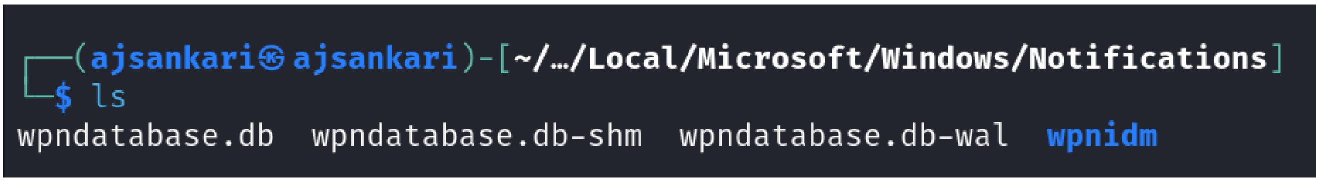
Sherlock - Jingle Bell

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.

FILES IN ZIP:

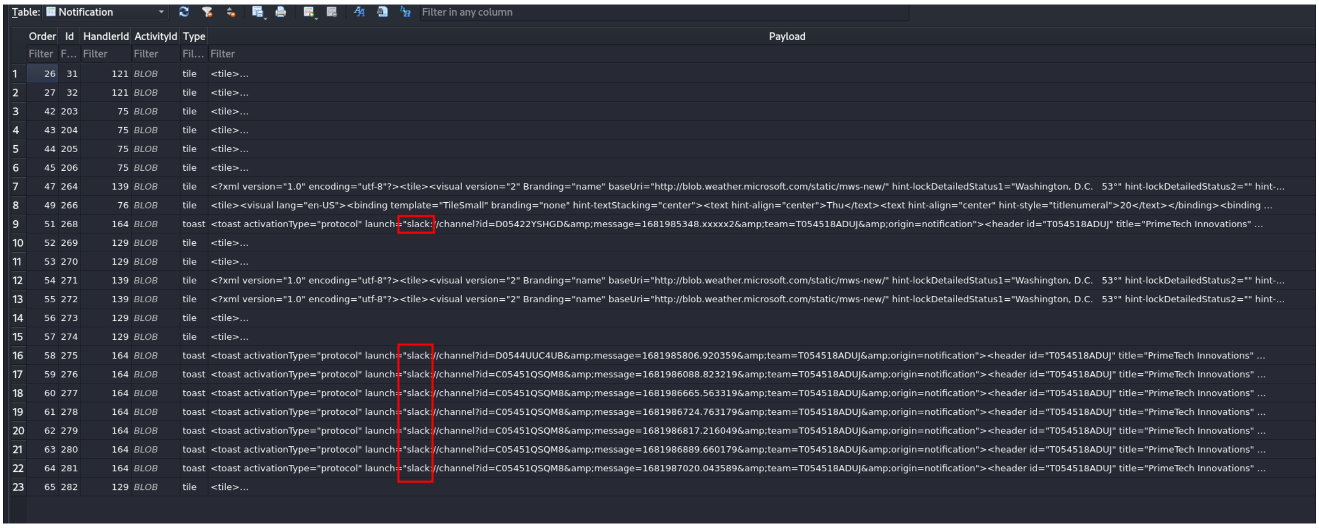


```
┌──(ajsankari㉿ajsankari)-[~/…/Local/Microsoft/Windows/Notifications]
└─$ ls
wpndatabase.db  wpndatabase.db-shm  wpndatabase.db-wal  wpnidm
```

- **wpndatabase.db**: This is the main SQLite database file that stores information about notifications in Windows. It holds data related to notifications that are shown in the Action Center.
- **wpndatabase.db-shm**: This is a shared memory file used by SQLite databases to handle multi-process access to the main database file (`wpndatabase.db`). It helps in improving the performance of the database.
- **wpndatabase.db-wal**: This is a write-ahead log file used by SQLite for transactional purposes. It temporarily stores changes to the database before they are committed to the main `wpndatabase.db` file, ensuring data integrity.

Q1 Which software/application did Torrin use to leak Forela's secrets?

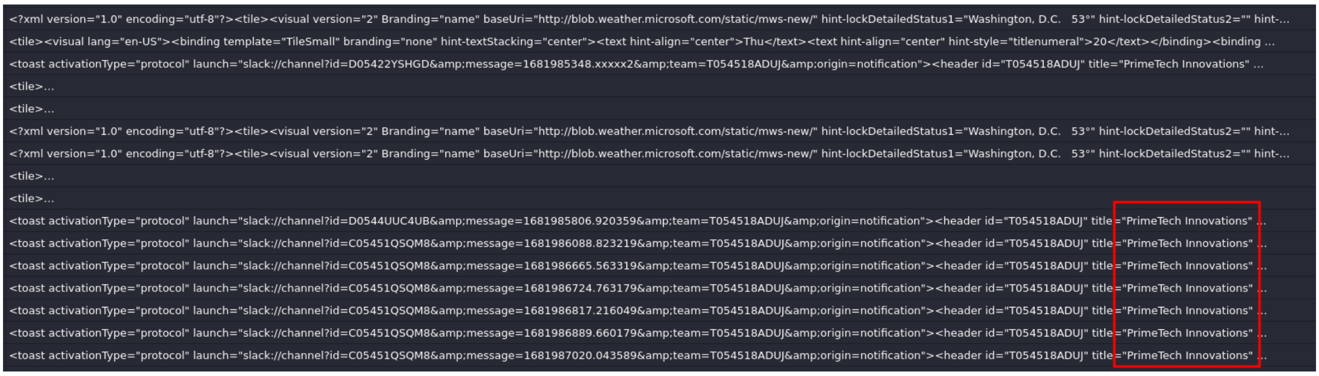
Looking at the database in **SQLITEBROWSER** under the table **NOTIFCATION** I see that Torrin used the application **SLACK** to leak the secrets.



	Order	Id	HandlerId	ActivityId	Type	Payload
	Filter	F...	Filter	Filter	Fil...	Filter
1	26	31	121	BLOB	tile	<tile>...
2	27	32	121	BLOB	tile	<tile>...
3	42	203	75	BLOB	tile	<tile>...
4	43	204	75	BLOB	tile	<tile>...
5	44	205	75	BLOB	tile	<tile>...
6	45	206	75	BLOB	tile	<tile>...
7	47	264	139	BLOB	tile	<?xml version="1.0" encoding="utf-8"?><tile><visual version="2" Branding="name" baseUri="http://blob.weather.microsoft.com/static/mws-new/" hint-lockDetailedStatus1="Washington, D.C. 53°" hint-lockDetailedStatus2="" hint-...
8	49	266	76	BLOB	tile	<tile><visual lang="en-US"><binding template="TileSmall" branding="none" hint-textStacking="center"><text hint-align="center">Thu</text><text hint-align="center" hint-style="titlenumeral">20</text></binding><binding ...
9	51	268	164	BLOB	toast	<toast activationType="protocol" launch="slack://channel?id=D05422YSHGD&amp;message=1681985348.xxxxx2&amp;team=T054518ADUJ&amp;origin=notification"><header id="T054518ADUJ" title="PrimeTech Innovations" ...
10	52	269	129	BLOB	tile	<tile>...
11	53	270	129	BLOB	tile	<tile>...
12	54	271	139	BLOB	tile	<?xml version="1.0" encoding="utf-8"?><tile><visual version="2" Branding="name" baseUri="http://blob.weather.microsoft.com/static/mws-new/" hint-lockDetailedStatus1="Washington, D.C. 53°" hint-lockDetailedStatus2="" hint-...
13	55	272	139	BLOB	tile	<?xml version="1.0" encoding="utf-8"?><tile><visual version="2" Branding="name" baseUri="http://blob.weather.microsoft.com/static/mws-new/" hint-lockDetailedStatus1="Washington, D.C. 53°" hint-lockDetailedStatus2="" hint-...
14	56	273	129	BLOB	tile	<tile>...
15	57	274	129	BLOB	tile	<tile>...
16	58	275	164	BLOB	toast	<toast activationType="protocol" launch="slack://channel?id=D0544UUC4UB&amp;message=1681985806.920359&amp;team=T054518ADUJ&amp;origin=notification"><header id="T054518ADUJ" title="PrimeTech Innovations" ...
17	59	276	164	BLOB	toast	<toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681986088.823219&amp;team=T054518ADUJ&amp;origin=notification"><header id="T054518ADUJ" title="PrimeTech Innovations" ...
18	60	277	164	BLOB	toast	<toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681986665.563319&amp;team=T054518ADUJ&amp;origin=notification"><header id="T054518ADUJ" title="PrimeTech Innovations" ...
19	61	278	164	BLOB	toast	<toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681986724.763179&amp;team=T054518ADUJ&amp;origin=notification"><header id="T054518ADUJ" title="PrimeTech Innovations" ...
20	62	279	164	BLOB	toast	<toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681986817.216049&amp;team=T054518ADUJ&amp;origin=notification"><header id="T054518ADUJ" title="PrimeTech Innovations" ...
21	63	280	164	BLOB	toast	<toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681986889.660179&amp;team=T054518ADUJ&amp;origin=notification"><header id="T054518ADUJ" title="PrimeTech Innovations" ...
22	64	281	164	BLOB	toast	<toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681987020.043589&amp;team=T054518ADUJ&amp;origin=notification"><header id="T054518ADUJ" title="PrimeTech Innovations" ...
23	65	282	129	BLOB	tile	<tile>...

Q2 What's the name of the rival company to which Torrin leaked the data?

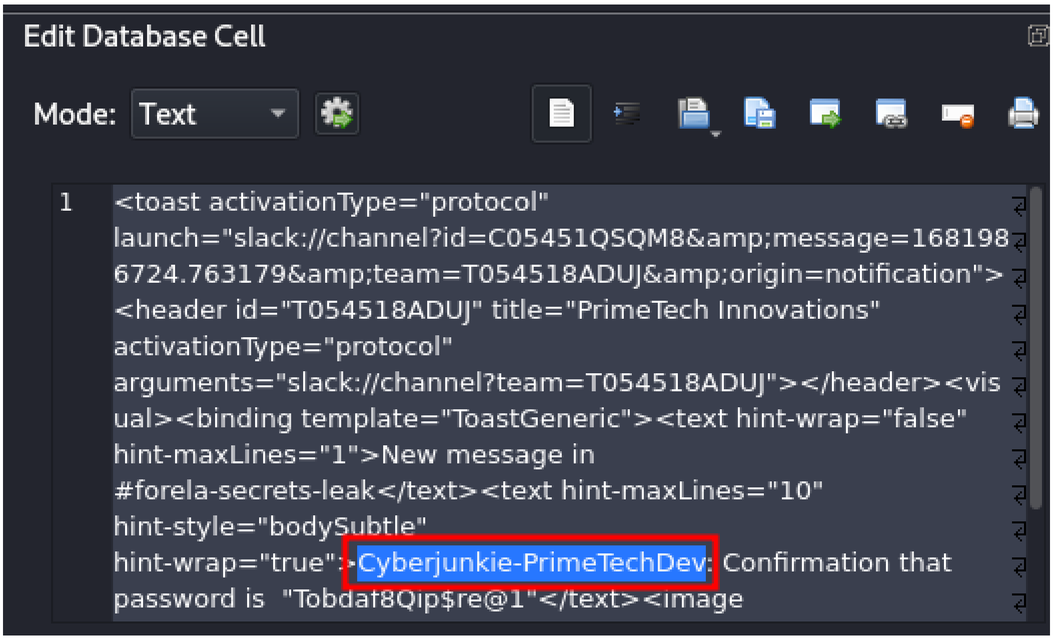
In the same table I can see the name of the company **PrimeTech Innovations**



```
<?xml version="1.0" encoding="utf-8"?><tile><visual version="2" Branding="name" baseUri="http://blob.weather.microsoft.com/static/mws-new/" hint-lockDetailedStatus1="Washington, D.C.   53°" hint-lockDetailedStatus2="" hint-...
<tile><visual lang="en-US"><binding template="TileSmall" branding="none" hint-textStacking="center"><text hint-align="center">Thu</text><text hint-align="center" hint-style="titlenumeral">20</text></binding><binding ...
<toast activationType="protocol" launch="slack://channel?id=D05422YSHGD&amp;message=1681985348.xxxxx2&amp;team=T054518ADUJ&amp;origin=notification"><header id="T054518ADUJ" title="PrimeTech Innovations" ...
<tile>...
<tile>...
<?xml version="1.0" encoding="utf-8"?><tile><visual version="2" Branding="name" baseUri="http://blob.weather.microsoft.com/static/mws-new/" hint-lockDetailedStatus1="Washington, D.C.   53°" hint-lockDetailedStatus2="" hint-...
<?xml version="1.0" encoding="utf-8"?><tile><visual version="2" Branding="name" baseUri="http://blob.weather.microsoft.com/static/mws-new/" hint-lockDetailedStatus1="Washington, D.C.   53°" hint-lockDetailedStatus2="" hint-...
<tile>...
<tile>...
<toast activationType="protocol" launch="slack://channel?id=D0544UUC4UB&amp;message=1681985806.920359&amp;team=T054518ADUJ&amp;origin=notification"><header id="T054518ADUJ" title="PrimeTech Innovations" ...
<toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681986088.823219&amp;team=T054518ADUJ&amp;origin=notification"><header id="T054518ADUJ" title="PrimeTech Innovations" ...
<toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681986665.563319&amp;team=T054518ADUJ&amp;origin=notification"><header id="T054518ADUJ" title="PrimeTech Innovations" ...
<toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681986724.763179&amp;team=T054518ADUJ&amp;origin=notification"><header id="T054518ADUJ" title="PrimeTech Innovations" ...
<toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681986817.216049&amp;team=T054518ADUJ&amp;origin=notification"><header id="T054518ADUJ" title="PrimeTech Innovations" ...
<toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681986889.660179&amp;team=T054518ADUJ&amp;origin=notification"><header id="T054518ADUJ" title="PrimeTech Innovations" ...
<toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681987020.043589&amp;team=T054518ADUJ&amp;origin=notification"><header id="T054518ADUJ" title="PrimeTech Innovations" ...
```

Q3 What is the username of the person from the competitor organization whom Torrin shared information with?

Looking at the DB Cell I find the username **Cyberjunkie-PrimeTechDev**



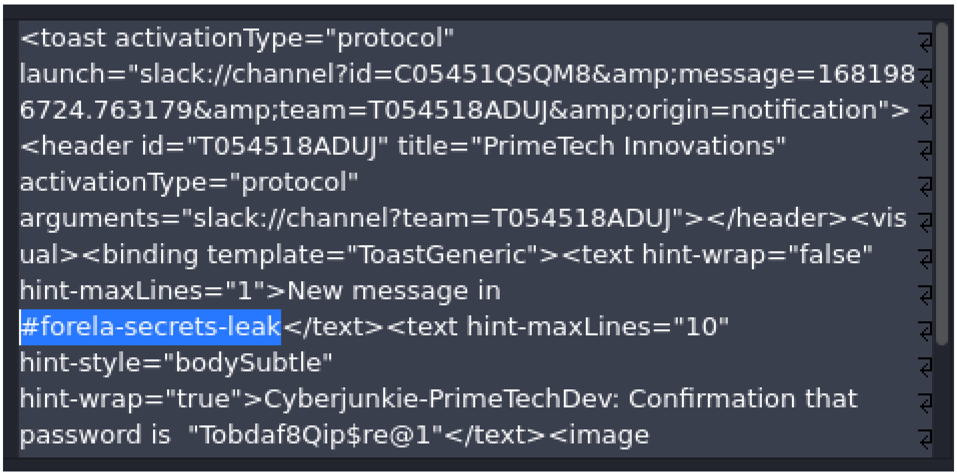
Edit Database Cell

Mode: Text

```
<toast activationType="protocol"
launch="slack://channel?id=C05451QSQM8&amp;message=168198
6724.763179&amp;team=T054518ADUJ&amp;origin=notification">
<header id="T054518ADUJ" title="PrimeTech Innovations"
activationType="protocol"
arguments="slack://channel?team=T054518ADUJ"></header><vis
ual><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
```

Q4 What's the channel name in which they conversed with each other?

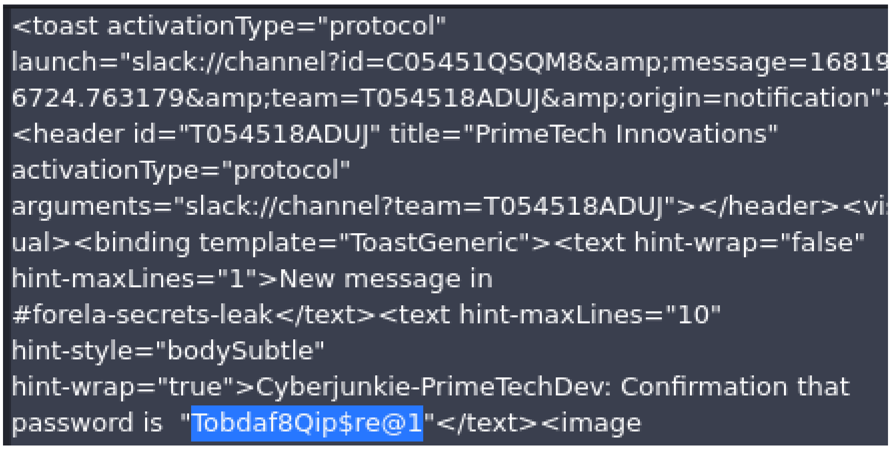
In the same cell I can see the channel name is **forela-secrets-leak**



```
<toast activationType="protocol"
launch="slack://channel?id=C05451QSQM8&amp;message=168198
6724.763179&amp;team=T054518ADUJ&amp;origin=notification">
<header id="T054518ADUJ" title="PrimeTech Innovations"
activationType="protocol"
arguments="slack://channel?team=T054518ADUJ"></header><vis
ual><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
```

Q5 What was the password for the archive server?

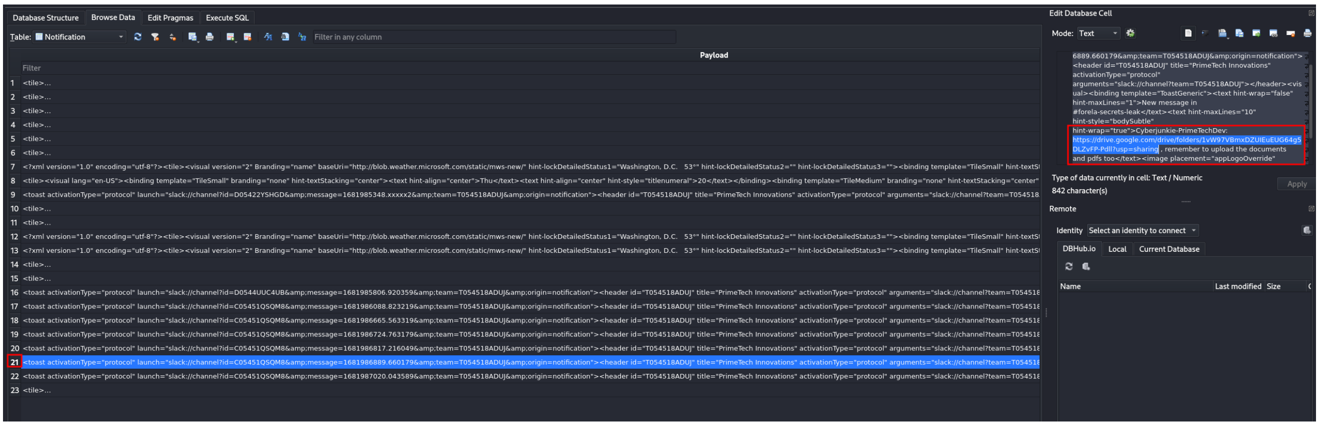
The user's password is **Tobdaf8Qip$re@1** as seen below:



```
<toast activationType="protocol"
launch="slack://channel?id=C05451QSQM8&amp;message=16819
6724.763179&amp;team=T054518ADUJ&amp;origin=notification">
<header id="T054518ADUJ" title="PrimeTech Innovations"
activationType="protocol"
arguments="slack://channel?team=T054518ADUJ"></header><vi
ual><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
```

Q6 What was the URL provided to Torrin to upload stolen data to?

In the 21st cell I can see the Cyberjunkie-PrimeTechDev says to upload to documents to the following link - https://drive.google.com/drive/folders/1vW97VBmxDZUIEuEUG64g5DLZvFP-Pdll?usp=sharing



```
1  <tile>...
2  <tile>...
3  <tile>...
4  <tile>...
5  <tile>...
6  <tile>...
7  <?xml version="1.0" encoding="utf-8"?><tile><visual version="2" Branding="name" baseUri="http://blob.weather.microsoft.com/static/mws-new/" hint-lockDetailedStatus1="Washington, D.C.   53°" hint-lockDetailedStatus2="" hint-lockDetailedStatus3=""><binding template="TileSmall" hint-textSt
8  <tile><visual lang="en-US"><binding template="TileSmall" branding="none" hint-textStacking="center"><text hint-align="center">Thu</text><text hint-align="center" hint-style="titlenumeral">20</text></binding><binding template="TileMedium" branding="none" hint-textStacking="center"
9  <toast activationType="protocol" launch="slack://channel?id=D05422YSHGD&amp;message=1681985348.xxxxx2&amp;team=T054518ADUJ&amp;origin=notification"><header id="T054518ADUJ" title="PrimeTech Innovations" activationType="protocol" arguments="slack://channel?team=T054518
10 <tile>...
11 <tile>...
12 <?xml version="1.0" encoding="utf-8"?><tile><visual version="2" Branding="name" baseUri="http://blob.weather.microsoft.com/static/mws-new/" hint-lockDetailedStatus1="Washington, D.C.   53°" hint-lockDetailedStatus2="" hint-lockDetailedStatus3=""><binding template="TileSmall" hint-textSt
13 <?xml version="1.0" encoding="utf-8"?><tile><visual version="2" Branding="name" baseUri="http://blob.weather.microsoft.com/static/mws-new/" hint-lockDetailedStatus1="Washington, D.C.   53°" hint-lockDetailedStatus2="" hint-lockDetailedStatus3=""><binding template="TileSmall" hint-textSt
14 <tile>...
15 <tile>...
16 <toast activationType="protocol" launch="slack://channel?id=D0544UUC4UB&amp;message=1681985806.920359&amp;team=T054518ADUJ&amp;origin=notification"><header id="T054518ADUJ" title="PrimeTech Innovations" activationType="protocol" arguments="slack://channel?team=T054518
17 <toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681986088.823219&amp;team=T054518ADUJ&amp;origin=notification"><header id="T054518ADUJ" title="PrimeTech Innovations" activationType="protocol" arguments="slack://channel?team=T054518
18 <toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681986665.563319&amp;team=T054518ADUJ&amp;origin=notification"><header id="T054518ADUJ" title="PrimeTech Innovations" activationType="protocol" arguments="slack://channel?team=T054518
19 <toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681986724.763179&amp;team=T054518ADUJ&amp;origin=notification"><header id="T054518ADUJ" title="PrimeTech Innovations" activationType="protocol" arguments="slack://channel?team=T054518
20 <toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681986817.216049&amp;team=T054518ADUJ&amp;origin=notification"><header id="T054518ADUJ" title="PrimeTech Innovations" activationType="protocol" arguments="slack://channel?team=T054518
21 <toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681986889.660179&amp;team=T054518ADUJ&amp;origin=notification"><header id="T054518ADUJ" title="PrimeTech Innovations" activationType="protocol" arguments="slack://channel?team=T054518
22 <toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681987020.043589&amp;team=T054518ADUJ&amp;origin=notification"><header id="T054518ADUJ" title="PrimeTech Innovations" activationType="protocol" arguments="slack://channel?team=T054518
23 <tile>...
```

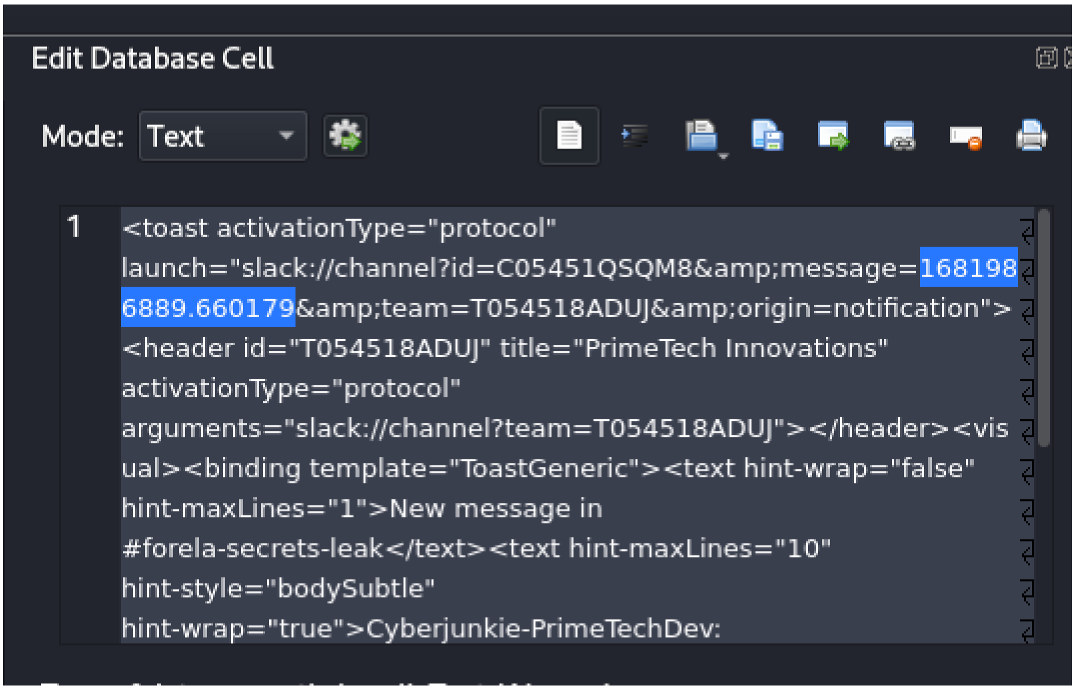
```
6889.660179&amp;team=T054518ADUJ&amp;origin=notification">
<header id="T054518ADUJ" title="PrimeTech Innovations"
activationType="protocol"
arguments="slack://channel?team=T054518ADUJ"></header><vis
ual><binding template="ToastGeneric"><text hint-wrap="false"
hint-maxLines="1">New message in
#forela-secrets-leak</text><text hint-maxLines="10"
hint-style="bodySubtle"
hint-wrap="true">Cyberjunkie-PrimeTechDev:
https://drive.google.com/drive/folders/1vW97VBmxDZUIEuEUG64g5
DLZvFP-Pdll?usp=sharing , remember to upload the documents
and pdfs too</text><image placement="appLogoOverride"
```

Type of data currently in cell: Text / Numeric
842 character(s)

Q7 When was the above link shared with Torrin?

In the following cell we can see that the '**message**' parameter includes a value `1681986889.660179`.

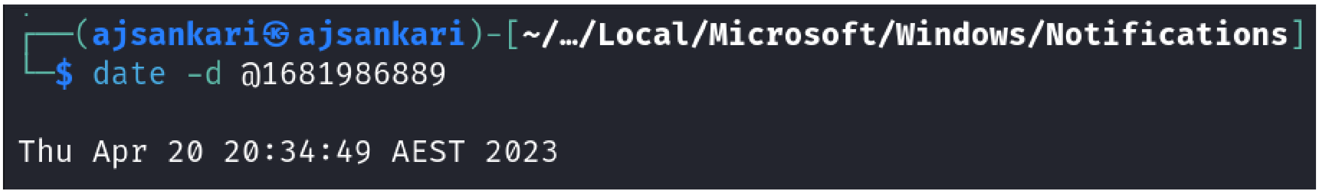
This value is in Unix epoch time format, which represents the number of seconds since January 1, 1970 (UTC).



```
1   <toast activationType="protocol"
    launch="slack://channel?id=C05451QSQM8&amp;message=168198
    6889.660179&amp;team=T054518ADUJ&amp;origin=notification">
    <header id="T054518ADUJ" title="PrimeTech Innovations"
    activationType="protocol"
    arguments="slack://channel?team=T054518ADUJ"></header><vis
    ual><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:
```

To convert `1681986889.660179` to a human-readable date and time I can use the **date** command

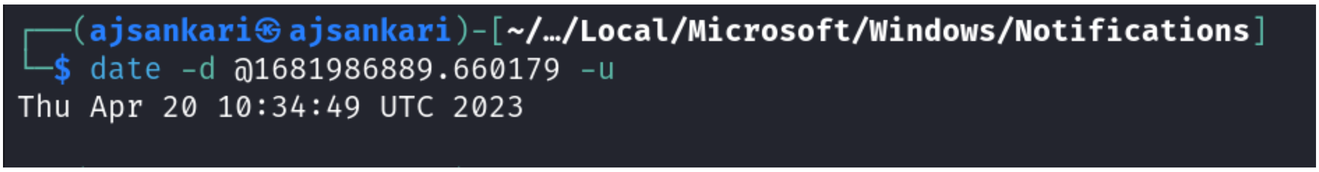
Using **date -d 1681986889** gives me the following results:



```
┌──(ajsankari㉿ajsankari)-[~/…/Local/Microsoft/Windows/Notifications]
└─$ date -d @1681986889

Thu Apr 20 20:34:49 AEST 2023
```

Since I know the box is in UTC time format, I can run the same command again but use **-u** to get the date in UTC.



```
┌──(ajsankari㉿ajsankari)-[~/…/Local/Microsoft/Windows/Notifications]
└─$ date -d @1681986889.660179 -u
Thu Apr 20 10:34:49 UTC 2023
```

2023-04-20 10:34:49

Q8 For how much money did Torrin leak Forela's secrets?

In the DB Cell 22 I can see that Torrin leaked the secrets for **10,000 £**

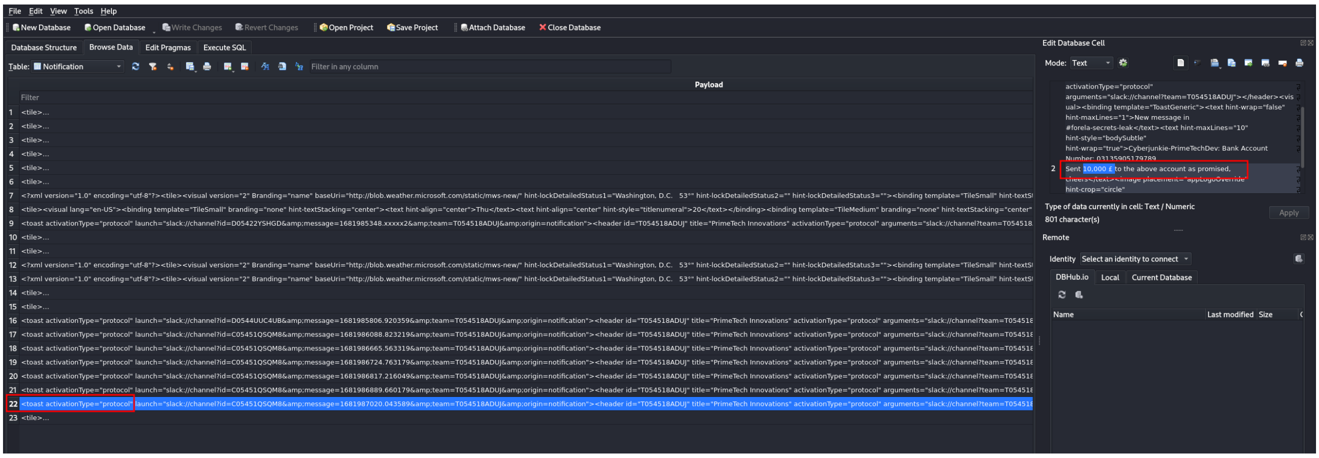


Table: Notification

```
Payload
1  <tile>...
2  <tile>...
3  <tile>...
4  <tile>...
5  <tile>...
6  <tile>...
7  <?xml version="1.0" encoding="utf-8"?><tile><visual version="2" Branding="name" baseUri="http://blob.weather.microsoft.com/static/mws-new/" hint-lockDetailedStatus1="Washington, D.C.   53°" hint-lockDetailedStatus2="" hint-lockDetailedStatus3=""><binding template="TileSmall" hint-textSt
8  <tile><visual lang="en-US"><binding template="TileSmall" branding="none" hint-textStacking="center"><text hint-align="center">Thu</text><text hint-align="center" hint-style="titlenumeral">20</text></binding><binding template="TileMedium" branding="none" hint-textStacking="center"
9  <toast activationType="protocol" launch="slack://channel?id=D05422YSHGD&amp;message=1681985348.xxxxx2&amp;team=T054518ADUJ&amp;origin=notification"><header id="T054518ADUJ" title="PrimeTech Innovations" activationType="protocol" arguments="slack://channel?team=T054518.
10 <tile>...
11 <tile>...
12 <?xml version="1.0" encoding="utf-8"?><tile><visual version="2" Branding="name" baseUri="http://blob.weather.microsoft.com/static/mws-new/" hint-lockDetailedStatus1="Washington, D.C.   53°" hint-lockDetailedStatus2="" hint-lockDetailedStatus3=""><binding template="TileSmall" hint-textSt
13 <?xml version="1.0" encoding="utf-8"?><tile><visual version="2" Branding="name" baseUri="http://blob.weather.microsoft.com/static/mws-new/" hint-lockDetailedStatus1="Washington, D.C.   53°" hint-lockDetailedStatus2="" hint-lockDetailedStatus3=""><binding template="TileSmall" hint-textSt
14 <tile>...
15 <tile>...
16 <toast activationType="protocol" launch="slack://channel?id=D0544UUC4UB&amp;message=1681985806.920359&amp;team=T054518ADUJ&amp;origin=notification"><header id="T054518ADUJ" title="PrimeTech Innovations" activationType="protocol" arguments="slack://channel?team=T054518
17 <toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681986088.823219&amp;team=T054518ADUJ&amp;origin=notification"><header id="T054518ADUJ" title="PrimeTech Innovations" activationType="protocol" arguments="slack://channel?team=T054518
18 <toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681986665.563319&amp;team=T054518ADUJ&amp;origin=notification"><header id="T054518ADUJ" title="PrimeTech Innovations" activationType="protocol" arguments="slack://channel?team=T054518
19 <toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681986724.763179&amp;team=T054518ADUJ&amp;origin=notification"><header id="T054518ADUJ" title="PrimeTech Innovations" activationType="protocol" arguments="slack://channel?team=T054518
20 <toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681986817.216049&amp;team=T054518ADUJ&amp;origin=notification"><header id="T054518ADUJ" title="PrimeTech Innovations" activationType="protocol" arguments="slack://channel?team=T054518
21 <toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681986889.660179&amp;team=T054518ADUJ&amp;origin=notification"><header id="T054518ADUJ" title="PrimeTech Innovations" activationType="protocol" arguments="slack://channel?team=T054518
22 <toast activationType="protocol" launch="slack://channel?id=C05451QSQM8&amp;message=1681987020.043589&amp;team=T054518ADUJ&amp;origin=notification"><header id="T054518ADUJ" title="PrimeTech Innovations" activationType="protocol" arguments="slack://channel?team=T054518
23 <tile>...
```

```
activationType="protocol"
arguments="slack://channel?team=T054518ADUJ"></header><vis
ual><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"
```

Type of data currently in cell: Text / Numeric
801 character(s)

SUMMARY

Here are the key findings from the HTB Sherlock writeup:

- **Software Used for Data Leak**: Torrin used **SLACK** to leak Forela's secrets.
- **Rival Company**: The data was leaked to **PrimeTech Innovations**.
- **Competitor's Username**: The username of the person at PrimeTech Innovations was **Cyberjunkie-PrimeTechDev**.
- **Conversation Channel**: The conversation took place in the **forela-secrets-leak** channel.
- **Password for Archive Server**: The password for the archive server was **Tobdaf8Qip$re@1**.
- **Upload URL**: Torrin was provided with the URL https://drive.google.com/drive/folders/1vW97VBmxDZUIEuEUG64g5DLZvFP-PdlI?usp=sharing to upload the stolen data.
- **Timestamp of URL Sharing**: The URL was shared with Torrin on **2023-04-20 10:34:49 UTC**.
- **Compensation**: Torrin leaked the secrets for **£10,000**.