TASK:

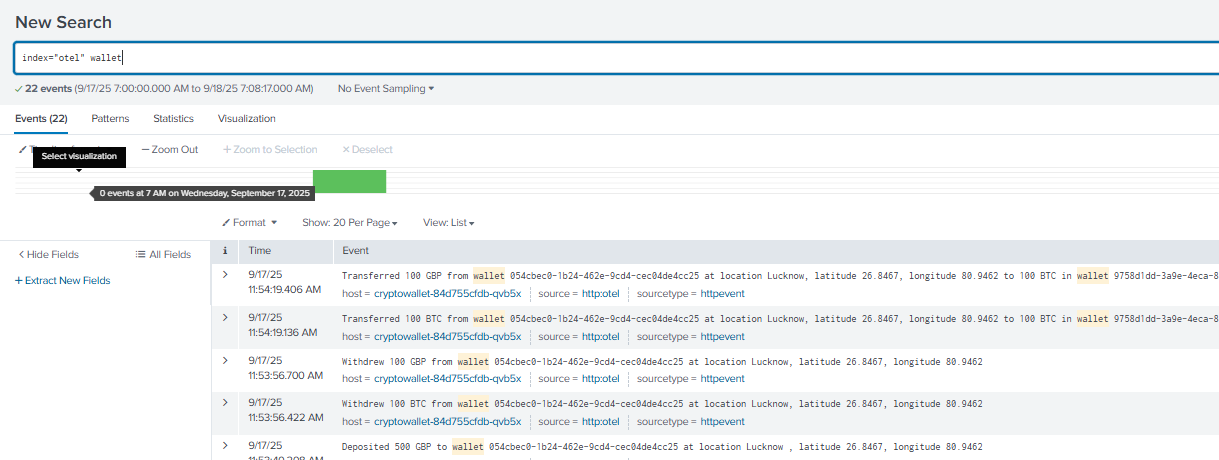
 Log data from Otel are sending to Splunk, please check for last 24hrs with **index="otel"** and **analyse the log and work on the dashboards**.

[Wallet Manager](https://cryptowallet.sflabs.ustpace.com/) - Crypto wallet web app to generate the logs.  
  
  
Actually we need to do: **analyse the log and work on the dashboards**TASK: Create dashboard of crypto wallet dashboard.

SOLUTION:

1. To see all events of wallet:

index="otel" wallet



22 events listed.

**SPL: It shows the details of deposit:**

index="otel" wallet earliest=-24h latest=now | search "Deposited" | rex "Deposited\s+(?<amount>\d+)\s+(?<currency>\w+)\s+to wallet\s+(?<wallet\_id>[a-z0-9-]+)" | rex "at location\s+(?<location>[^,]+),\s\*latitude\s+(?<lat>[\d\.]+),\s\*longitude\s+(?<lon>[\d\.]+)" | table \_time wallet\_id amount currency location lat lon | sort -\_time

**SPL: It shows the details of Transfer:**

index="otel" wallet earliest=-24h latest=now

| search "Transferred"

| rex "Transferred\s+(?<amount\_from>\d+)\s+(?<currency\_from>\w+)\s+from wallet\s+(?<wallet\_from>[a-z0-9-]+).\*to\s+(?<amount\_to>\d+)\s+(?<currency\_to>\w+)\s+in wallet\s+(?<wallet\_to>[a-z0-9-]+)"

| rex "from wallet\s+[a-z0-9-]+\s+at location\s+(?<location\_from>[^,]+),\s\*latitude\s+(?<lat\_from>[\d\.]+),\s\*longitude\s+(?<lon\_from>[\d\.]+)"

| rex "in wallet\s+[a-z0-9-]+\s+at location\s+(?<location\_to>[^,]+),\s\*latitude\s+(?<lat\_to>[\d\.]+),\s\*longitude\s+(?<lon\_to>[\d\.]+)"

| table \_time wallet\_from wallet\_to amount\_from currency\_from amount\_to currency\_to location\_from lat\_from lon\_from location\_to lat\_to lon\_to

| sort -\_time

**SPL: it shows the details of Withdrawel:**

index="otel" wallet earliest=-24h latest=now | search "Withdrew" | rex "Withdrew\s+(?<amount>\d+)\s+(?<currency>\w+)\s+from wallet\s+(?<wallet\_id>[a-z0-9-]+)" | rex "at location\s+(?<location>[^,]+),\s\*latitude\s+(?<lat>[\d\.]+),\s\*longitude\s+(?<lon>[\d\.]+)" | table \_time wallet\_id amount currency location lat lon | sort -\_time

**IMP:**

Lost all data so changed the time range of every panels to yesterday and also removed this from every querry.

* ( earliest=-24h latest=now) = remove this

**PANELS CREATION:**

1. Panel 1: Total events(stat)

Spl:

index=otel host="cryptowallet-84d755cfdb-qvb5x" earliest=-24h latest=now

| stats count AS "Total Events"

Drilldown:  
details = events

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

1. Panel 2: Total wallet created(stat)

Spl:

index="otel" earliest=-24h latest=now "Created wallet"

| stats count as "Total Wallets Created"

Drilldown:

details = wallets\_created

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

1. Panel 3: Total wallet deleted(stat)

Spl:

index=otel host="cryptowallet-84d755cfdb-qvb5x" earliest=-24h latest=now "Deleted wallet" | stats count as "Total Wallets Deleted"

drilldown:  
details= wallets\_deleted  
A screenshot of a computer

AI-generated content may be incorrect.

1. Panel 4: Total errors (wallet not found)(stat)

Spl:

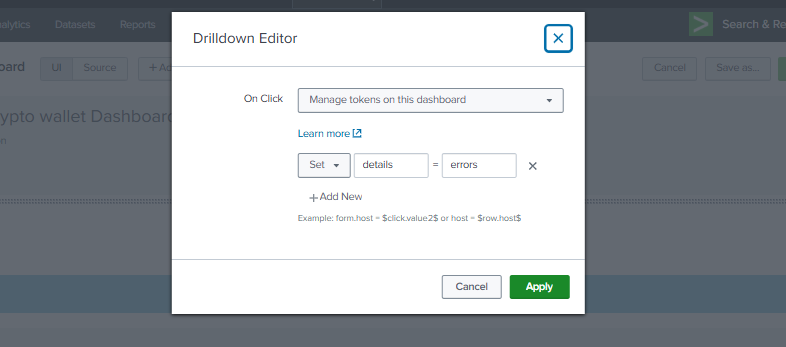
index="otel" wallet earliest=-24h latest=now

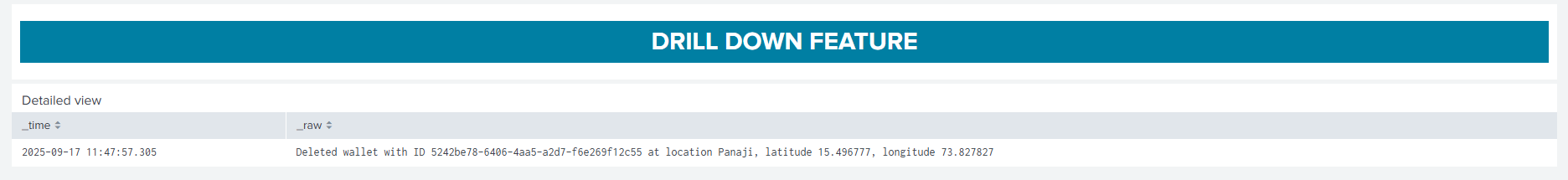
| rex "Wallet with ID (?<wallet\_id>[a-z0-9-]+) not found"

| where isnotnull(wallet\_id)

| stats count as total\_wallet\_errors

Drilldown:

details=error  




1. Panel 5: error %

Spl:

index=otel host="cryptowallet-84d755cfdb-qvb5x" earliest=-24h latest=now

| eval is\_error=if(like(\_raw,"%not found%"),1,0)

| stats count as total\_events sum(is\_error) as total\_errors

| eval error\_percentage = round((total\_errors/total\_events)\*100,2)

| fields error\_percentage

Drilldown:

details=error

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

1. Panel 6: failed Operations

Spl:

index=otel host="cryptowallet-84d755cfdb-qvb5x" earliest=-24h latest=now "not found"

| stats count AS "Failed Operations"

Drilldown:

details=error

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

1. Panel 7: Total no of deposits

Spl:

index="otel" wallet earliest=-24h latest=now

| where like(\_raw, "Deposited%")

| stats count as total\_deposits

Drilldown:

details=deposits

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

1. Panel 8: Total number of withdrawals

Spl:

index="otel" wallet earliest=-24h latest=now

| where like(\_raw, "Withdrew%")

| stats count as total\_withdrawals

Drilldown:

details= withdrawals

A screenshot of a computer

AI-generated content may be incorrect.

A screen shot of a computer

AI-generated content may be incorrect.

1. Panel 9: Total number of Transfers

Spl:

index="otel" wallet earliest=-24h latest=now

| where like(\_raw, "Transferred%")

| stats count as total\_transfers

Drilldown:

details= transfers

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

1. Panel 10: Total number of Transactions

Spl:

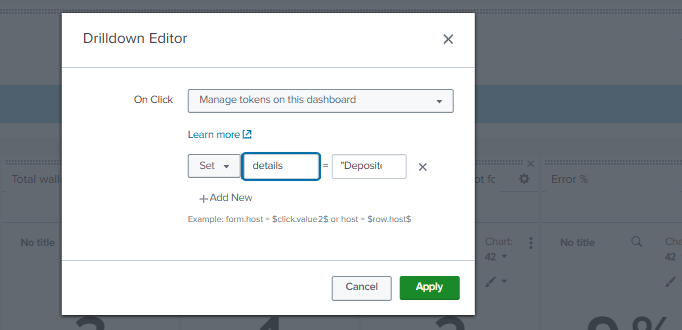
index="otel" wallet earliest=-24h latest=now

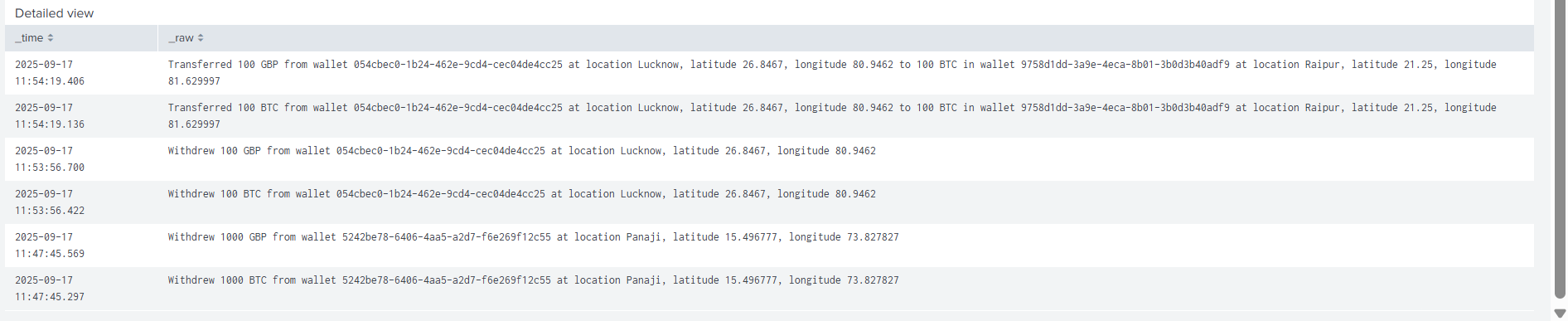
| eval is\_transaction=if(like(\_raw,"Deposited%") OR like(\_raw,"Withdrew%") OR like(\_raw,"Transferred%"), 1, 0)

| stats sum(is\_transaction) as total\_transactions

Drilldown:

details= "Deposited" OR "Withdrew" OR "Transferred"





1. Panel 11: Transaction by Location and type (Choropleth Map)

Spl:

index="otel" wallet earliest=-24h latest=now

| rex "at location\s+(?<location>[^,]+),\s\*latitude\s+(?<lat>[\d\.]+),\s\*longitude\s+(?<lon>[\d\.]+)"

| eval type=case(

match(\_raw,"Deposited"),"Deposit",

match(\_raw,"Withdrew"),"Withdrawal",

match(\_raw,"Transferred"),"Transfer"

)

| stats count by location lat lon type

1. Panel 12: Number of transaction per currency(column chart)

Spl:

index="otel" wallet earliest=-24h latest=now

| eval type=case(

match(\_raw,"Deposited"),"Deposit",

match(\_raw,"Withdrew"),"Withdrawal",

match(\_raw,"Transferred"),"Transfer"

)

| rex field=\_raw "Deposited\s+\d+\s+(?<deposit\_currency>\w+)"

| rex field=\_raw "Withdrew\s+\d+\s+(?<withdraw\_currency>\w+)"

| rex field=\_raw "Transferred\s+\d+\s+(?<transfer\_currency\_from>\w+).\*to\s+\d+\s+(?<transfer\_currency\_to>\w+)"

| eval currency=coalesce(deposit\_currency, withdraw\_currency, transfer\_currency\_from)

| stats count as transactions by currency

| sort -transactions

1. Panel 13: Deposit per currency (column chart)

Spl:

index="otel" wallet earliest=-24h latest=now

| where like(\_raw, "Deposited%")

| eval currency=mvindex(split(\_raw," "),2)

| stats count as deposits by currency

1. Panel 14: withdrawal per currency(column chart)

Spl:

index="otel" wallet earliest=-24h latest=now

| where like(\_raw, "Withdrew%")

| eval currency=mvindex(split(\_raw," "),2)

| stats count as withdrawals by currency

1. Panel 15: Outgoing transfer per currency (column chart)

Spl:

index="otel" wallet earliest=-24h latest=now

| where like(\_raw, "Transferred%")

| eval currency=mvindex(split(\_raw," "),2)

| stats count as outgoing\_transfers by currency

1. Panel 16: Number of deposit per wallet (column chart)

Spl:

index="otel" wallet earliest=-24h latest=now

| where like(\_raw, "Deposited%")

| eval wallet\_id=mvindex(split(\_raw," "),6)

| stats count as deposits by wallet\_id

| sort -deposits

1. Panel 17: number of withdrawels per wallet

Spl:

index="otel" wallet earliest=-24h latest=now

| where like(\_raw, "Withdrew%")

| eval wallet\_id=mvindex(split(\_raw," "),6)

| stats count as withdrawals by wallet\_id

| sort -withdrawals

1. Panel 18: number of transfers per wallet

Spl:

index="otel" wallet earliest=-24h latest=now

| where like(\_raw, "Transferred%")

| eval wallet\_from=mvindex(split(\_raw," "),6)

| eval wallet\_to=mvindex(split(\_raw," "),13)

| stats count as transfers by wallet\_from

| sort -transfers

1. Table 19: Detailed view (table)->DRILLDOWN

Spl:

index=otel host="cryptowallet-84d755cfdb-qvb5x" earliest=-24h latest=now

| eval category=case(

match(\_raw,"Created wallet"),"wallets\_created",

match(\_raw,"Deleted wallet"),"wallets\_deleted",

match(\_raw,"Deposited"),"deposits",

match(\_raw,"Withdrew"),"withdrawals",

match(\_raw,"Transferred"),"transfers",

like(\_raw,"%not found%"),"errors",

true(),"events")

| search category=$details$

| table \_time \_raw

**TITLE:**

1. CRYPTO WALLET DASHBOARD

<row>

<panel>

<html>

<h1 style="text-align: center; color: black; background-color:#94D2EC; padding: 15px; font-size: 30px;">CRYPTO WALLET DASHBOARD</h1>

</html>

</panel>

</row>

1. DRILL DOWN FEATURE

<row>

<panel>

<html>

<h1 style="text-align: center; color: white; background-color: #007FA3; padding: 15px; font-size: 30px;"> DRILL DOWN FEATURE</h1>

</html>

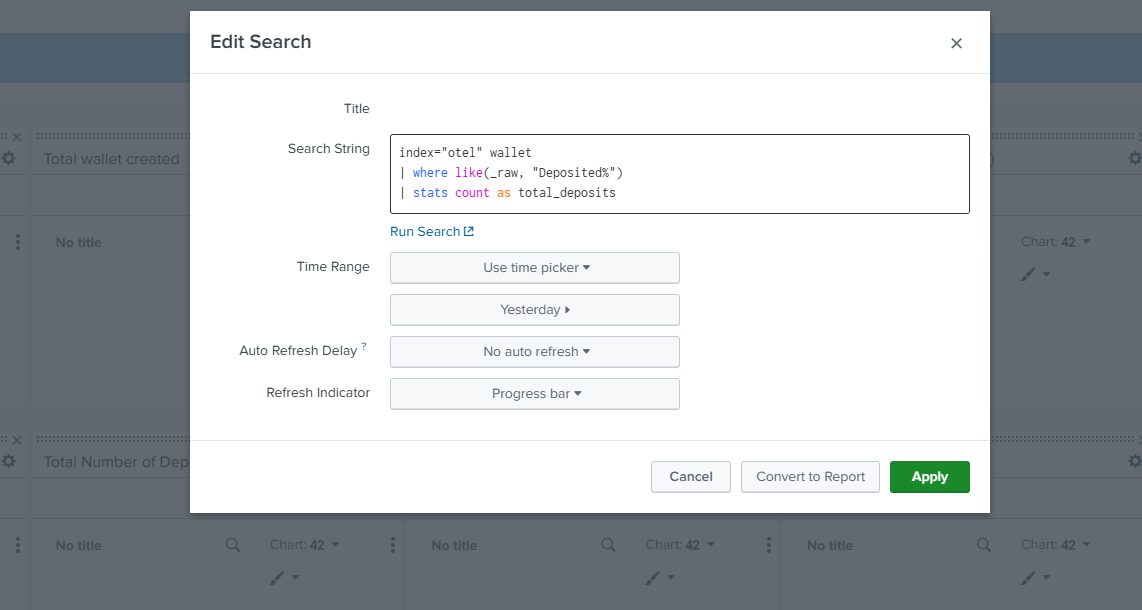
</panel>

</row>

PROBLEM: NO DATA

1. Removed the latest and 24 hr from all the querries and changed to yesterday.( earliest=-24h latest=now)

Eg:



DASHBOARD:

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

ALERT:

Don’t forget to keep time range as yesterday.

Spl:   
index=otel host="cryptowallet-84d755cfdb-qvb5x" "not found"

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A close-up of a computer screen

AI-generated content may be incorrect.