**Tips :**

1. Les transactions concernant les cryptomonnaies ne sont anonymes que si le contexte n’est pas connu
2. **Une bonne connaissance de la blockchain et du fonctionnement des cryptomonnaies est requise pour faire de l’OSINT sur une cible en passant par la blockchain – Point essentiel à appliquer selon SANS Institute !**
3. Le numéro de portefeuille crypto est en fait une version encodée de la clé publique de ce même portefeuille, **et le portefeuille crypto contient la clé privé**
4. En corrélant les entrées et les sorties sur la base de facteurs comme le montant des transactions, les horodatages, et les comportements de réseau, les attaquants peuvent parfois retrouver l'origine des fonds.
5. Bien que les mixers crypto sont vraiment efficaces pour anonymisé les transactions, il est nécessaire de stipuler qu’ils sont principalement contrôlés par des machines, et les machines sont déterministe, en faisant une rétro-ingénierie sur le mixer, il est possible de casser le processus d’anonymisation et ainsi faire des suppositions logiques sur quelles transactions appartient à qui, il est à noter que les mixers prennent un pourcentage sur les transactions
6. L’analyse temporelle est une bonne méthode pour remonter à la source des transactions (ex : En fonction des heures où le portefeuille est actif, on peut en déduire le fuseau horaire)
7. Les transactions ayant été faite sur la blockchain sont **publique**
8. La blockchain n’est pas anonyme, mais pseudo anonyme
9. Pratiquement tout courtier en cryptomonnaies légitime et réglementé dans l'Union Européenne aura un numéro d'enregistrement ou un agrément, comme l'exige la nouvelle réglementation MiCA
10. Il est possible d’identifié la blockchain via l’encodage d’une adresse de portefeuille (un portefeuille bitcoin commence généralement par bc1)
11. Les "seed words" (ou phrases de récupération) sont une série de 12, 18 ou 24 mots qui constituent la clé de sauvegarde de votre portefeuille de cryptomonnaies. Elles servent à retrouver l'accès à vos fonds si vous perdez votre appareil ou votre mot de passe, car elles permettent de régénérer toutes vos clés privées. Il est essentiel de les garder en lieu sûr et de ne jamais les partager, car **quiconque les possède à un accès complet à votre portefeuille et à vos actifs**.
12. Une bonne technique pour retrouver quelqu’un à partir d’une adresse de portefeuille crypto est d’utiliser du google dorking
13. L’utilisation d’outils de visualisation aide beaucoup lors de l’investigation axé sur les cryptomonnaies
14. Dans la plupart des pays, les organisations proposant des services de cryptomonnaies sont obligées de respecté le KYC (Know Your Customer), c’est-à-dire connaître l’identité de leurs clients, et d’avoir un moyen de la contrôler, en partant de ce principe, il est possible pour les forces de l’ordre de mettre en relation une transaction et l’identité d’une personne, du point de vue de l’anonymat, il est possible de se protégé de se principe en utilisant des mixers crypto, des cryptomonnaies axés sur la confidentialité (Ex : Monero), d’effectué des échanges décentralisés (DEX), ou encore d’utiliser une plateforme étant sous une juridiction ne demandant pas le KYC
15. Dans la blockchain Etherium, il existe le ENS (Etherium Name Service) qui permet d’associer un nom lisible par l’homme avec une adresse d’un portefeuille crypto
16. Le moyen le plus simple de tracer quelqu’un, est de le laisser faire des erreurs dans son Opsec
17. Les transactions faites dans le but d’acheté quelque chose est facilement traçable, car il est possible de mettre en relation les informations relatives à la blockchain et les informations utilisé pour l’achat en lui-même (ex : si un site web a été acheté via de la cryptomonnaies, alors la personne a du donné des informations personnelles au registraire du site)
18. Certains tips nécessite que l’analyste ait le pouvoir d'assignation à comparaître afin de les effectués ou au moins une collaboration avec quelqu’un qui à ce pouvoir
19. **Partie Planification – technique opsec :**  Créé des personna afin de protéger son identité véritable
20. C’est toujours possible de faire de l’OSINT complètement gratuitement, bien que les meilleurs outils soient généralement payant, il est toujours possible d’improvisé, (Ex : Utiliser Excel ou draw.io à la place de Maltego)

**Tools :**

* Etherscan.io