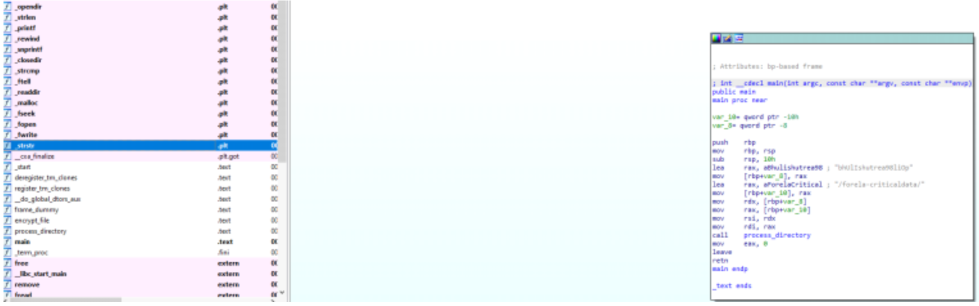
Lockpick Challenge

Sherlock Scenario

Forela needs your help! A whole portion of our UNIX servers have been hit with what we think is ransomware. We are refusing to pay the attackers and need you to find a way to recover the files provided.
Warning This is a warning that this Sherlock includes software that is going to interact with your computer and files. This software has been intentionally included for educational purposes and is NOT intended to be executed or used otherwise. Always handle such files in isolated, controlled, and secure environments. Once the Sherlock zip has been unzipped, you will find a DANGER.txt file. Please read this to proceed.

Task 1:
Please confirm the encryption key string utilised for the encryption of the files provided?

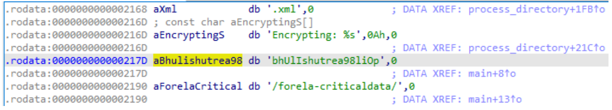
I opened the file "bescrypt3.2" with IDA and the first Function "_strstr" appears and contains some suspicious string



```
_opendir                .plt
_strlen                 .plt
_printf                 .plt
_rewind                 .plt
_snprintf               .plt
_closedir               .plt
_strcmp                 .plt
_ftell                  .plt
_readdir                .plt
_malloc                 .plt
_fseek                  .plt
_fopen                  .plt
_fwrite                 .plt
_strstr                 .plt
__cxa_finalize          .plt.got
_start                  .text
deregister_tm_clones    .text
register_tm_clones      .text
__do_global_dtors_aux   .text
frame_dummy             .text
encrypt_file            .text
process_directory       .text
main                    .text
_term_proc              .fini
free                    extern
__libc_start_main       extern
remove                  extern
fread                   extern
```

```
; Attributes: bp-based frame

; int __cdecl main(int argc, const char **argv, const char **envp)
public main
main proc near

var_10= qword ptr -10h
var_8= qword ptr -8

push    rbp
mov     rbp, rsp
sub     rsp, 10h
lea     rax, aBhulishutrea98 ; "bhUlIshutrea98liOp"
mov     [rbp+var_8], rax
lea     rax, aForelaCritical ; "/forela-criticaldata/"
mov     [rbp+var_10], rax
mov     rdx, [rbp+var_8]
mov     rax, [rbp+var_10]
mov     rsi, rdx
mov     rdi, rax
call    process_directory
mov     eax, 0
leave
retn
main endp

_text ends
```

I clicked on the string and right above him there is a string called "Encrypting" which might be the answer for the question

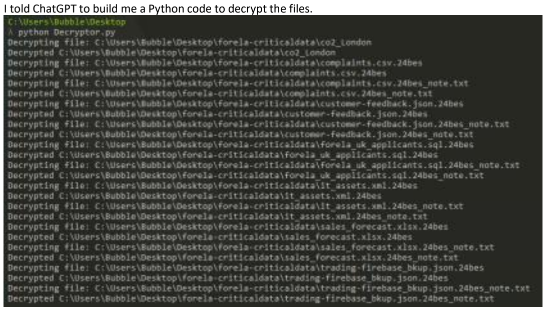


```
.rodata:0000000000002168 aXml            db '.xml',0             ; DATA XREF: process_directory+1FB↑o
.rodata:000000000000216D ; const char aEncryptingS[]
.rodata:000000000000216D aEncryptingS    db 'Encrypting: %s',0Ah,0
.rodata:000000000000216D                                         ; DATA XREF: process_directory+21C↑o
.rodata:000000000000217D aBhulishutrea98 db 'bhUlIshutrea98liOp',0
.rodata:000000000000217D                                         ; DATA XREF: main+8↑o
.rodata:0000000000002190 aForelaCritical db '/forela-criticaldata/',0
.rodata:0000000000002190                                         ; DATA XREF: main+13↑o
```

Answer: bhUllshutrea98liOp

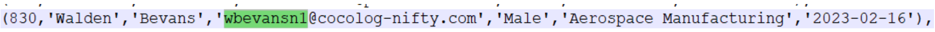
Task 2:
We have recently recieved an email from wbevansn1@cocolog-nifty.com demanding to know the first and last name we have him registered as. They believe they made a mistake in the application process. Please confirm the first and last name of this applicant.

I told ChatGPT to build me a Python code to decrypt the files.



```
C:\Users\Bubble\Desktop
λ python Decryptor.py
Decrypting file: C:\Users\Bubble\Desktop\forela-criticaldata\co2_London
Decrypted C:\Users\Bubble\Desktop\forela-criticaldata\co2_London
Decrypting file: C:\Users\Bubble\Desktop\forela-criticaldata\complaints.csv.24bes
Decrypted C:\Users\Bubble\Desktop\forela-criticaldata\complaints.csv.24bes
Decrypting file: C:\Users\Bubble\Desktop\forela-criticaldata\complaints.csv.24bes_note.txt
Decrypted C:\Users\Bubble\Desktop\forela-criticaldata\complaints.csv.24bes_note.txt
Decrypting file: C:\Users\Bubble\Desktop\forela-criticaldata\customer-feedback.json.24bes
Decrypted C:\Users\Bubble\Desktop\forela-criticaldata\customer-feedback.json.24bes
Decrypting file: C:\Users\Bubble\Desktop\forela-criticaldata\customer-feedback.json.24bes_note.txt
Decrypted C:\Users\Bubble\Desktop\forela-criticaldata\customer-feedback.json.24bes_note.txt
Decrypting file: C:\Users\Bubble\Desktop\forela-criticaldata\forela_uk_applicants.sql.24bes
Decrypted C:\Users\Bubble\Desktop\forela-criticaldata\forela_uk_applicants.sql.24bes
Decrypting file: C:\Users\Bubble\Desktop\forela-criticaldata\forela_uk_applicants.sql.24bes_note.txt
Decrypted C:\Users\Bubble\Desktop\forela-criticaldata\forela_uk_applicants.sql.24bes_note.txt
Decrypting file: C:\Users\Bubble\Desktop\forela-criticaldata\it_assets.xml.24bes
Decrypted C:\Users\Bubble\Desktop\forela-criticaldata\it_assets.xml.24bes
Decrypting file: C:\Users\Bubble\Desktop\forela-criticaldata\it_assets.xml.24bes_note.txt
Decrypted C:\Users\Bubble\Desktop\forela-criticaldata\it_assets.xml.24bes_note.txt
Decrypting file: C:\Users\Bubble\Desktop\forela-criticaldata\sales_forecast.xlsx.24bes
Decrypted C:\Users\Bubble\Desktop\forela-criticaldata\sales_forecast.xlsx.24bes
Decrypting file: C:\Users\Bubble\Desktop\forela-criticaldata\sales_forecast.xlsx.24bes_note.txt
Decrypted C:\Users\Bubble\Desktop\forela-criticaldata\sales_forecast.xlsx.24bes_note.txt
Decrypting file: C:\Users\Bubble\Desktop\forela-criticaldata\trading-firebase_bkup.json.24bes
Decrypted C:\Users\Bubble\Desktop\forela-criticaldata\trading-firebase_bkup.json.24bes
Decrypting file: C:\Users\Bubble\Desktop\forela-criticaldata\trading-firebase_bkup.json.24bes_note.txt
Decrypted C:\Users\Bubble\Desktop\forela-criticaldata\trading-firebase_bkup.json.24bes_note.txt
```

After decrypting the files using the key from task 1, I searched using Notepad++ the name wbevansn1 and found the details on him from the forela_uk_applicants.sql.24bes

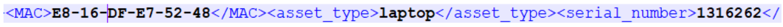


```
(830,'Walden','Bevans','wbevansn1@cocolog-nifty.com','Male','Aerospace Manufacturing','2023-02-16'),
```

Answer: Walden Bevans

Task 3:
What is the MAC address and serial number of the laptop assigned to Hart Manifould?

I searched Manlfould in Notepad++

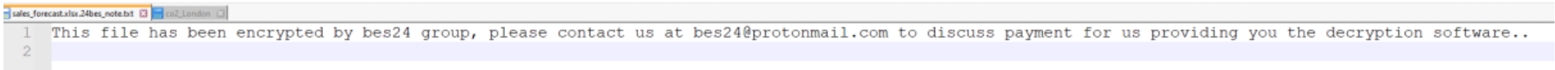


```
<MAC>E8-16-DF-E7-52-48</MAC><asset_type>laptop</asset_type><serial_number>1316262</
```

Answer: E8-16-DF-E7-52-48, 1316262

Task 4:
What is the email address of the attacker?

While opening the txt files from the extracted directory we can see the attacker note



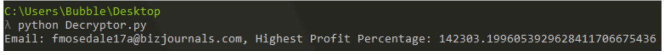
```
This file has been encrypted by bes24 group, please contact us at bes24@protonmail.com to discuss payment for us providing you the decryption software..
```

Answer: bes24@protonmail.com

Task 5:
City of London Police have suspicions of some insider trading taking part within our trading

organisation. Please confirm the email address of the person with the highest profit percentage in a single trade alongside the profit percentage.

To find the answer I asked ChatGPT to make a Python code

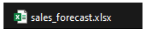


```
C:\Users\Bubble\Desktop
λ python Decryptor.py
Email: fmosedale17a@bizjournals.com, Highest Profit Percentage: 142303.1996053929628411706675436
```

Answer: fmosedale17a@bizjournals.com, 142303.1996053929628411706675436

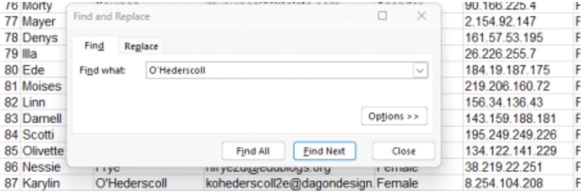
Task 6:
Our E-Discovery team would like to confirm the IP address detailed in the Sales Forecast log for a user who is suspected of sharing their account with a colleague. Please confirm the IP address for Karylin O'Hederscoll.

After decrypting the files, the file "sales_forecast.xlsx.24bes" still look like its encrypted when opening it with Notepad but after removing the .24bes extensions the file is converted to xlsx so I opened the file with Excel



sales_forecast.xlsx

Then I searched for O'Hederscoll

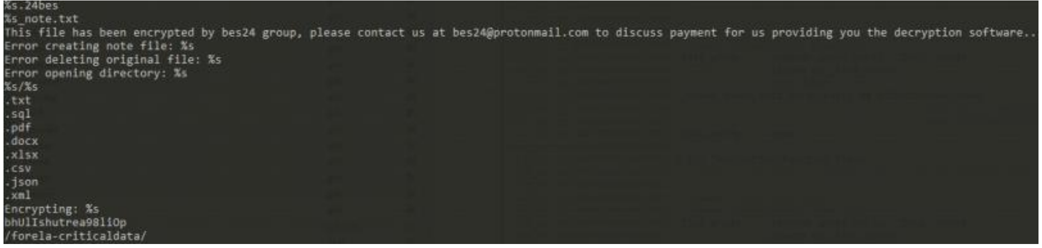


76	Morty				90.166.225.4	F
77	Mayer				2.154.92.147	F
78	Denys				161.57.53.195	F
79	Illa				26.226.255.7	F
80	Ede				184.19.187.175	F
81	Moises				219.206.160.72	F
82	Linn				156.34.136.43	F
83	Darnell				143.159.188.181	F
84	Scotti				195.249.249.226	F
85	Olivette				134.122.141.229	F
86	Nessie	Frye		Female	38.219.22.251	F
87	Karylin	O'Hederscoll	kohederscoll2e@dagondesign	Female	8.254.104.208	F

Answer: 8.254.104.208

Task 7:
Which of the following file extensions is not targeted by the malware? .txt, .sql,.ppt, .pdf, .docx, .xlsx, .csv, .json, .xml

I used strings to see if I can found something that will be related to the extensions question and I noticed some extensions at the output



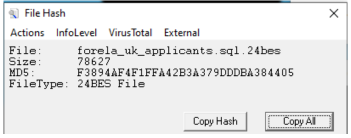
```
%s.24bes
%s_note.txt
This file has been encrypted by bes24 group, please contact us at bes24@protonmail.com to discuss payment for us providing you the decryption software..
Error creating note file: %s
Error deleting original file: %s
Error opening directory: %s
%s/%s
.txt
.sql
.pdf
.docx
.xlsx
.csv
.json
.xml
Encrypting: %s
bhUlIshutrea98liOp
/forela-criticaldata/
```

The extension that is not being targeted is .ppt

Answer: .ppt

Task 8:
We need to confirm the integrity of the files once decrypted. Please confirm the MD5 hash of the applicants DB.

After decrypting the files I used MD5 hash to see the hash

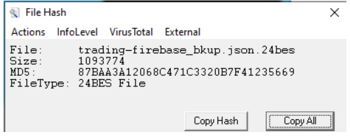


```
File:     forela_uk_applicants.sql.24bes
Size:     78627
MD5:      F3894AF4F1FFA42B3A379DDDBA384405
FileType: 24BES File
```

Answer: F3894AF4F1FFA42B3A379DDDBA384405

Task 9:
We need to confirm the integrity of the files once decrypted. Please confirm the MD5 hash of the trading backup.

After decrypting the files I used MD5 hash to see the hash

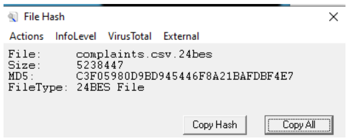


```
File:     trading-firebase_bkup.json.24bes
Size:     1093774
MD5:      87BAA3A12068C471C3320B7F41235669
FileType: 24BES File
```

Answer: 87BAA3A12068C471C3320B7F41235669

Task 10:
We need to confirm the integrity of the files once decrypted. Please confirm the MD5 hash of the complaints file.

After decrypting the files I used MD5 hash to see the hash



```
File:     complaints.csv.24bes
Size:     5238447
MD5:      C3F05980D9BD945446F8A21BAFDBF4E7
FileType: 24BES File
```

Answer: C3F05980D9BD945446F8A21BAFDBF4E7