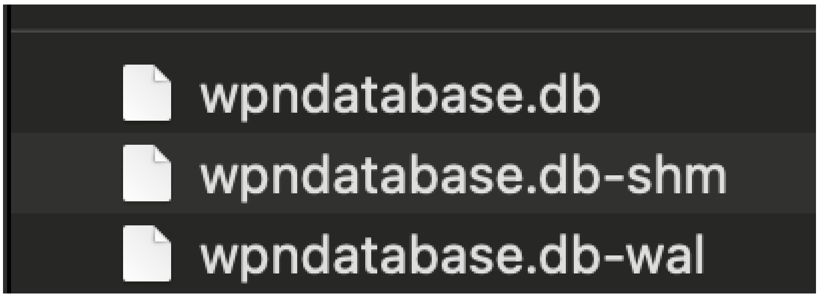
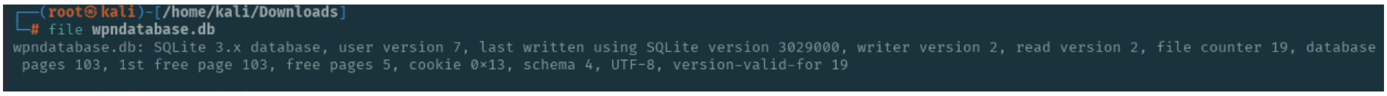
Jingle Bell,sqlite3

```
Sherlock Scenario
Torrin is suspected to be an insider threat in Forela. He is believed to
have leaked some data and removed certain applications from their
workstation. They managed to bypass some controls and installed unauthorised
software. Despite the forensic team's efforts, no evidence of data leakage
was found. As a senior incident responder, you have been tasked with
investigating the incident to determine the conversation between the two
parties involved.
* * *
About Jingle Bell
Jingle Bell is an easy difficulty Sherlock where you are presented with a
set of Windows artefacts and must uncover the source of a leak within
Forela's corporate environment.
```



```
wpndatabase.db
wpndatabase.db-shm
wpndatabase.db-wal
```

是sqlite3



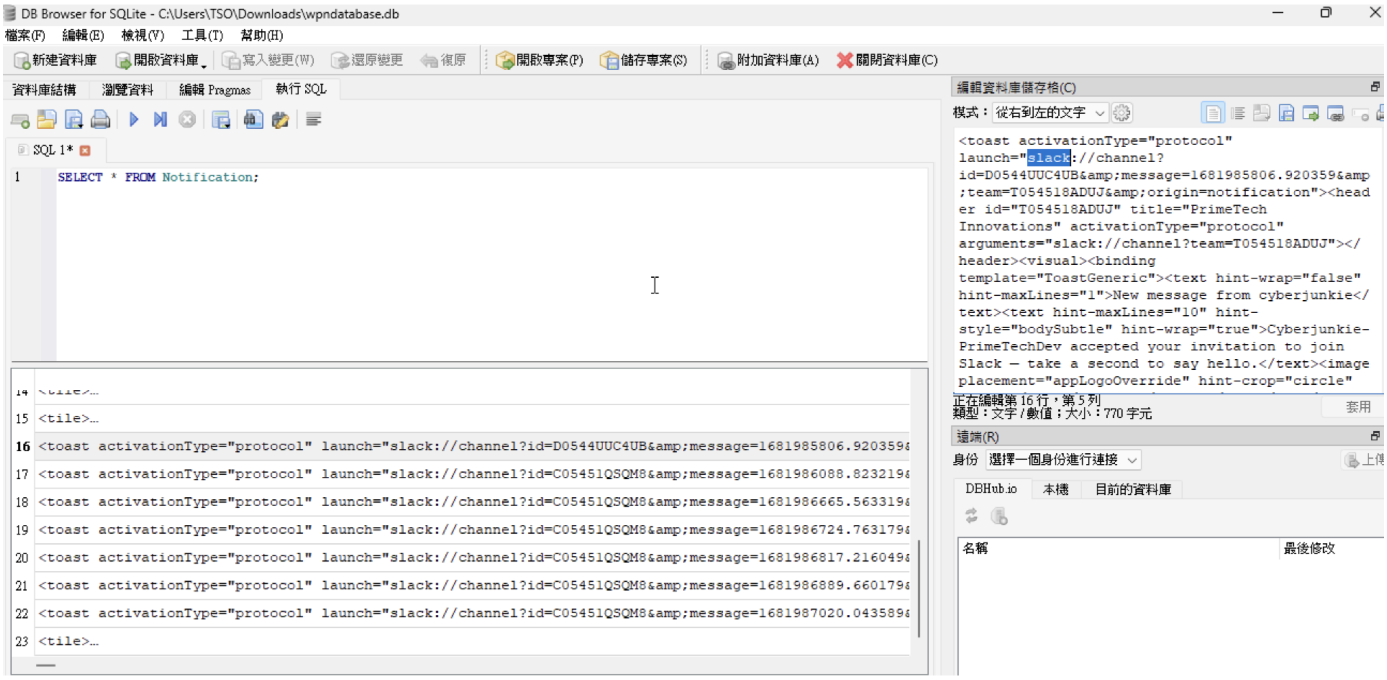
```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# file wpndatabase.db
wpndatabase.db: SQLite 3.x database, user version 7, last written using SQLite version 3029000, writer version 2, read version 2, file counter 19, database
 pages 103, 1st free page 103, free pages 5, cookie 0×13, schema 4, UTF-8, version-valid-for 19
```

我這邊用win開啟比較方便

Task 1

Which software/application did Torrin use to leak Forela's secrets?

指令：`SELECT * FROM Notification;`


DB Browser for SQLite - C:\Users\TSO\Downloads\wpndatabase.db
檔案(F) 編輯(E) 檢視(V) 工具(T) 幫助(H)
新建資料庫 開啟資料庫 寫入變更(W) 還原變更 復原 開啟專案(P) 儲存專案(S) 附加資料庫(A) 關閉資料庫(C)
資料庫結構 瀏覽資料 編輯 Pragmas 執行 SQL
SQL 1*
編輯資料庫儲存格(C)
模式：從右到左的文字
套用
遠端(R)
身份 選擇一個身份進行連接
上傳
DBHub.io 本機 目前的資料庫
名稱 最後修改

```
SELECT * FROM Notification;
```

```
14 <tile>…
15 <tile>…
16 <toast activationType="protocol" launch="slack://channel?id=D0544UUC4UB&amp;message=1681985806.920359&
17 <toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681986088.823219&
18 <toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681986665.563319&
19 <toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681986724.763179&
20 <toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681986817.216049&
21 <toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681986889.660179&
22 <toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681987020.043589&
23 <tile>…
```

```
<toast activationType="protocol"
launch="slack://channel?
id=D0544UUC4UB&amp;message=1681985806.920359&amp
;team=T054518ADUJ&amp;origin=notification"><head
er id="T054518ADUJ" title="PrimeTech
Innovations" activationType="protocol"
arguments="slack://channel?team=T054518ADUJ"></
header><visual><binding
template="ToastGeneric"><text hint-wrap="false"
hint-maxLines="1">New message from cyberjunkie</
text><text hint-maxLines="10" hint-
style="bodySubtle" hint-wrap="true">Cyberjunkie-
PrimeTechDev accepted your invitation to join
Slack — take a second to say hello.</text><image
placement="appLogoOverride" hint-crop="circle"
```

正在編輯第 16 行，第 5 列
類型：文字 / 數值；大小：770 字元

`slack`

Task 2

What's the name of the rival company to which Torrin leaked the data?

同上，
查看他的title
`PrimeTech Innovations`

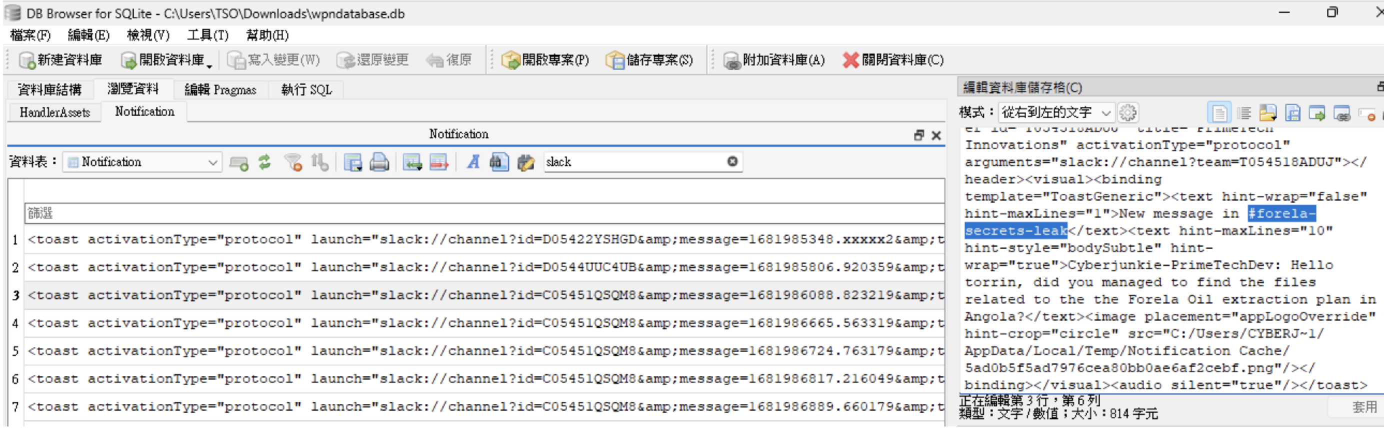
Task 3

What is the username of the person from the competitor organization whom Torrin shared information with?

看到快眼瞎
`Cyberjunkie-PrimeTechDev`

Task 4

What's the channel name in which they conversed with each other?


DB Browser for SQLite - C:\Users\TSO\Downloads\wpndatabase.db
檔案(F) 編輯(E) 檢視(V) 工具(T) 幫助(H)
新建資料庫 開啟資料庫 寫入變更(W) 還原變更 復原 開啟專案(P) 儲存專案(S) 附加資料庫(A) 關閉資料庫(C)
資料庫結構 瀏覽資料 編輯 Pragmas 執行 SQL
HandlerAssets Notification
Notification
資料表： Notification
slack
篩選
編輯資料庫儲存格(C)
模式： 從右到左的文字
套用

```
1 <toast activationType="protocol" launch="slack://channel?id=D05422YSHGD&amp;message=1681985348.xxxxx2&amp;t
2 <toast activationType="protocol" launch="slack://channel?id=D0544UUC4UB&amp;message=1681985806.920359&amp;t
3 <toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681986088.823219&amp;t
4 <toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681986665.563319&amp;t
5 <toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681986724.763179&amp;t
6 <toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681986817.216049&amp;t
7 <toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681986889.660179&amp;t
```

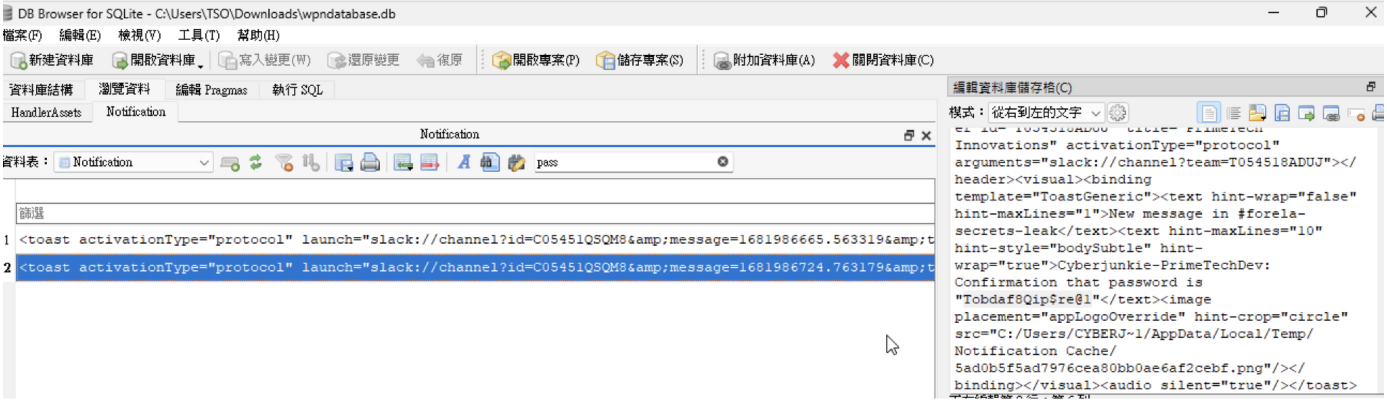
```
Innovations" activationType="protocol"
arguments="slack://channel?team=T054518ADUJ"></
header><visual><binding
template="ToastGeneric"><text hint-wrap="false"
hint-maxLines="1">New message in #forela-
secrets-leak</text><text hint-maxLines="10"
hint-style="bodySubtle" hint-
wrap="true">Cyberjunkie-PrimeTechDev: Hello
torrin, did you managed to find the files
related to the the Forela Oil extraction plan in
Angola?</text><image placement="appLogoOverride"
hint-crop="circle" src="C:/Users/CYBERJ~1/
AppData/Local/Temp/Notification Cache/
5ad0b5f5ad7976cea80bb0ae6af2cebf.png"/></
binding></visual><audio silent="true"/></toast>
```

正在編輯第 3 行，第 6 列
類型：文字 / 數值；大小：814 字元

`#forela-secrets-leak`

Task 5

What was the password for the archive server?


DB Browser for SQLite - C:\Users\TSO\Downloads\wpndatabase.db
檔案(F) 編輯(E) 檢視(V) 工具(T) 幫助(H)
新建資料庫 開啟資料庫 寫入變更(W) 還原變更 復原 開啟專案(P) 儲存專案(S) 附加資料庫(A) 關閉資料庫(C)
資料庫結構 瀏覽資料 編輯 Pragmas 執行 SQL
HandlerAssets Notification
Notification
資料表： Notification
pass
篩選
編輯資料庫儲存格(C)
模式： 從右到左的文字

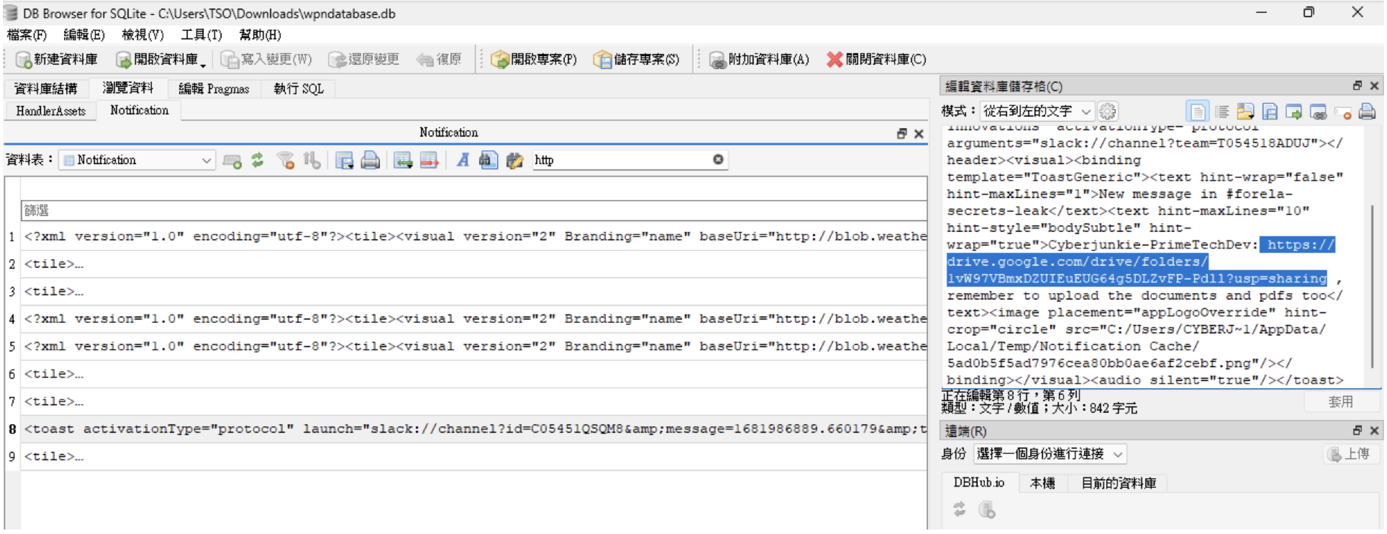
```
1 <toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681986665.563319&amp;t
2 <toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681986724.763179&amp;t
```

```
Innovations" activationType="protocol"
arguments="slack://channel?team=T054518ADUJ"></
header><visual><binding
template="ToastGeneric"><text hint-wrap="false"
hint-maxLines="1">New message in #forela-
secrets-leak</text><text hint-maxLines="10"
hint-style="bodySubtle" hint-
wrap="true">Cyberjunkie-PrimeTechDev:
Confirmation that password is
"Tobdaf8Qip$re@1"</text><image
placement="appLogoOverride" hint-crop="circle"
src="C:/Users/CYBERJ~1/AppData/Local/Temp/
Notification Cache/
5ad0b5f5ad7976cea80bb0ae6af2cebf.png"/></
binding></visual><audio silent="true"/></toast>
```

`Tobdaf8Qip$re@1`

Task 6

What was the URL provided to Torrin to upload stolen data to?


DB Browser for SQLite - C:\Users\TSO\Downloads\wpndatabase.db
檔案(F) 編輯(E) 檢視(V) 工具(T) 幫助(H)
新建資料庫 開啟資料庫 寫入變更(W) 還原變更 復原 開啟專案(P) 儲存專案(S) 附加資料庫(A) 關閉資料庫(C)
資料庫結構 瀏覽資料 編輯 Pragmas 執行 SQL
HandlerAssets Notification
Notification
資料表： Notification
http
篩選
編輯資料庫儲存格(C)
模式： 從右到左的文字
套用
遠端(R)
身份 選擇一個身份進行連接
上傳
DBHub.io 本機 目前的資料庫

```
1 <?xml version="1.0" encoding="utf-8"?><tile><visual version="2" Branding="name" baseUri="http://blob.weathe
2 <tile>...
3 <tile>...
4 <?xml version="1.0" encoding="utf-8"?><tile><visual version="2" Branding="name" baseUri="http://blob.weathe
5 <?xml version="1.0" encoding="utf-8"?><tile><visual version="2" Branding="name" baseUri="http://blob.weathe
6 <tile>...
7 <tile>...
8 <toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681986889.660179&amp;t
9 <tile>...
```

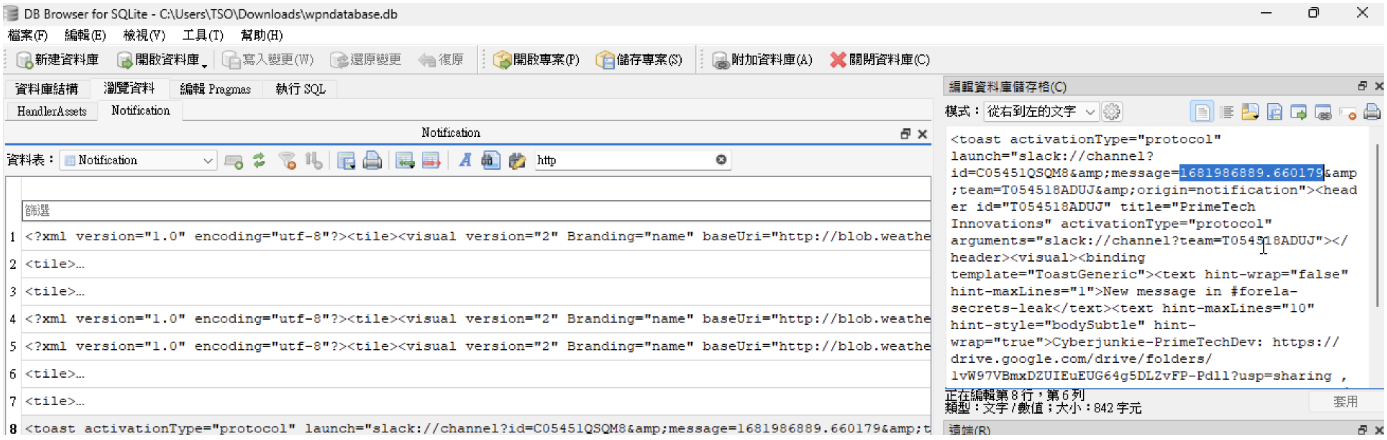
```
arguments="slack://channel?team=T054518ADUJ"></
header><visual><binding
template="ToastGeneric"><text hint-wrap="false"
hint-maxLines="1">New message in #forela-
secrets-leak</text><text hint-maxLines="10"
hint-style="bodySubtle" hint-
wrap="true">Cyberjunkie-PrimeTechDev: https://
drive.google.com/drive/folders/
1vW97VBmxDZUIEuEUG64g5DLZvFP-Pdll?usp=sharing ,
remember to upload the documents and pdfs too</
text><image placement="appLogoOverride" hint-
crop="circle" src="C:/Users/CYBERJ~1/AppData/
Local/Temp/Notification Cache/
5ad0b5f5ad7976cea80bb0ae6af2cebf.png"/></
binding></visual><audio silent="true"/></toast>
```

正在編輯第 8 行，第 6 列
類型：文字 / 數值；大小：842 字元

```
https://drive.google.com/drive/folders/1vW97VBmxDZUIEuEUG64g5DLZvFP-Pdll?usp=sharing
```

Task 7

When was the above link shared with Torrin?



DB Browser for SQLite - C:\Users\TSO\Downloads\wpndatabase.db
檔案(F) 編輯(E) 檢視(V) 工具(T) 幫助(H)
新建資料庫 開啟資料庫 寫入變更(W) 還原變更 復原 開啟專案(P) 儲存專案(S) 附加資料庫(A) 關閉資料庫(C)
資料庫結構 瀏覽資料 編輯 Pragmas 執行 SQL
HandlerAssets Notification
Notification
篩選
編輯資料庫儲存格(C)
套用
遠端(R)

資料表：Notification

http

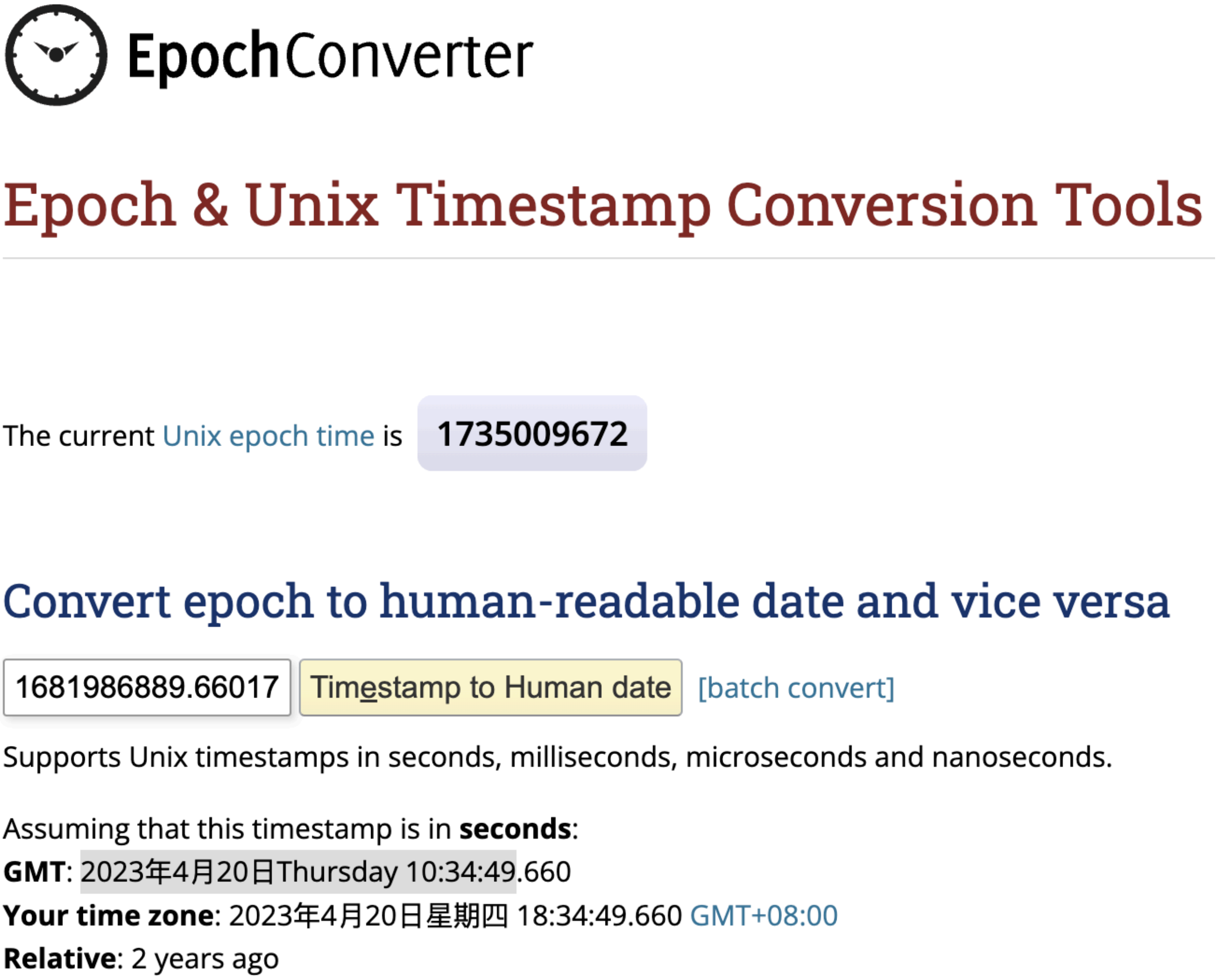
```
1 <?xml version="1.0" encoding="utf-8"?><tile><visual version="2" Branding="name" baseUri="http://blob.weathe
2 <tile>…
3 <tile>…
4 <?xml version="1.0" encoding="utf-8"?><tile><visual version="2" Branding="name" baseUri="http://blob.weathe
5 <?xml version="1.0" encoding="utf-8"?><tile><visual version="2" Branding="name" baseUri="http://blob.weathe
6 <tile>…
7 <tile>…
8 <toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681986889.660179&amp;t
```

模式：從右到左的文字

```
<toast activationType="protocol"
launch="slack://channel?
id=C05451QSQM8&amp;message=1681986889.660179&amp
;team=T054518ADUJ&amp;origin=notification"><head
er id="T054518ADUJ" title="PrimeTech
Innovations" activationType="protocol"
arguments="slack://channel?team=T054518ADUJ"></
header><visual><binding
template="ToastGeneric"><text hint-wrap="false"
hint-maxLines="1">New message in #forela-
secrets-leak</text><text hint-maxLines="10"
hint-style="bodySubtle" hint-
wrap="true">Cyberjunkie-PrimeTechDev: https://
drive.google.com/drive/folders/
1vW97VBmxDZUIEuEUG64g5DLZvFP-Pdll?usp=sharing ,
```

正在編輯第 8 行，第 6 列
類型：文字 / 數值；大小：842 字元

`1681986889.660179`



Epoch & Unix Timestamp Conversion Tools

The current Unix epoch time is 1735009672

Convert epoch to human-readable date and vice versa

1681986889.66017

Supports Unix timestamps in seconds, milliseconds, microseconds and nanoseconds.

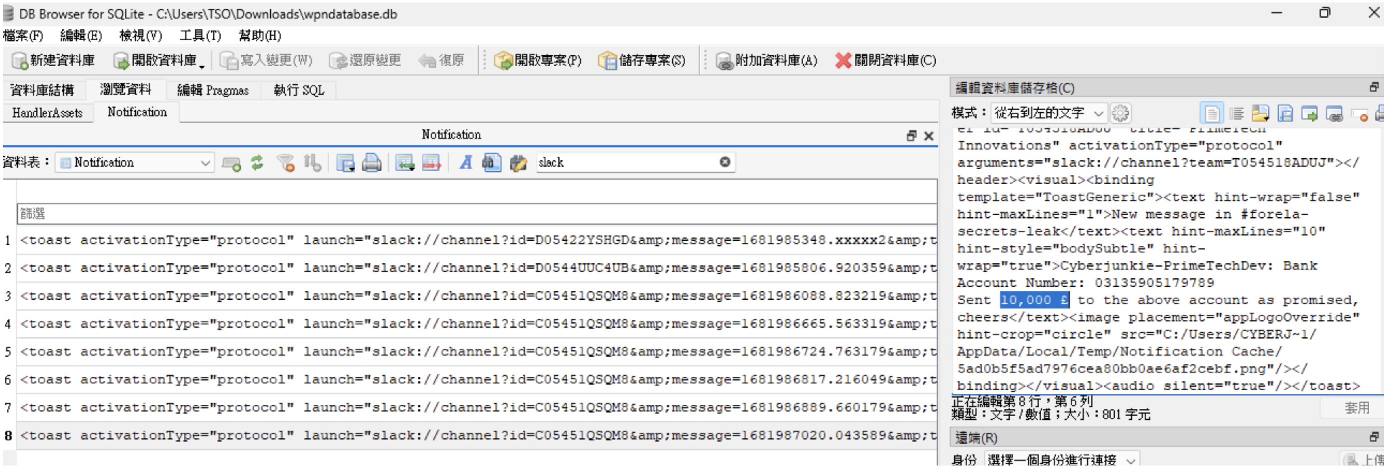
Assuming that this timestamp is in **seconds**:
GMT: 2023年4月20日Thursday 10:34:49.660
Your time zone: 2023年4月20日星期四 18:34:49.660 GMT+08:00
Relative: 2 years ago

轉換後

`2023-4-20 10:34:49`

Task 8

For how much money did Torrin leak Forela's secrets?



DB Browser for SQLite - C:\Users\TSO\Downloads\wpndatabase.db
檔案(F) 編輯(E) 檢視(V) 工具(T) 幫助(H)
新建資料庫 開啟資料庫 寫入變更(W) 還原變更 復原 開啟專案(P) 儲存專案(S) 附加資料庫(A) 關閉資料庫(C)
資料庫結構 瀏覽資料 編輯 Pragmas 執行 SQL
HandlerAssets Notification
Notification
資料表： Notification
slack
篩選
編輯資料庫儲存格(C)
模式： 從右到左的文字
套用
遠端(R)
身份 選擇一個身份進行連接
上傳

```
1 <toast activationType="protocol" launch="slack://channel?id=D05422YSHGD&amp;message=1681985348.xxxxx2&amp;t
2 <toast activationType="protocol" launch="slack://channel?id=D0544UUC4UB&amp;message=1681985806.920359&amp;t
3 <toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681986088.823219&amp;t
4 <toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681986665.563319&amp;t
5 <toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681986724.763179&amp;t
6 <toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681986817.216049&amp;t
7 <toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681986889.660179&amp;t
8 <toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681987020.043589&amp;t
```

```
el id="T054518ADUJ" title="PrimeTech
Innovations" activationType="protocol"
arguments="slack://channel?team=T054518ADUJ"></
header><visual><binding
template="ToastGeneric"><text hint-wrap="false"
hint-maxLines="1">New message in #forela-
secrets-leak</text><text hint-maxLines="10"
hint-style="bodySubtle" hint-
wrap="true">Cyberjunkie-PrimeTechDev: Bank
Account Number: 03135905179789
Sent 10,000 £ to the above account as promised,
cheers</text><image placement="appLogoOverride"
hint-crop="circle" src="C:/Users/CYBERJ~1/
AppData/Local/Temp/Notification Cache/
5ad0b5f5ad7976cea80bb0ae6af2cebf.png"/></
binding></visual><audio silent="true"/></toast>
```

正在編輯第 8 行，第 6 列
類型：文字 / 數值；大小：801 字元

`£10000`