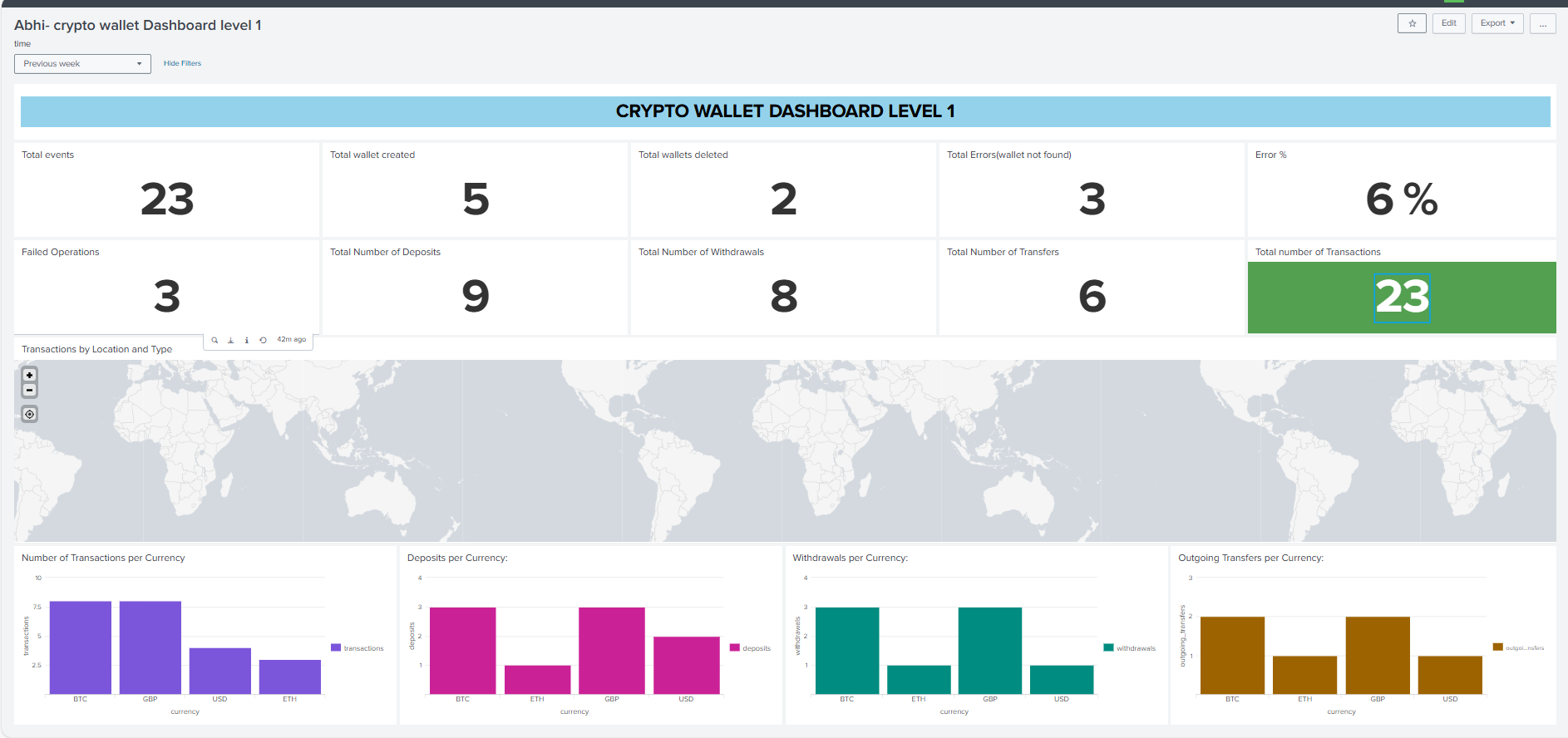
Dashboard: Crypto wallet dashboard

**Level 1:**



1. Panel 1: Total events

index=otel host=cryptowallet-\*

| stats count AS "Total Events"

1. Panel 2: Total wallet created

index=otel "Created wallet"

| stats count as "Total Wallets Created"

1. Panel 3: Total wallets deleted

index=otel "Deleted wallet" | stats count as "Total Wallets Deleted"

1. Panel 4: Total Errors(wallet not found)

index=otel host=cryptowallet-\* "not found"

| stats count as "Total Errors"

1. Panel 5: Error %

index=otel host=cryptowallet-\* | 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

1. Panel 6: Failed Operations

index=otel host=cryptowallet-\* "not found"

| stats count AS "Failed Operations"

1. Panel 7: Total Number of Deposits

index="otel" wallet

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

| stats count as total\_deposits

1. Panel 8: Total Number of Withdrawals

index="otel" wallet

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

| stats count as total\_withdrawals

1. Panel 9: Total Number of Transfers

index="otel" wallet

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

| stats count as total\_transfers

1. Panel 10: Total number of Transactions

index="otel" wallet

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

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

1. Panel 11: Transactions by Location and Type:

index=otel "wallet"

| rex field=\_raw "Transferred\s+(?<amount>\d+)\s+(?<currency>[A-Z]{3})\s+from wallet\s+(?<from\_wallet>[0-9a-f-]+)\s+at location\s+(?<from\_location>[^,]+),\s+latitude\s+(?<from\_lat>[-\d\.]+),\s+longitude\s+(?<from\_lon>[-\d\.]+)\s+to\s+(?<to\_amount>\d+)\s+(?<to\_currency>[A-Z]{3})\s+in wallet\s+(?<to\_wallet>[0-9a-f-]+)\s+at location\s+(?<to\_location>[^,]+),\s+latitude\s+(?<to\_lat>[-\d\.]+),\s+longitude\s+(?<to\_lon>[-\d\.]+)"

| eval amount=tonumber(amount), to\_amount=tonumber(to\_amount)

| eval from\_lat=tonumber(from\_lat), from\_lon=tonumber(from\_lon), to\_lat=tonumber(to\_lat), to\_lon=tonumber(to\_lon)

| geostats latfield=from\_lat longfield=from\_lon count by currency

1. Panel 12: Number of Transactions per Currency

index="otel" wallet

| 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: Deposits per Currency:

index="otel" wallet

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

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

| stats count as deposits by currency

1. Panel 14: Withdrawals per Currency:

index="otel" wallet

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

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

| stats count as withdrawals by currency

1. Panel 15: Outgoing Transfers per Currency:

index="otel" wallet

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

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

| stats count as outgoing\_transfers by currency

**Time feature:**

A screenshot of a computer

AI-generated content may be incorrect.

**Drilldown to level 2:**

**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 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.

**ADDED TITLE:**

<row>

<panel>

<html>

<h1 style="text-align: center; color: black; background-color:#94D2EC; padding: 15px; font-size: 30px;">CRYPTO WALLET DASHBOARD LEVEL 1</h1>

</html>

</panel>

</row>

**LEVEL 2:**

**A screenshot of a computer

AI-generated content may be incorrect.**

**Timerange feature and details feature**

**A screenshot of a computer

AI-generated content may be incorrect.**

**A screenshot of a computer

AI-generated content may be incorrect.**

**Panels:**

1. Number of Deposits per Wallet:

index="otel" host=cryptowallet-\*

| regex \_raw="Deposited"

| rex "wallet\s(?<wallet\_id>[a-f0-9\-]{36})"

| stats count as deposits by wallet\_id

| sort -deposits

1. Number of Withdrawals per Wallet:

index="otel" host=cryptowallet-\*

| regex \_raw="Withdrew"

| rex "wallet\s(?<wallet\_id>[a-f0-9\-]{36})"

| stats count as withdrawals by wallet\_id

| sort -withdrawals

1. Number of Transfers per Wallet:

index="otel" host=cryptowallet-\*

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

| rex "from wallet\s(?<wallet\_from>[a-f0-9\-]{36})"

| rex "to wallet\s(?<wallet\_to>[a-f0-9\-]{36})"

| eval wallet\_id=mvappend(wallet\_from, wallet\_to)

| mvexpand wallet\_id

| stats count as transfers by wallet\_id

| sort -transfers

1. Number of transactions per wallet:

index="otel" "wallet"

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

| where is\_transaction=1

| rex field=\_raw max\_match=2 "wallet\s(?<wallet\_id>[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12})"

| mvexpand wallet\_id

| stats count as transactions by wallet\_id

| sort -transactions

**Drill down feature implemented: The level 1 detailed drill down in level 2**

index=otel host=cryptowallet-\*

| 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")

| eval selected="$wallet\_id$"

| where isnull(selected)

OR selected="all"

OR (selected="transactions" AND category IN ("deposits","withdrawals","transfers"))

OR category=selected

| rex field=\_raw "wallet\s(?<wallet\_id>[a-f0-9\-]{36})"

| rex field=\_raw "username\s(?<username>\w+)"

| rex field=\_raw "location\s(?<location>[^,]+),\s+latitude\s(?<latitude>[-\d\.]+),\s+longitude\s(?<longitude>[-\d\.]+)"

| table \_time category wallet\_id username location latitude longitude

| sort -\_time

**Drilldown of level 2 : Going to level 3:(same for every panels)**

**A screenshot of a computer

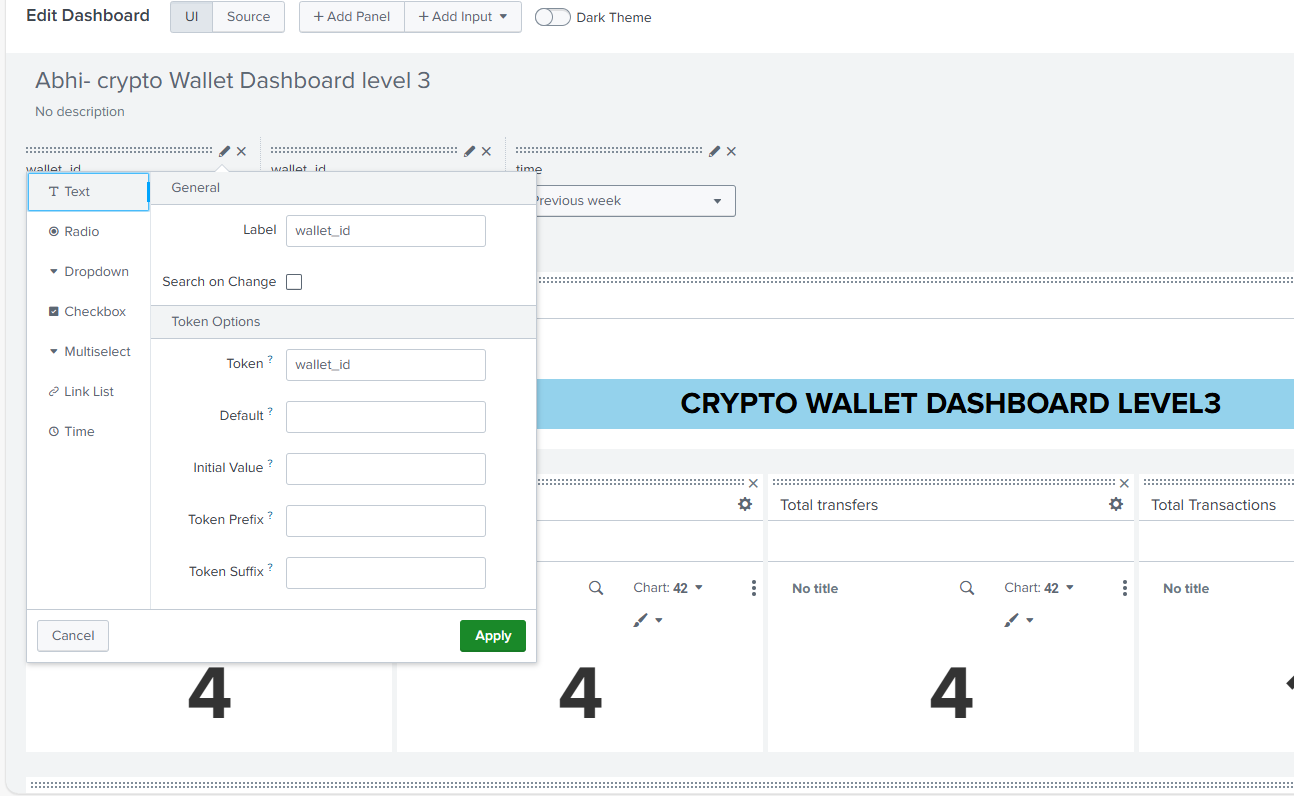
AI-generated content may be incorrect.**

**LEVEL 3:**

**A screenshot of a computer

AI-generated content may be incorrect.**

**Time range and wallet id feature:**

****

**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.**

**I have edited this spl to pick up the time range what we select in 1st level to all levels: Also the dropdown querry should pick up the wallet\_id acc to time range:**

index=otel "Created wallet"

earliest=$time.earliest$ latest=$time.latest$

| rex field=\_raw "wallet (?<wallet\_id>[a-f0-9\-]{36})"

| stats count by wallet\_id

| fields wallet\_id  
  
Also gave previous week

**A screenshot of a computer

AI-generated content may be incorrect.**

**Panels:**

1. Total deposits:

index=otel host=cryptowallet-\*

| search "Deposited"

| rex "wallet (?<wallet\_id\_extracted>[a-f0-9\-]{36})"

| where wallet\_id\_extracted="$wallet\_id$"

| stats count as total\_deposits

1. Total withdrawals:

index=otel host=cryptowallet-\*

| search "Withdrew"

| rex "wallet (?<wallet\_id\_extracted>[a-f0-9\-]{36})"

| where wallet\_id\_extracted="$wallet\_id$"

| stats count as total\_withdrawals

1. Total transfers:

index=otel host=cryptowallet-\*

| search "Transferred"

| rex "wallet (?<wallet\_id\_extracted>[a-f0-9\-]{36})"

| where wallet\_id\_extracted="$wallet\_id$"

| stats count as total\_transfers

1. Total transactions:

index=otel host=cryptowallet-\*

| rex "wallet (?<wallet\_id\_extracted>[a-f0-9\-]{36})"

| where wallet\_id\_extracted="$wallet\_id$"

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

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

1. Total errors:

index="otel" host=cryptowallet-\* wallet

| where like(\_raw, "%not found%")

| rex "Wallet with ID (?<wallet\_id\_extracted>[a-f0-9\-]{36})"

| where wallet\_id\_extracted="$wallet\_id$"

| stats count as total\_errors

**DRILLDOWN**

**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 screenshot of a computer

AI-generated content may be incorrect.**

**DRILLDOWN PANEL:**

1. Transaction details:

index=otel "wallet"

| rex "wallet (?<wallet\_id\_extracted>[a-f0-9\-]{36})"

| eval category=case(

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

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

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

)

| where (wallet\_id\_extracted="$wallet\_id$" OR "$wallet\_id$"="")

AND (

"$details$"="transactions"

OR category="$details$"

)

| rex field=\_raw "(?i)(Deposited|Withdrew|Transferred) (?<amount>\d+) (?<currency>\w+)"

| rex field=\_raw "from wallet (?<from\_wallet>[a-f0-9\-]{36})"

| rex field=\_raw "to (?<to\_currency\_amount>\d+ \w+) in wallet (?<to\_wallet>[a-f0-9\-]{36})"

| rex field=\_raw "location (?<city>[\w\s]+), latitude (?<lat>[\d\.]+), longitude (?<lon>[\d\.]+)"

| table \_time category wallet\_id\_extracted from\_wallet to\_wallet amount currency city lat lon

1. Error details:

index=otel "wallet"

| eval category=case(

match(\_raw,"Wallet with ID.\*not found"),"errors"

)

| eval wallet\_id\_extracted=mvindex(split(replace(\_raw,"Wallet with ID ","")," "),0)

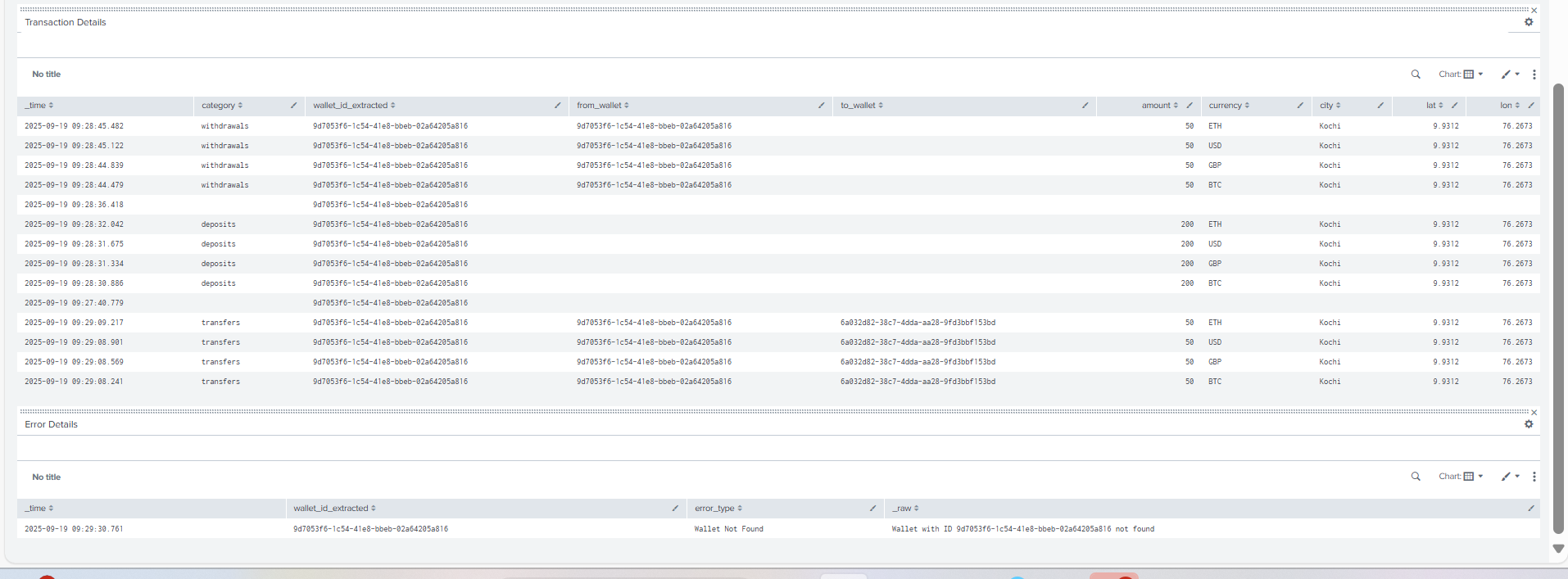
| eval error\_type=if(match(\_raw,"Wallet with ID.\*not found"),"Wallet Not Found","Other Error")

| where category="$error\_token$" AND (wallet\_id\_extracted="$wallet\_id$" OR "$wallet\_id$"="")

| table \_time wallet\_id\_extracted error\_type \_raw

| sort -\_time

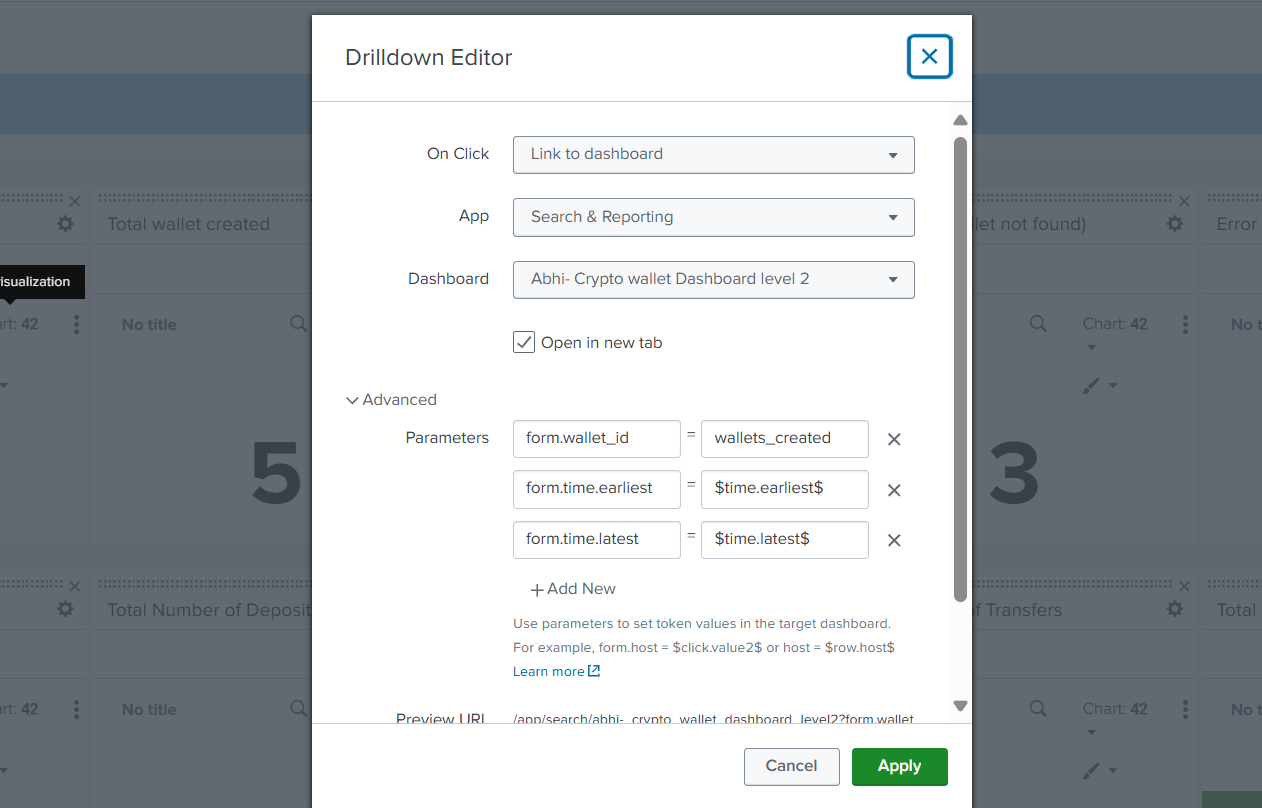
Screenshots:



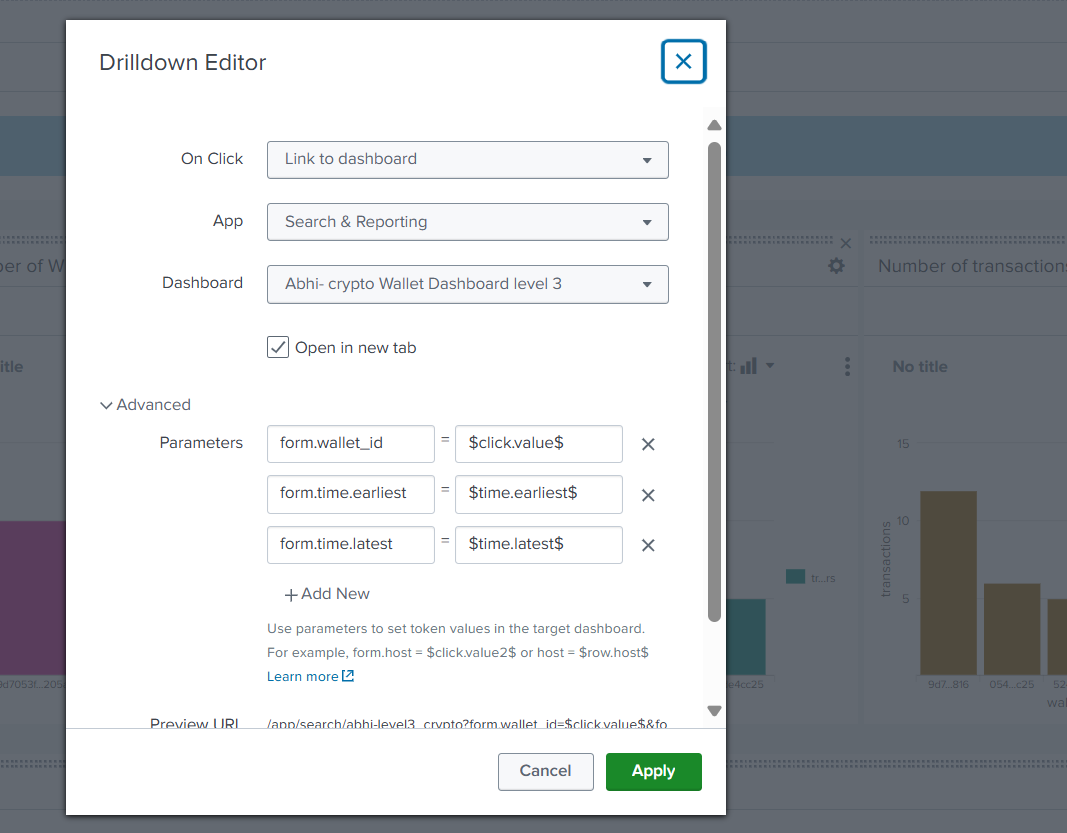
**Timerange should be same in every levels:**

when I pick a time range and click on any panel will redirect to next level with same time range:

1. Add advanced parameter token for time in each panels.

Level 1 screenshot in every panels:  


Level 2 screenshot in panels:



Click.value -> redirect to next dashboard

Form.wallet\_id = errors.. -> redirect to next dashboard which shows errors on text and details in drill down panel.