BTC DFIR 手順

1. **調査目的の明確化**

   最初に、DFIR（Digital Forensics and Incident Response）の専門家が何を調査し、どのような情報を得たいのかを明確にします。具体的な目的がないと、調査が複雑になる可能性があります。

2. **Bitcoinアドレスの特定**

   調査対象のBitcoinアドレスを特定します。これは、調査の対象や犯罪の性質によって異なります。

   アドレスは次の規則に従います。

   `^[13][a-km-zA-HJ-NP-Z1-9]{25,34}$'`

   有効性を確認するために、チェックサムを調査する必要があります。

3. **ブロックチェーンエクスプローラの利用**

   Bitcoinのブロックチェーンエクスプローラを使用して、対象のBitcoinアドレスに関連するトランザクションの詳細情報を取得します。一般的なエクスプローラには、Blockchain.infoやBlockchairなどがあります。

4. **トランザクションの解析**

   取得したトランザクション情報を分析し、送金元や送金先のアドレス、金額などを確認します。これにより、アクティビティのパターンや特定のアドレスとの関連性を特定できます。

   例えば、資金洗浄やサイバー犯罪に関連した取引が行われた場合、特定の日付や時間帯にパターンが現れる可能性があります。

5. **クラスタリングと関連アドレスの特定**

   同じユーザーまたは組織によるアクティビティを特定するために、クラスタリング技術を使用して関連するBitcoinアドレスを特定します。これにより、複数のアドレスが同じ実体に関連している可能性があります。

6. **取引所やサービスとの連携**

   取引所やBitcoin関連のサービスと連携して、アドレスの所有者に関する情報を取得します。これには、法的なプロセスを経て取引所からの情報提供が含まれます。

7. **顧客情報の取得**

   関連するBitcoinアドレスが取引所で使用されている場合、取引所からの法的手続きを通じて関連する顧客情報を取得します。

8. **法的手続きの遵守**

   全ての手続きは、法的な要件とプロセスに厳密に従う必要があります。プライバシーと個人情報保護法を遵守し、適切な法的権限を取得することが不可欠です。

9. **レポートの作成**

   調査結果をまとめ、法的な手続きや倫理的な観点から報告書を作成します。必要に応じて、調査結果を法執行機関や関係者に提供します。