HTB SHERLOCKS - JINGLE BELL

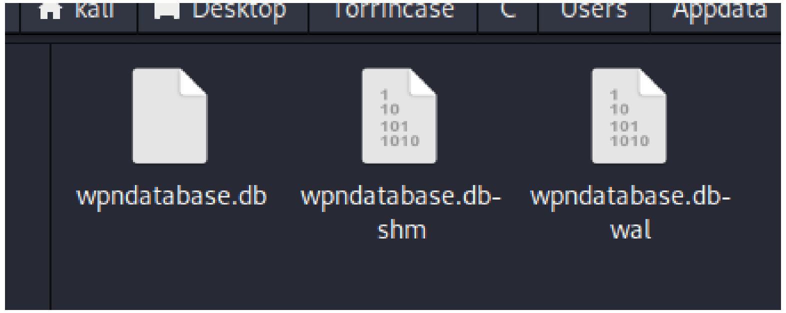
write-up by Chanan Shenker

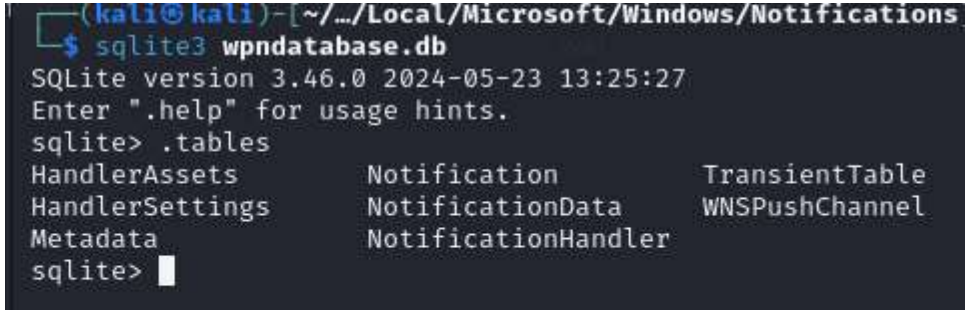
Sherlock scenario:

- 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.

Strat:

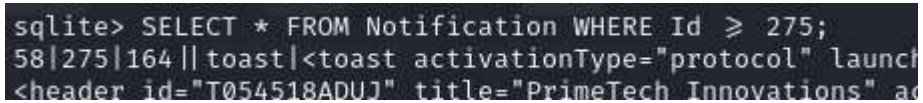
- The whole challenge revolves around analyzing a SQLite3 database that holds a conversation between two individuals.





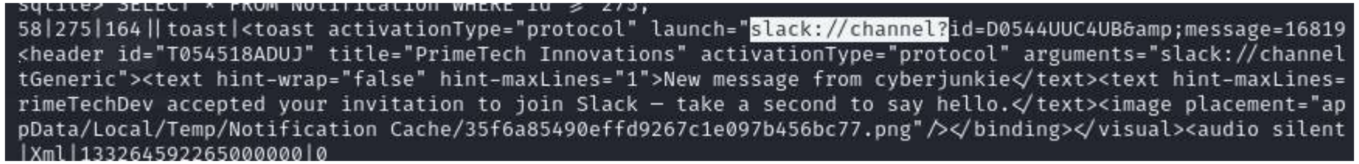
```
┌──(kali㉿kali)-[~/…/Local/Microsoft/Windows/Notifications
└─$ sqlite3 wpndatabase.db
SQLite version 3.46.0 2024-05-23 13:25:27
Enter ".help" for usage hints.
sqlite> .tables
HandlerAssets          Notification           TransientTable
HandlerSettings        NotificationData       WNSPushChannel
Metadata               NotificationHandler
sqlite> █
```

- After doing some looking around, I found that in the ‘notification’ table there is a problematic conversation. So I narrowed down the search to 5 entries in the ‘notification’ tables.



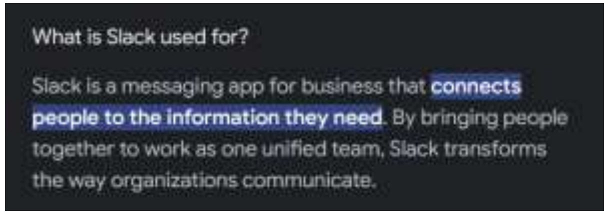
```
sqlite> SELECT * FROM Notification WHERE Id ≥ 275;
58|275|164||toast|<toast activationType="protocol" launch
<header id="T054518ADUJ" title="PrimeTech Innovations" ac
```

- First the entry with the ID 275. In it, I could see that an invite was sent to join ‘cyberjunkie’ to a conversation. We can see that



```
sqlite> SELECT * FROM Notification WHERE Id ≥ 275;
58|275|164||toast|<toast activationType="protocol" launch="slack://channel?id=D0544UUC4UB&amp;message=16819
<header id="T054518ADUJ" title="PrimeTech Innovations" activationType="protocol" arguments="slack://channel
tGeneric"><text hint-wrap="false" hint-maxLines="1">New message from cyberjunkie</text><text hint-maxLines=
rimeTechDev accepted your invitation to join Slack — take a second to say hello.</text><image placement="ap
pData/Local/Temp/Notification Cache/35f6a85490effd9267c1e097b456bc77.png"/></binding></visual><audio silent
|Xml|133264592265000000|0
```

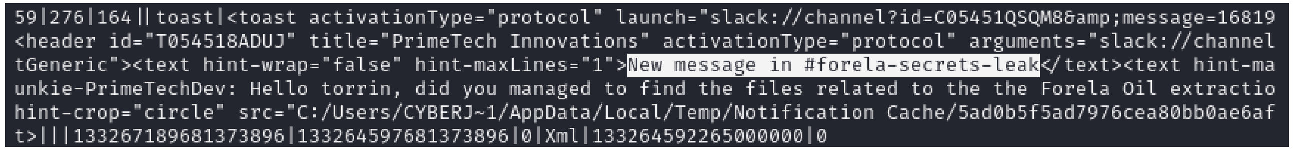
- Looking at the URL being used in the entry and the invitation message, I saw that they were using an app named slack. (task 1)
- A quick search, and I could confirm that it is a messaging app.



What is Slack used for?

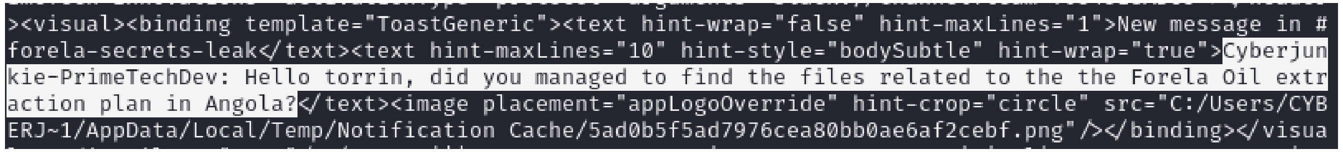
Slack is a messaging app for business that connects people to the information they need. By bringing people together to work as one unified team, Slack transforms the way organizations communicate.

- In the next entry, I could see that the user joined a messaging group named ‘forela secrets leak’ (task 4), which is foolishly suspicious. Looking at the actual message, I could see that the user ‘Torrin’ is being asked to send sensitive data about the forela oil extractions.



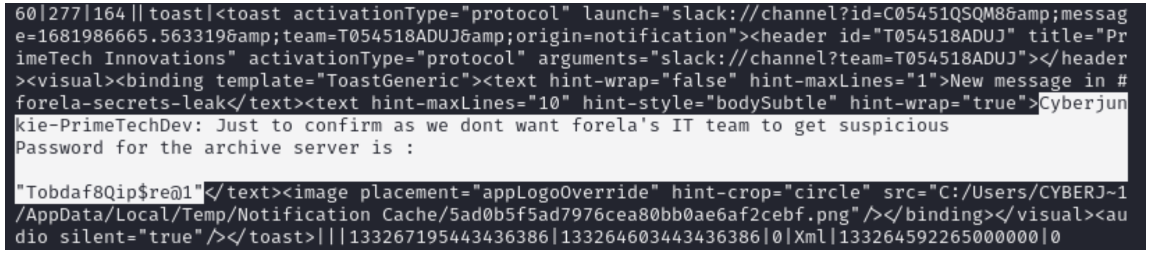
```
59|276|164||toast|<toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=16819
<header id="T054518ADUJ" title="PrimeTech Innovations" activationType="protocol" arguments="slack://channel
tGeneric"><text hint-wrap="false" hint-maxLines="1">New message in #forela-secrets-leak</text><text hint-ma
unkie-PrimeTechDev: Hello torrin, did you managed to find the files related to the the Forela Oil extractio
hint-crop="circle" src="C:/Users/CYBERJ~1/AppData/Local/Temp/Notification Cache/5ad0b5f5ad7976cea80bb0ae6af
t>|||133267189681373896|133264597681373896|0|Xml|133264592265000000|0
```

- I can also see the username that sent the message, ‘Cyberjunkie-PrimeTechDev’. (task 3)



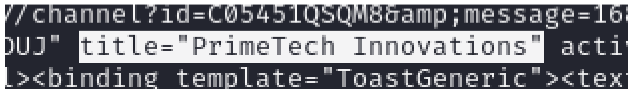
```
><visual><binding template="ToastGeneric"><text hint-wrap="false" hint-maxLines="1">New message in #
forela-secrets-leak</text><text hint-maxLines="10" hint-style="bodySubtle" hint-wrap="true">Cyberjun
kie-PrimeTechDev: Hello torrin, did you managed to find the files related to the the Forela Oil extr
action plan in Angola?</text><image placement="appLogoOverride" hint-crop="circle" src="C:/Users/CYB
ERJ~1/AppData/Local/Temp/Notification Cache/5ad0b5f5ad7976cea80bb0ae6af2cebf.png"/></binding></visua
```

- In the next entry, I could see the continuation of their conversation where the user ‘torrin’ shares the password for the archive server ‘Tobdaf8Qip$re@1’ (task 5).
- By this time I also noticed that the title of each message is ‘PrimeTech Innovations’ (task 2), assuming it’s the company name of the ‘Cyberjunkie-PrimeTechDev’ user.



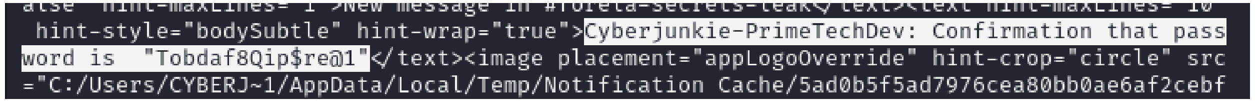
```
60|277|164||toast|<toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;messag
e=1681986665.563319&amp;team=T054518ADUJ&amp;origin=notification"><header id="T054518ADUJ" title="Pr
imeTech Innovations" activationType="protocol" arguments="slack://channel?team=T054518ADUJ"></header
><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">Cyberjun
kie-PrimeTechDev: Just to confirm as we dont want forela's IT team to get suspicious
Password for the archive server 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><au
dio silent="true"/></toast>|||133267195443436386|133264603443436386|0|Xml|133264592265000000|0
```

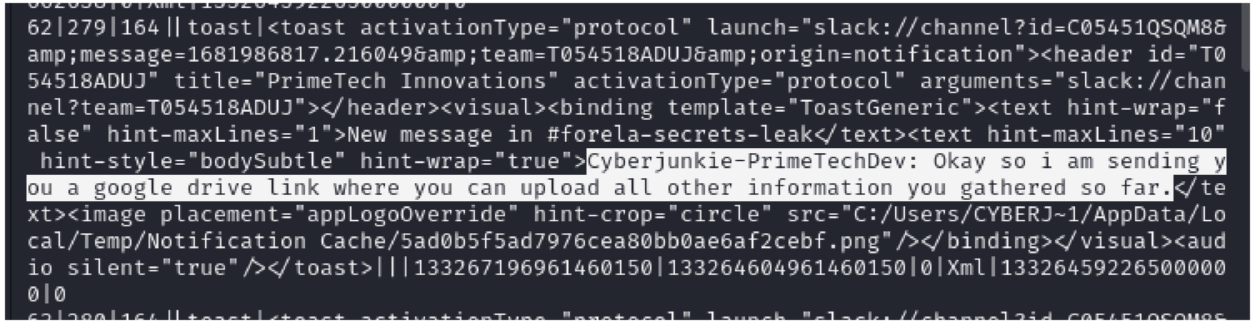


```
//channel?id=C05451QSQM8&amp;message=16
DUJ" title="PrimeTech Innovations" acti
l><binding template="ToastGeneric"><tex
```

- In the next entry, I saw the user asking to confirm.

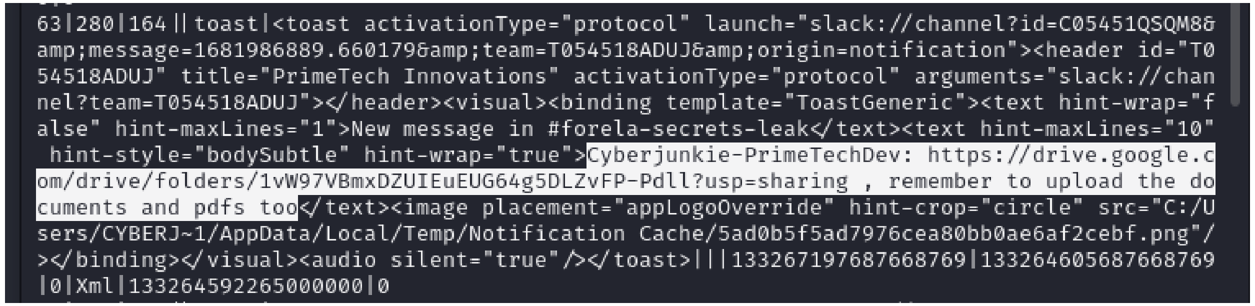


```
alse" hint-maxLines="1">New message in #forela-secrets-leak</text><text hint-maxLines="10"
 hint-style="bodySubtle" hint-wrap="true">Cyberjunkie-PrimeTechDev: Confirmation that pass
word is  "Tobdaf8Qip$re@1"</text><image placement="appLogoOverride" hint-crop="circle" src
="C:/Users/CYBERJ~1/AppData/Local/Temp/Notification Cache/5ad0b5f5ad7976cea80bb0ae6af2cebf
```



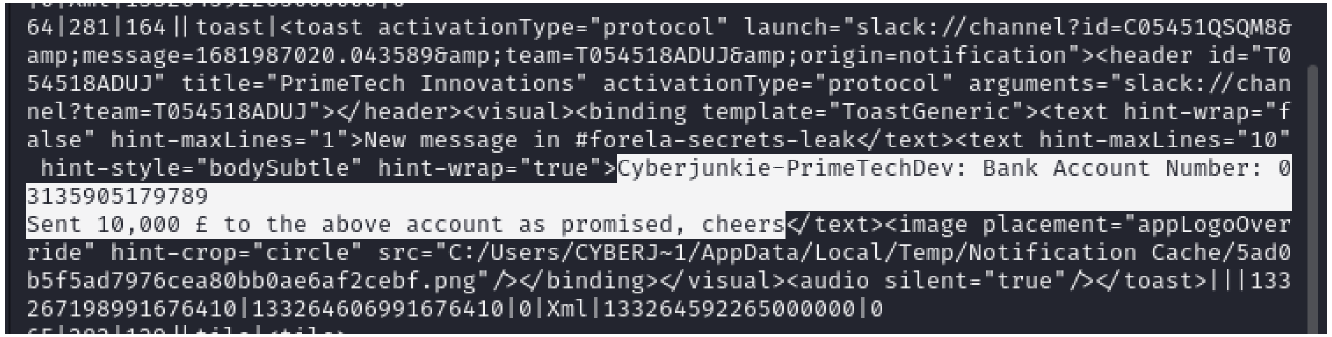
```
62|279|164||toast|<toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&
amp;message=1681986817.216049&amp;team=T054518ADUJ&amp;origin=notification"><header id="T0
54518ADUJ" title="PrimeTech Innovations" activationType="protocol" arguments="slack://chan
nel?team=T054518ADUJ"></header><visual><binding template="ToastGeneric"><text hint-wrap="f
alse" hint-maxLines="1">New message in #forela-secrets-leak</text><text hint-maxLines="10"
 hint-style="bodySubtle" hint-wrap="true">Cyberjunkie-PrimeTechDev: Okay so i am sending y
ou a google drive link where you can upload all other information you gathered so far.</te
xt><image placement="appLogoOverride" hint-crop="circle" src="C:/Users/CYBERJ~1/AppData/Lo
cal/Temp/Notification Cache/5ad0b5f5ad7976cea80bb0ae6af2cebf.png"/></binding></visual><aud
io silent="true"/></toast>|||133267196961460150|133264604961460150|0|Xml|13326459226500000
0|0
```

- Next, the user says that they’ll send a google drive link to upload all the evidence.
- The next entry has the actual google drive link (task 6) .



```
63|280|164||toast|<toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&
amp;message=1681986889.660179&amp;team=T054518ADUJ&amp;origin=notification"><header id="T0
54518ADUJ" title="PrimeTech Innovations" activationType="protocol" arguments="slack://chan
nel?team=T054518ADUJ"></header><visual><binding template="ToastGeneric"><text hint-wrap="f
alse" 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.c
om/drive/folders/1vW97VBmxDZUIEuEUG64g5DLZvFP-Pdll?usp=sharing , remember to upload the do
cuments and pdfs too</text><image placement="appLogoOverride" hint-crop="circle" src="C:/U
sers/CYBERJ~1/AppData/Local/Temp/Notification Cache/5ad0b5f5ad7976cea80bb0ae6af2cebf.png"/
></binding></visual><audio silent="true"/></toast>|||133267197687668769|133264605687668769
|0|Xml|133264592265000000|0
```

- Lastly we can see that the user sent 'torrin' 10000 pounds for leaking them the information (task 8.).



```
64|281|164||toast|<toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&
amp;message=1681987020.043589&amp;team=T054518ADUJ&amp;origin=notification"><header id="T0
54518ADUJ" title="PrimeTech Innovations" activationType="protocol" arguments="slack://chan
nel?team=T054518ADUJ"></header><visual><binding template="ToastGeneric"><text hint-wrap="f
alse" 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: 0
3135905179789
Sent 10,000 £ to the above account as promised, cheers</text><image placement="appLogoOver
ride" hint-crop="circle" src="C:/Users/CYBERJ~1/AppData/Local/Temp/Notification Cache/5ad0
b5f5ad7976cea80bb0ae6af2cebf.png"/></binding></visual><audio silent="true"/></toast>|||133
267198991676410|133264606991676410|0|Xml|133264592265000000|0
```

Answers:

Task 1: Which software/application did Torrin use to leak Forela's secrets?

Answer 1: slack (page 3).

Task 2: What's the name of the rival company to which Torrin leaked the data?

Answer 2: PrimeTech Innovations (page 4).

Task 3:What is the username of the person from the competitor organization whom Torrin shared information with?

Answer 3: Cyberjunkie-PrimeTechDev (page 3).

Task 4: What's the channel name in which they conversed with each other?

Answer 4: forela-secrets-leak (page 3).

Task 5: What was the password for the archive server?

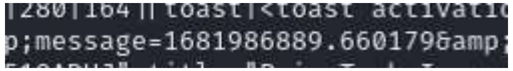
Answer 5: Tobdaf8Qip$re@1 (page 4).

Task 6: What was the URL provided to Torrin to upload stolen data to?

Answer 6 : https://drive.google.com/drive/folders/1vW97VBmxDZUIEuEUG64g5DLZvFP-Pdll?usp=sharing (page 4).

Task 7: When was the above link shared with Torrin?

Answer 7: when looking at the entry we can see a part that has a value that looks a lot like and epoch time value. After converting that value to UTC time we get: 2023-04-20 10:34:49



```
|280|164||toast|<toast activatio
p;message=1681986889.660179&amp;
```

Task 8: For how much money did Torrin leak Forela's secrets?

Answer 8: £10000 (page 5).

Jingle Bell has been Solved!

Congratulations chananshenker, best of luck in capturing flags ahead!