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.**

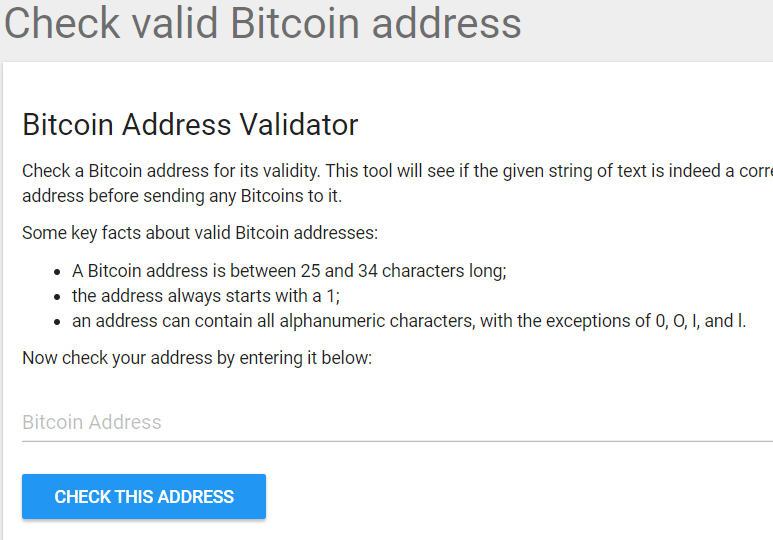
**As an Investigator**

* **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**

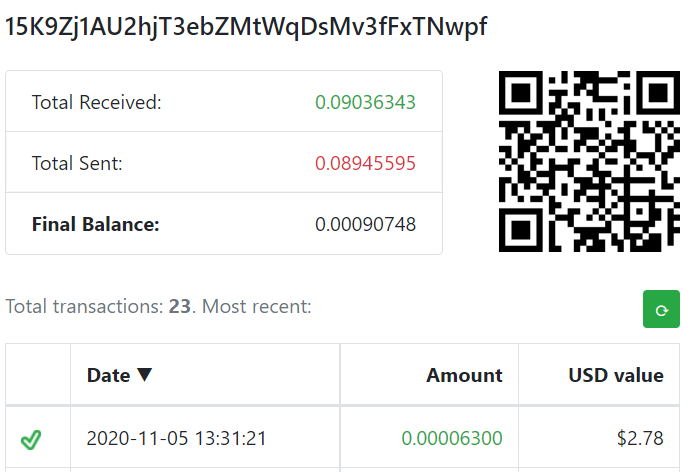
* **Start by checking the suspicious address is a valid address before diving into investigation.**
* **Tools :**
  + [**https://thomas.vanhoutte.be/tools/validate-bitcoin-address.php**](https://thomas.vanhoutte.be/tools/validate-bitcoin-address.php)
  + [**https://awebanalysis.com/en/bitcoin-address-validate/**](https://awebanalysis.com/en/bitcoin-address-valid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

****

**Step 2 : Confirm the Address Balance**

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

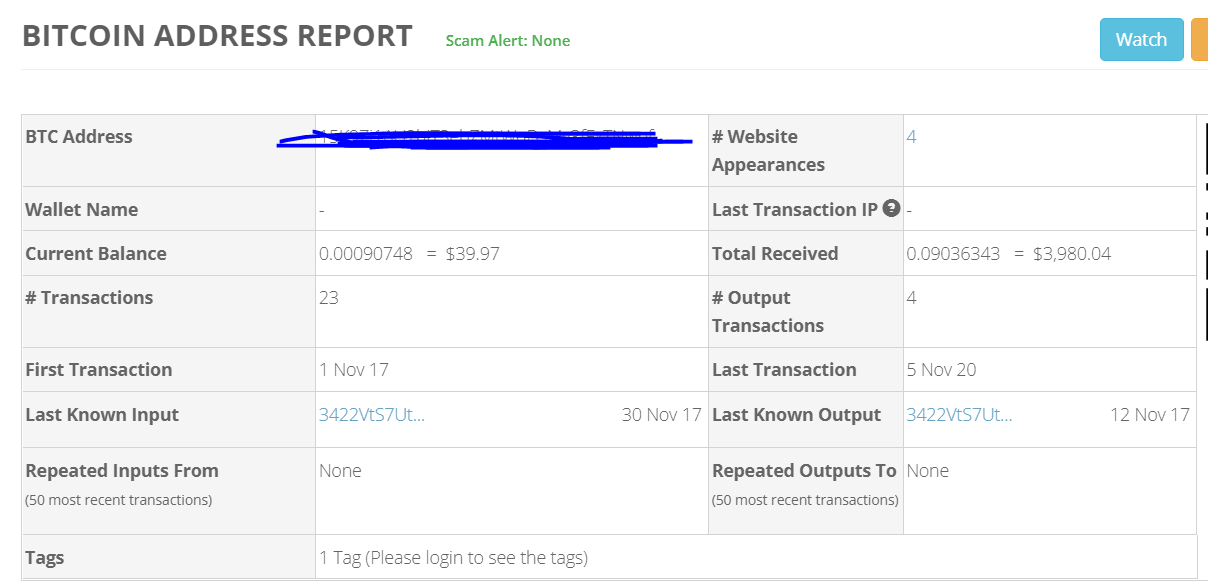
* **Tools :**
  + [**https://www.homebitcoin.com/easybalance/**](https://www.homebitcoin.com/easybalance/)
  + [**https://www.cointracker.io/wallet/bitcoin**](https://www.cointracker.io/wallet/bitcoin)
  + [**https://bitref.com/**](https://bitref.com/)
  + [**https://www.blockonomics.co/**](https://www.blockonomics.co/)

****

**Step 3 : Prepare Reports On Bitcoin Address**

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

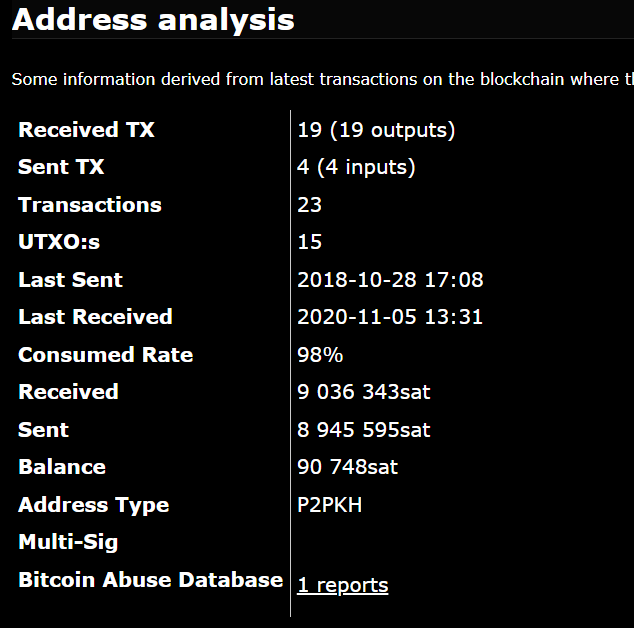
* **Tools :**
  + [**https://bitcoinwhoswho.com**](https://bitcoinwhoswho.com) **(Need to Register to get details)**

****

**Step 4 : Link Transactions**

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

* **Tools :**
  + [**https://hashxp.org/**](https://hashxp.org/)

****

**Step 5 : Identify Related Domains**

**Passive DNS**

* **Tools :**
  + [**https://passivedns.mnemonic.no/**](https://passivedns.mnemonic.no/)
  + [**https://whois.domaintools.com/**](https://whois.domaintools.com/)
  + [**https://bgpview.io/**](https://bgpview.io/)

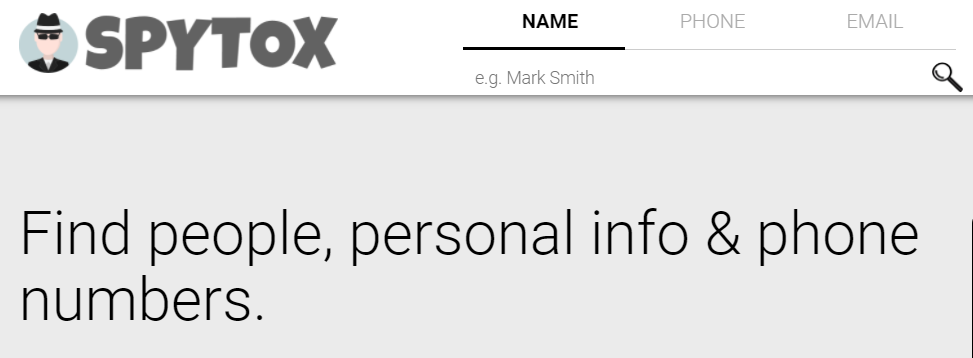
****

****

**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**

****

**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**