctf101.org/. [Accessed: 12-Nov-2021].

[12] ctftime team, "CTFtime.org / What is Capture The Flag?," *Ctftime.org*. [Online]. Available: https://ctftime.org/ctf-wtf/. [Accessed: 13-Nov-2021].

[13] HackEDU Team, "What is a Capture The Flag event, and how does it benefit developers?," *Hackedu.com*. [Online]. Available: https://www.hackedu.com/blog/what-is-a-capture-the-flag-ctf-event-and-how-can-it-benefit-developers. [Accessed: 14-Nov-2021].

[14] "SecurityCTF : CTF announcements & writeups," *Reddit.com*. [Online]. Available: https://www.reddit.com/r/securityCTF/. [Accessed: 14-Nov-2021].

[15] gurdeep, "Here's how I organized a jeopardy style Capture-The-Flag competition," *Hackernoon.com*, 15-Nov-2020. [Online]. Available:

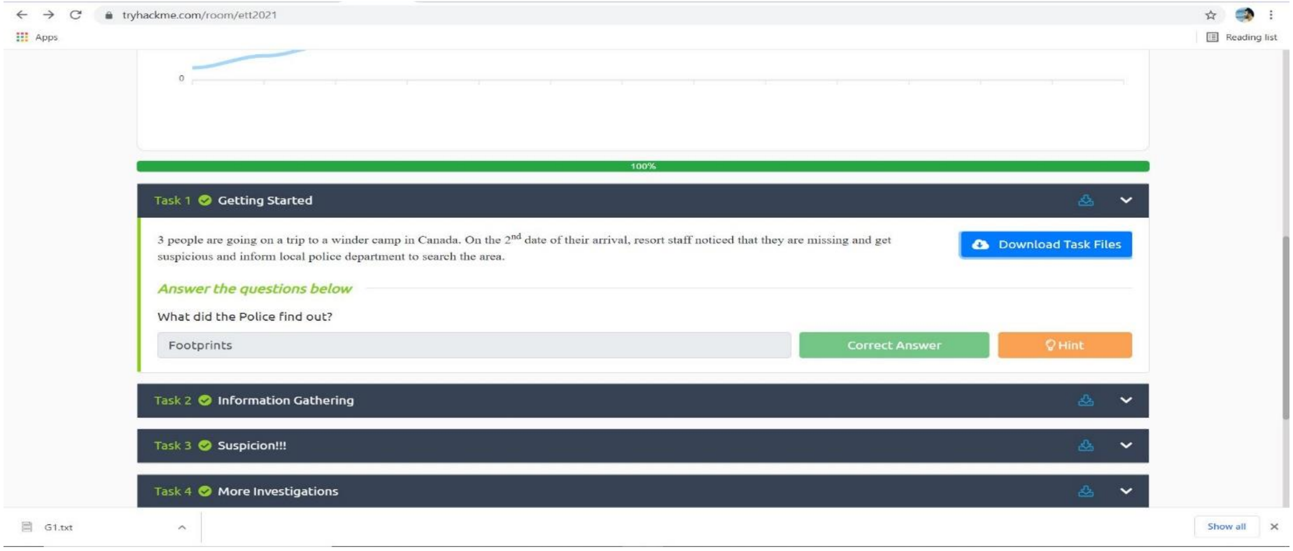
https://hackernoon.com/heres-how-i-organized-a-jeopardy-style-capture-the-flag-competition-123l3z9q. [Accessed: 14-Nov-2021].

[16] K. C. // Llc, "What is Capture The Flag?," *Ctfd.io*. [Online]. Available: https://ctfd.io/whats-a-ctf/. [Accessed: 14-Nov-2021].

Appendix A: Walkthrough

Task 1

For the first task, Ceaser chipper has been used for the encryption of the first answer. Also Cryptool is used for this. Users need to download the text file and decrypt the cipher text and submit the correct answer to complete the task. Users will get the first clue of the lost tourists here.



Task 1 Getting Started

3 people are going on a trip to a winder camp in Canada. On the 2nd date of their arrival, resort staff noticed that they are missing and get suspicious and inform local police department to search the area.

Answer the questions below

What did the Police find out?

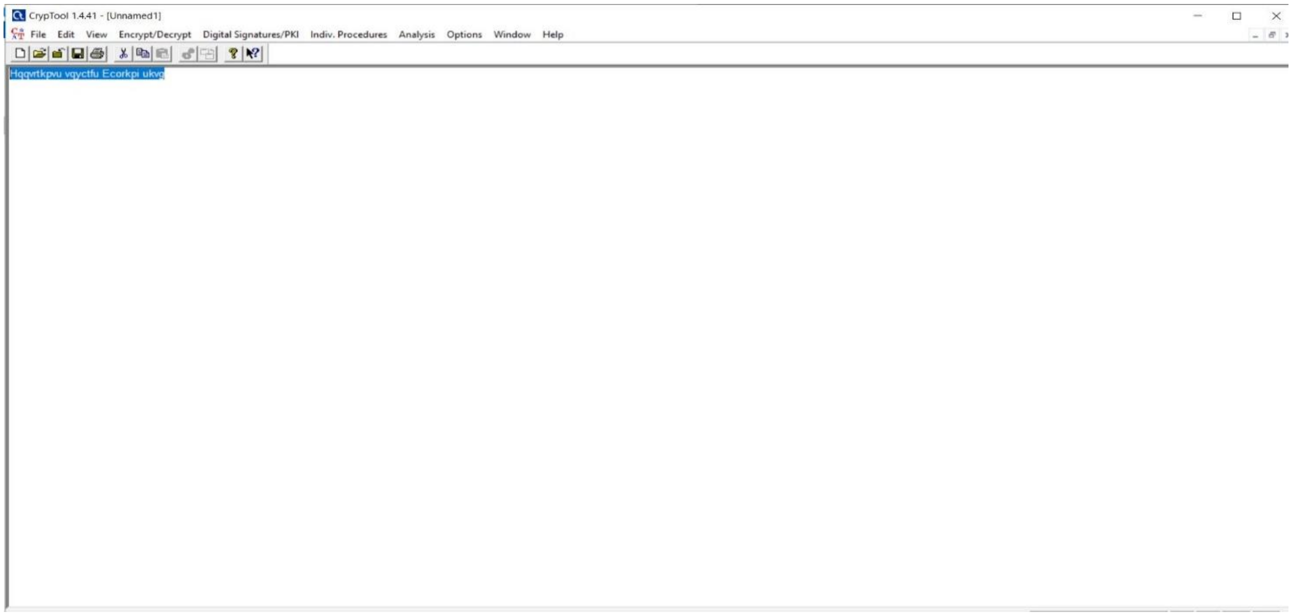
Footprints

Task 2 Information Gathering

Task 3 Suspicion!!!

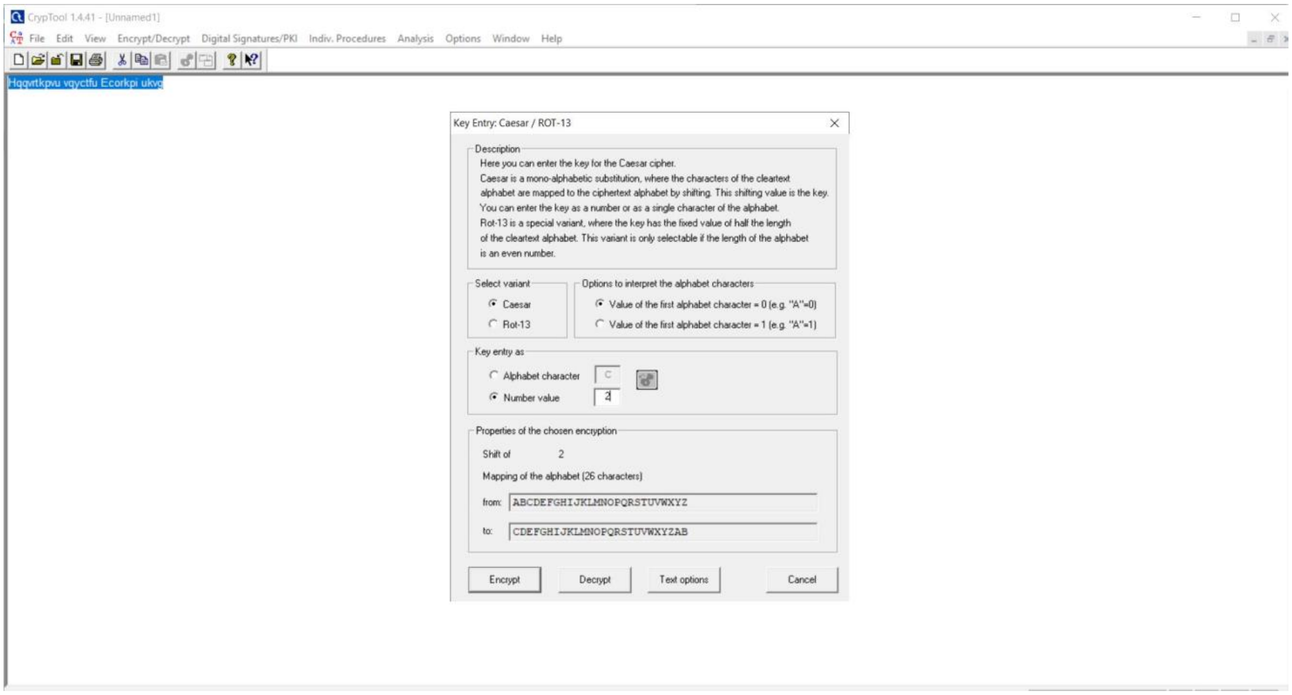
Task 4 More Investigations

Figure 3



Hqqvrtkpvu vqyctfu Ecorkpi ukvg

Figure 4



Hqqvrtkpvu vqyctfu Ecorkpi ukvg

Key Entry: Caesar / ROT-13

Description

Here you can enter the key for the Caesar cipher.
Caesar is a mono-alphabetic substitution, where the characters of the cleartext alphabet are mapped to the ciphertext alphabet by shifting. This shifting value is the key.
You can enter the key as a number or as a single character of the alphabet.
Rot-13 is a special variant, where the key has the fixed value of half the length of the cleartext alphabet. This variant is only selectable if the length of the alphabet is an even number.

Select variant

● Caesar
○ Rot-13

Options to interpret the alphabet characters

● Value of the first alphabet character = 0 (e.g. "A"=0)
○ Value of the first alphabet character = 1 (e.g. "A"=1)

Key entry as

○ Alphabet character C
● Number value 2

Properties of the chosen encryption

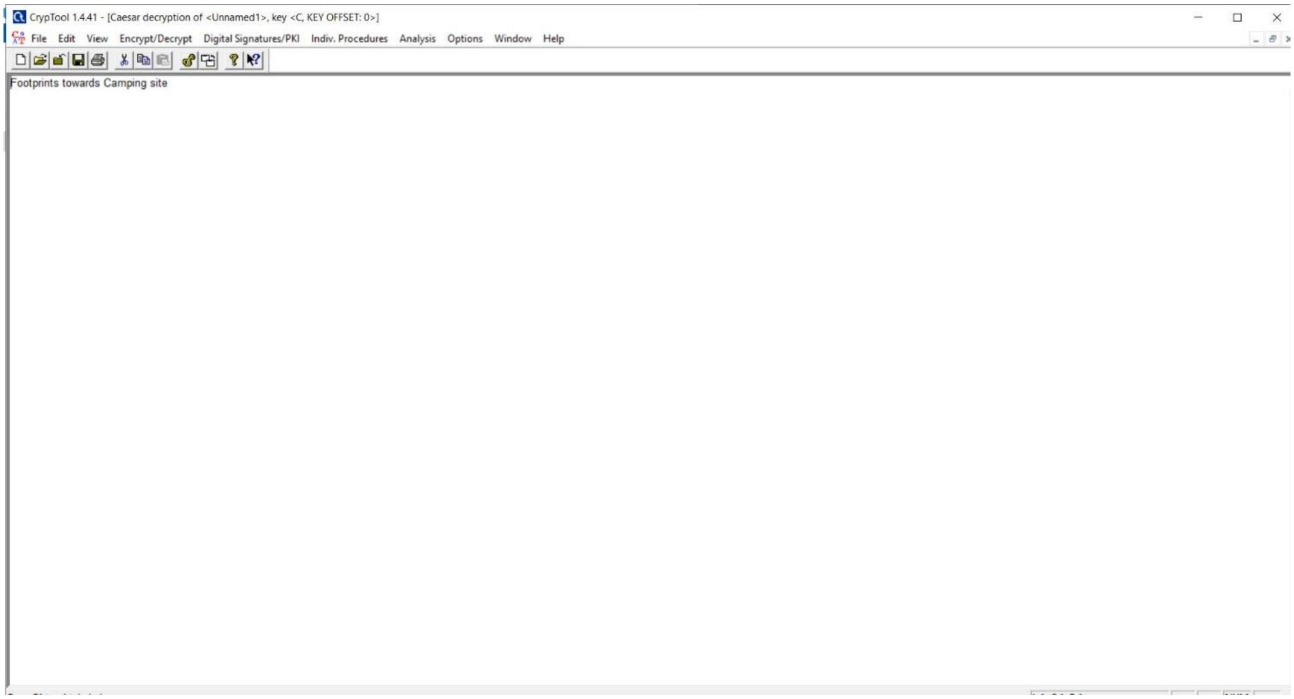
Shift of 2

Mapping of the alphabet (26 characters)

from: ABCDEFGHIJKLMNOPQRSTUVWXYZ

to: CDEFGHIJKLMNOPQRSTUVWXYZAB

Figure 5

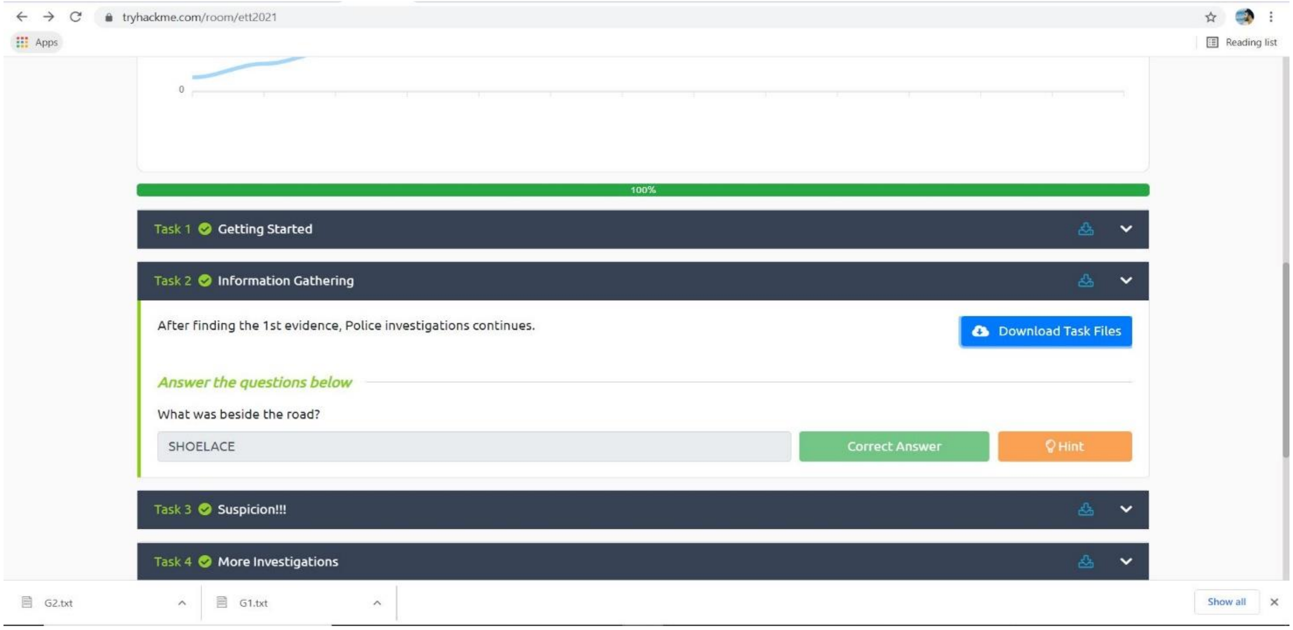


Footprints towards Camping site

Figure 6

Task 2

For the 2nd task, MOS codes has been used to encrypt the answer. Also relevant hints have added to ease this for the users. They can use and online tool to decrypt and enter the correct answer. Users will get important clues of the lost tourists here as well.



Task 1 Getting Started

Task 2 Information Gathering

After finding the 1st evidence, Police investigations continues.

Download Task Files

Answer the questions below

What was beside the road?

SHOELACE

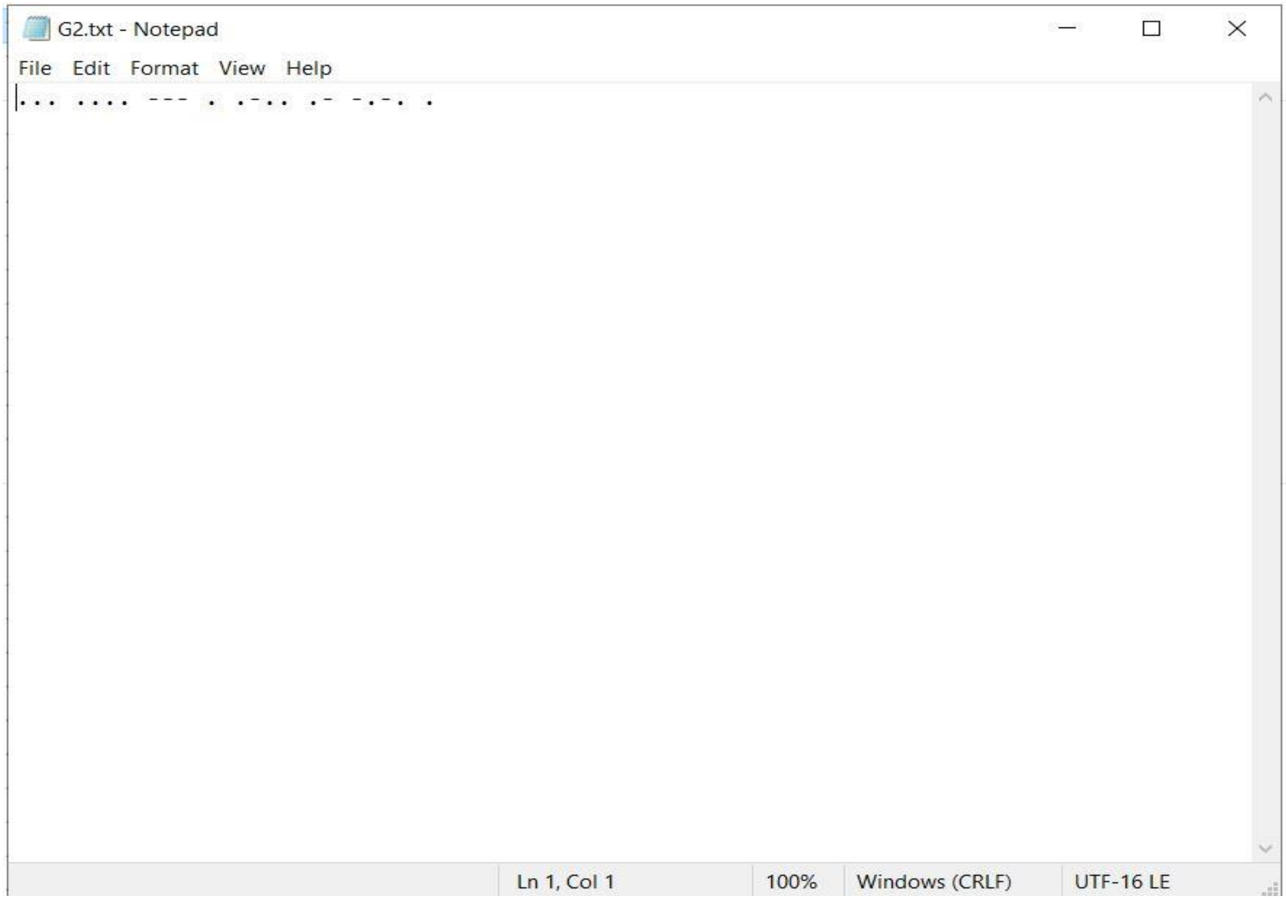
Correct Answer

Hint

Task 3 Suspicion!!!

Task 4 More Investigations

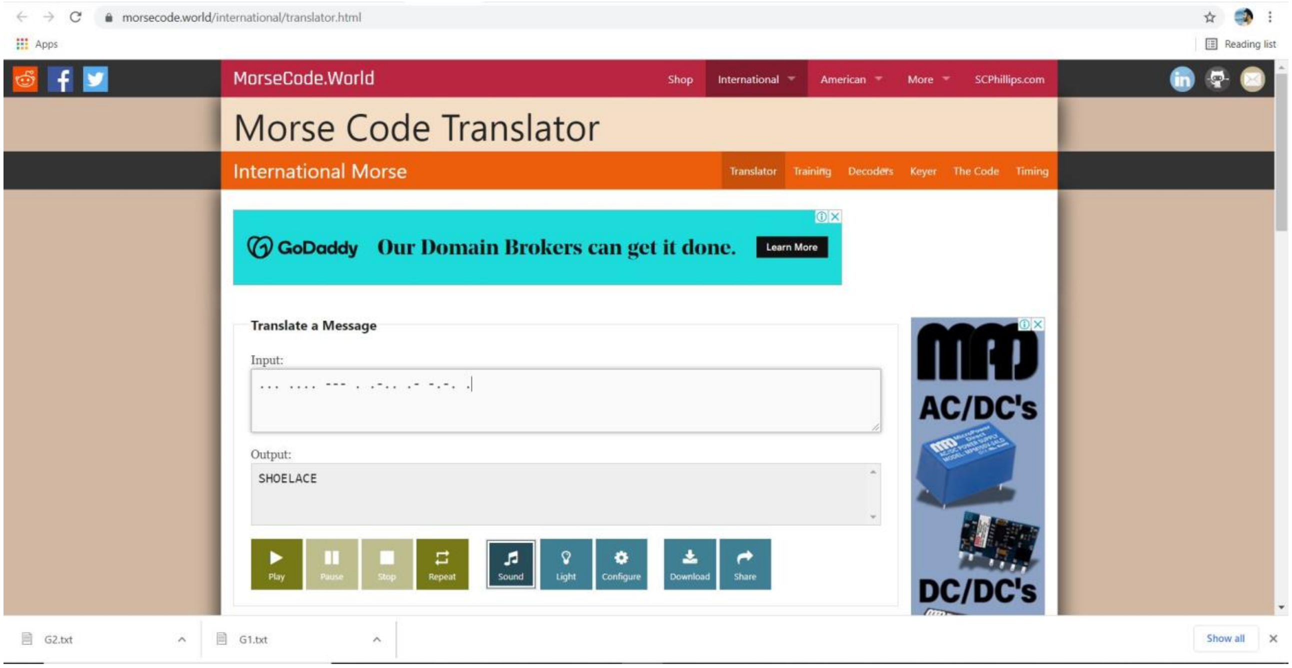
Figure 7



```
... .... --- . .-.. .- -.-. .
```

Ln 1, Col 1 | 100% | Windows (CRLF) | UTF-16 LE

Figure 8



Translate a Message

Input:

```
... .... --- . .-.. .- -.-. .
```

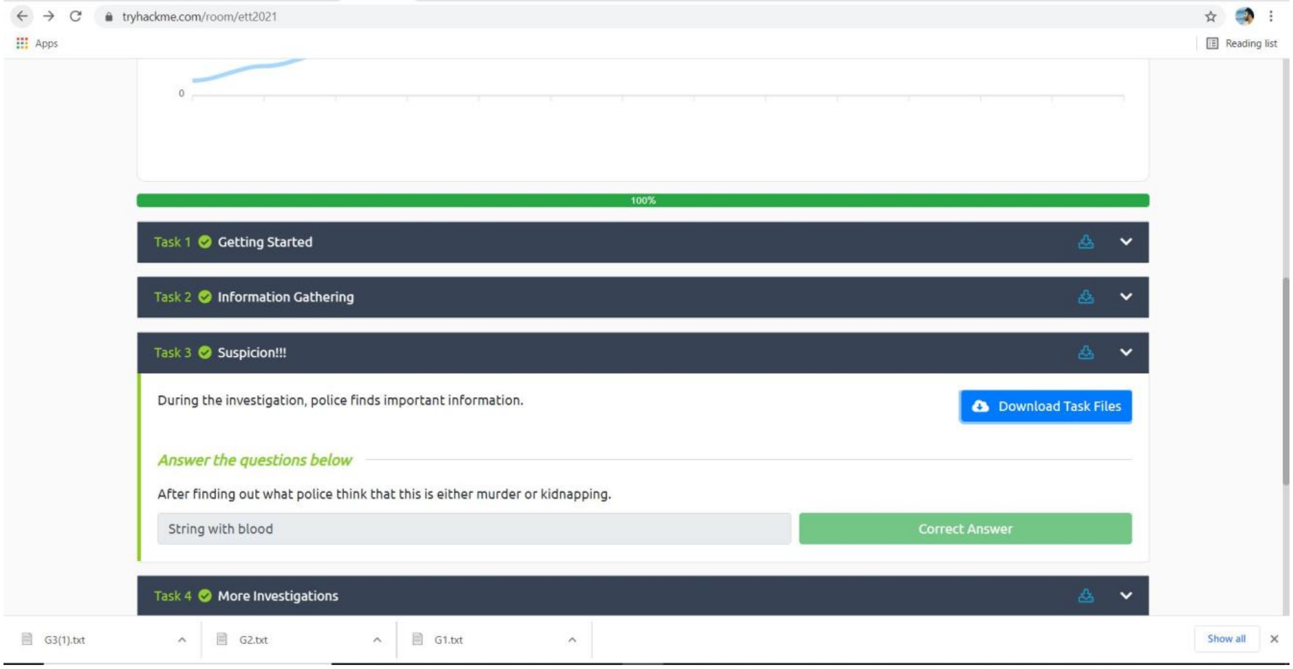
Output:

```
SHOELACE
```

Figure 9

Task 3

Next task is fairly easy task compared to the ones before. There's a downloadable file and users need to view that and find the answer. During the task, users find crucial information about tourists and police suspect this is either a murder or a kidnapping.



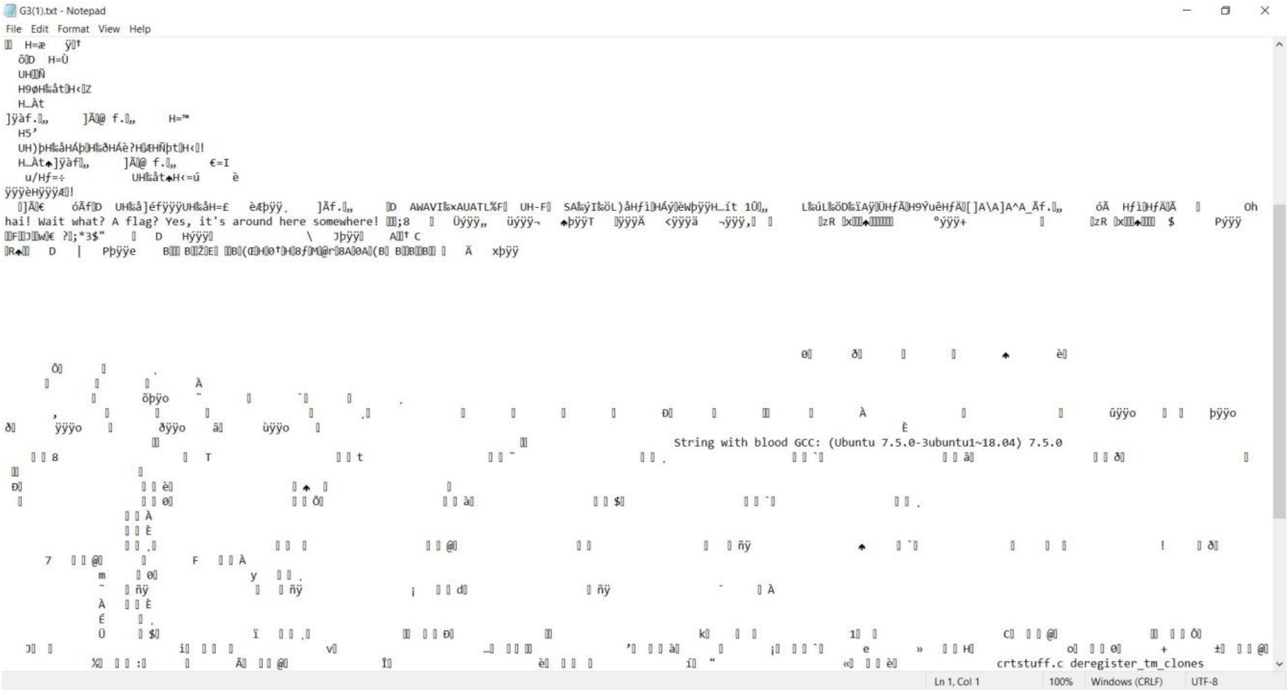
During the investigation, police finds important information.

Answer the questions below

After finding out what police think that this is either murder or kidnapping.

String with blood — Correct Answer

Figure 10

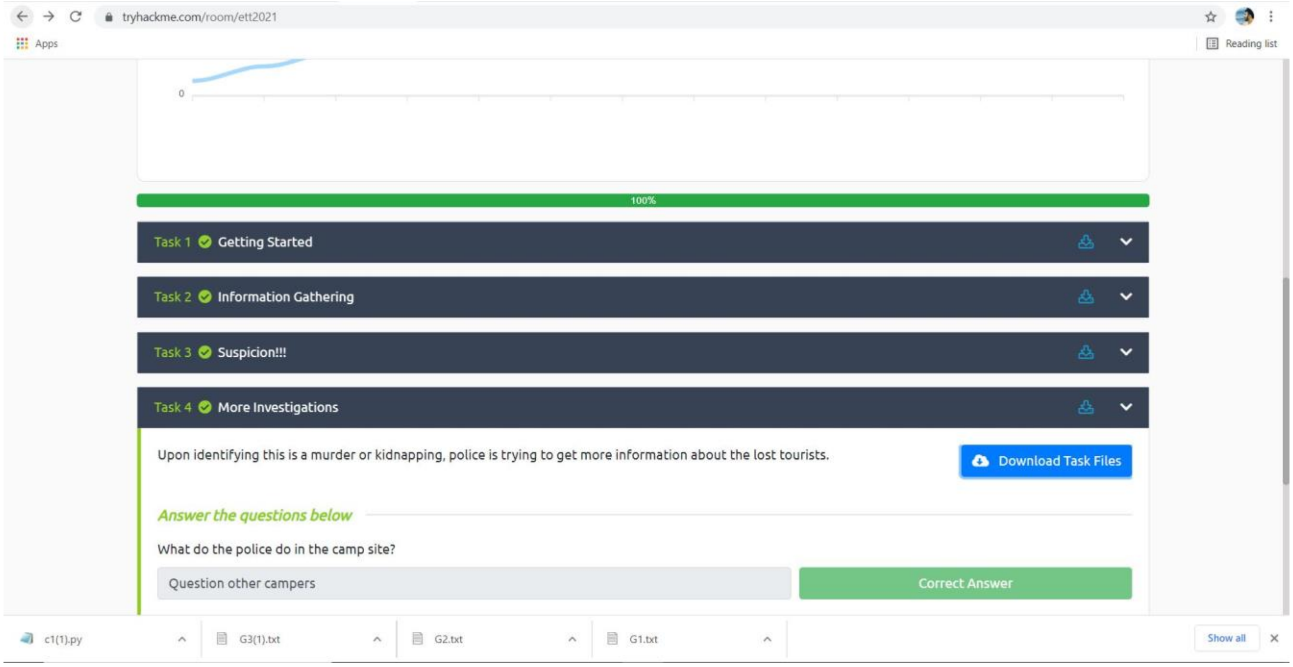


```
 H=æ    ÿ†
  õD   H=Ù
  UHÑ
  H9øH‰åtH‹Z
  H…Àt
]ÿàf.„      ]Ã@ f.„      H=™
  H5’
  UH)þH‰åHÁþH‰ðHÁè?HÆHÑþtH‹!
  H…Àt]ÿàf„      ]Ã@ f.„      €=I
   u/Hƒ=÷           UH‰åtH‹=ú      è
ÿÿÿèHÿÿÿÆ!
 ]Ã€     óÃfD  UH‰å]éfÿÿÿUH‰åH=£    èÆþÿÿ.     ]Ãf.„      D  AWAVI‰×AUATL%F  UH-F  SA‰ýI‰öL)åHƒìHÁýèwþÿÿH…ít 1Û„      L‰úL‰öD‰ïAÿÜHƒÃH9ÝuêHƒÄ[]A\A]A^A_Ãf.„      óÃ  HƒìHƒÄÃ          Oh
hai! Wait what? A flag? Yes, it's around here somewhere! ;8      Üÿÿÿ„    üÿÿÿ¬    þÿÿT    ÿÿÿÄ    <ÿÿÿä    ¬ÿÿÿ,         zR x             °ÿÿÿ+                zR x        $      Pÿÿÿ
FJw€ ?;*3$"      D    Hýÿÿ                  \    Jþÿÿ      A† C
R     D    |    Pþÿÿe      B BŽE B(ŒH0†H8ƒM@r8A0A(B BBB      Ä    xþÿÿ

String with blood GCC: (Ubuntu 7.5.0-3ubuntu1~18.04) 7.5.0

crtstuff.c deregister_tm_clones
```

Figure 11

Task 4

Fourth task is based on base 64 encoder. Users will have to download a file in here as well and decode it to get the answer. Police will do questioning on other campers in this task to identify the key elements of the investigation. Police have the first sight on kidnappers and the tourists here.



Task 1 Getting Started

Task 2 Information Gathering

Task 3 Suspicion!!!

Task 4 More Investigations

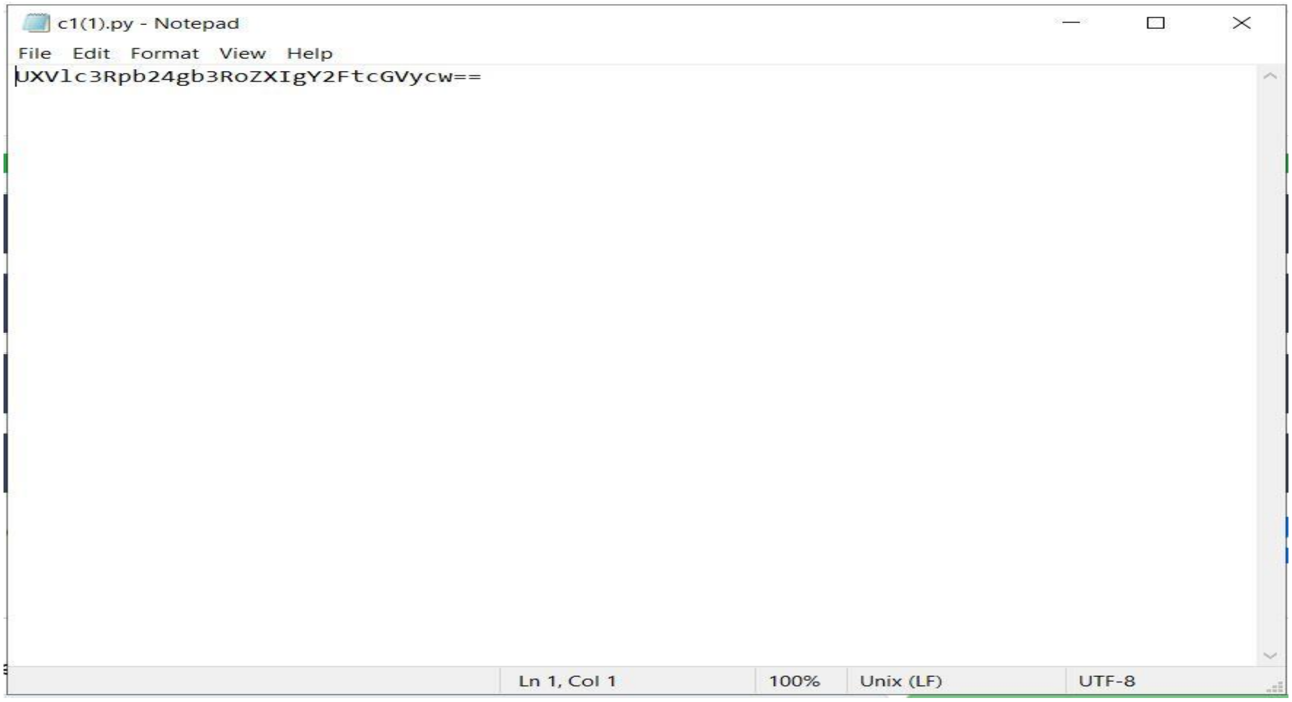
Upon identifying this is a murder or kidnapping, police is trying to get more information about the lost tourists.

Answer the questions below

What do the police do in the camp site?

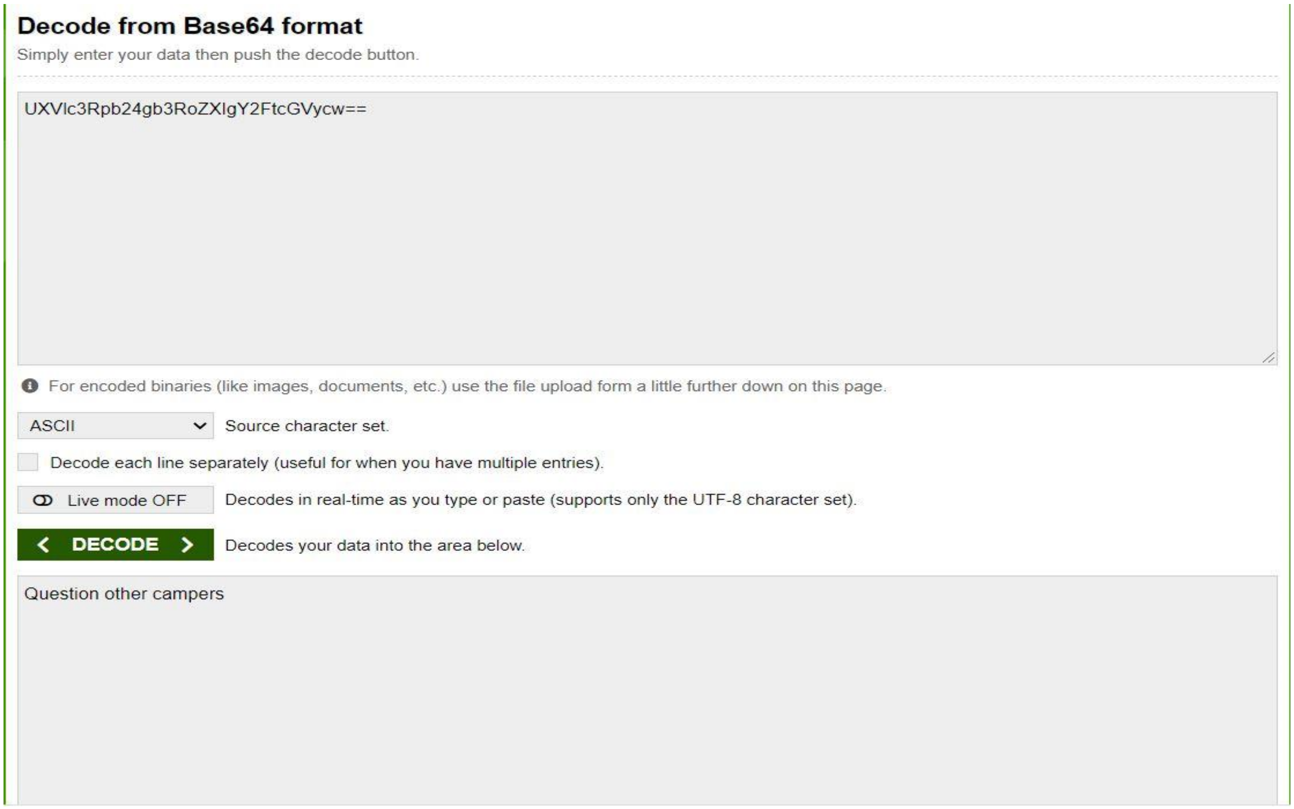
Question other campers

Figure 12



```
UXVlc3Rpb24gb3RoZXIgY2FtcGVycw==
```

Figure 13



Decode from Base64 format

Simply enter your data then push the decode button.

```
UXVlc3Rpb24gb3RoZXIgY2FtcGVycw==
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

ASCII Source character set.

□ Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

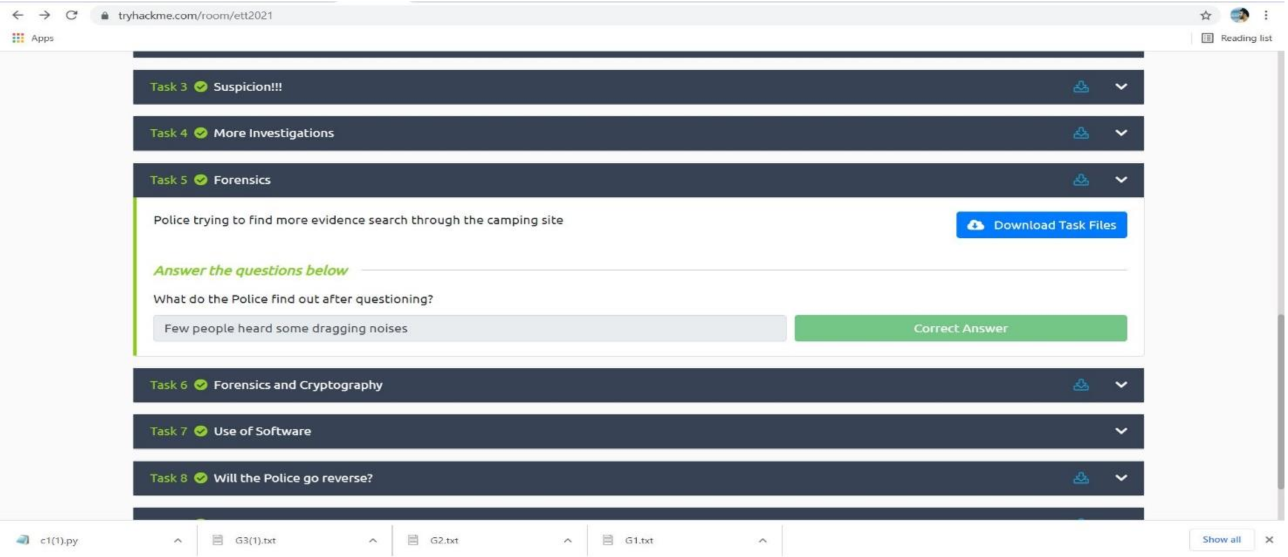
< DECODE > Decodes your data into the area below.

```
Question other campers
```

Figure 14

Task 5

In the next task, forensic departments comes to aid the investigation. We have hidden the answer and some useful information for upcoming tasks in a QRcode. Users will have to scan it and find those information and submit the answer.



tryhackme.com/room/ett2021

Task 3 Suspicion!!!

Task 4 More Investigations

Task 5 Forensics

Police trying to find more evidence search through the camping site

Answer the questions below

What do the Police find out after questioning?

Few people heard some dragging noises

Task 6 Forensics and Cryptography

Task 7 Use of Software

Task 8 Will the Police go reverse?

Figure 15

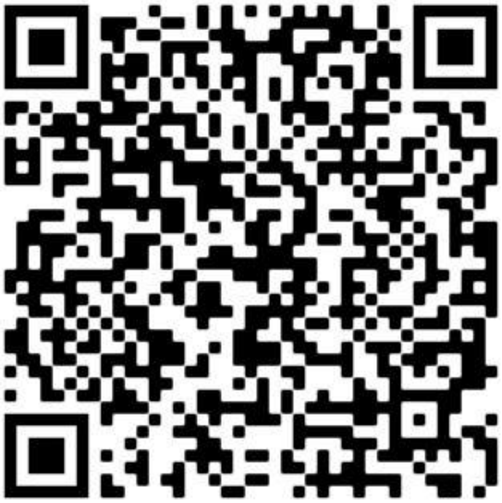


Figure 16

Task 6

In the sixth task, downloadable image has been added which has been created by merging and image and a txt file. The images needs to be opened in notepad to get the information about the task. Same as the previous task, this also include both answer and valuable information for upcoming tasks.

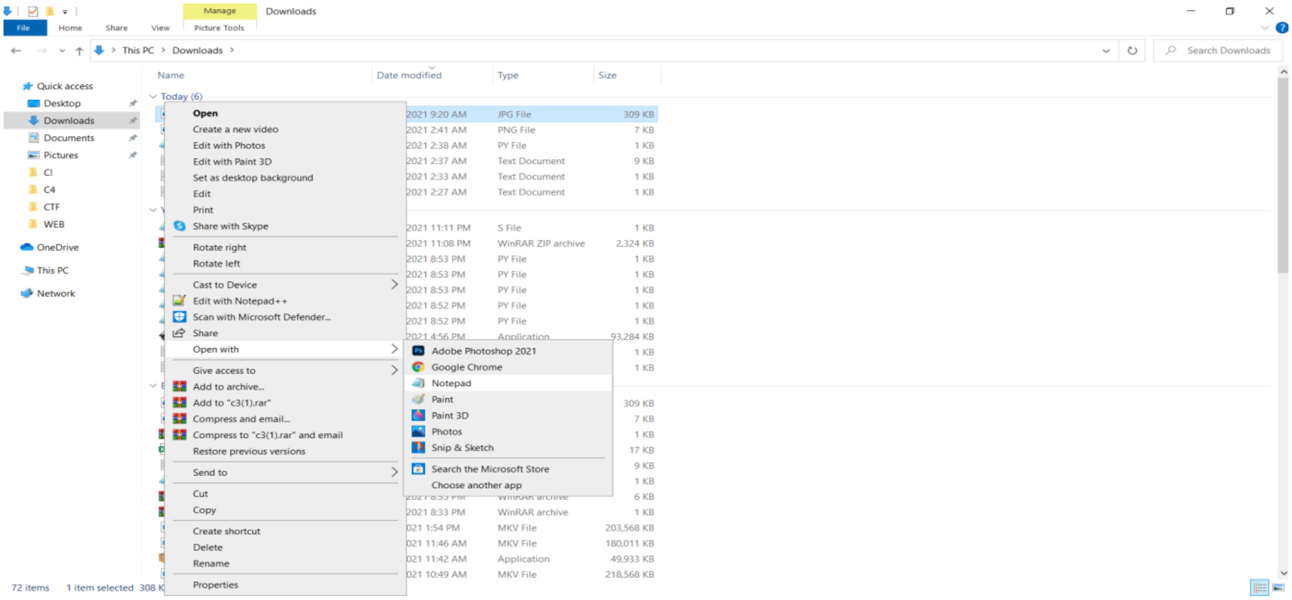
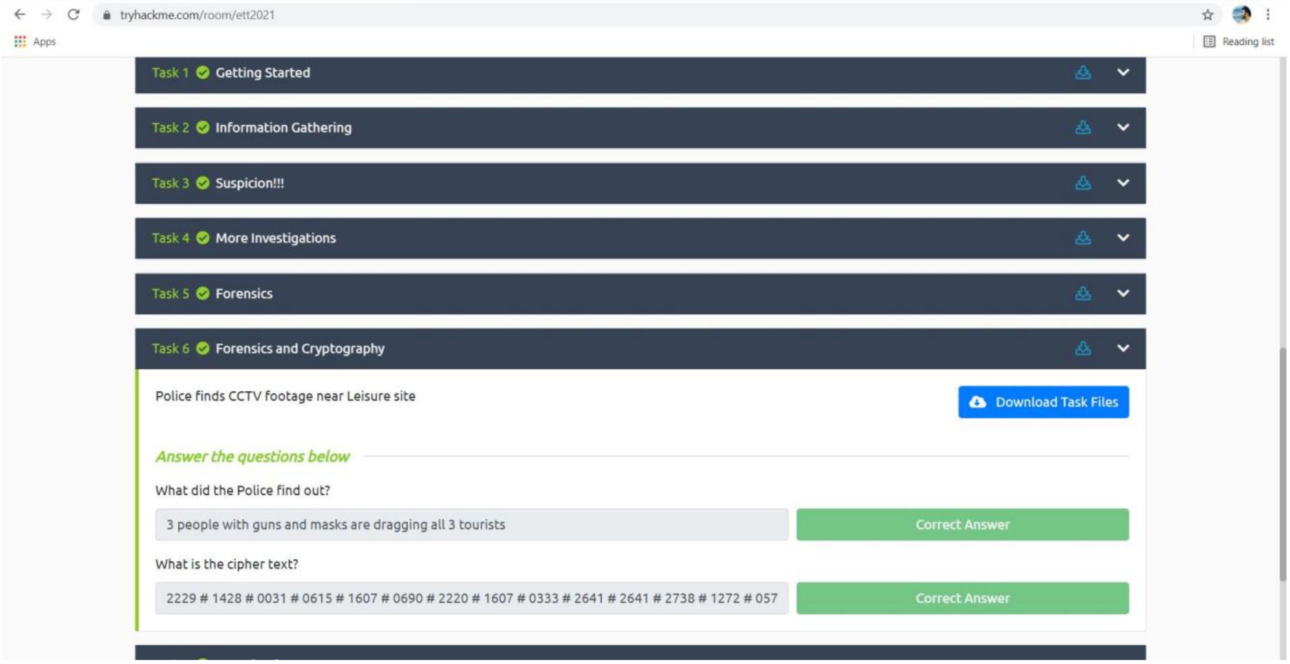


Figure 17



tryhackme.com/room/ett2021

Task 1 Getting Started

Task 2 Information Gathering

Task 3 Suspicion!!!

Task 4 More Investigations

Task 5 Forensics

Task 6 Forensics and Cryptography

Police finds CCTV footage near Leisure site

Download Task Files

Answer the questions below

What did the Police find out?

3 people with guns and masks are dragging all 3 tourists

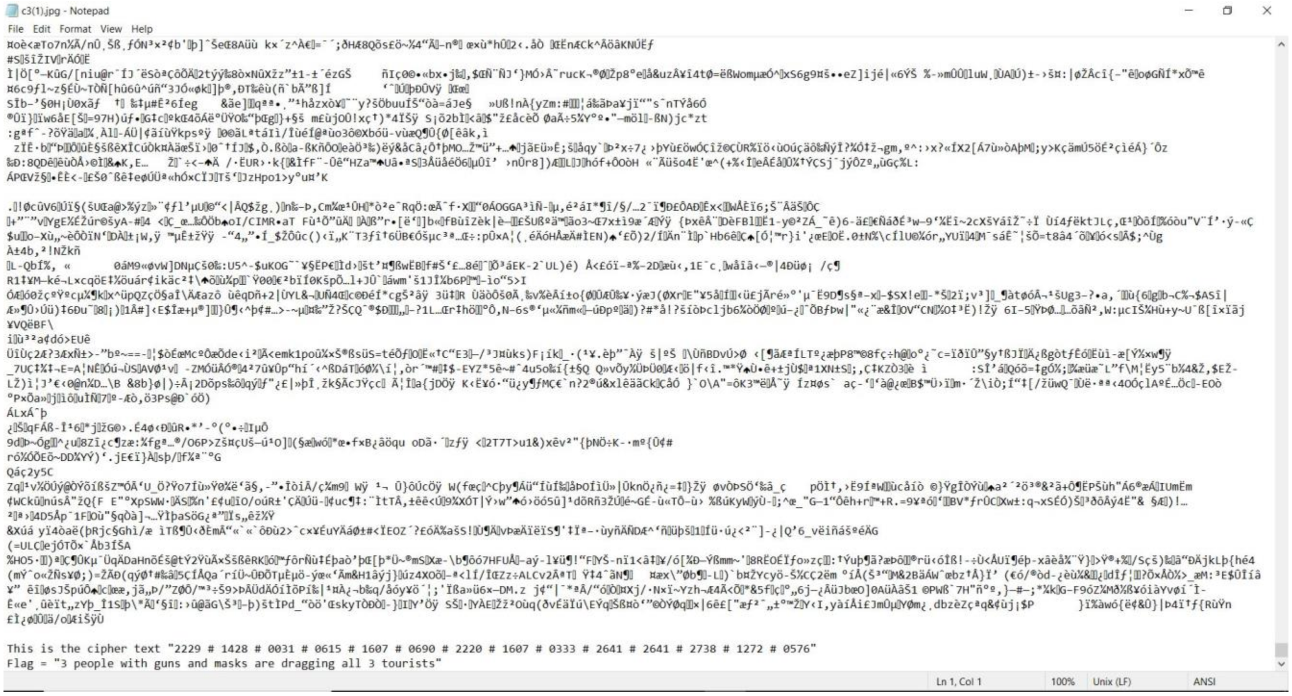
Correct Answer

What is the cipher text?

2229 # 1428 # 0031 # 0615 # 1607 # 0690 # 2220 # 1607 # 0333 # 2641 # 2641 # 2738 # 1272 # 057

Correct Answer

Figure 18



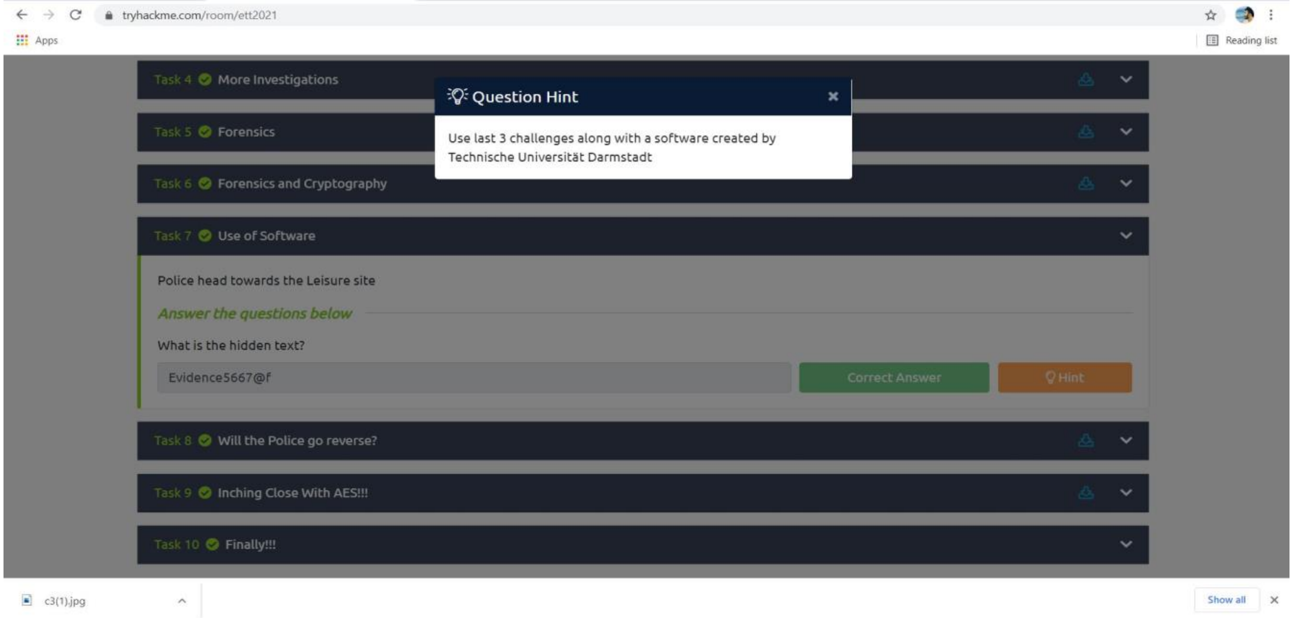
c3(1).jpg - Notepad

```
This is the cipher text "2229 # 1428 # 0031 # 0615 # 1607 # 0690 # 2220 # 1607 # 0333 # 2641 # 2641 # 2738 # 1272 # 0576"
Flag = "3 people with guns and masks are dragging all 3 tourists"
```

Figure 19

Task 7

Software comes handy in search of the lost tourists in this task. Using the information from the above tasks, this needs to be completed in cryptool. We have hid the information needed to decode the cipher text using RSA. This will be used as the password for an email address later on.



tryhackme.com/room/ett2021

Apps
Reading list
Task 4 More Investigations
Task 5 Forensics
Task 6 Forensics and Cryptography
Task 7 Use of Software

Question Hint

Use last 3 challenges along with a software created by Technische Universität Darmstadt

Police head towards the Leisure site

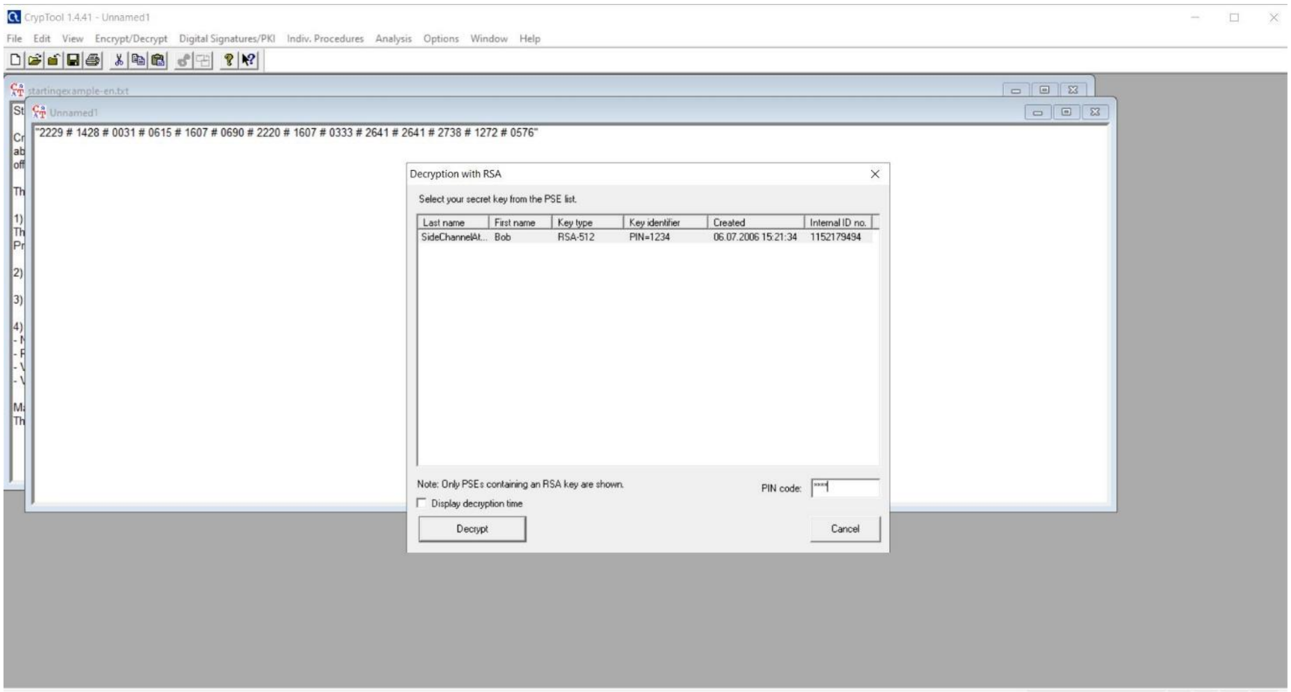
Answer the questions below

What is the hidden text?

Evidence5667@f

Correct Answer
Hint
Task 8 Will the Police go reverse?
Task 9 Inching Close With AES!!!
Task 10 Finally!!!
c3(1).jpg
Show all

Figure 20


CrypTool 1.4.41 - Unnamed1
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
startingexample-en.txt
Unnamed1

"2229 # 1428 # 0031 # 0615 # 1607 # 0690 # 2220 # 1607 # 0333 # 2641 # 2641 # 2738 # 1272 # 0576"

Decryption with RSA

Select your secret key from the PSE list.

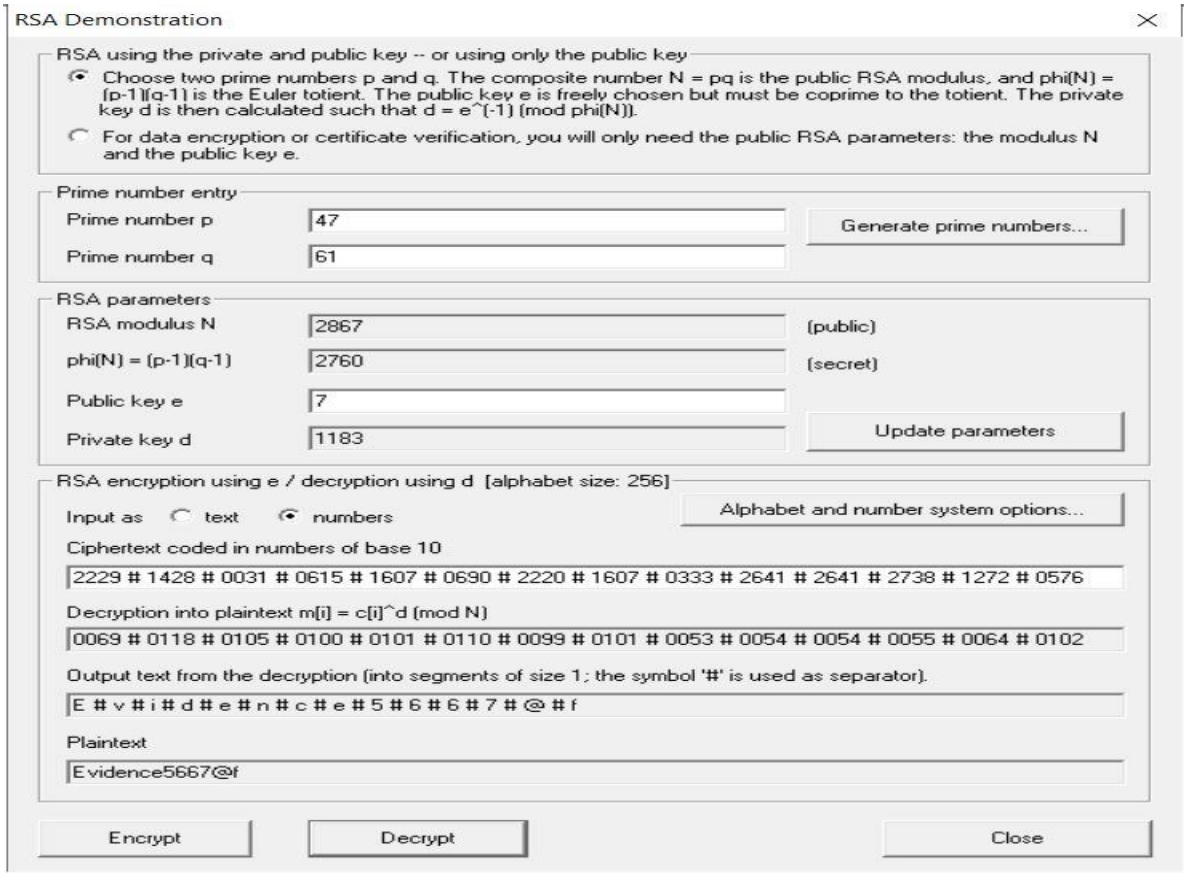
Last name	First name	Key type	Key identifier	Created	Internal ID no.
SideChannelAt...	Bob	RSA-512	PIN=1234	06.07.2006 15:21:34	1152179494

Note: Only PSEs containing an RSA key are shown.

PIN code: ****

□ Display decryption time

Figure 21


RSA Demonstration

RSA using the private and public key -- or using only the public key

● Choose two prime numbers p and q. The composite number N = pq is the public RSA modulus, and phi(N) = (p-1)(q-1) is the Euler totient. The public key e is freely chosen but must be coprime to the totient. The private key d is then calculated such that d = e^(-1) (mod phi(N)).

○ For data encryption or certificate verification, you will only need the public RSA parameters: the modulus N and the public key e.

Prime number entry

Prime number p: 47

Prime number q: 61

RSA parameters

RSA modulus N: 2867 (public)

phi(N) = (p-1)(q-1): 2760 (secret)

Public key e: 7

Private key d: 1183

RSA encryption using e / decryption using d [alphabet size: 256]

Input as ○ text ● numbers

Ciphertext coded in numbers of base 10

2229 # 1428 # 0031 # 0615 # 1607 # 0690 # 2220 # 1607 # 0333 # 2641 # 2641 # 2738 # 1272 # 0576

Decryption into plaintext m[i] = c[i]^d (mod N)

0069 # 0118 # 0105 # 0100 # 0101 # 0110 # 0099 # 0101 # 0053 # 0054 # 0054 # 0055 # 0064 # 0102

Output text from the decryption (into segments of size 1; the symbol '#' is used as separator).

E # v # i # d # e # n # c # e # 5 # 6 # 6 # 7 # @ # f

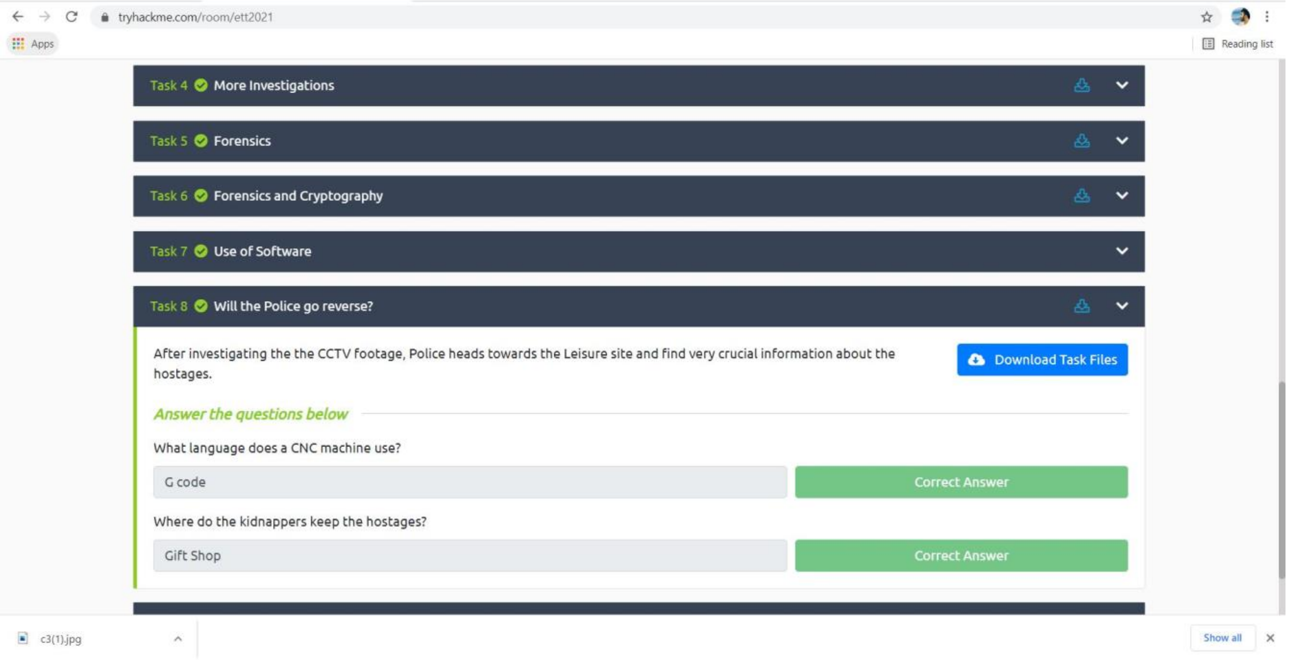
Plaintext

Evidence5667@f

Figure 22

Task 8

Investigations will continue and police finally finds out the location where the hostages are kept. Using a software named Inkspace, we have generated a code which needed to the task. It is named a g code and it uses in CNC machines. To get the answer, file needs to be downloaded and use the command nc filename in terminal to get the g code. Then, it needs to be copied and insert in to nc viewer tool to get the answer. It reveals that they kept somewhere in the gift shop.


tryhackme.com/room/ett2021
Apps
Reading list
Task 4 More Investigations
Task 5 Forensics
Task 6 Forensics and Cryptography
Task 7 Use of Software
Task 8 Will the Police go reverse?
Download Task Files
c3(1).jpg
Show all

After investigating the the CCTV footage, Police heads towards the Leisure site and find very crucial information about the hostages.

Answer the questions below

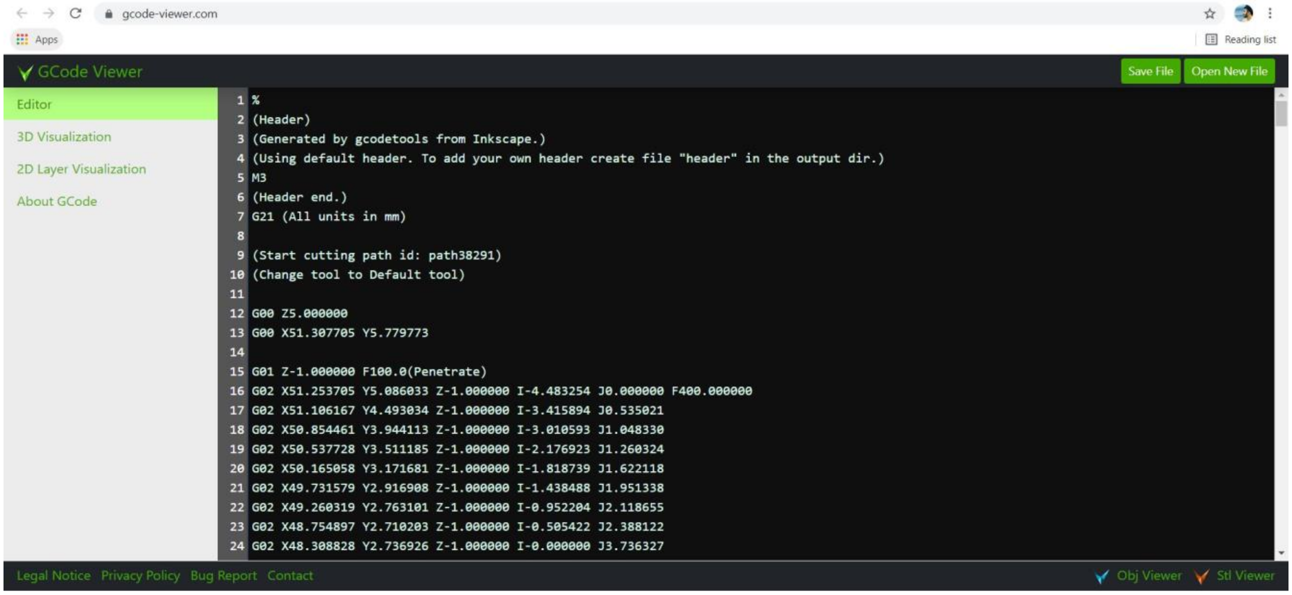
What language does a CNC machine use?

G code — Correct Answer

Where do the kidnappers keep the hostages?

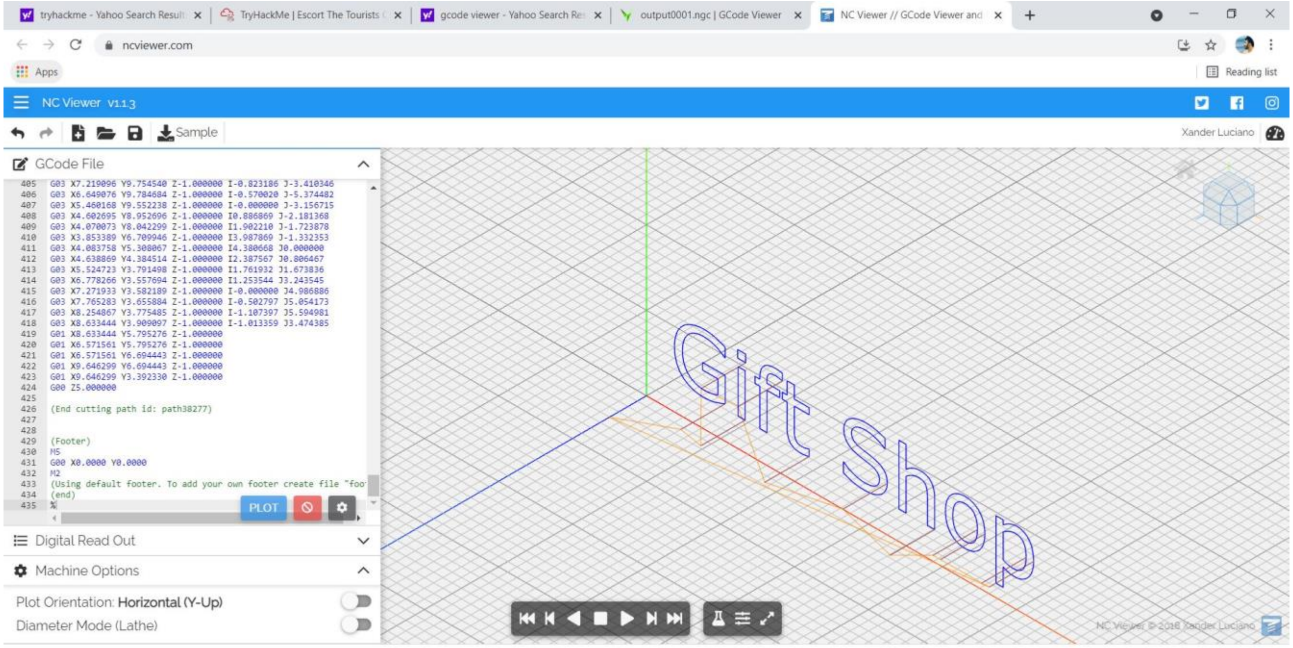
Gift Shop — Correct Answer

Figure 23



```
%
(Header)
(Generated by gcodetools from Inkscape.)
(Using default header. To add your own header create file "header" in the output dir.)
M3
(Header end.)
G21 (All units in mm)

(Start cutting path id: path38291)
(Change tool to Default tool)

G00 Z5.000000
G00 X51.307705 Y5.779773

G01 Z-1.000000 F100.0(Penetrate)
G02 X51.253705 Y5.086033 Z-1.000000 I-4.483254 J0.000000 F400.000000
G02 X51.106167 Y4.493034 Z-1.000000 I-3.415894 J0.535021
G02 X50.854461 Y3.944113 Z-1.000000 I-3.010593 J1.048330
G02 X50.537728 Y3.511185 Z-1.000000 I-2.176923 J1.260324
G02 X50.165058 Y3.171681 Z-1.000000 I-1.818739 J1.622118
G02 X49.731579 Y2.916908 Z-1.000000 I-1.438488 J1.951338
G02 X49.260319 Y2.763101 Z-1.000000 I-0.952204 J2.118655
G02 X48.754897 Y2.710203 Z-1.000000 I-0.505422 J2.388122
G02 X48.308828 Y2.736926 Z-1.000000 I-0.000000 J3.736327
```

Figure 24


tryhackme - Yahoo Search Results
TryHackMe | Escort The Tourists
gcode viewer - Yahoo Search Res
output0001.ngc | GCode Viewer
NC Viewer // GCode Viewer and
ncviewer.com
Apps
Reading list
NC Viewer v1.1.3
Sample
Xander Luciano
GCode File
PLOT
Digital Read Out
Machine Options
Gift Shop
NC Viewer © 2018 Xander Luciano

```
G03 X7.219096 Y9.754540 Z-1.000000 I-0.823186 J-3.410346
G03 X6.649076 Y9.784684 Z-1.000000 I-0.570020 J-5.374482
G03 X5.460168 Y9.552238 Z-1.000000 I-0.000000 J-3.156715
G03 X4.602695 Y8.952696 Z-1.000000 I0.886869 J-2.181368
G03 X4.070073 Y8.042299 Z-1.000000 I1.902210 J-1.723878
G03 X3.853389 Y6.709946 Z-1.000000 I3.987869 J-1.332353
G03 X4.083758 Y5.308067 Z-1.000000 I4.380668 J0.000000
G03 X4.638869 Y4.384514 Z-1.000000 I2.387567 J0.806467
G03 X5.524723 Y3.791498 Z-1.000000 I1.761932 J1.673836
G03 X6.778266 Y3.557694 Z-1.000000 I1.253544 J3.243545
G03 X7.271933 Y3.582189 Z-1.000000 I-0.000000 J4.986886
G03 X7.765283 Y3.655884 Z-1.000000 I-0.502797 J5.054173
G03 X8.254867 Y3.775485 Z-1.000000 I-1.107397 J5.594981
G03 X8.633444 Y3.909097 Z-1.000000 I-1.013359 J3.474385
G01 X8.633444 Y5.795276 Z-1.000000
G01 X6.571561 Y5.795276 Z-1.000000
G01 X6.571561 Y6.694443 Z-1.000000
G01 X9.646299 Y6.694443 Z-1.000000
G01 X9.646299 Y3.392330 Z-1.000000
G00 Z5.000000

(End cutting path id: path38277)


(Footer)
M5
G00 X0.0000 Y0.0000
M2
(Using default footer. To add your own footer create file "foo
(end)
%
```

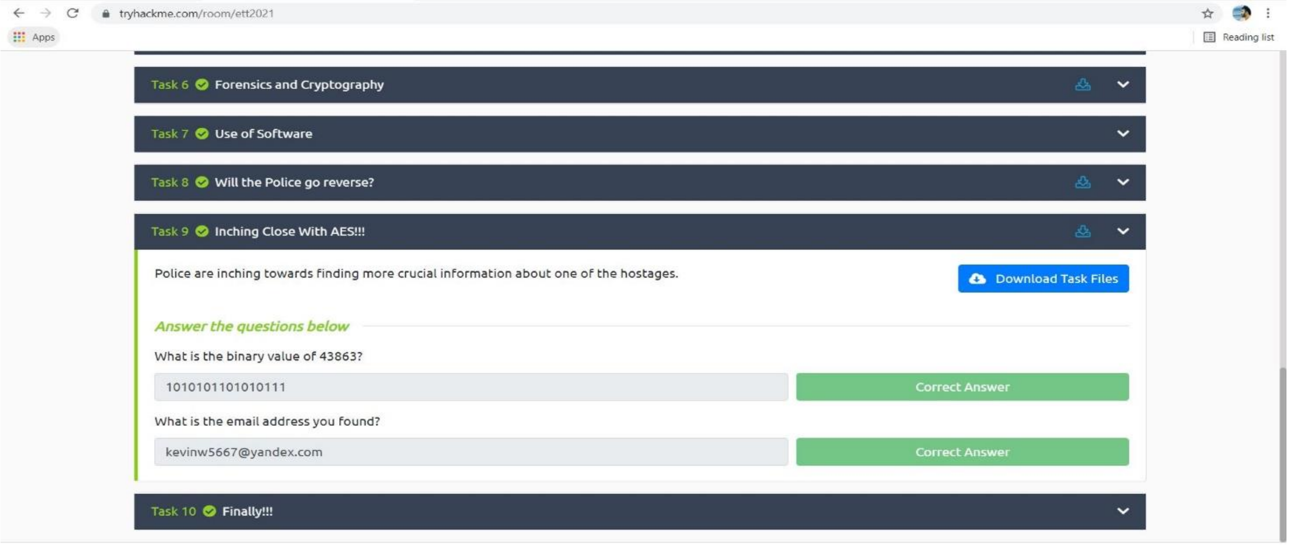
Plot Orientation: Horizontal (Y-Up)

Diameter Mode (Lathe)

Figure 25

Task 9

To identify the kidnappers, police finds a email address of a hostage and trying to log in to it just see if they can get some information. We use the above mentioned answer as the password. Email address is encrypted using AES and a hint is given to get the key.



Task 6 Forensics and Cryptography

Task 7 Use of Software

Task 8 Will the Police go reverse?

Task 9 Inching Close With AES!!!

Police are inching towards finding more crucial information about one of the hostages.

Download Task Files

Answer the questions below

What is the binary value of 43863?

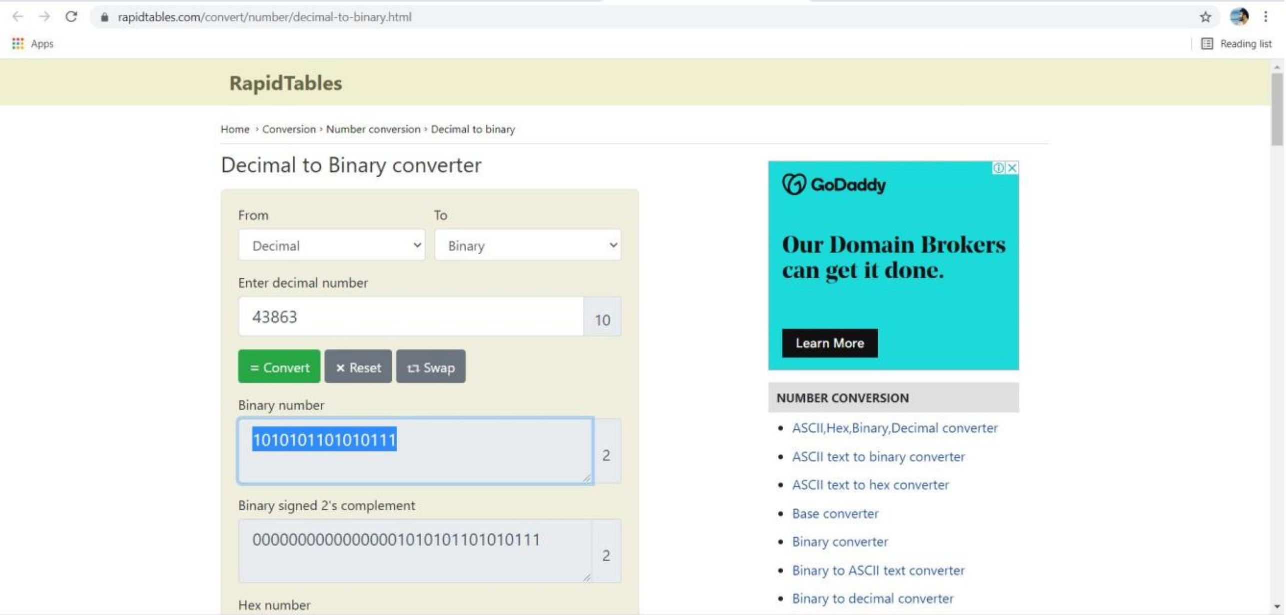
1010101101010111 — Correct Answer

What is the email address you found?

kevinw5667@yandex.com — Correct Answer

Task 10 Finally!!!

Figure 26


rapidtables.com/convert/number/decimal-to-binary.html
Apps
Reading list
RapidTables
Home › Conversion › Number conversion › Decimal to binary
GoDaddy
Our Domain Brokers can get it done.
Learn More
NUMBER CONVERSION
ASCII,Hex,Binary,Decimal converter
ASCII text to binary converter
ASCII text to hex converter
Base converter
Binary converter
Binary to ASCII text converter
Binary to decimal converter
= Convert
× Reset
⇆ Swap

Decimal to Binary converter

From: Decimal

To: Binary

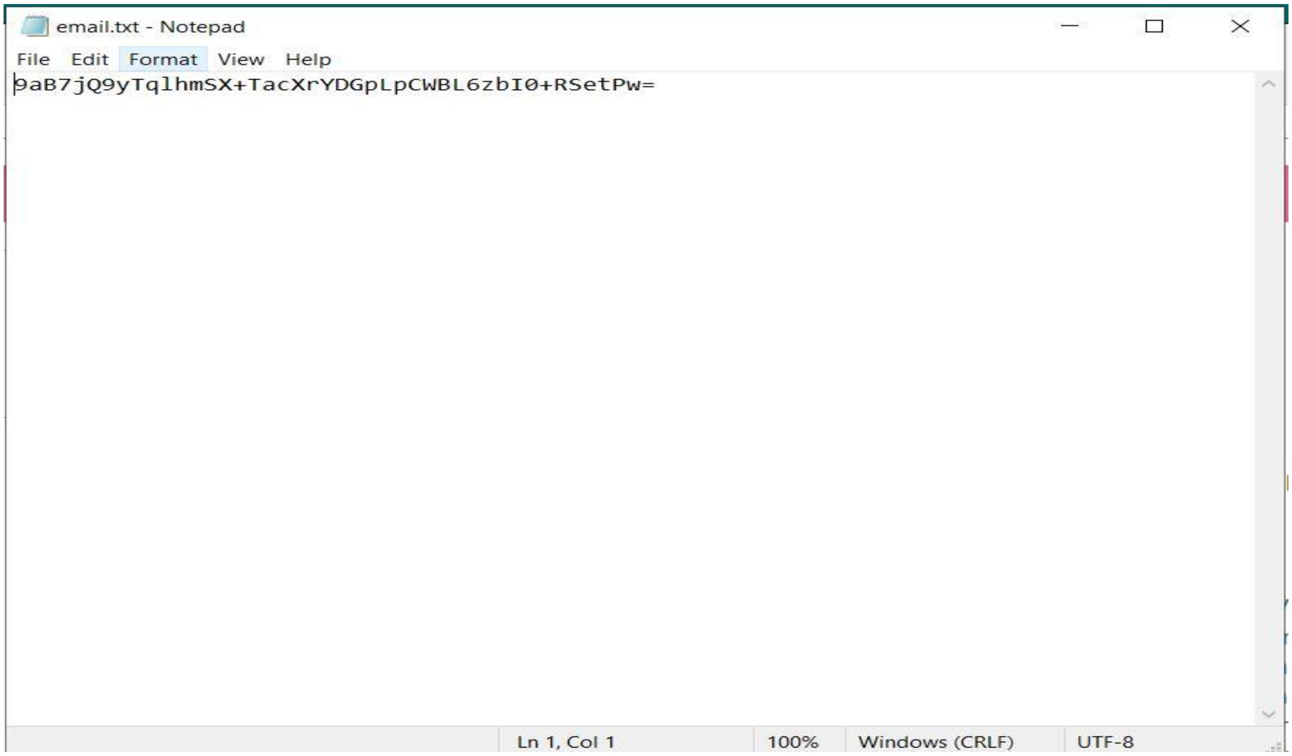
Enter decimal number: 43863 (10)

Binary number: 1010101101010111 (2)

Binary signed 2's complement: 00000000000000001010101101010111 (2)

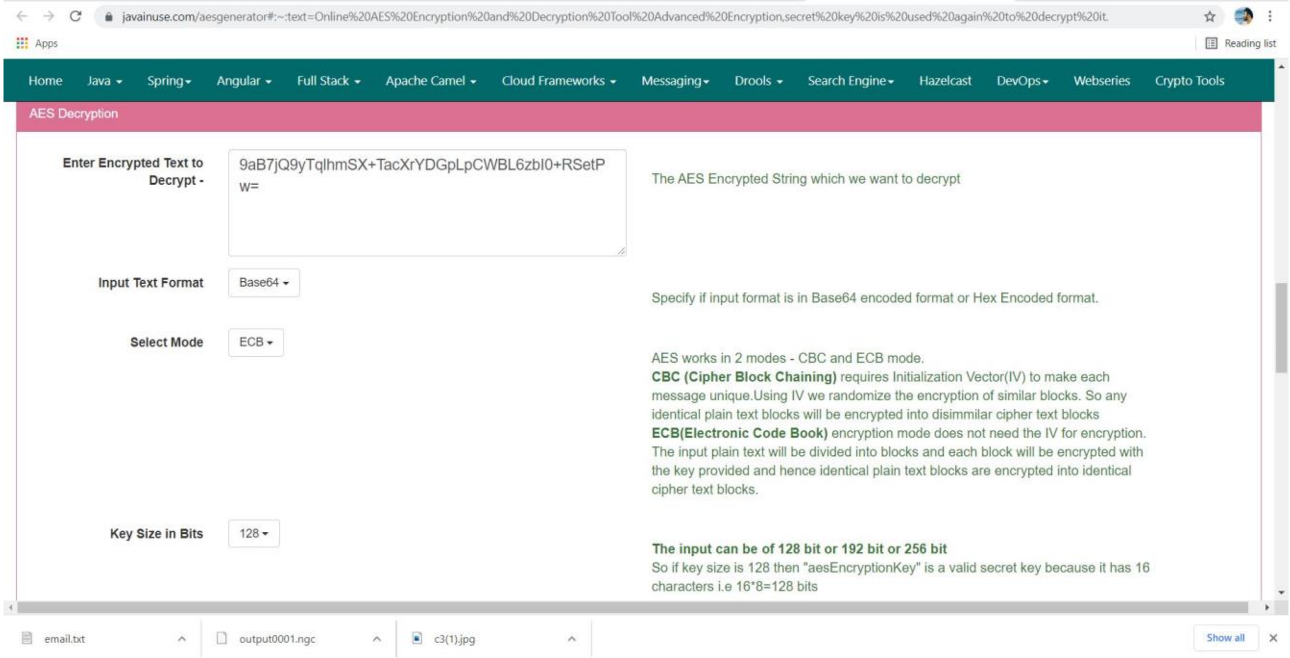
Hex number

Figure 27



```
9aB7jQ9yTqlhmSX+TacXrYDGpLpCWBL6zbI0+RSetPw=
```

Figure 28



AES Decryption

Enter Encrypted Text to Decrypt - 9aB7jQ9yTqlhmSX+TacXrYDGpLpCWBL6zbI0+RSetPw=

The AES Encrypted String which we want to decrypt

Input Text Format: Base64

Specify if input format is in Base64 encoded format or Hex Encoded format.

Select Mode: ECB

AES works in 2 modes - CBC and ECB mode.
CBC (Cipher Block Chaining) requires Initialization Vector(IV) to make each message unique.Using IV we randomize the encryption of similar blocks. So any identical plain text blocks will be encrypted into disimmilar cipher text blocks
ECB(Electronic Code Book) encryption mode does not need the IV for encryption. The input plain text will be divided into blocks and each block will be encrypted with the key provided and hence identical plain text blocks are encrypted into identical cipher text blocks.

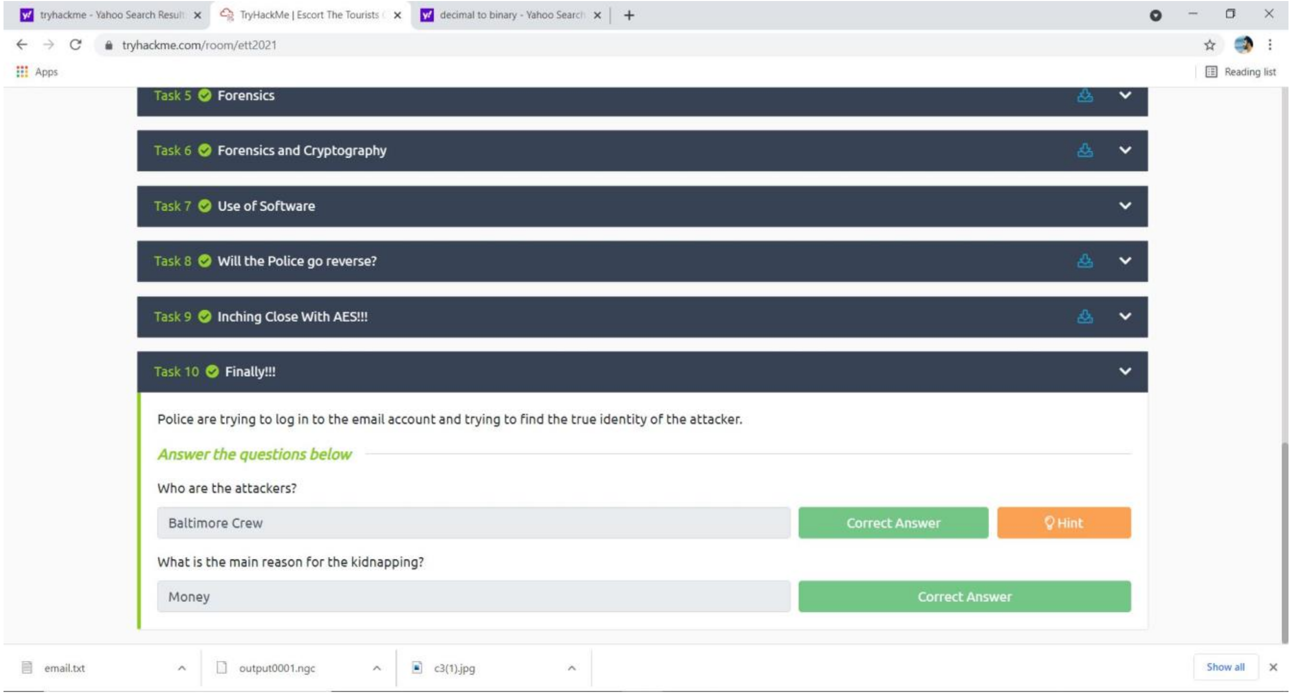
Key Size in Bits: 128

The input can be of 128 bit or 192 bit or 256 bit
So if key size is 128 then "aesEncryptionKey" is a valid secret key because it has 16 characters i.e 16*8=128 bits

Figure 29

Task 10

After logging to the email address, police will be able to reveal the identity of the kidnappers and the reason for the kidnapping. We have added an email with an attachment to find these information after login in to the email account.


tryhackme - Yahoo Search Result
TryHackMe | Escort The Tourists
decimal to binary - Yahoo Search
tryhackme.com/room/ett2021
Apps
Reading list
email.txt
output0001.ngc
c3(1).jpg
Show all

Task 5 Forensics

Task 6 Forensics and Cryptography

Task 7 Use of Software

Task 8 Will the Police go reverse?

Task 9 Inching Close With AES!!!

Task 10 Finally!!!

Police are trying to log in to the email account and trying to find the true identity of the attacker.

Answer the questions below

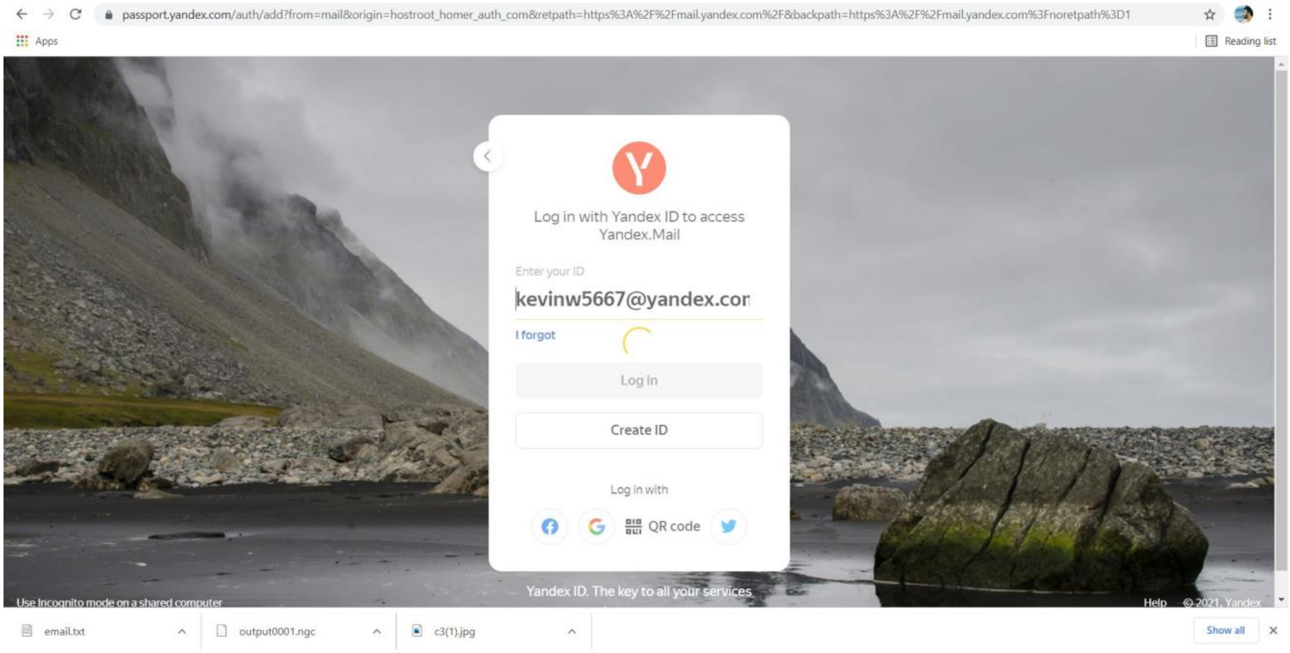
Who are the attackers?

Baltimore Crew — Correct Answer — Hint

What is the main reason for the kidnapping?

Money — Correct Answer

Figure 30


passport.yandex.com/auth/add?from=mail&origin=hostroot_homer_auth_com&retpath=https%3A%2F%2Fmail.yandex.com%2F&backpath=https%3A%2F%2Fmail.yandex.com%3Fnoretpath%3D1
Apps
Reading list
Log in
Create ID
Log in with
QR code
Use Incognito mode on a shared computer
Yandex ID. The key to all your services
Help
© 2021, Yandex
email.txt
output0001.ngc
c3(1).jpg
Show all

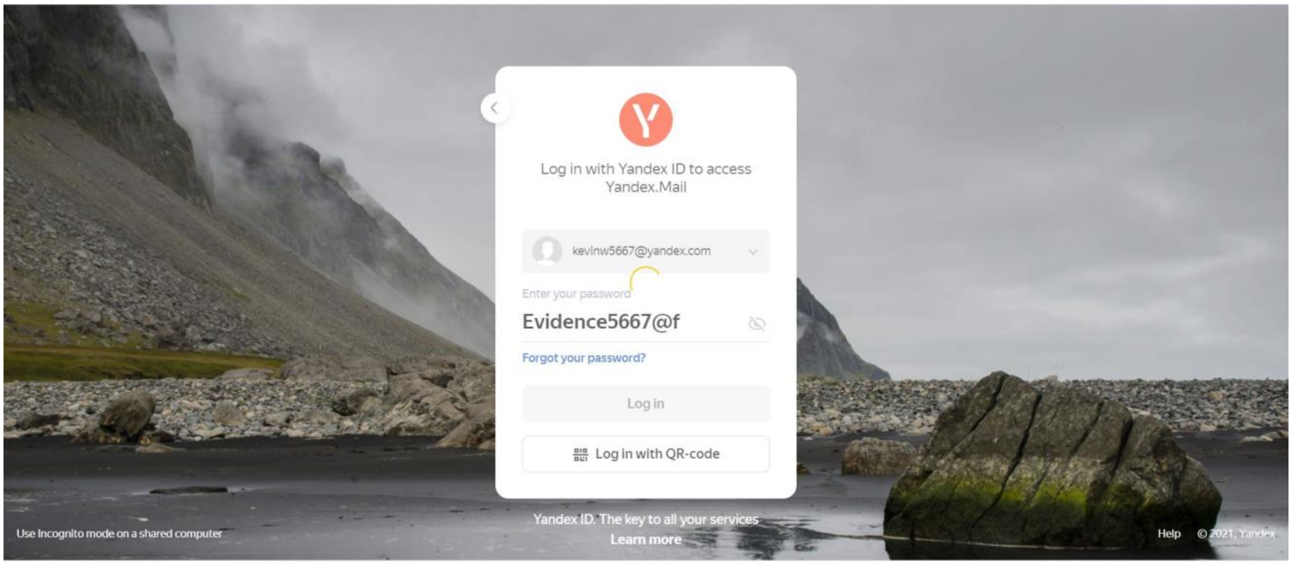
Log in with Yandex ID to access Yandex.Mail

Enter your ID

kevinw5667@yandex.cor

I forgot

Figure 31



Log in with Yandex ID to access Yandex.Mail

kevinw5667@yandex.com

Enter your password

Evidence5667@f

Forgot your password?

Log in

Log in with QR-code

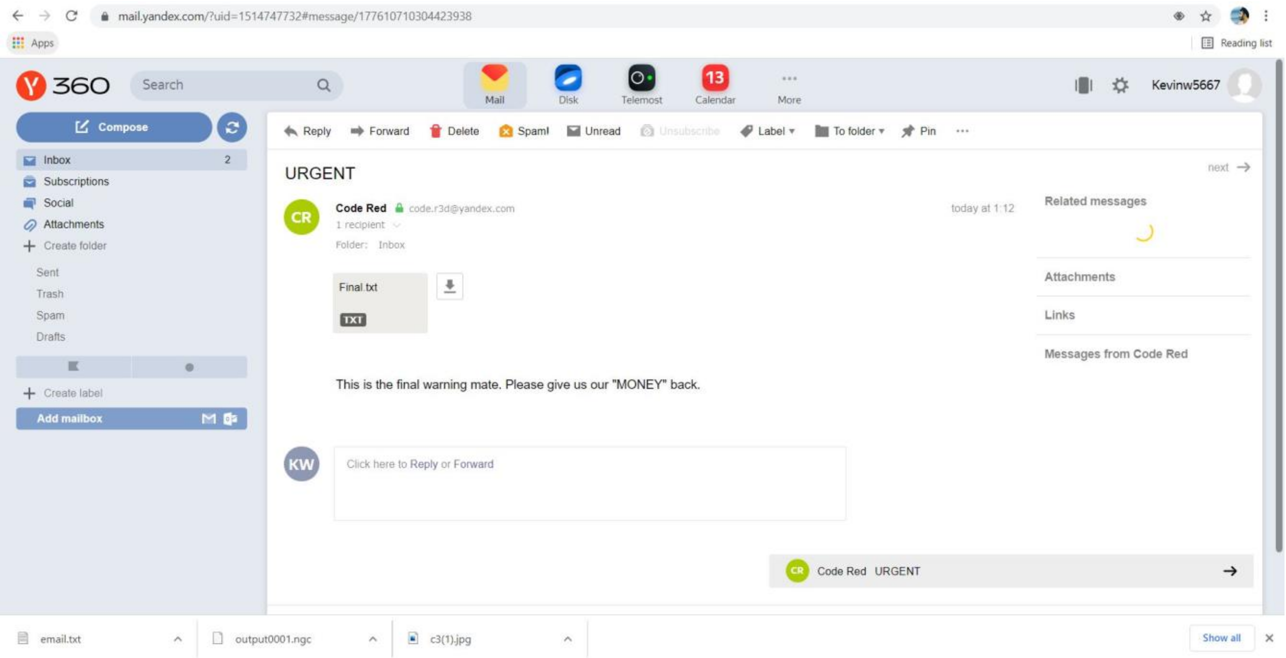
Use Incognito mode on a shared computer

Yandex ID. The key to all your services

Learn more

Help © 2021, Yandex

Figure 32



URGENT

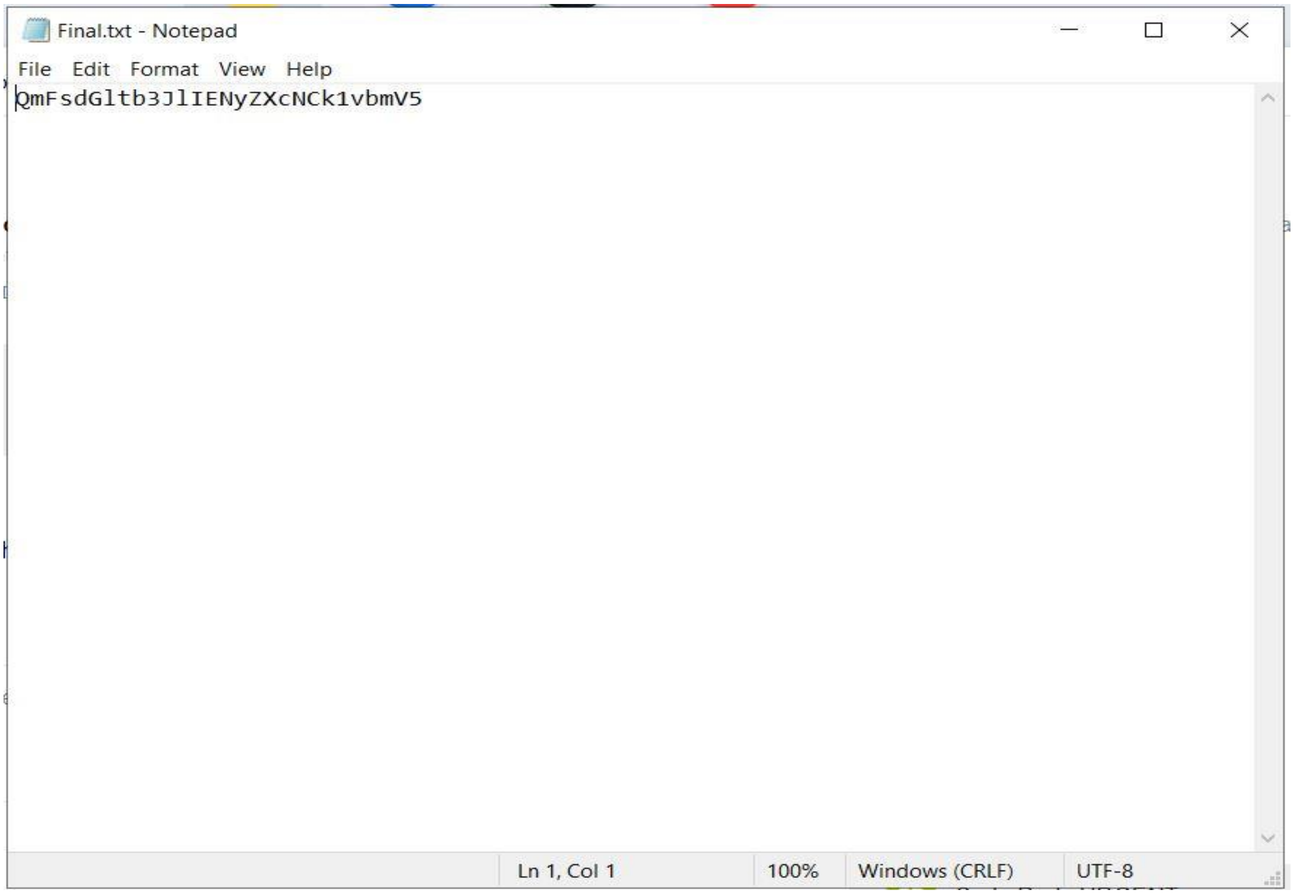
Code Red code.r3d@yandex.com today at 1:12
1 recipient
Folder: Inbox

Final.txt TXT

This is the final warning mate. Please give us our "MONEY" back.

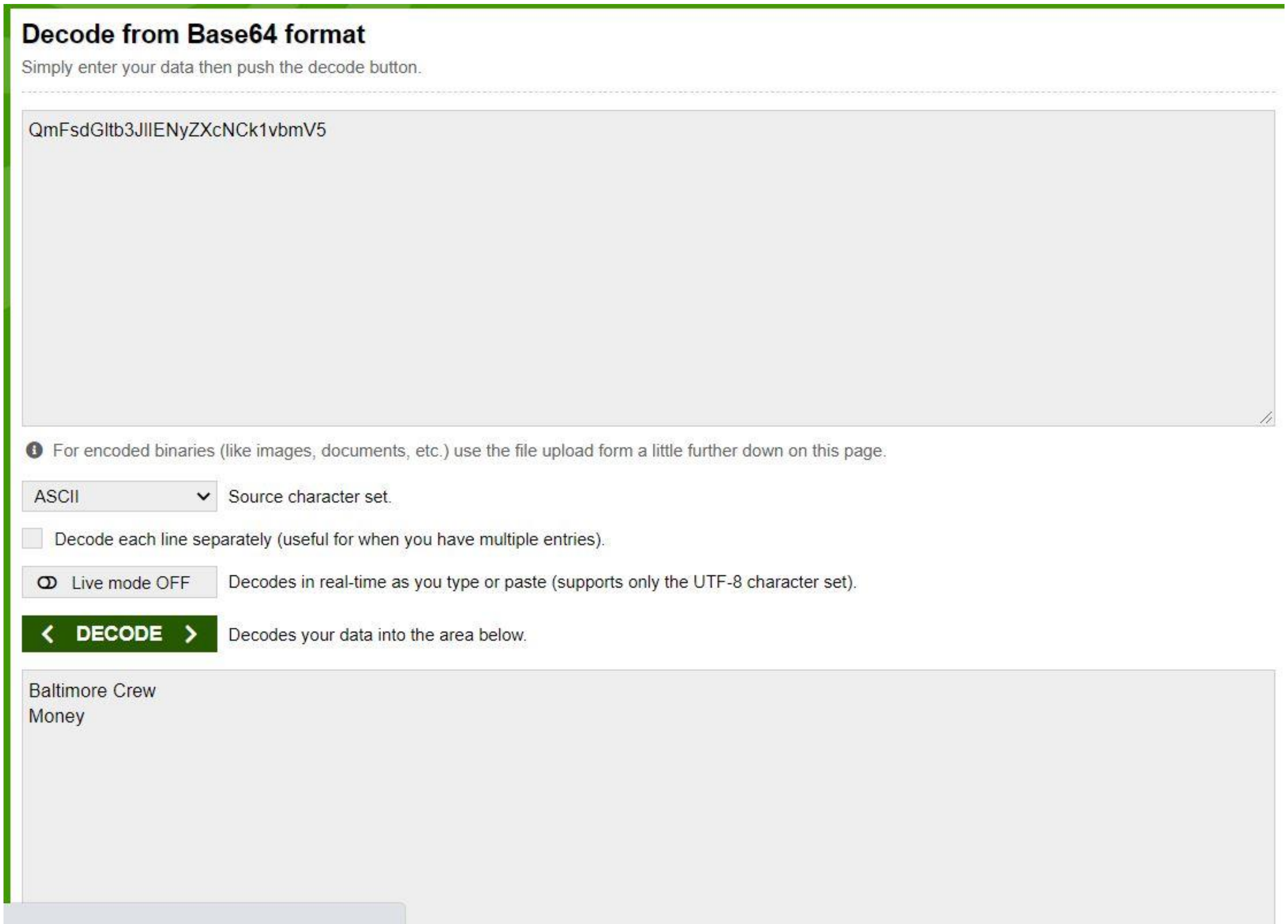
Code Red URGENT

Figure 33



```
QmFsdGltb3JlIENyZXcNCk1vbmV5
```

Figure 34



Decode from Base64 format

Simply enter your data then push the decode button.

QmFsdGltb3JlIENyZXcNCk1vbmV5

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

ASCII Source character set.

□ Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

DECODE Decodes your data into the area below.

```
Baltimore Crew
Money
```

Figure 35