# What are the steps and stages of an investigation?

10/25/2024 12:32 am EDT

The stages an investigation might take varies considerably from one case to another, but below is an overview of the stages of a semi-typical investigation.

1. User submits incident report to Cryptoforensic Investigators. This includes background on what happened, and the blockchain transaction data associated with the loss.

2. Cryptoforensic Investigators performs a preliminary assessment of the case. In this assessment, we assess the status of the funds, exchanges involved so far, the prospects of the case, the likelihood of a positive outcome for the victim, the size of the loss (if not already known), the scope of work that ought to be performed, the amount of time we think we'd need to do the work, and ultimately, if we think the case is viable and worthy of an engagement.

The majority of incidents reported to us are not appropriate for us to engage on, but for the sake of this answer, we'll assume this one is. The victim is then made an engagement offer. Again, for the sake of this answer, we'll assume they proceed with the engagement offer.

3. The victim is asked to provide some supporting evidence of the claim, and additional background if appropriate. This could include chat logs, browser history, emails, exchange statements or screenshots

4. After assessing to help ensure the reported incident is authentic, Cryptoforensic Investigators will normally flag or report relevant addresses to major forensic software providers, if the client is agreeable to this. This increases the odds of exchanges flagging or freezing stolen funds.

5. We will try to identify the current location of the funds, or what's left of them, and flag these addresses with relevant exchanges as well.

6. We conduct a more in depth analysis of the flow of funds and identify all relevant on-chain leads, tracing through DeFi exchanges and DeFi bridges as needed, or to other blockchains.

7. We contact and notify relevant cryptocurrency exchanges that are closely connected to the incident so that they can take action about suspicious activity if they wish to do so, such as freezing accounts.

8. Usually, we investigate details about the attacker that we learn about, to try and better identify where they reside, or occasionally even identify them. This can involve researching email address, IP addresses, websites, usernames, forums, and phone numbers.

9. When/if data is obtained from exchanges, typically through law enforcement, we conduct additional blockchain analysis to see what else can be learned about what happened to the stolen funds, and what other important leads have arisen with the new data.

10. Findings are drawn up in a report, which is typically provided to law enforcement

11. Throughout the case, we monitor any dormant/unlaundered funds, and attempt to notify relevant exchanges ASAP if the illicit funds are sent to them, so they can freeze relevant accounts or transfers.

12. We liaise with law enforcement on an as-needed basis throughout the duration of the case.