How to decide that 1KKhtG8XygZM7ioyWFWUzSwGZTjFcs8nR4 bitcoin address has suspicious activities.

1. First visit to bitcoinabuse portal to verify that address belongs to bitcoin blockchain.
2. Verify that the address is reported by someone as a malicious or not if yes then the address is malicious otherwise we need to check financial transactions of that account
3. Visit bitref and insert suspected bitcoin address in the search box and hit enter. This will give us details about list of transactions are done by that address.
4. Search number of transactions and intended source and recipient for those transaction on blockchain.com
5. If after six or more hopes bitcoin is again resend to this address it indicates that address is suspicious.
6. Search current address and all other suspicious address on bitcoinwhoswho portal to get its IP.
7. Search that IP on the passivedns to get URL for that IP address.
8. After getting URL finally search who owns that URL on the whois.domaintolls.com

Rihan sir!!!

Let's Investigate & be a Crypto-Investigator in 30 Minutes.

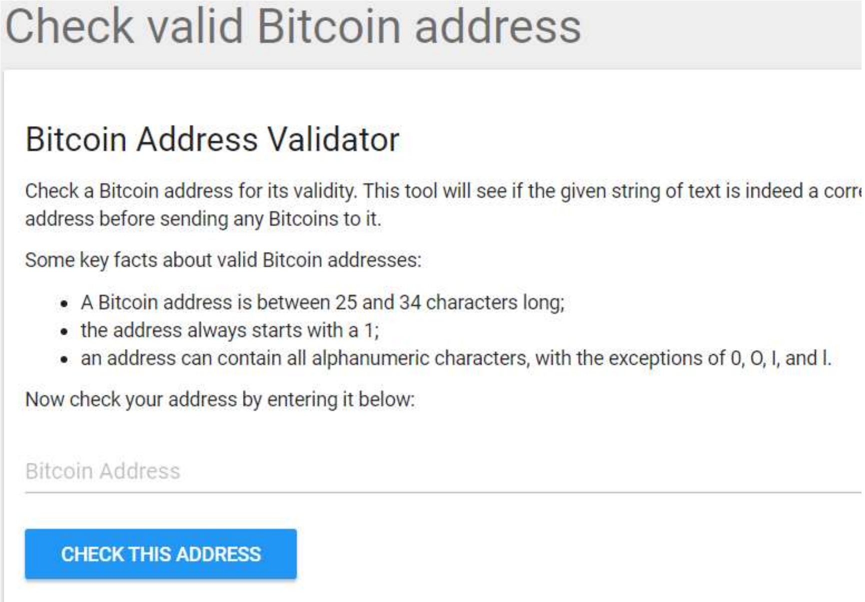
As an Investigator

- **To find details associated with the suspicious cryptocurrency address in any given case.**
- **To use commercial tools but to also use Open Source Intelligence.**

Investigating Crypto-Assets

Step 1 : Validate The Address First

- **Start by checking the suspicious address is a valid address before diving into investigation.**
- **Tools :**
  - **https://thomas.vanhoutte.be/tools/validate-bitcoin-address.php**
  - **https://awebanalysis.com/en/bitcoin-address-validate/**



Check valid Bitcoin address

Bitcoin Address Validator

Check a Bitcoin address for its validity. This tool will see if the given string of text is indeed a corr
address before sending any Bitcoins to it.

Some key facts about valid Bitcoin addresses:

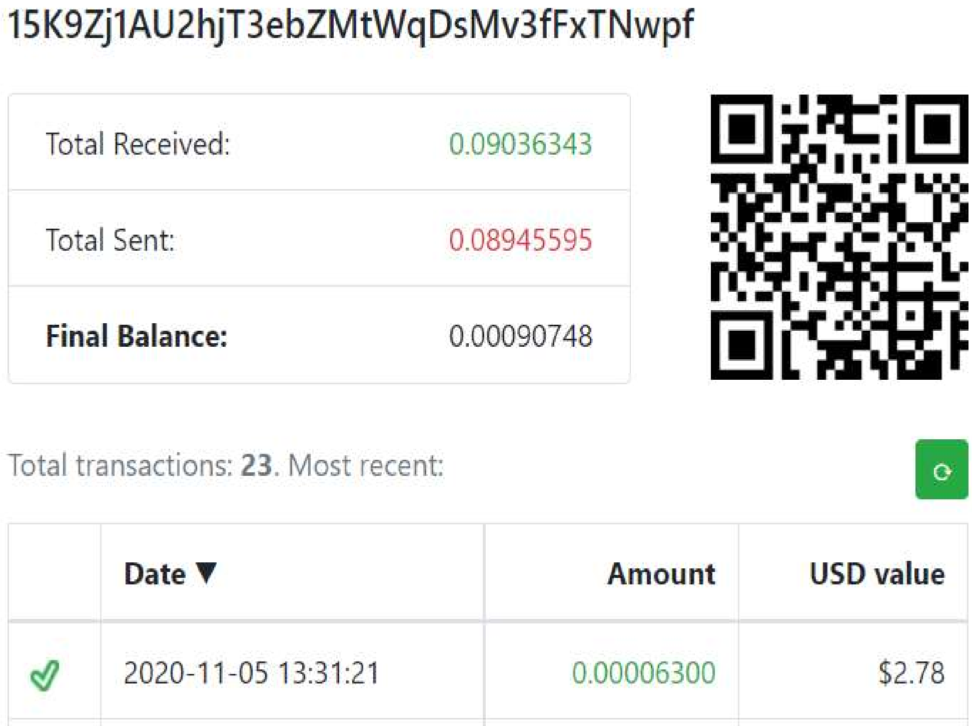
- A Bitcoin address is between 25 and 34 characters long;
- the address always starts with a 1;
- an address can contain all alphanumeric characters, with the exceptions of 0, O, I, and l.

Now check your address by entering it below:

Step 2 : Confirm the Address Balance

Start by confirming and preparing the reports on the address Balance.

- **Tools :**
  - https://www.homebitcoin.com/easybalance/
  - https://www.cointracker.io/wallet/bitcoin
  - https://bitref.com/
  - https://www.blockonomics.co/



15K9Zj1AU2hjT3ebZMtWqDsMv3fFxTNwpf

Total Received:	0.09036343
Total Sent:	0.08945595
Final Balance:	0.00090748

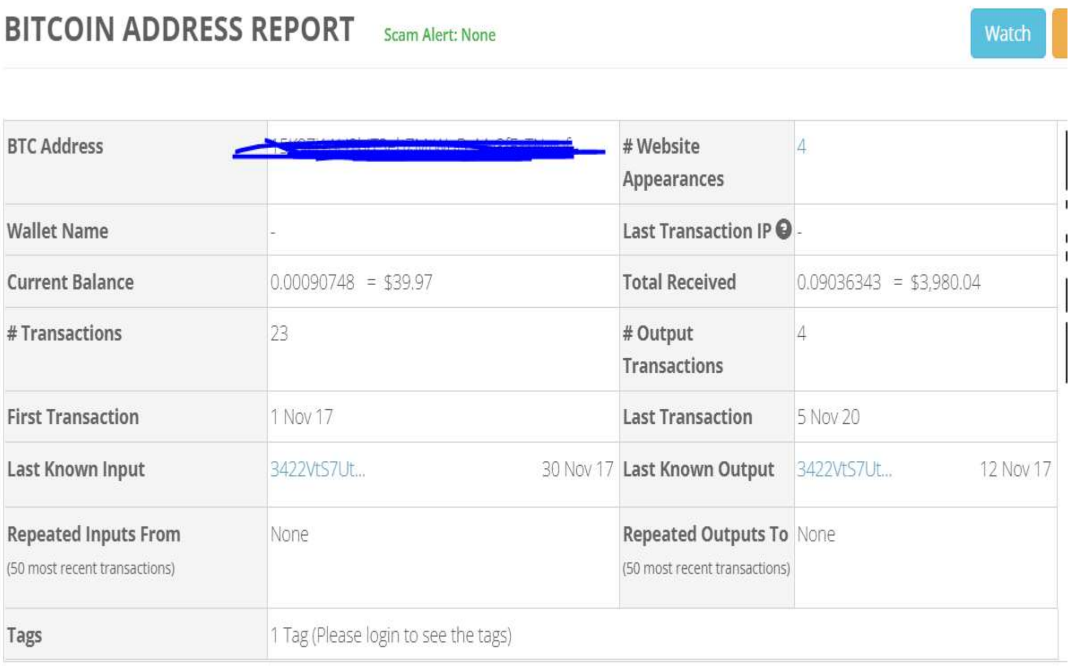
Total transactions: **23**. Most recent:

	Date ▼	Amount	USD value
✓	2020-11-05 13:31:21	0.00006300	$2.78

Step 3 : Prepare Reports On Bitcoin Address

Check for SPAM/SCAM Alert, Current Balance, I/O Transact-ions, IP Address, Web Appearance, etc…

- **Tools :**
  - **https://bitcoinwhoswho.com (Need to Register to get details)**



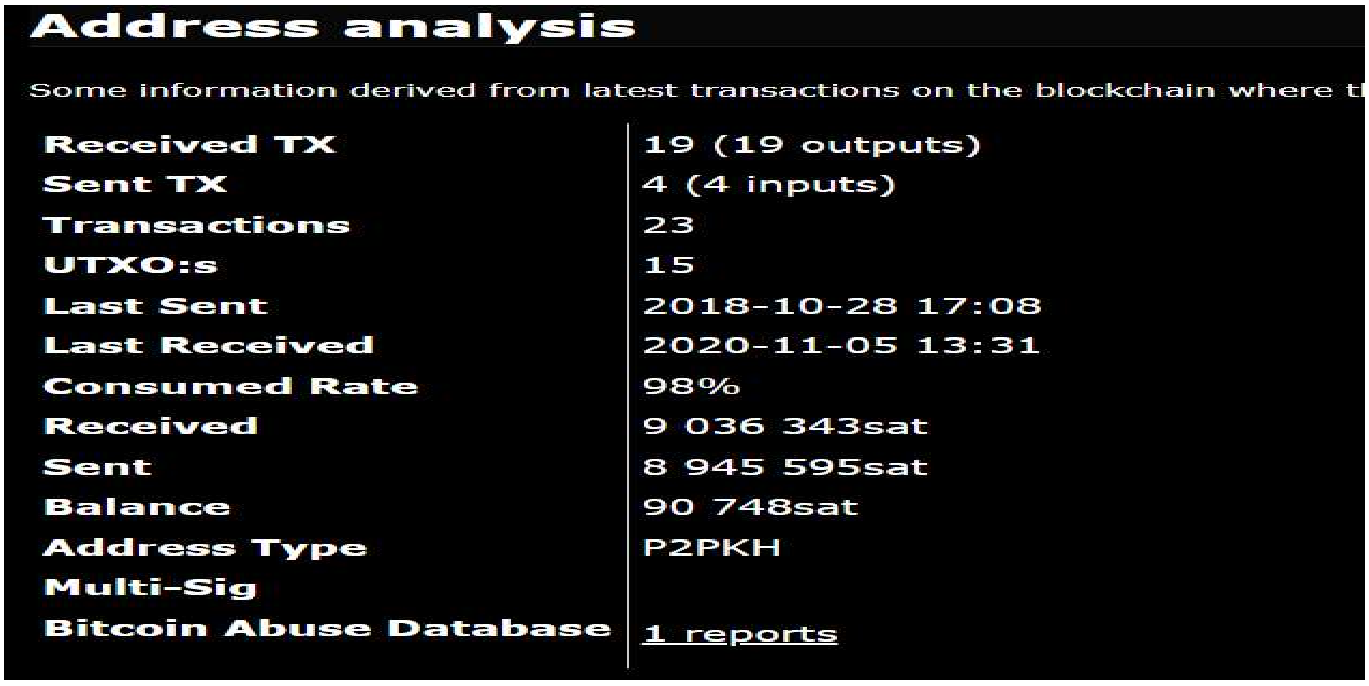
BITCOIN ADDRESS REPORT Scam Alert: None

BTC Address	[redacted]	# Website Appearances	4
Wallet Name	-	Last Transaction IP ?	-
Current Balance	0.00090748 = $39.97	Total Received	0.09036343 = $3,980.04
# Transactions	23	# Output Transactions	4
First Transaction	1 Nov 17	Last Transaction	5 Nov 20
Last Known Input	3422VtS7Ut... 30 Nov 17	Last Known Output	3422VtS7Ut... 12 Nov 17
Repeated Inputs From (50 most recent transactions)	None	Repeated Outputs To (50 most recent transactions)	None
Tags	1 Tag (Please login to see the tags)		

Step 4 : Link Transactions

Identify Transactions, Identify Blocks, Checked for Mined Blocks and search for exchange names

- **Tools :**
  - **https://hashxp.org/**



Address analysis

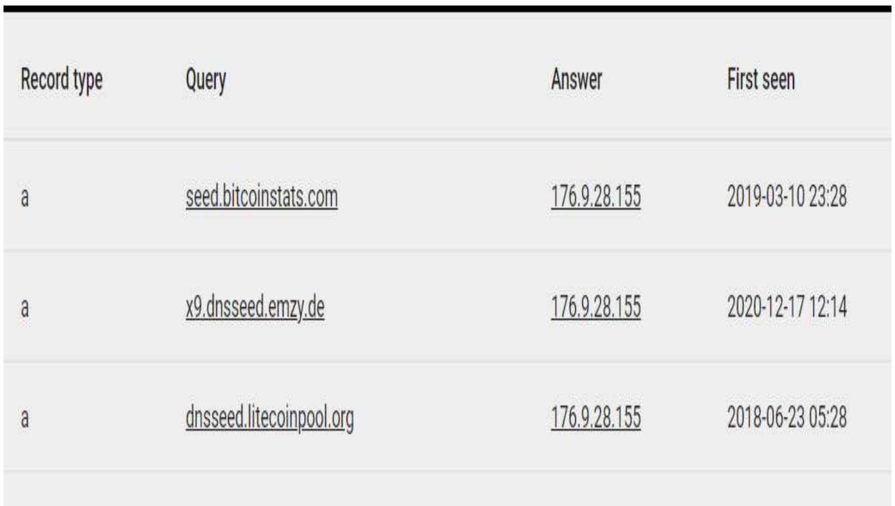
Some information derived from latest transactions on the blockchain where t

Received TX	19 (19 outputs)
Sent TX	4 (4 inputs)
Transactions	23
UTXO:s	15
Last Sent	2018-10-28 17:08
Last Received	2020-11-05 13:31
Consumed Rate	98%
Received	9 036 343sat
Sent	8 945 595sat
Balance	90 748sat
Address Type	P2PKH
Multi-Sig	
Bitcoin Abuse Database	1 reports

Step 5 : Identify Related Domains

Passive DNS

- **Tools :**
  - **https://passivedns.mnemonic.no/**
  - **https://whois.domaintools.com/**
  - **https://bgpview.io/**



Record type	Query	Answer	First seen
a	seed.bitcoinstats.com	176.9.28.155	2019-03-10 23:28
a	x9.dnsseed.emzy.de	176.9.28.155	2020-12-17 12:14
a	dnsseed.litecoinpool.org	176.9.28.155	2018-06-23 05:28

Step 6 : Search Engine, Social Media & Email Investigation

Everyone exists somewhere on internet. Search them.

- **Tools :**
  - **Search Engine Search**
  - **Social Media Search**
  - **MXToolBox – Email Search**
  - **SPYTOX – Email Search**

Find people, personal info & phone numbers.

Step 7 : Identify Wallet & Exchange

Use Basic Algorithm to determine wallet address. Search for possible exchanges based on wallet and link the traces.

- **Tools :**
  - **WalletExplorer**
  - **oxt.me**