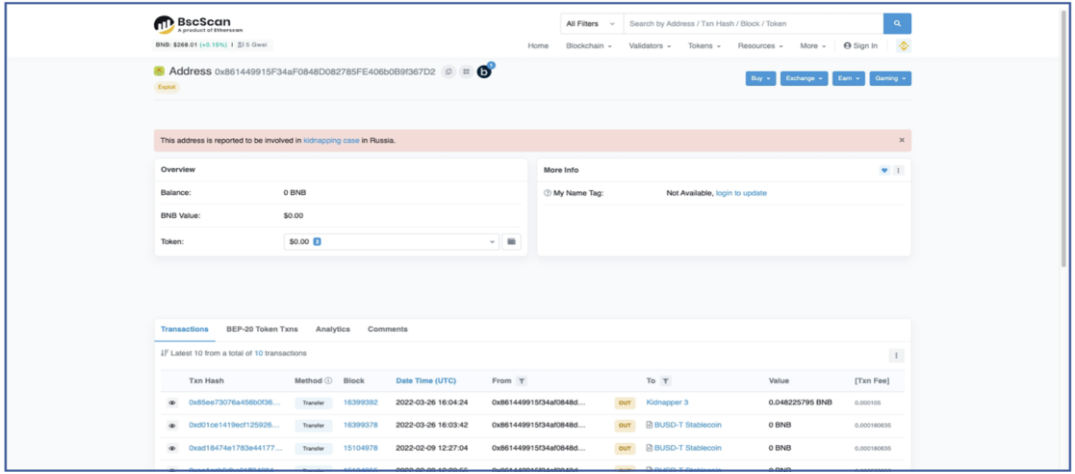
Smart contract blockchain analysis

Intelligence input

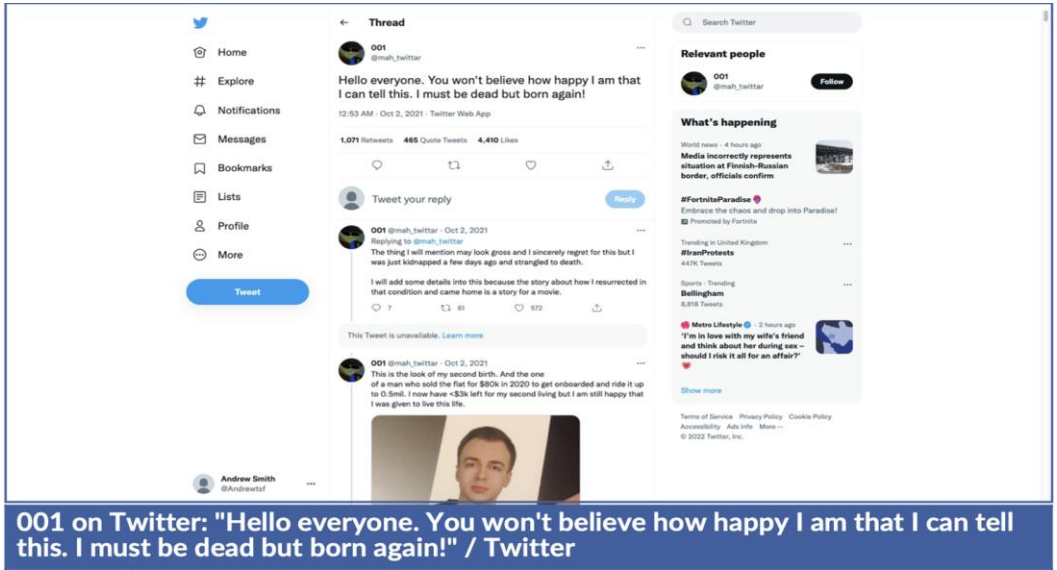
- The following cryptocurrency address has been identified as high risk in a SAR/STR: 0x861449915F34aF0848D082785FE406b0B9f367D2

- Find the context for the assessment of high risk
  - What criminality is the address linked with?
  - What cryptocurrency protocols/networks is the address present on?
  - Can you identify any other addresses linked to this criminality?



https://bscscan.com/address/0x861449915f34af0848d082785fe406b0b9f367d2#tokentxns

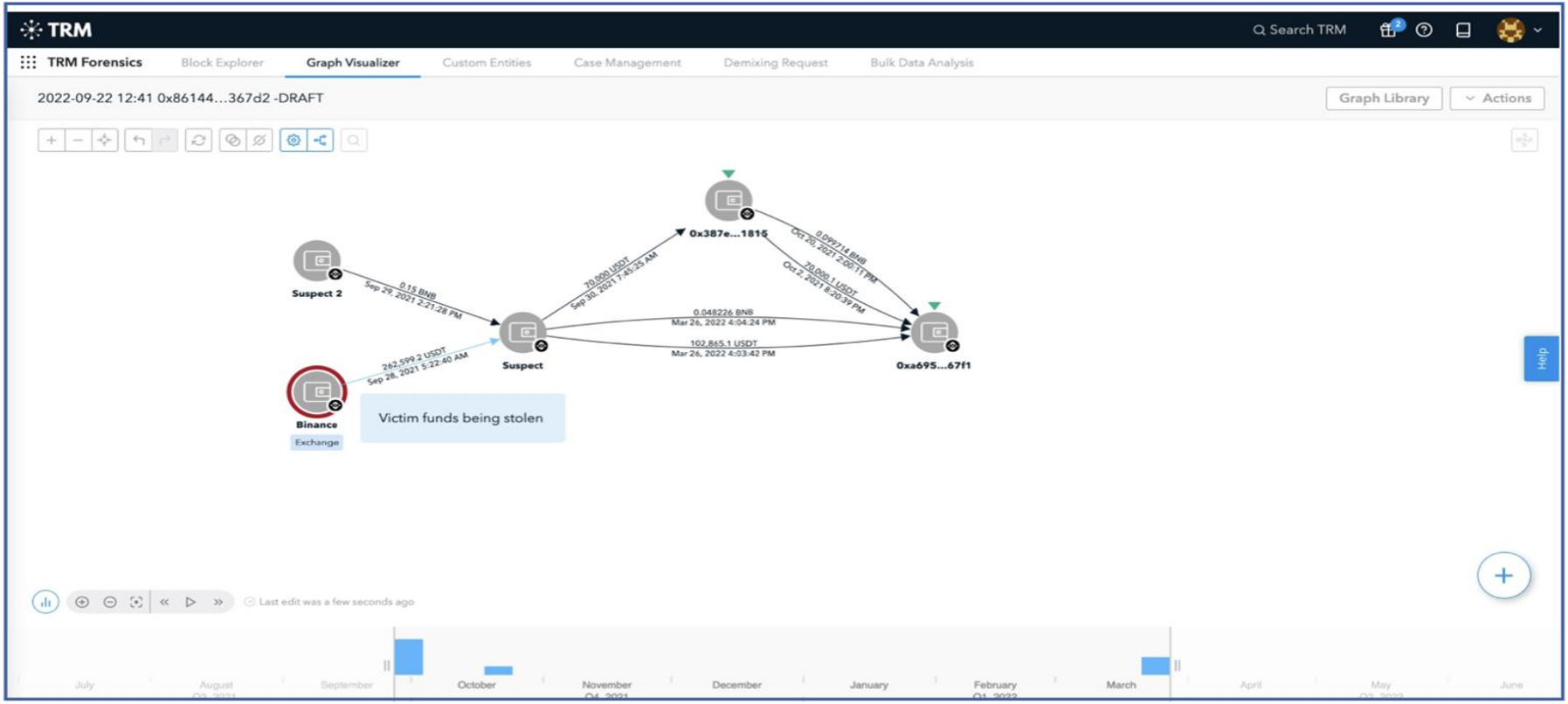
https://twitter.com/mah_twittar/status/1444088020483952646



001 on Twitter: "Hello everyone. You won't believe how happy I am that I can tell this. I must be dead but born again!" / Twitter

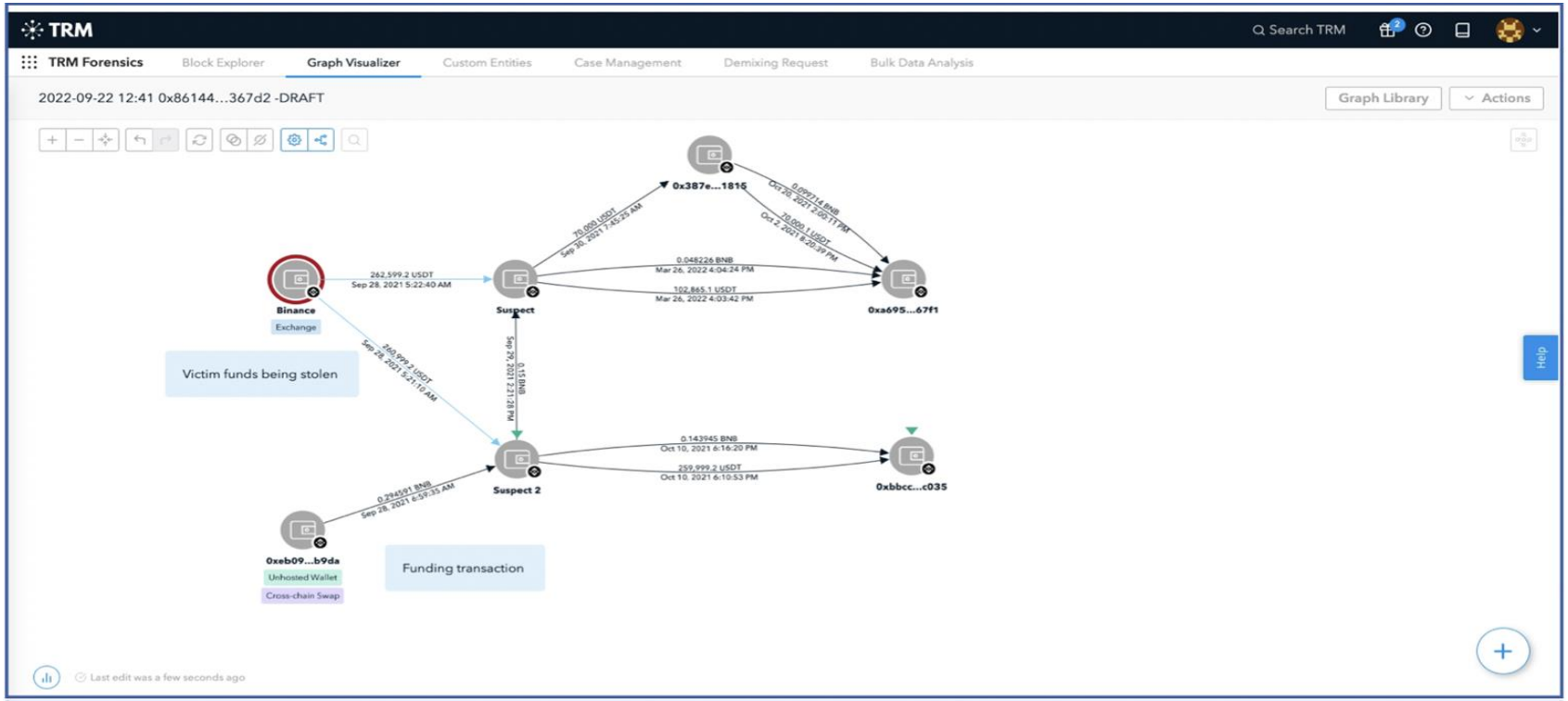
Blockchain analysis

- Go to TRM and plot out the initial suspect address
- What immediate opportunities present themselves?
- What does this tell us in respect of the address outlined to focus on?
- From the transfers tab plot the transactions you believe are relevant

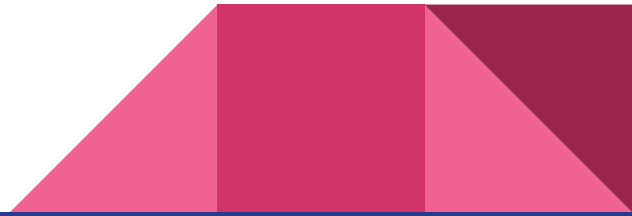

TRM
Search TRM
TRM Forensics
Block Explorer
Graph Visualizer
Custom Entities
Case Management
Demixing Request
Bulk Data Analysis
2022-09-22 12:41 0x86144...367d2 -DRAFT
Graph Library
Actions
Suspect 2
0.15 BNB
Sep 29, 2021 2:21:28 PM
0x387e...1815
70,000 USDT
Sep 30, 2021 7:43:25 AM
0.099714 BNB
Oct 20, 2021 2:00:11 PM
70,000.1 USDT
Oct 2, 2021 9:20:39 PM
0.048226 BNB
Mar 26, 2022 4:04:24 PM
102,865.1 USDT
Mar 26, 2022 4:03:42 PM
Suspect
0xa695...67f1
262,599.2 USDT
Sep 28, 2021 5:22:40 AM
Binance
Exchange
Victim funds being stolen
Help
Last edit was a few seconds ago
July
August
September
October
November
December
January
February
March
April
May
June

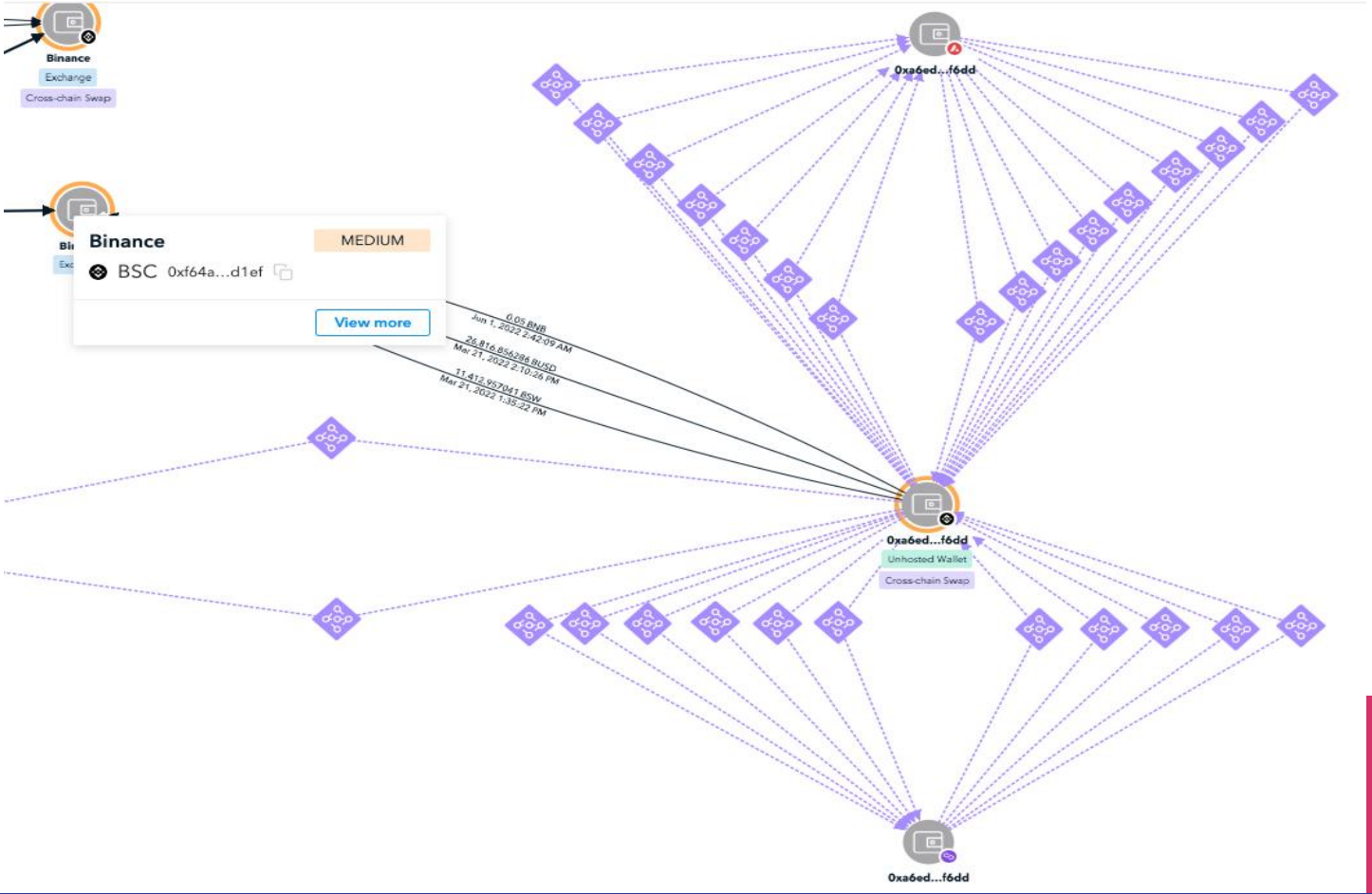
Blockchain analysis cont.

- Do the same for suspect address 2
- Why is the initial deposit of BNB worth reviewing?



- Continue forward, what exchange are funds cashed out at?
- Create a custom cluster for the addresses you believe are controlled by the suspect. Make sure you check which protocols the addresses have been active on.
- 0xf64af01774ac8d0d0af933fc1fc1e0964531d1ef, would you consider any further tracing based on the incoming transactions detailed?
- What further addresses would you add to your custom cluster?




Binance
Exchange
Cross-chain Swap
Binance
MEDIUM
BSC 0xf64a...d1ef
View more
0.05 BNB
Jun 1, 2022 2:42:09 AM
26,816.856286 BUSD
Mar 21, 2022 2:10:26 PM
11,412.957041 BSW
Mar 21, 2022 1:35:22 PM
0xa6ed...f6dd
0xa6ed...f6dd
Unhosted Wallet
Cross-chain Swap
0xa6ed...f6dd

Blockchain analysis cont.

- Search for and click on 0xa6ed50d06c420a3c540f9e4955772600f7c3f6dd in bscscan.com. Navigate to ERC-721 and review the NFT transactions. What NFT's are involved in these TX's?
- Plot the address in TRM and map out some of the NFT transactions. What do you notice?
- Now click on the Cross-chain Swap detail
- Plot these transactions, what bridges are used by the entity? What protocols does the entity transact on?
- On BSC protocol follow the most significant counterparty in respect of outgoing volume. Which exchange is used to cash out these funds?
- On Polygon there is a transaction involving the Hop protocol, search for the address 0x76b22b8c1079a44f1211d867d68b1eda76a635a7 in counterparties. This is an address linked to the Hop Protocol. What do you notice?
- Navigate to https://explorer.hop.exchange/ and use the filters to search for 0xa6ed50d06c420a3c540f9e4955772600f7c3f6dd. See which of these transactions you can plot in TRM. What do you find?
- On ETH the entity engages with Thorswap, what BNB address is associated with this? Search for the transactions on Etherscan and scroll "More details". Click to see more and then choose decode.
- Plot the BNB address in TRM and identify any exchanges funds are sent to.