Introduction Générale

Dans un contexte où la sécurité des réseaux est devenue une préoccupation majeure pour les organisations, l'analyse du trafic réseau (Network Traffic Analysis, NTA) joue un rôle central dans la détection, la compréhension et la neutralisation des menaces potentielles.

Ce projet se concentre sur l'observation et l'analyse du trafic réseau en temps réel, avec pour objectif principal de comprendre la réaction des dispositifs de sécurité, tels que les pare-feux, les systèmes de détection d'intrusion (IDS) et de prévention d'intrusion (IPS), face à différents types d’attaques de reconnaissance

En simulant des techniques de reconnaissance, comme des scans réseau variés (ARP, TCP SYN, ICMP, etc.), l'application capture, log et visualise les paquets réseau pour une évaluation approfondie des défenses, identifiant ainsi les vulnérabilités potentielles.

L'outil propose une interface intuitive qui facilite l'analyse et la visualisation des comportements réseau, renforçant ainsi la capacité des systèmes de sécurité à contrer les menaces sophistiquées.

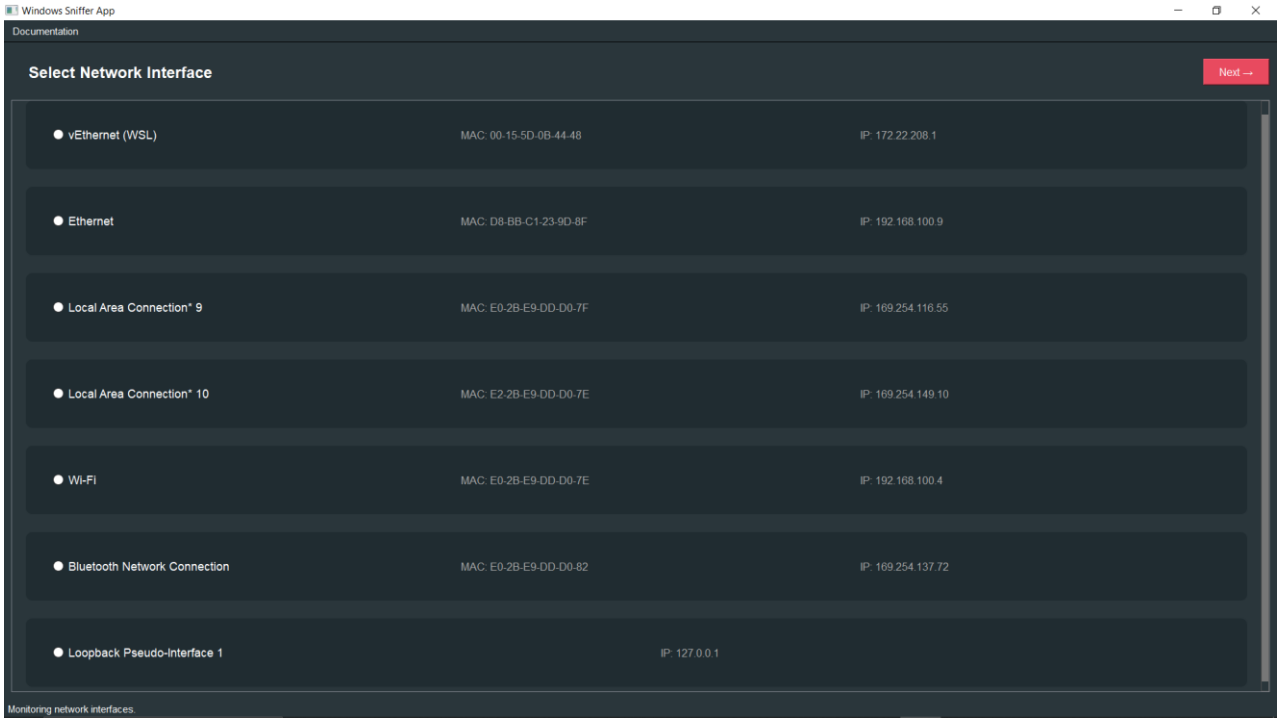
IV. Projet du Stage

Présentation de NetSecPy

NetSecPy est une application de sécurité réseau et d'analyse du trafic que j'ai développée pour offrir une solution pour la gestion des réseaux. Ce projet a été conçu avec l'intention de fournir un outil intuitif pour surveiller et analyser le trafic réseau en temps réel.

NetSecPy permet une capture et une analyse approfondie des paquets, facilitant ainsi la détection des anomalies et des menaces potentielles. Grâce à une interface utilisateur conviviale, les utilisateurs peuvent filtrer et examiner les paquets capturés, exécuter des scans de reconnaissance, et analyser les services réseau , créer et envoyer des paquets dans le réseaux .

Sélection de l'Interface Réseau



La première page de l'application est conçue pour permettre à l'utilisateur de sélectionner l'interface réseau à surveiller. Elle constitue une étape essentielle avant de commencer toute opération de capture de trafic réseau.

Objectif de la page

Cette page est cruciale car elle prépare l'environnement pour les fonctionnalités principales de l'application, en permettant à l'utilisateur de définir sur quelle interface réseau il souhaite opérer. Cela garantit que les analyses de trafic sont effectuées sur la bonne connexion

Fonctionnalités

- **Liste des interfaces réseau** : L'utilisateur peut parcourir une liste interactive des interfaces réseau disponibles, chacune accompagnée d'informations comme l'adresse IP et l'adresse MAC associées.
- **Sélection d'une interface** : L'utilisateur sélectionne une interface via

une option intuitive, lui permettant de spécifier le point de capture du trafic.

- **Navigation vers la prochaine étape** : Une fois l'interface sélectionnée, un bouton "Next" permet de valider la sélection et de passer à la page suivante, où l'analyse et la capture réseau seront effectuées.

Onglet Sniffer

Description Générale

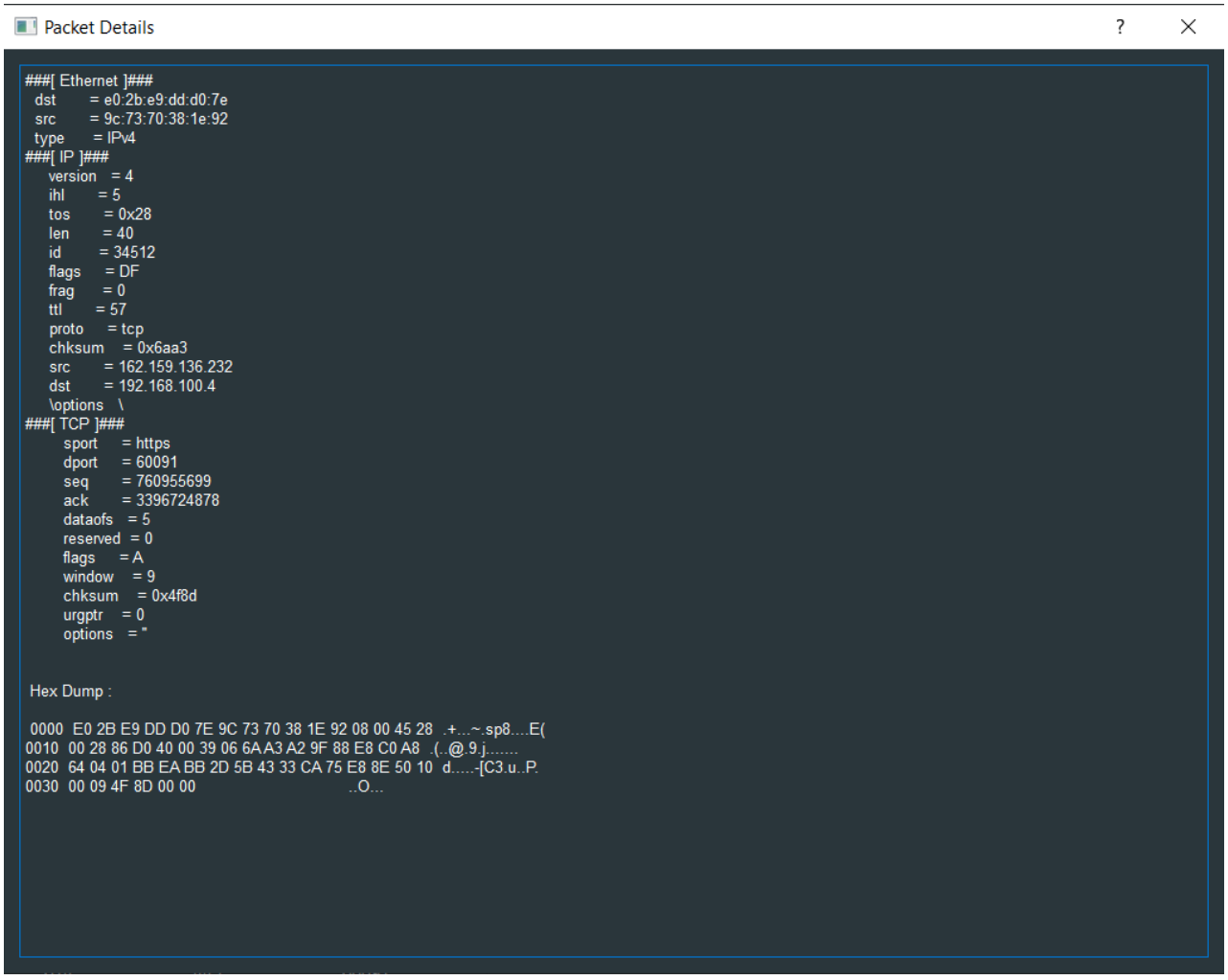
L'onglet Sniffer de l'application est conçu pour capturer, afficher et analyser le trafic

réseau en temps réel. Il offre une interface conviviale permettant aux utilisateurs de surveiller le trafic réseau, d'appliquer des filtres pour affiner les résultats, et d'examiner les paquets individuels capturés.

Fonctionnalités Principales

- **Affichage des Paquets Capturés** : L'onglet dispose d'un tableau interactif qui affiche les détails des paquets réseau capturés. Les colonnes incluent l'horodatage, l'adresse IP source, l'adresse IP de destination, le protocole, la longueur du paquet, le port source et le port de destination.

  Le tableau permet aux utilisateurs de sélectionner une ligne pour afficher les détails d'un paquet spécifique dans une autre fenêtre

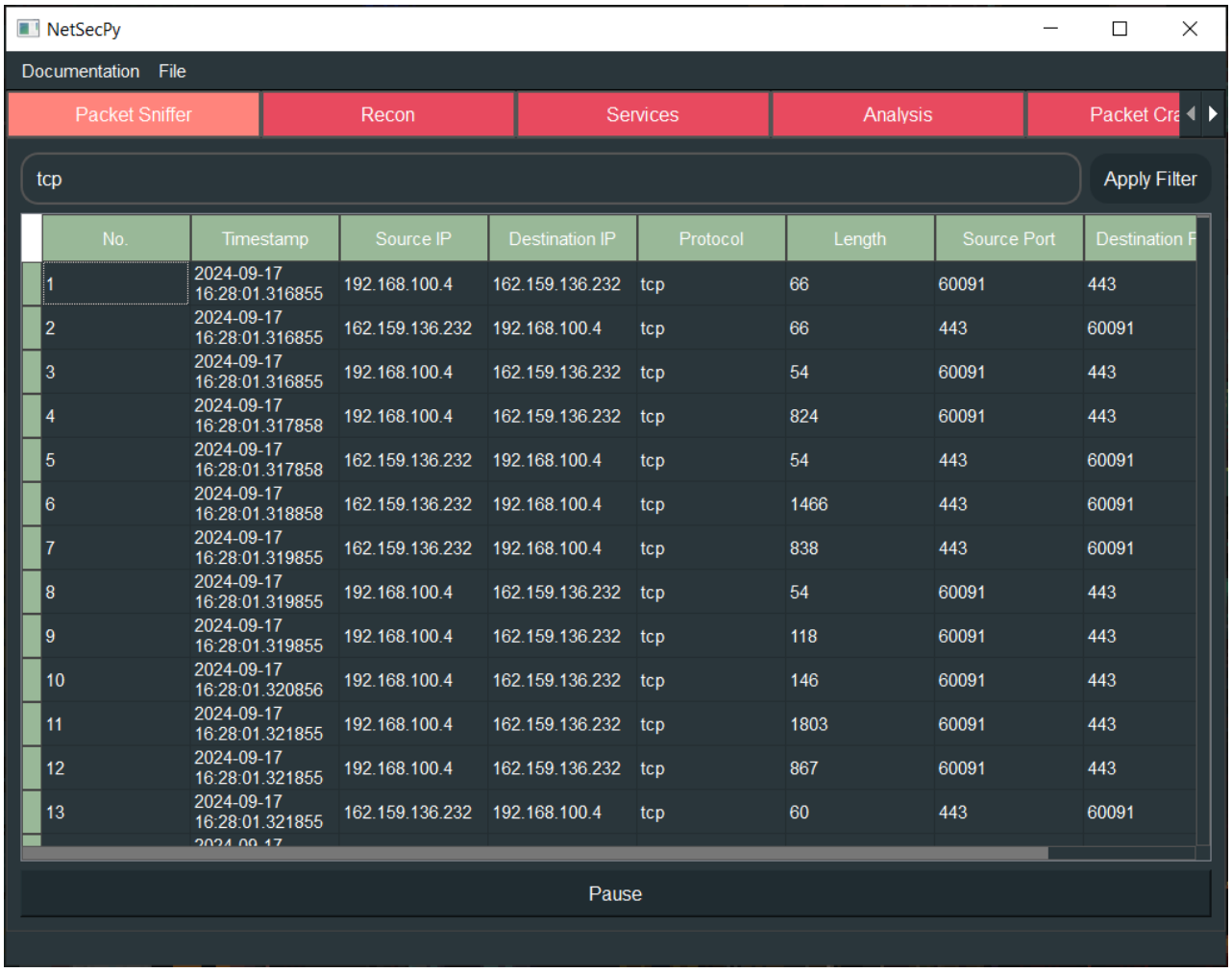


- **Système de Filtrage** : Les utilisateurs peuvent appliquer des filtres (wireshark display filters) via un champ de texte

Le filtrage affecte deux aspects essentiels :

- **Paquets déjà capturés** : Dès qu'un filtre est appliqué, les paquets précédemment capturés sont réévalués en fonction de ce critère, et seuls ceux qui correspondent au filtre restent visibles.

- **Paquets futurs** : Après l'application du filtre, tous les nouveaux paquets capturés seront automatiquement comparés au filtre actif. Ainsi, seuls les paquets répondant aux critères définis seront affichés, ce qui permet de maintenir une vue actualisée des données pertinentes en temps réel.



Exemple Filtre “tcp”

- **Pause et Reprise de la Capture** :

Un bouton de pause permet de stopper temporairement la capture de sans fermer l'application. Lorsqu'il est en mode pause, le texte du bouton change en "Resume", permettant ainsi de reprendre la capture là où elle s'était arrêtée

- **Exporter au format PCAP :** Permet de sauvegarder les paquets capturés dans un fichier PCAP, compatible avec des outils comme Wireshark.

- **Exporter au format CSV :**Permet de sauvegarder les données de la table en fichier CSV

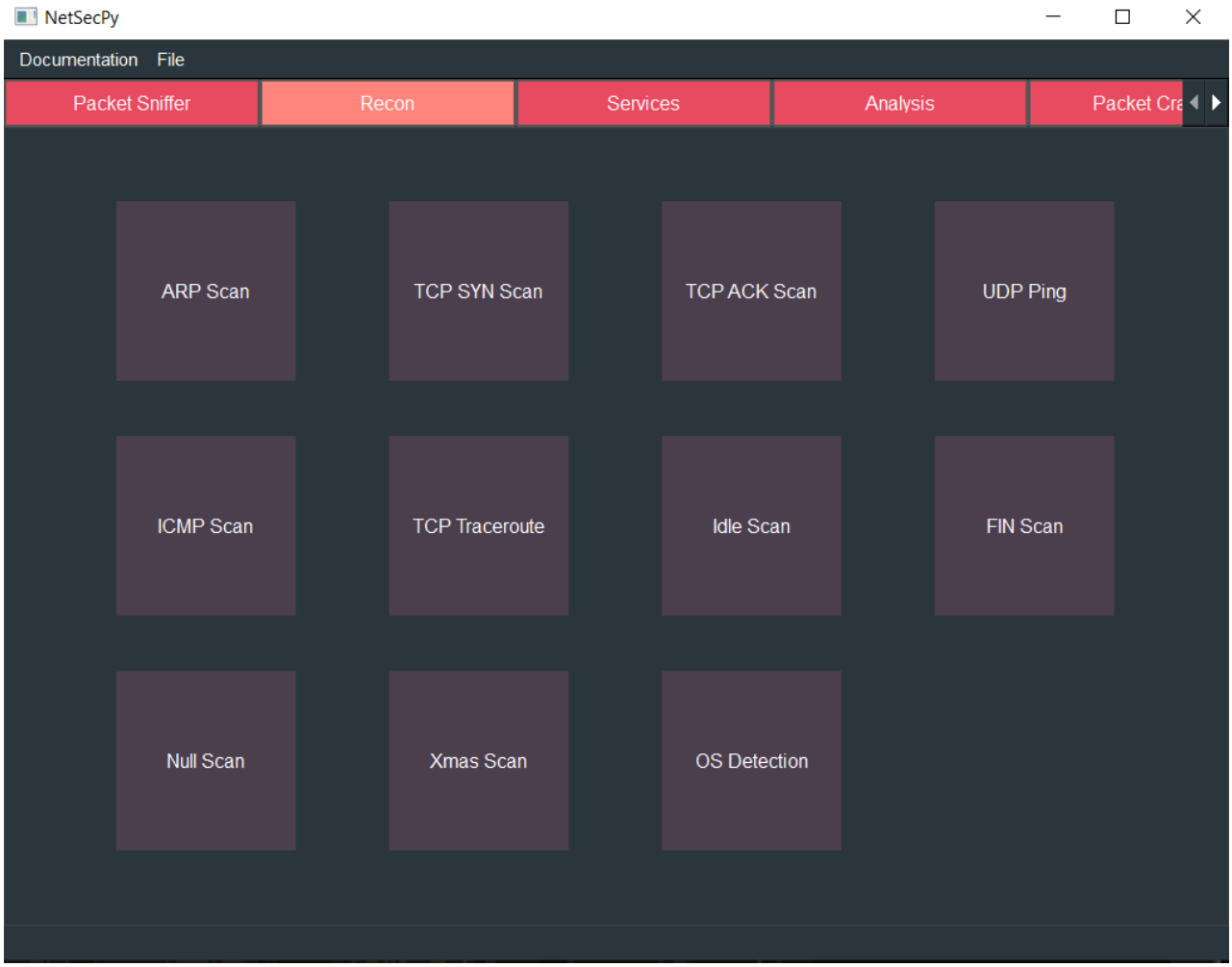
- **Exporter au format JSON :** Permet de sauvegarder les données de la table en fichier JSON, un format léger et lisible, souvent utilisé pour l es échanges de données.

- **Lien vers la Documentation :** Ouvre la documentation de l'application (GitHub) dans un navigateur web.

Note : Les paquets capturés sont stockés dans une variable pour Leur analyse ultérieur

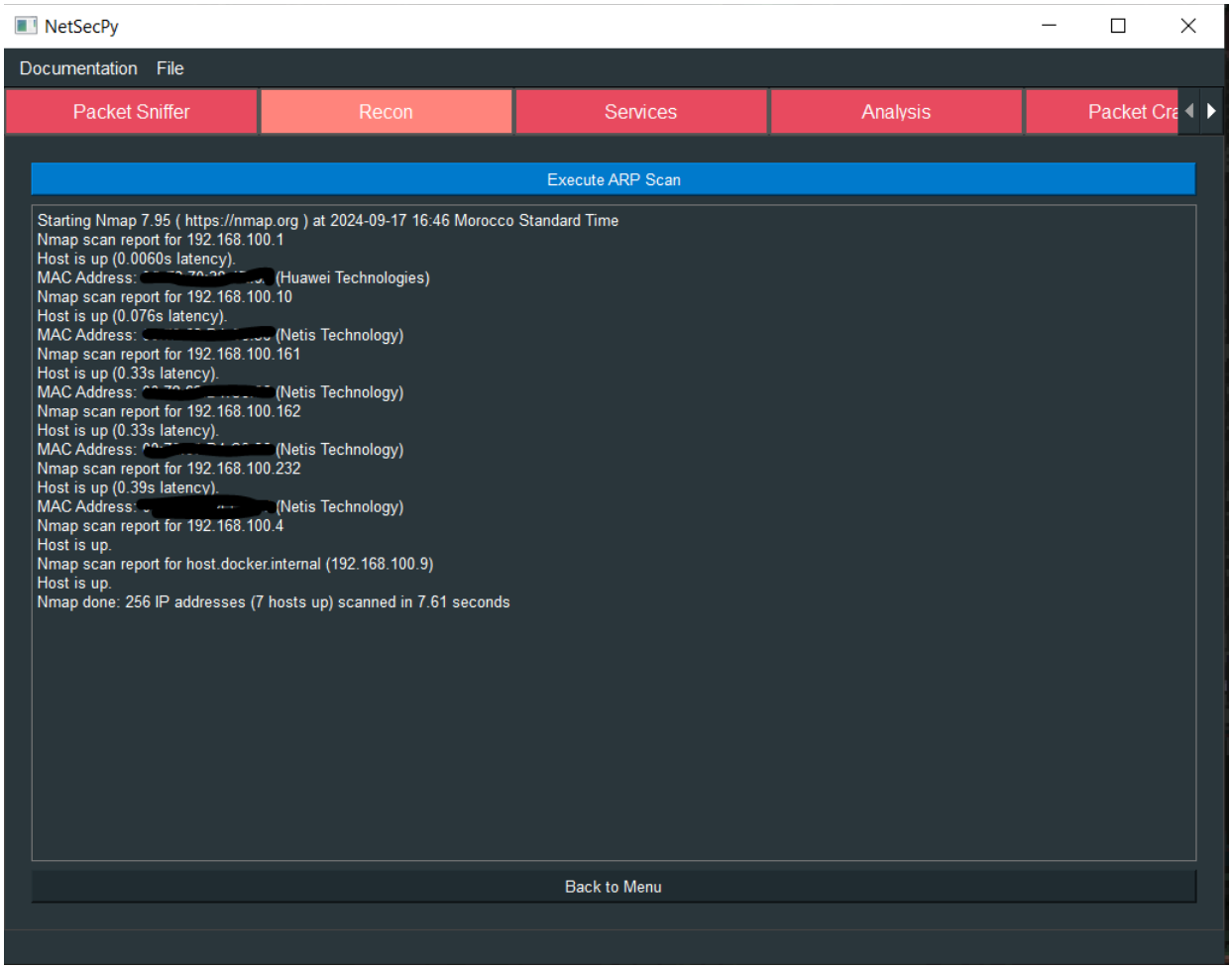
Onglet Recon

L'onglet Recon de NetSecPy est conçu pour fournir une interface intuitive et fonctionnelle pour les opérations de reconnaissance réseau. Cet onglet permet aux utilisateurs d'exécuter divers types de scans pour analyser et collecter des informations sur le réseau. Les types de scans proposés reposent sur des paquets spécialement conçus et des scans basés sur Nmap, offrant ainsi une large gamme d'outils pour évaluer la configuration et la sécurité du réseau cible.

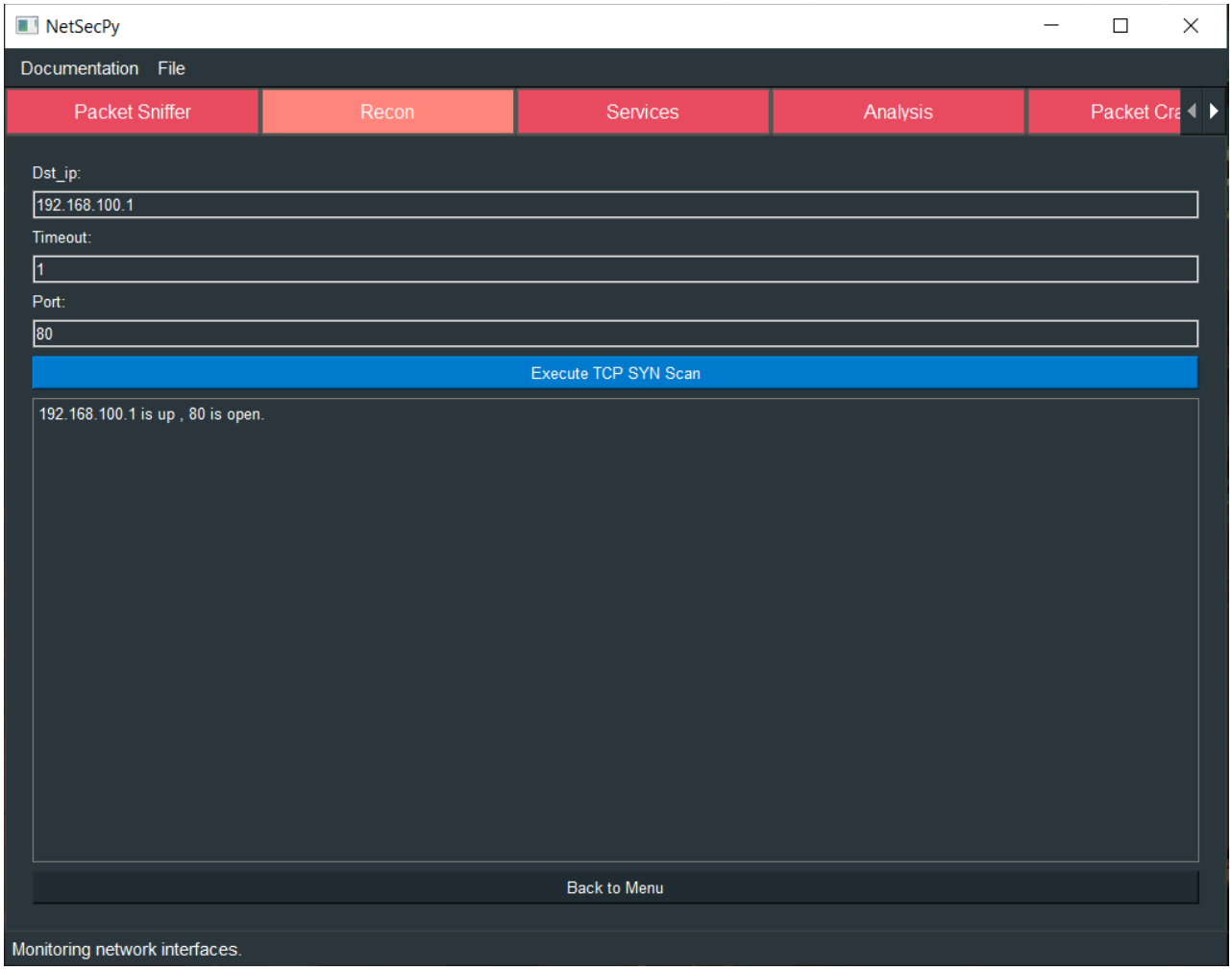


Types de scans :

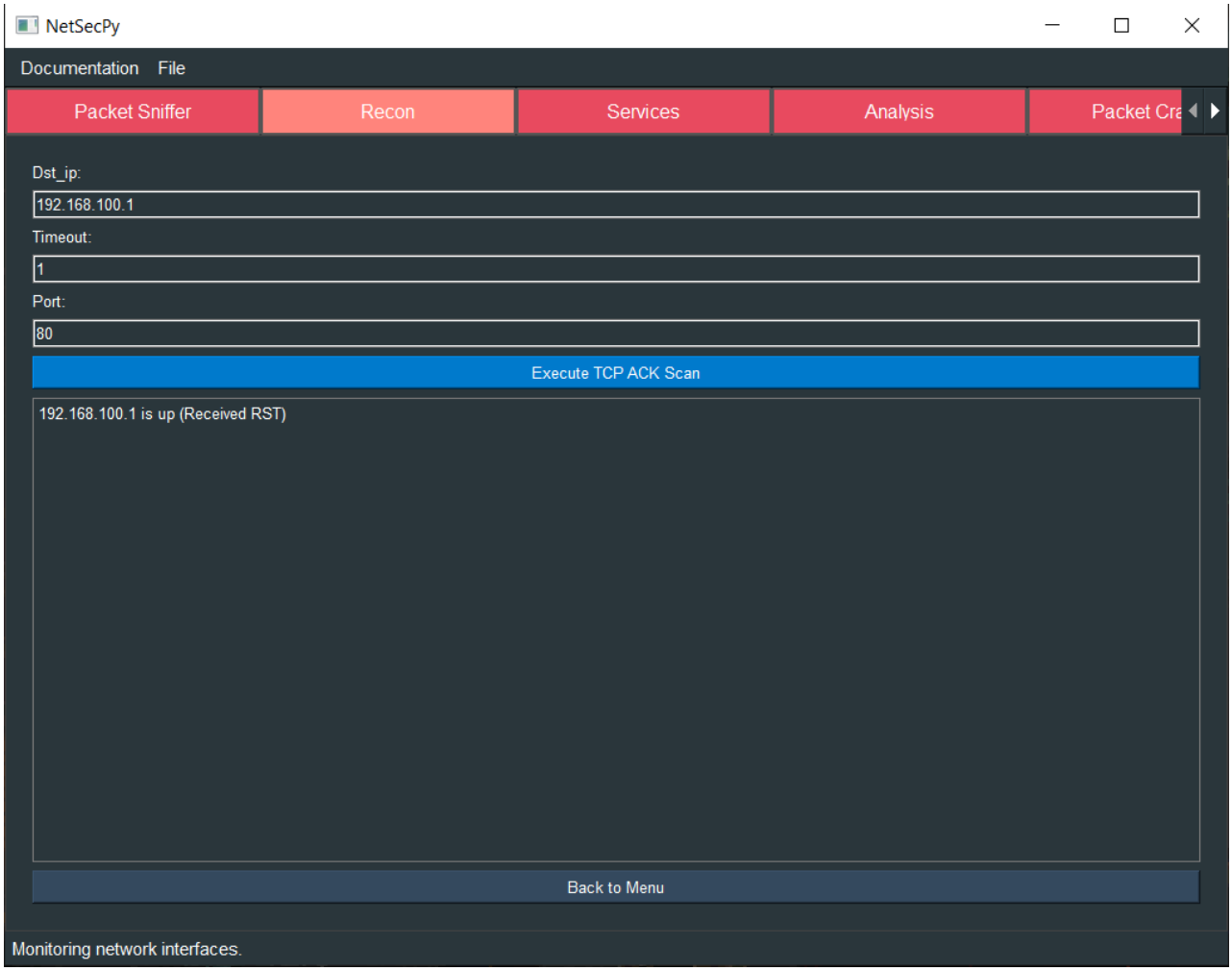
- **ARP Scan** : permet d'identifier les hôtes actifs sur un réseau local. Il envoie des requêtes ARP pour chaque adresse IP sur le réseau cible. Si une machine répond à une requête ARP avec son adresse MAC, elle est considérée comme active.



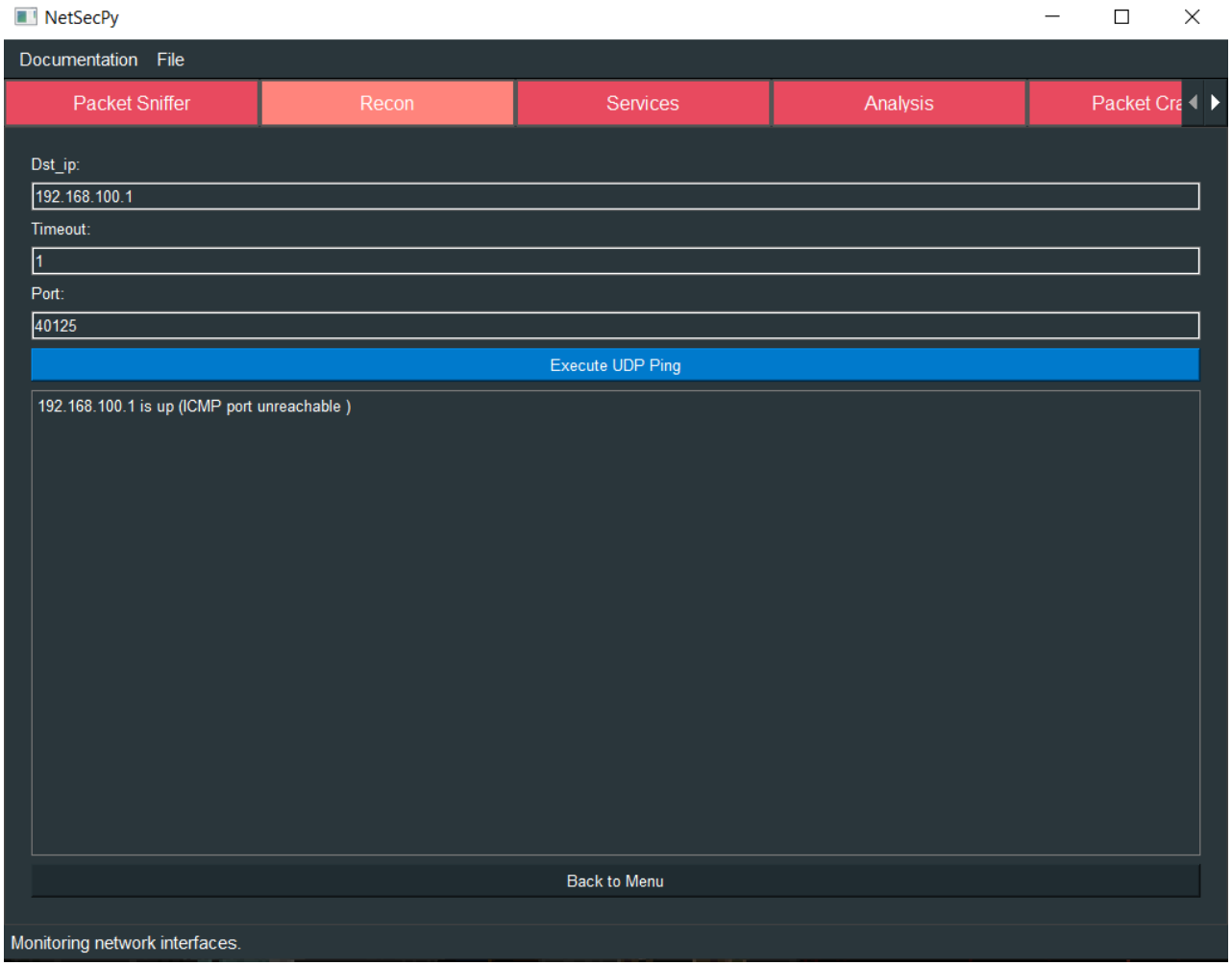
- **TCP SYN Scan** : Cette méthode de scan envoie un paquet TCP avec le drapeau SYN activé vers un port spécifique sur un hôte cible. Si l'hôte répond avec un paquet SYN-ACK, cela signifie que le port est ouvert.
  Si l'hôte répond avec un paquet RST, le port est fermé. Si aucune réponse n'est reçue, cela peut indiquer que l'hôte est injoignable ou que le port est filtré.



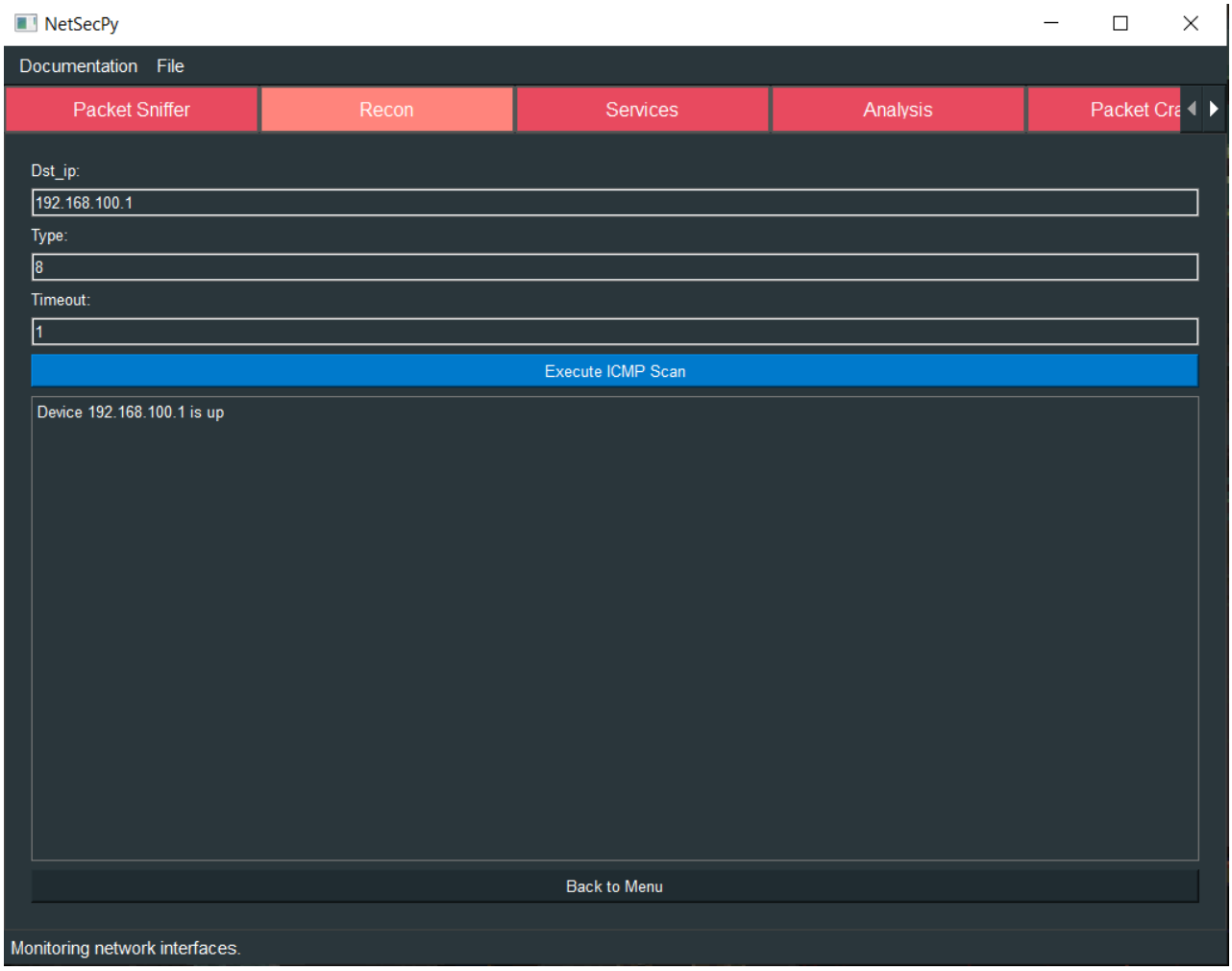
- **TCP ACK Scan** : Ce scan envoie des paquets avec le drapeau ACK activé. S'il reçoit un paquet RST en réponse, cela indique que le port est accessible mais pas nécessairement ouvert. Si aucune réponse n'est reçue, cela peut indiquer que le port est filtré par un pare-feu.



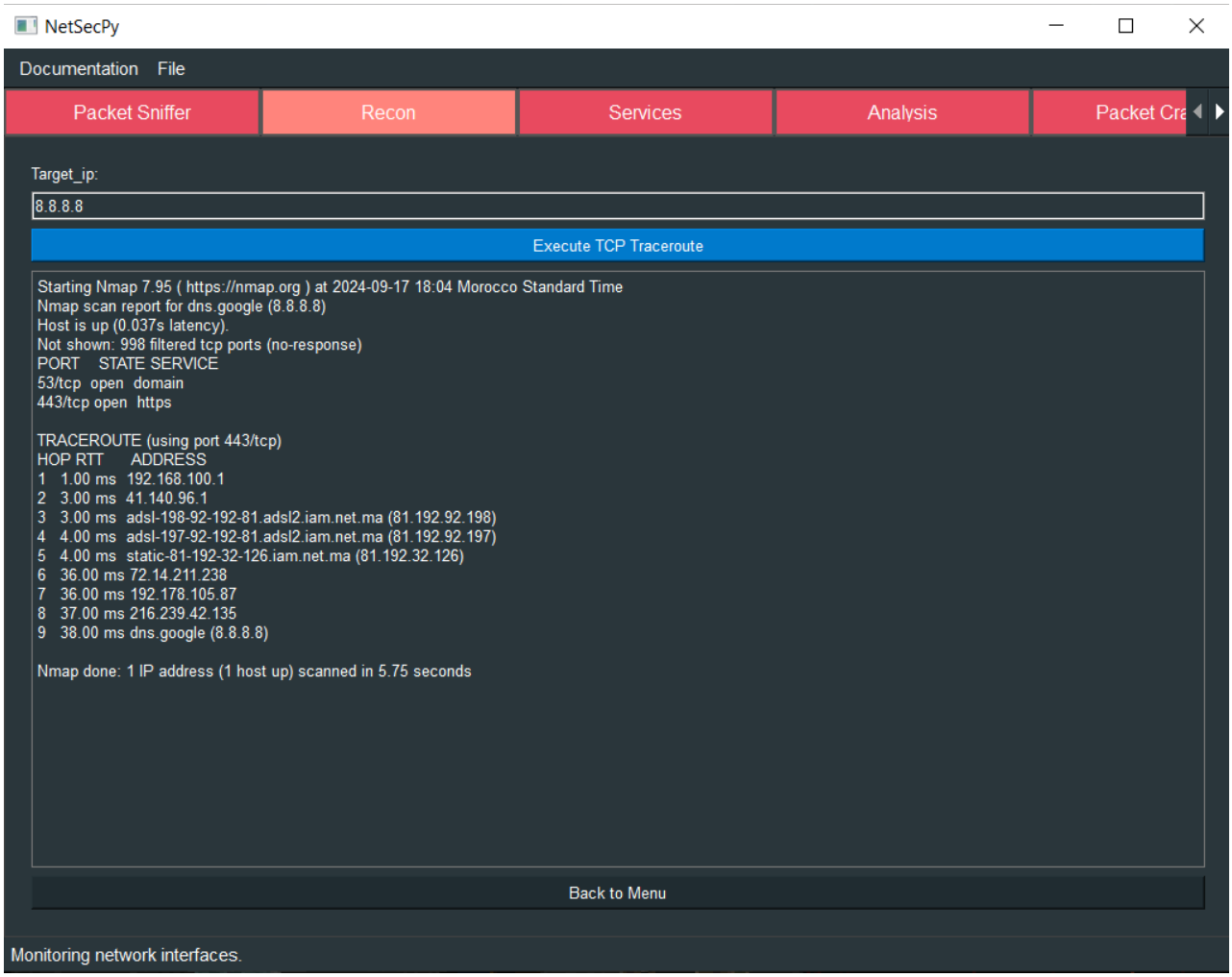
- **UDP Ping** : un paquet UDP est envoyé vers un port spécifique d'un hôte cible. un message ICMP de type 3 indique que le hôte est connecté et que le port est inaccessible, cela montre que l'hôte est actif.



- **ICMP Scan** : Cette méthode envoie un paquet ICMP (comme un ping) à un hôte cible. Si l'hôte répond avec un message ICMP de type 0 (réponse au ping), cela signifie que l'hôte est en ligne. Si un message ICMP de type 3 (destination inaccessible) est reçu, cela signifie que l'hôte est injoignable ou bloqué.



- **Traceroute** : Le traceroute TCP permet de tracer le chemin emprunté par les paquets pour atteindre un hôte cible. En envoyant des paquets TCP avec un TTL (Time to Live) qui augmente progressivement, il est possible d'identifier chaque routeur ou nœud entre la source et la destination.



- **Idle Scan** : Ce scan exploite un hôte "zombie" qui ne génère pas de réseau actif. En manipulant les numéros d'identification d'un zombie, il est possible de déterminer si un port sur une cible est ouvert ou fermé, tout en rendant difficile l'identification de la machine qui réalise réellement le scan

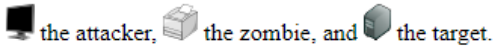
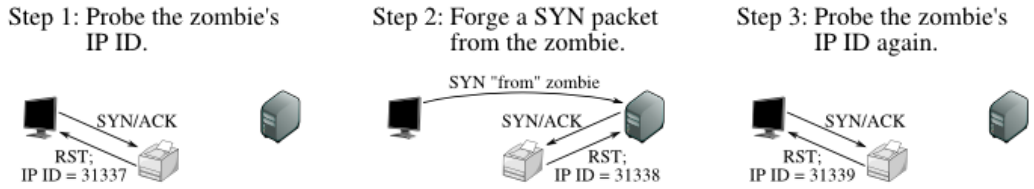


Figure 5.6. Idle scan of an open port

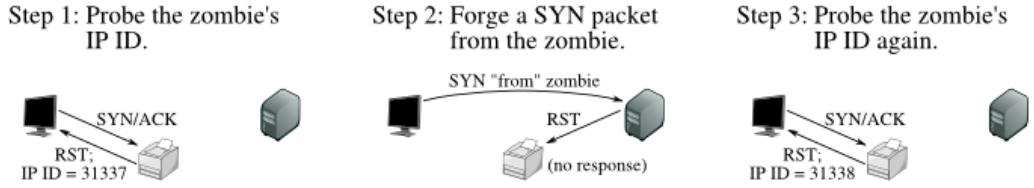


The attacker sends a SYN/ACK to the zombie. The zombie, not expecting the SYN/ACK, sends back a RST, disclosing its IP ID.

The target sends a SYN/ACK in response to the SYN that appears to come from the zombie. The zombie, not expecting it, sends back a RST, incrementing its IP ID in the process.

The zombie's IP ID has increased by 2 since step 1, so the port is open!

Figure 5.7. Idle scan of a closed port

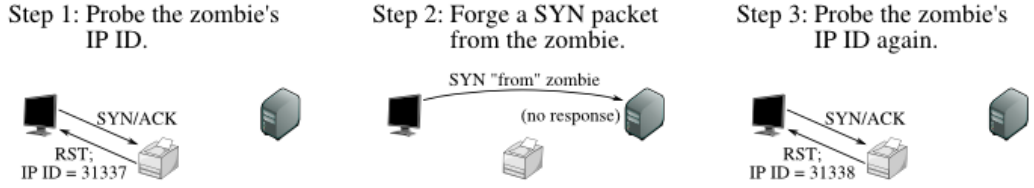


The attacker sends a SYN/ACK to the zombie. The zombie, not expecting the SYN/ACK, sends back a RST, disclosing its IP ID. This step is always the same.

The target sends a RST (the port is closed) in response to the SYN that appears to come from the zombie. The zombie ignores the unsolicited RST, leaving its IP ID unchanged.

The zombie's IP ID has increased by only 1 since step 1, so the port is not open.

Figure 5.8. Idle scan of a filtered port

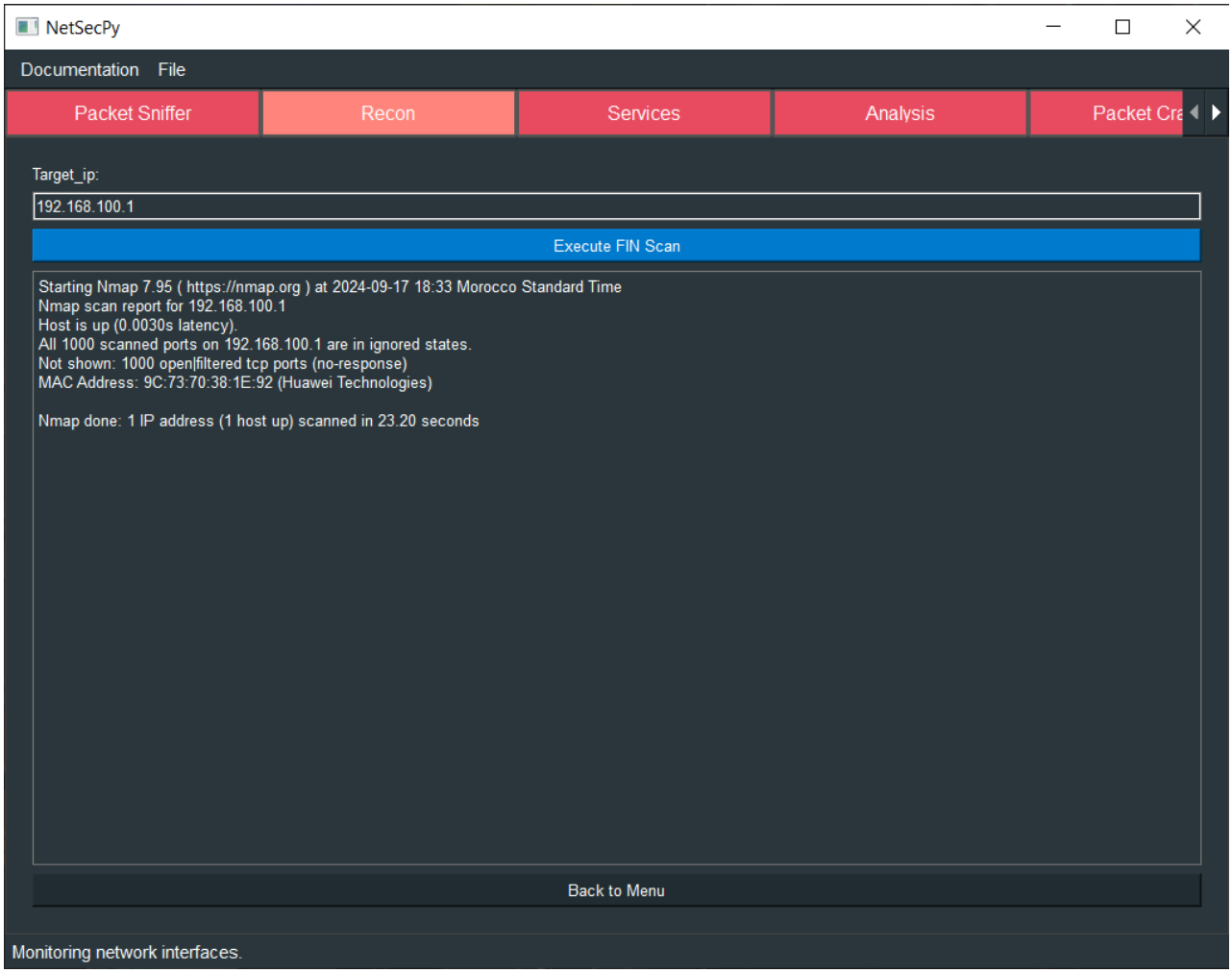


Just as in the other two cases, the attacker sends a SYN/ACK to the zombie. The zombie discloses its IP ID.

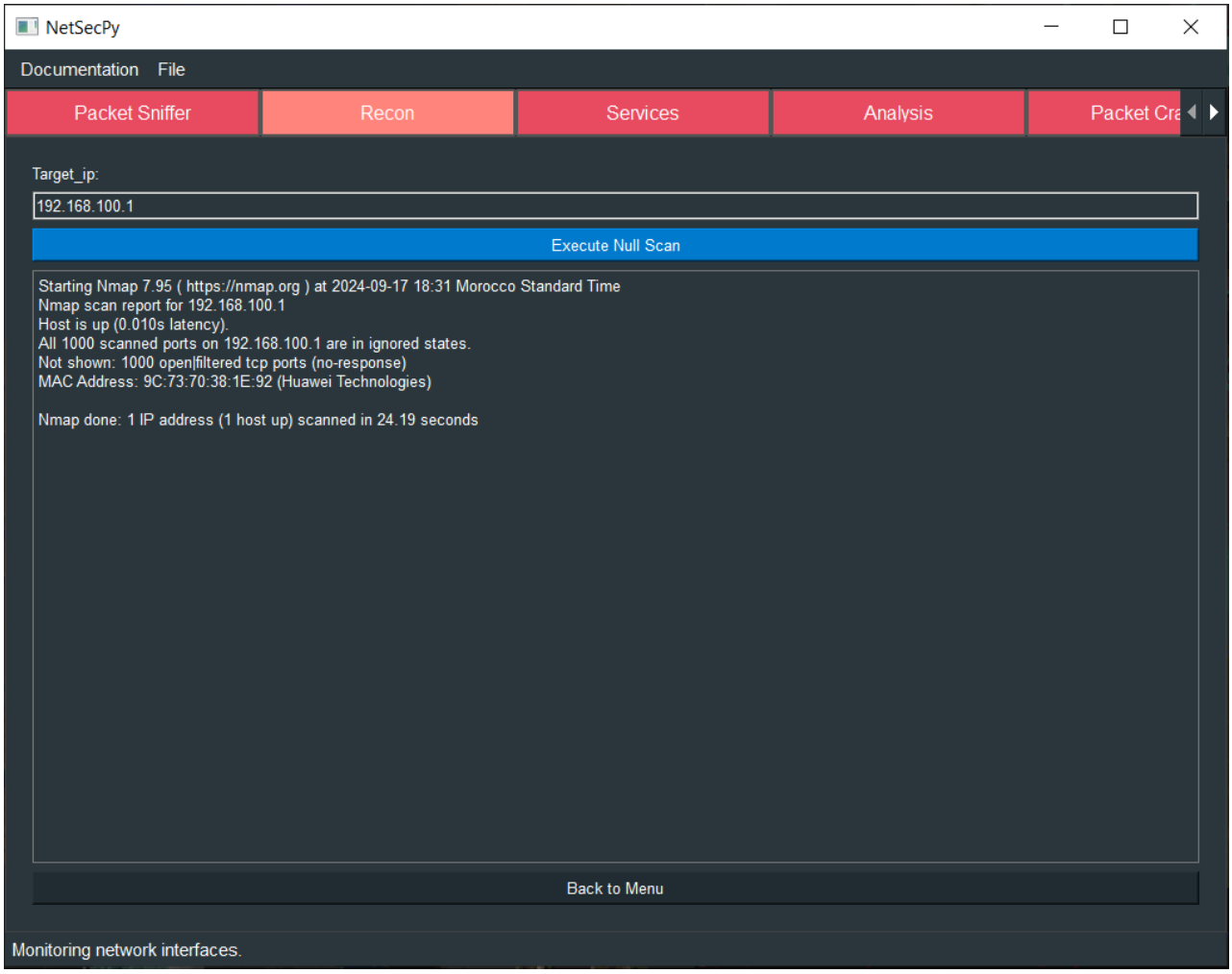
The target, obstinately filtering its port, ignores the SYN that appears to come from the zombie. The zombie, unaware that anything has happened, does not increment its IP ID.

The zombie's IP ID has increased by only 1 since step 1, so the port is not open. From the attacker's point of view this filtered port is indistinguishable from a closed port.

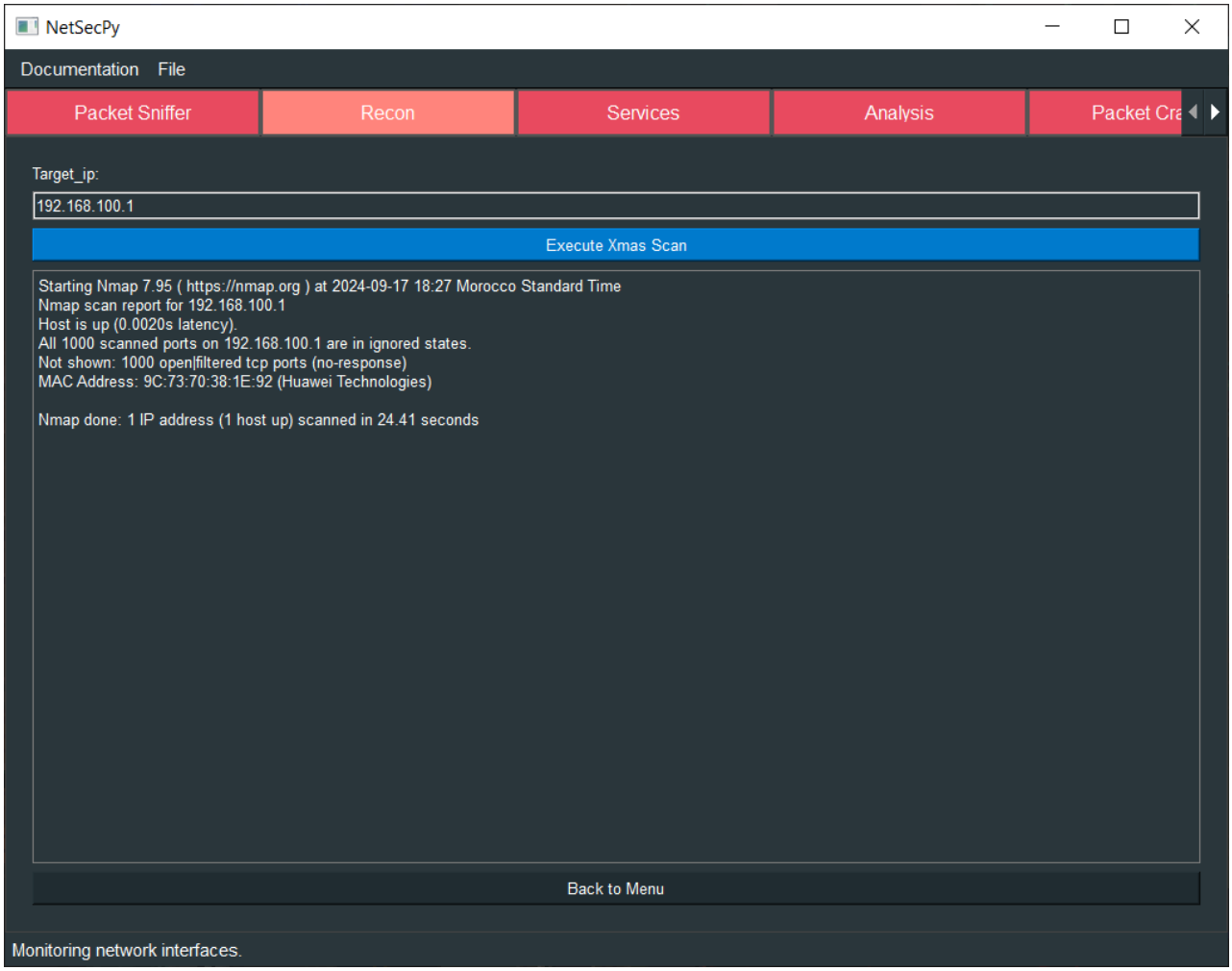
- **FIN Scan** : Le scan FIN envoie des paquets avec le drapeau FIN activé vers les ports cibles. Si un port est fermé, l'hôte répondra avec un paquet RST. Si le port est ouvert, il ne répondra pas. Ce type de scan est souvent utilisé pour éviter d'être détecté par des pare-feu ou systèmes de détection d'intrusions.



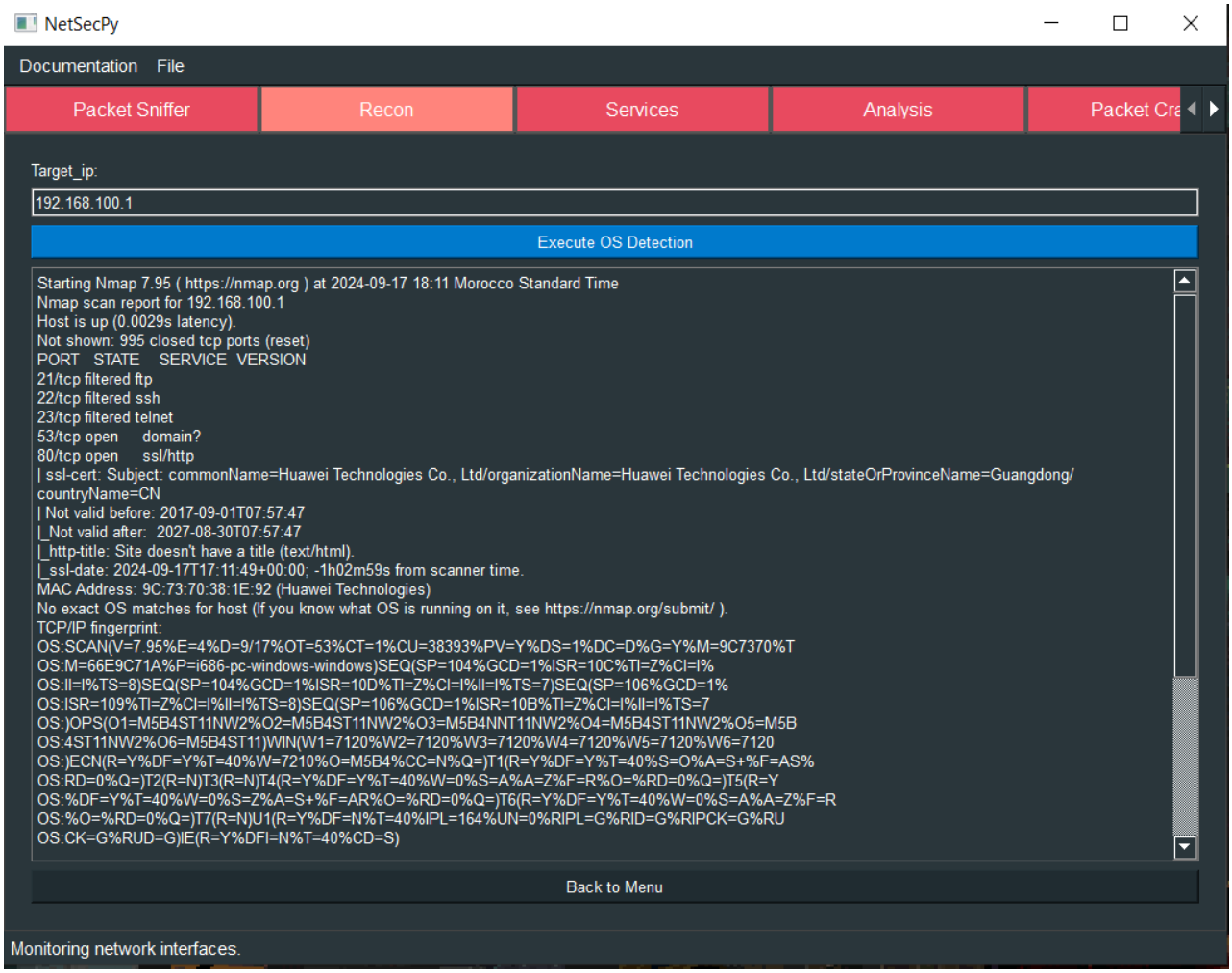
- **Null Scan** : Ce scan envoie des paquets sans aucun drapeau activé (aucun indicateur SYN, FIN, ou ACK). Si un port est fermé, l'hôte cible répondra avec un paquet RST. Si le port est ouvert, aucune réponse n'est reçue. Cela permet d'identifier les ports ouverts sans trop attirer l'attention.



- **Xmas Scan** : Détecte les ports ouverts en envoyant des paquets avec des drapeaux FIN, PSH, et URG.



- **OS Detection** : Ce scan essaie de détecter le système d'exploitation utilisé par un hôte en analysant les caractéristiques des paquets TCP/IP (TTL, window size, TCP options) ,Les réponses de la cible sont comparées à une base de données contenant des empreintes numériques connues de systèmes d'exploitation , la base de donnée se trouve dans le fichier Nmap\nmap-os-db



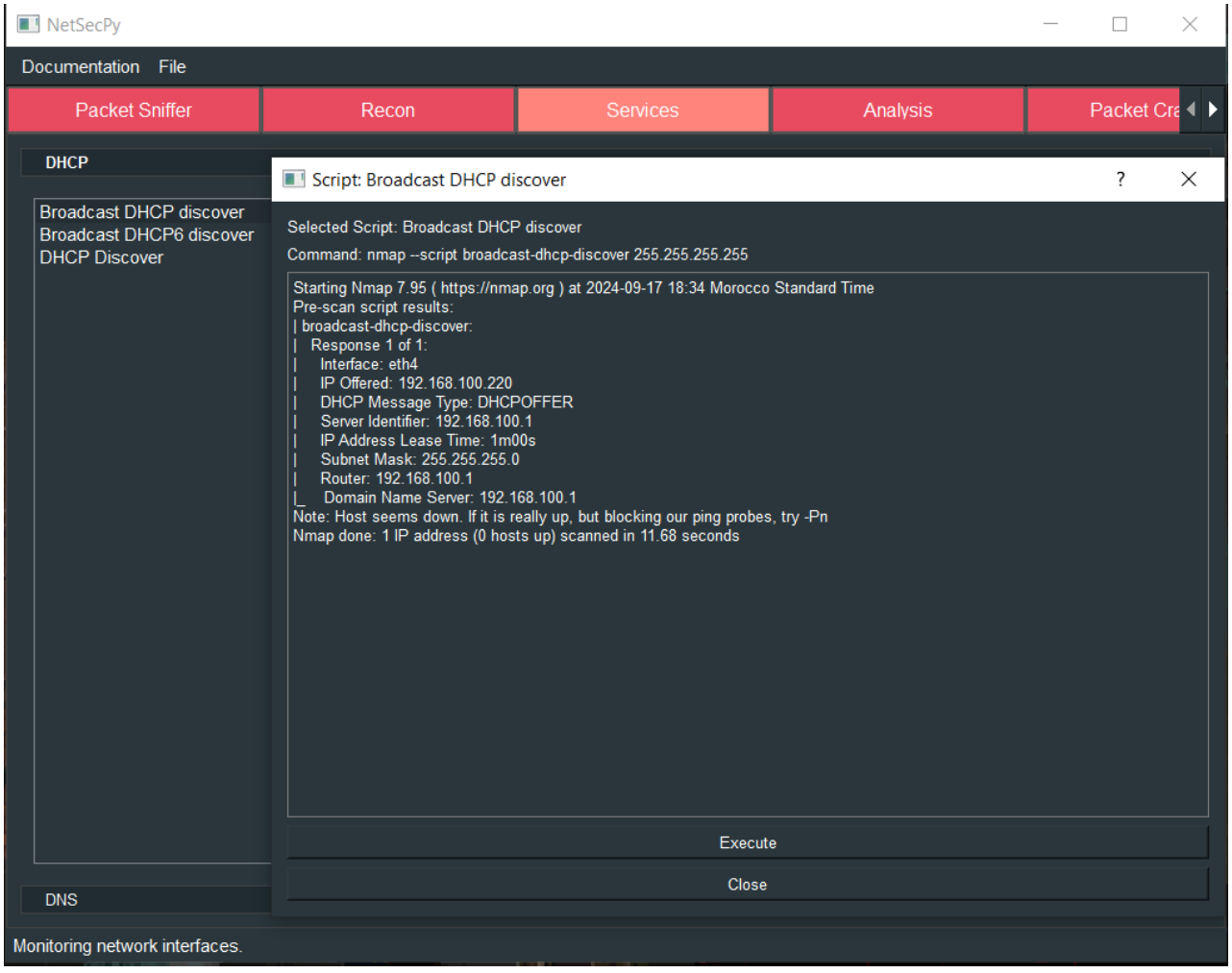
Onglet Services

L'onglet "Services" de NetSecPy offre une interface dédiée à la gestion et à l'exécution des scripts associés à divers services réseau. Il permet aux utilisateurs de sélectionner et d'exécuter des scripts spécifiques pour analyser ou interagir avec des services tels que DHCP et DNS. En utilisant un affichage sous forme d'onglets, les utilisateurs peuvent facilement naviguer entre les différents services, choisir les scripts à exécuter, et visualiser les résultats directement dans une fenêtre dédiée.

Scans DHCP :

Broadcast DHCP Discover

Objectif : Découvrir les serveurs DHCP disponibles sur le réseau local.
Fonctionnement : Ce scan envoie un message de découverte DHCP (DHCP Discover) en broadcast . Les serveurs DHCP qui reçoivent ce message répondent avec leurs informations, permettant de découvrir les serveurs DHCP actifs sur le réseau.



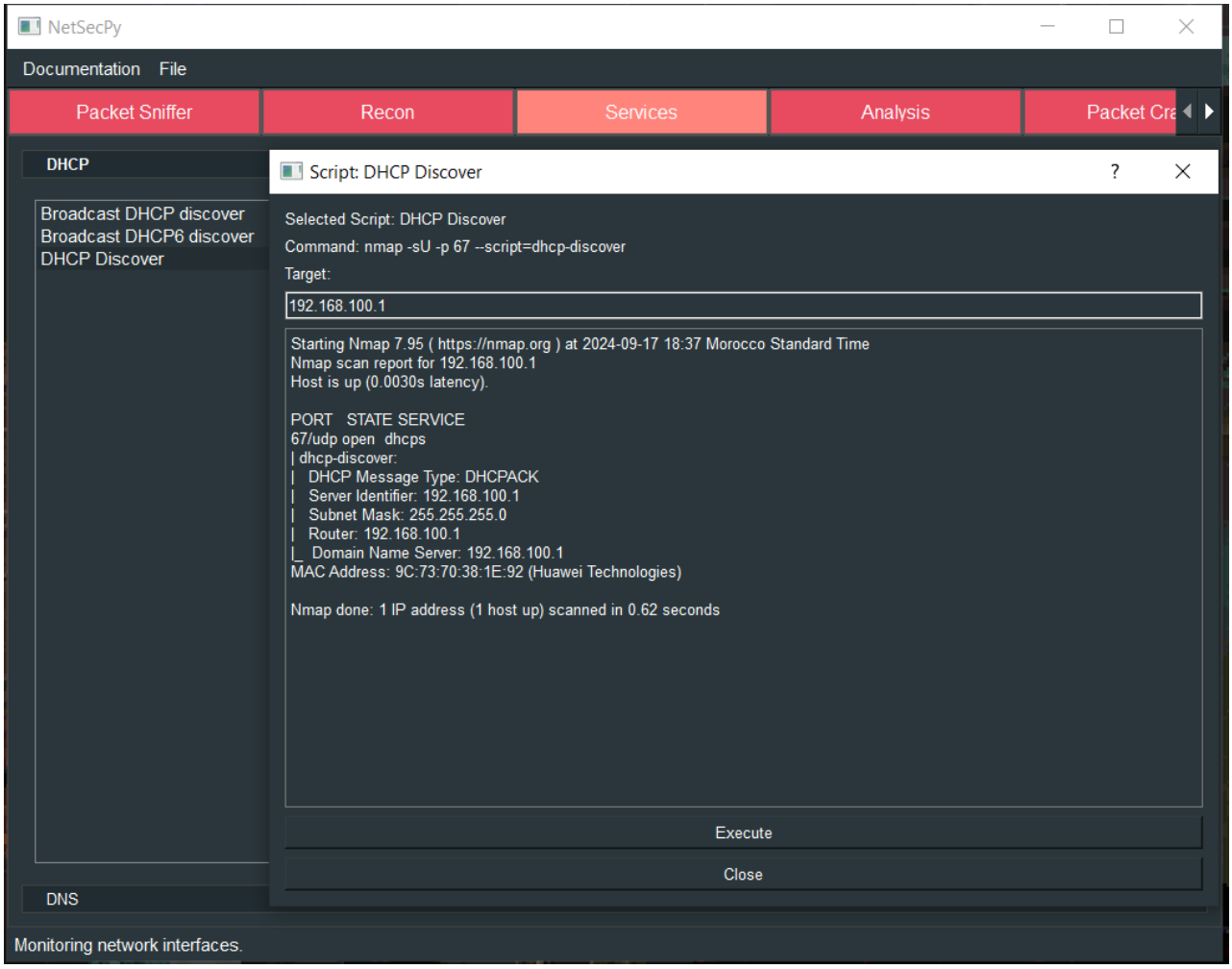
Broadcast DHCP6 Discover

Objectif : Découvrir les serveurs DHCPv6 disponibles sur le réseau.
Fonctionnement : Semblable au scan DHCP pour IPv4, ce scan envoie un message de découverte DHCPv6 en broadcast. Les serveurs DHCPv6 répondent avec des

informations sur leur configuration, ce qui aide à identifier les serveurs DHCPv6 actifs sur le réseau.

DHCP Discover

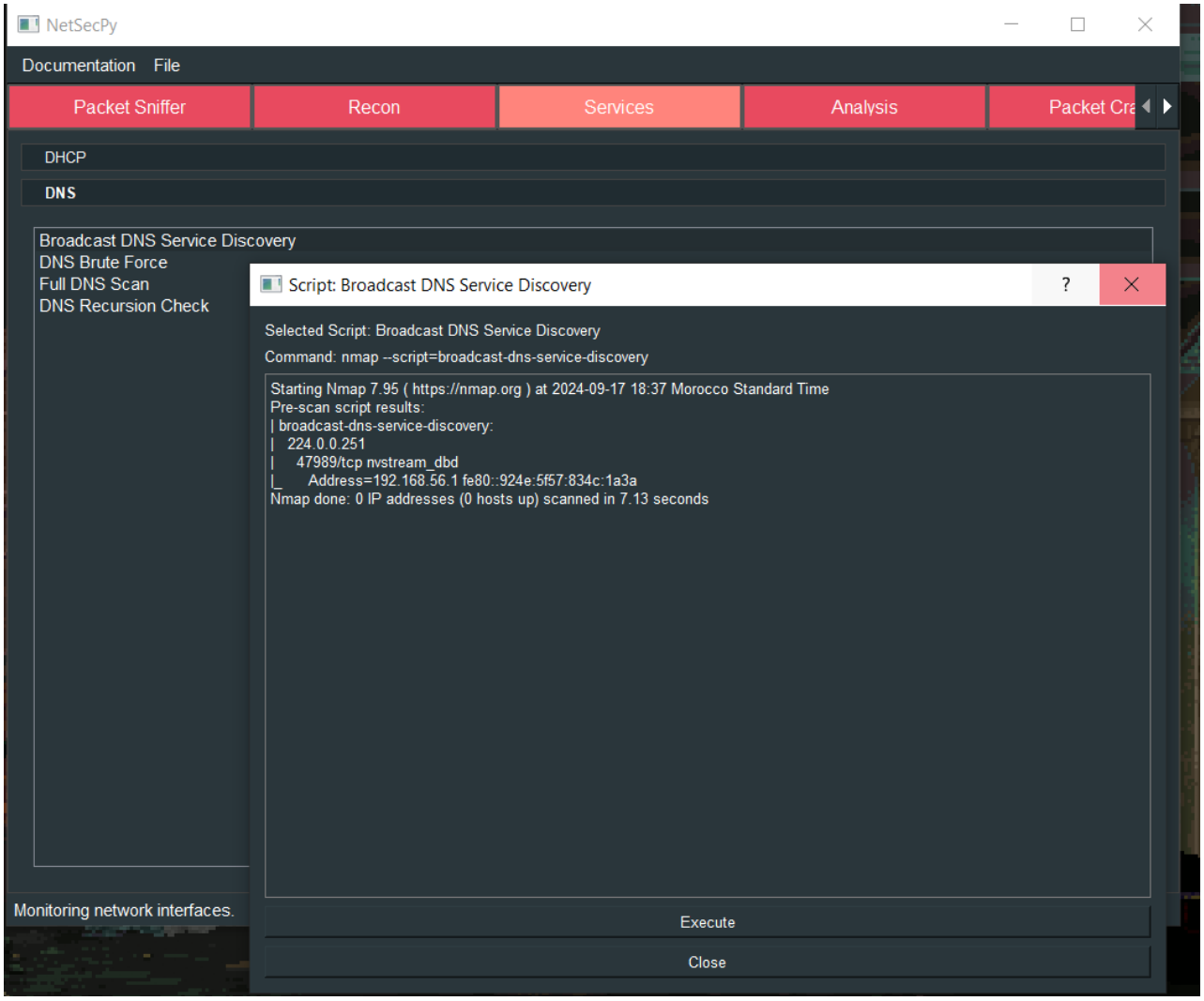
Objectif : Envoie une requête DHCPINFORM à un hôte sur le port UDP 67 pour obtenir tous les paramètres de configuration locaux sans attribuer une nouvelle adresse.



Scans DNS

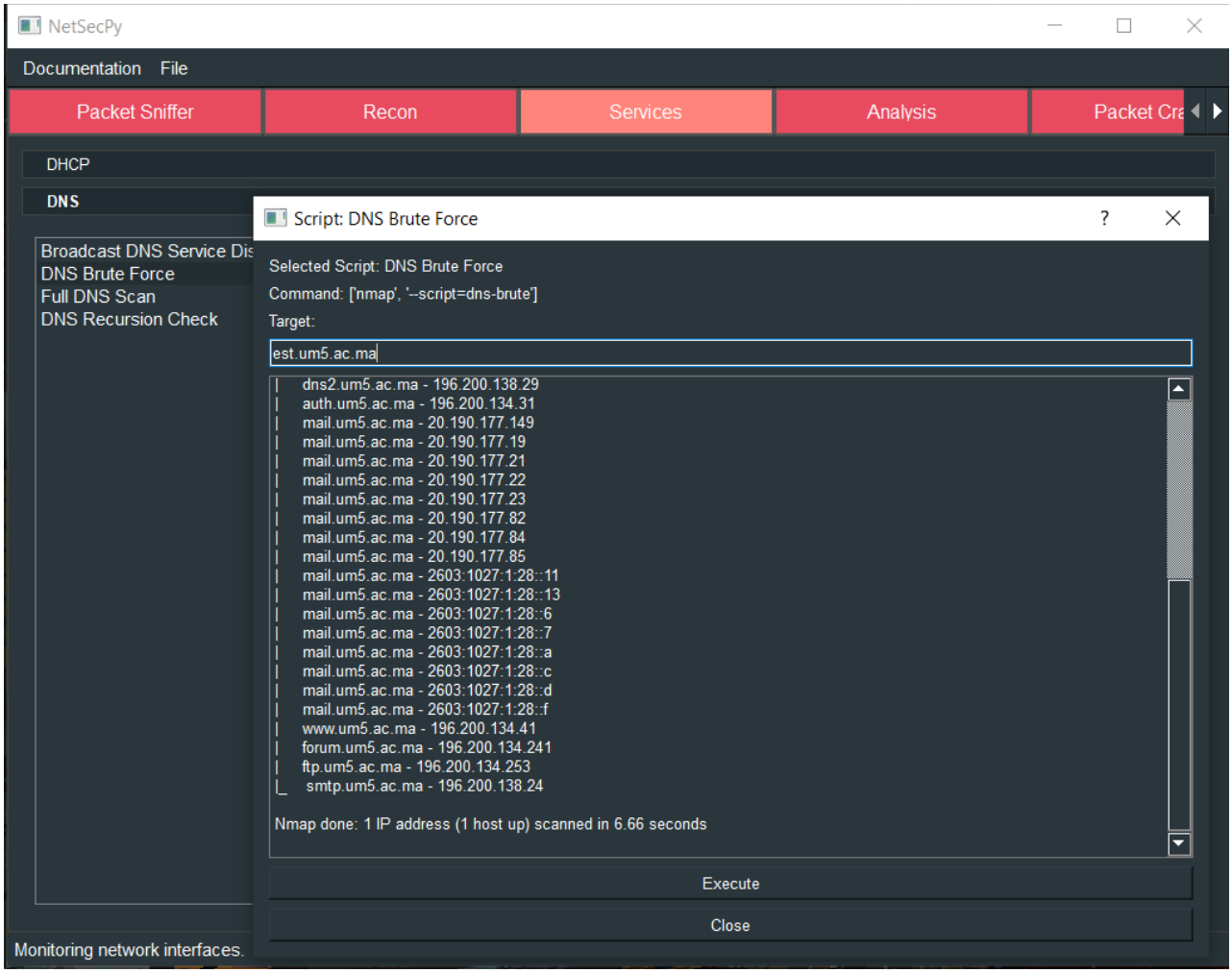
Broadcast DNS Service Discovery

Ce scan utilise une requête DNS en broadcast pour identifier les services DNS sur le réseau local. Les réponses permettent de découvrir les serveurs DNS actifs et leurs informations associées.



DNS Brute Force

Ce scan effectue une attaque de force brute sur les noms de domaine pour identifier les sous-domaines et les noms d'hôtes qui pourraient ne pas être immédiatement visibles dans les réponses DNS standard. Il aide à trouver des noms de domaine cachés ou moins évidents.

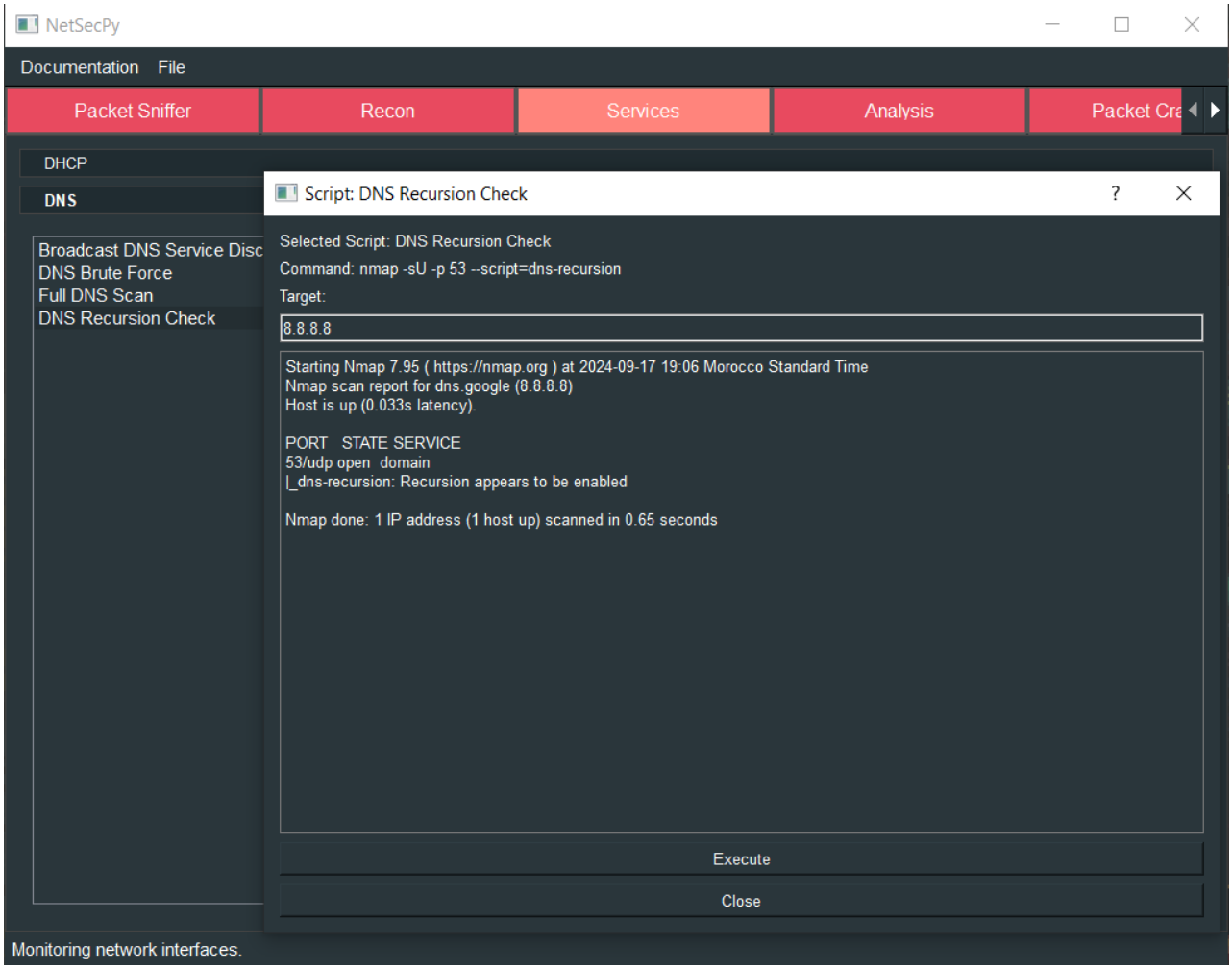


Full DNS Scan

Ce scan envoie des requêtes DNS au port 53 pour collecter des informations sur les différents services DNS disponibles. Il utilise plusieurs scripts Nmap pour obtenir des détails complets sur la configuration DNS d'un hôte.

DNS Recursion Check

Ce scan envoie des requêtes DNS pour vérifier si un serveur DNS est configuré pour effectuer des résolutions récursives. Les serveurs DNS récursifs peuvent résoudre des noms de domaine non seulement pour les clients mais aussi pour d'autres serveurs DNS, ce qui peut être un problème de sécurité s'ils sont exposés publiquement.



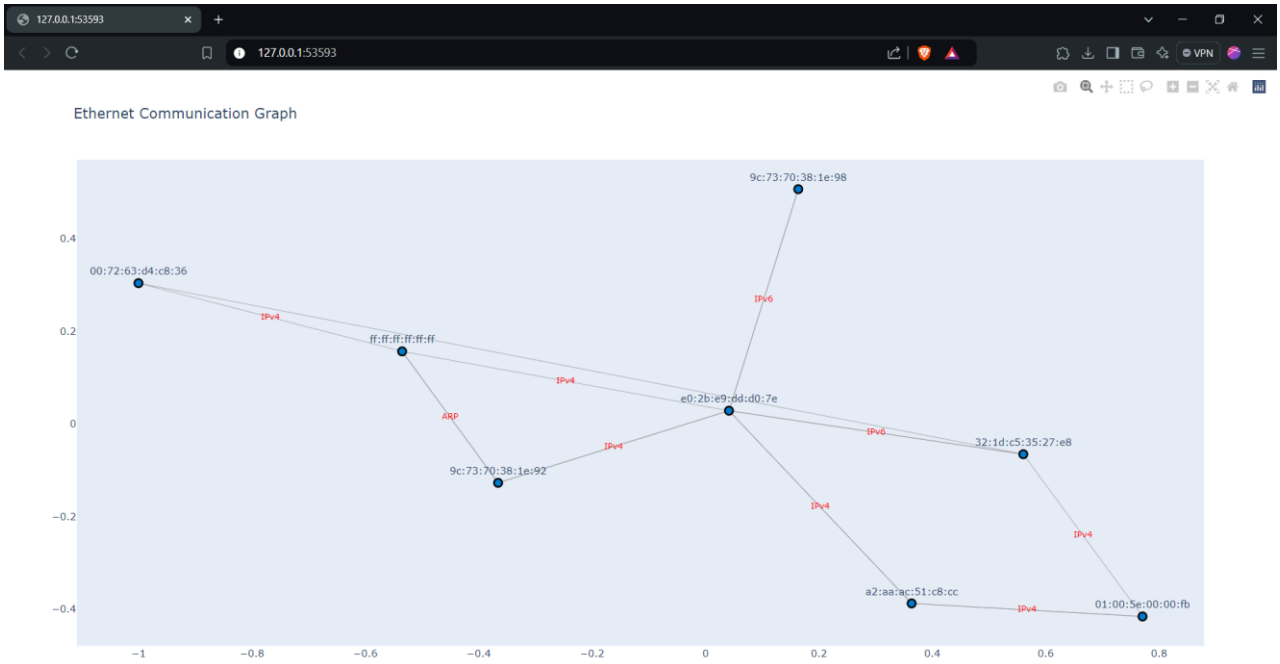
Onglet Analyse :

L'onglet "Analyse" de l’application est conçu pour fournir des outils avancés d'analyse et des données réseau et de sécurité. Cet onglet offre une interface organisée et intuitive pour explorer divers aspects des données réseau et mener des analyses approfondies pour chaque couche des packets

Analyse Ethernet

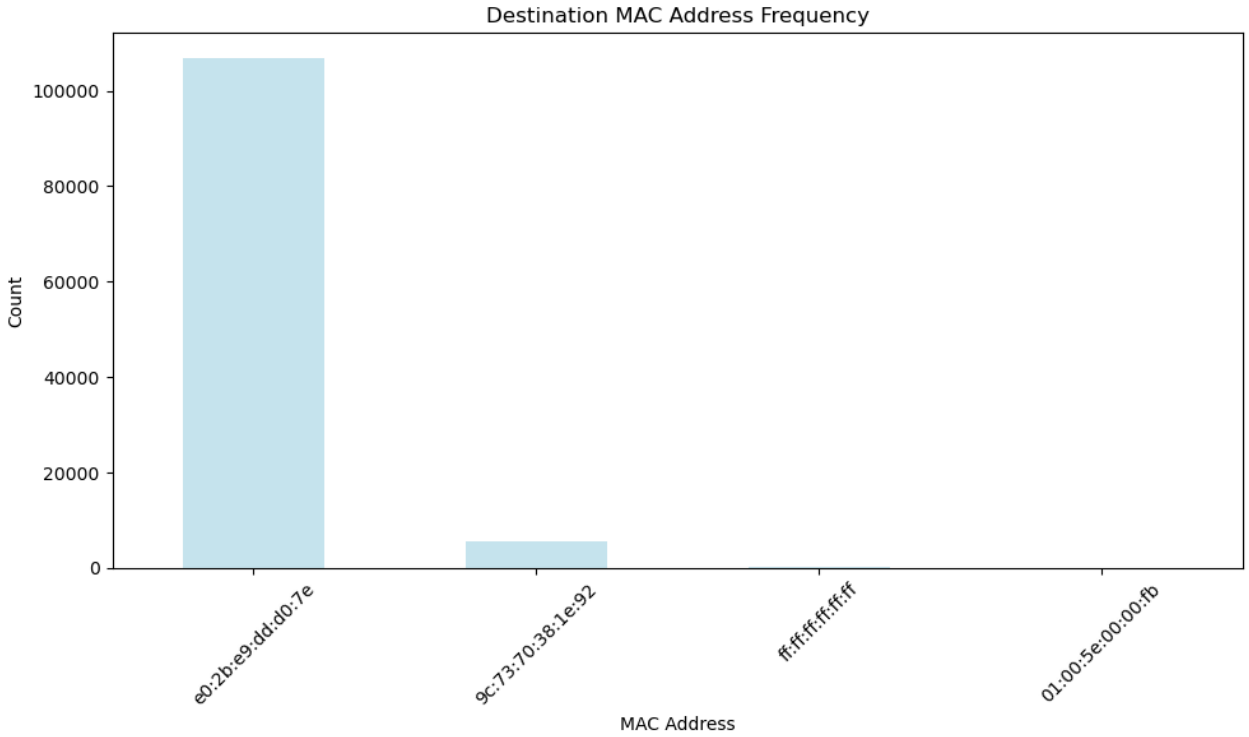
Communication Graph

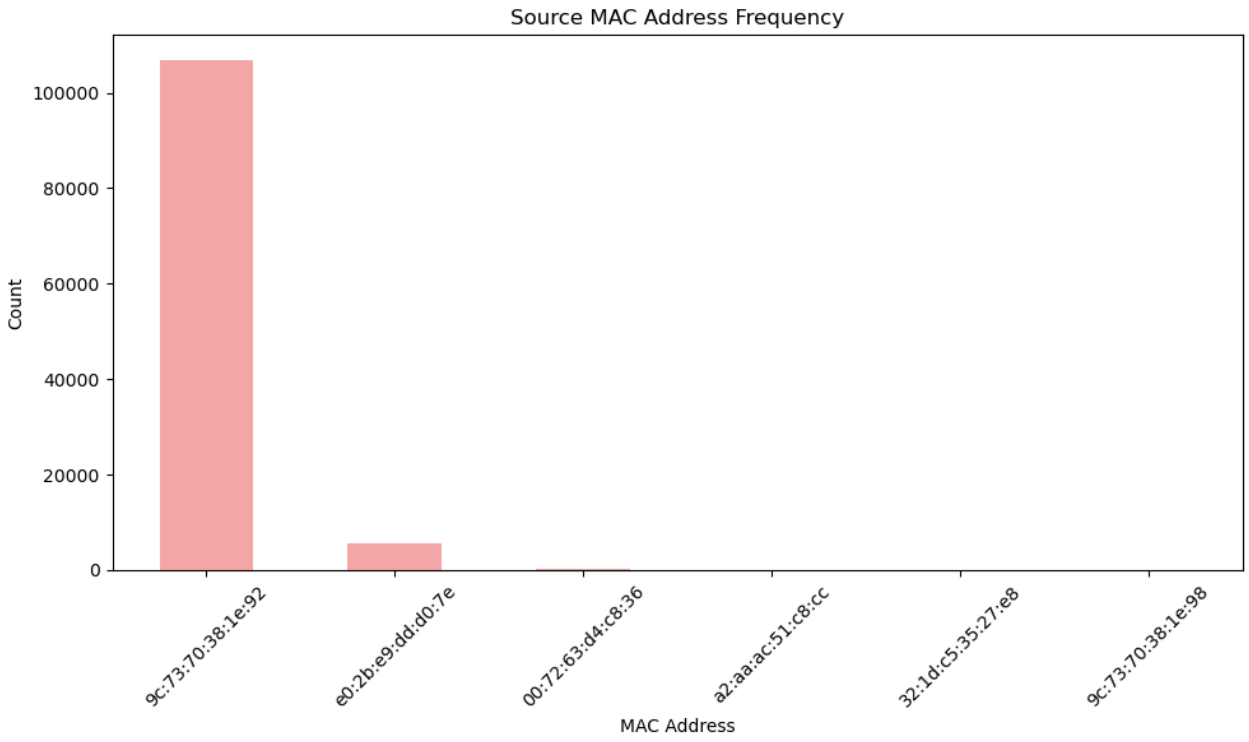
Crée un graphe pour visualiser les connexions entre différentes adresses MAC, facilitant l'identification des interactions entre les périphériques.



MAC Frequency Analysis

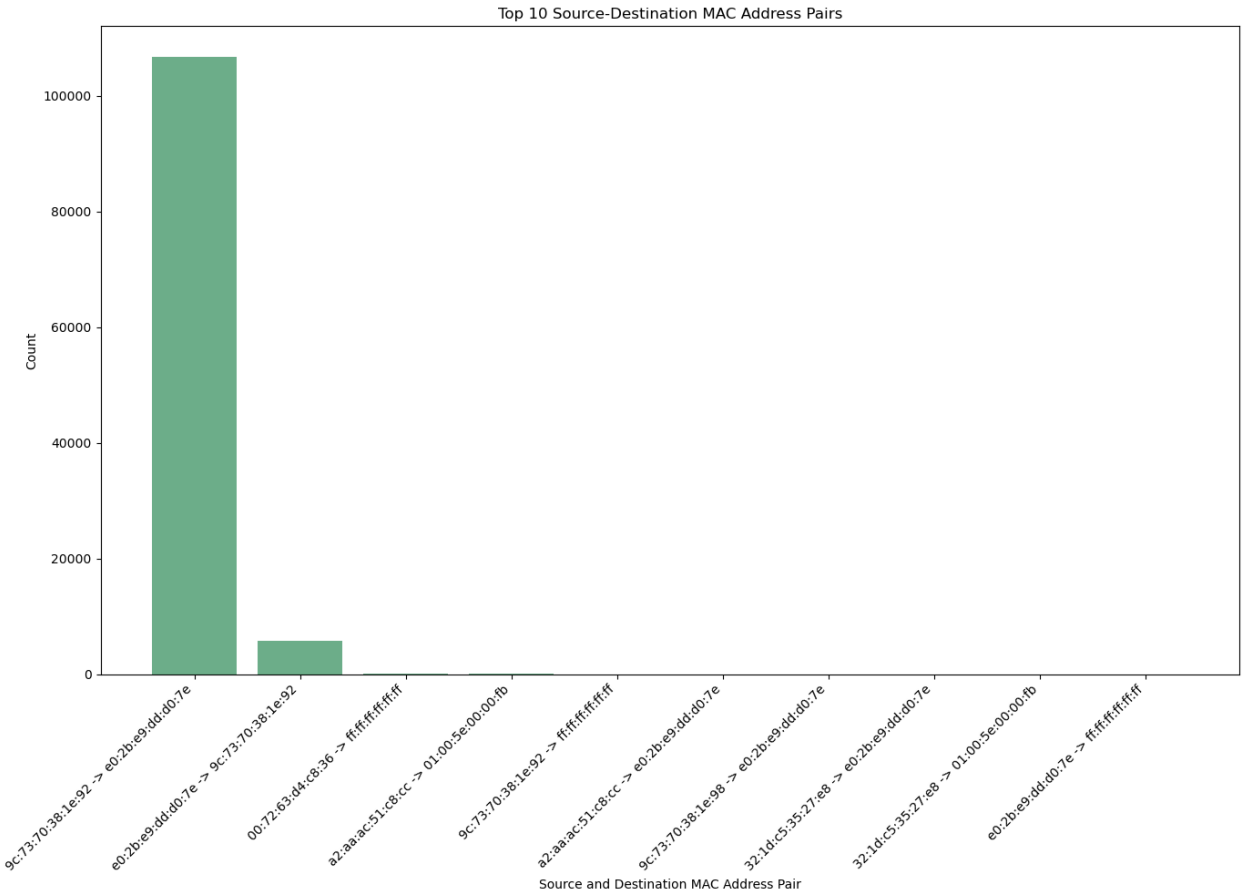
Analyser la fréquence des adresses MAC observées. En calculant combien de fois chaque adresse MAC source et destination apparaît dans les paquets capturés





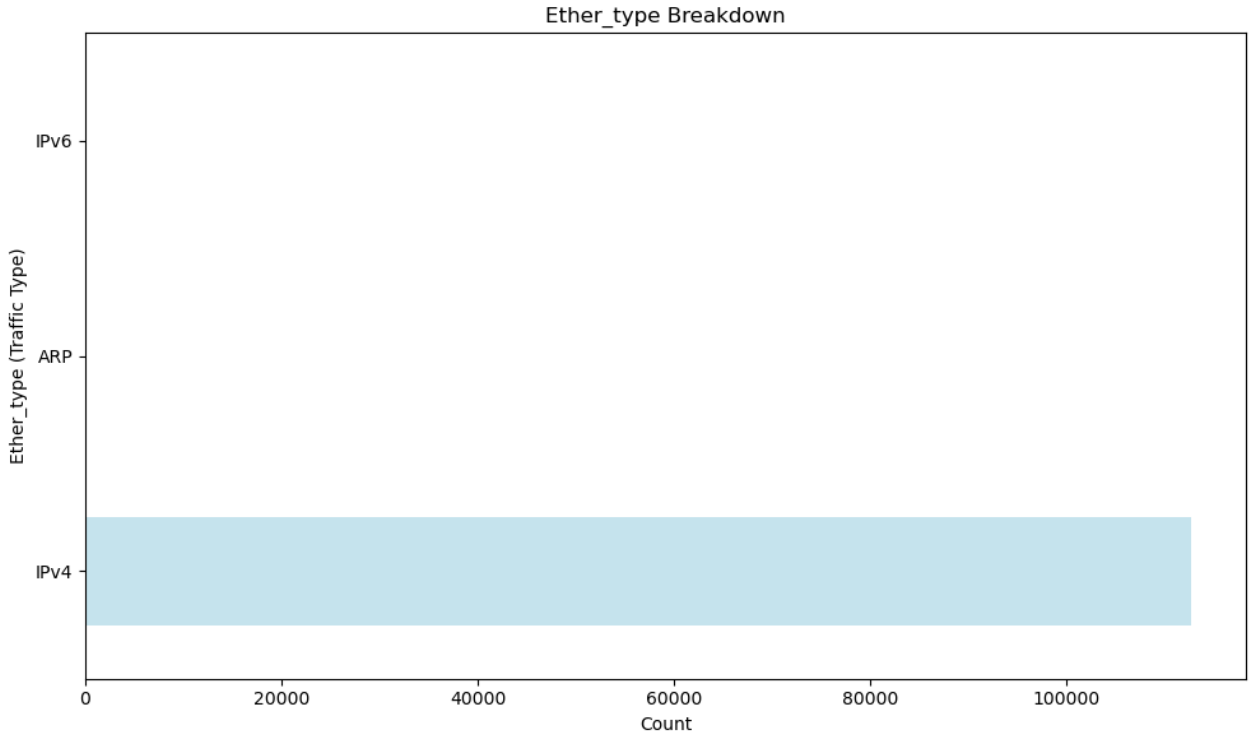
Mac Pairs Analysis

Examine les interactions entre les paires d'adresses MAC



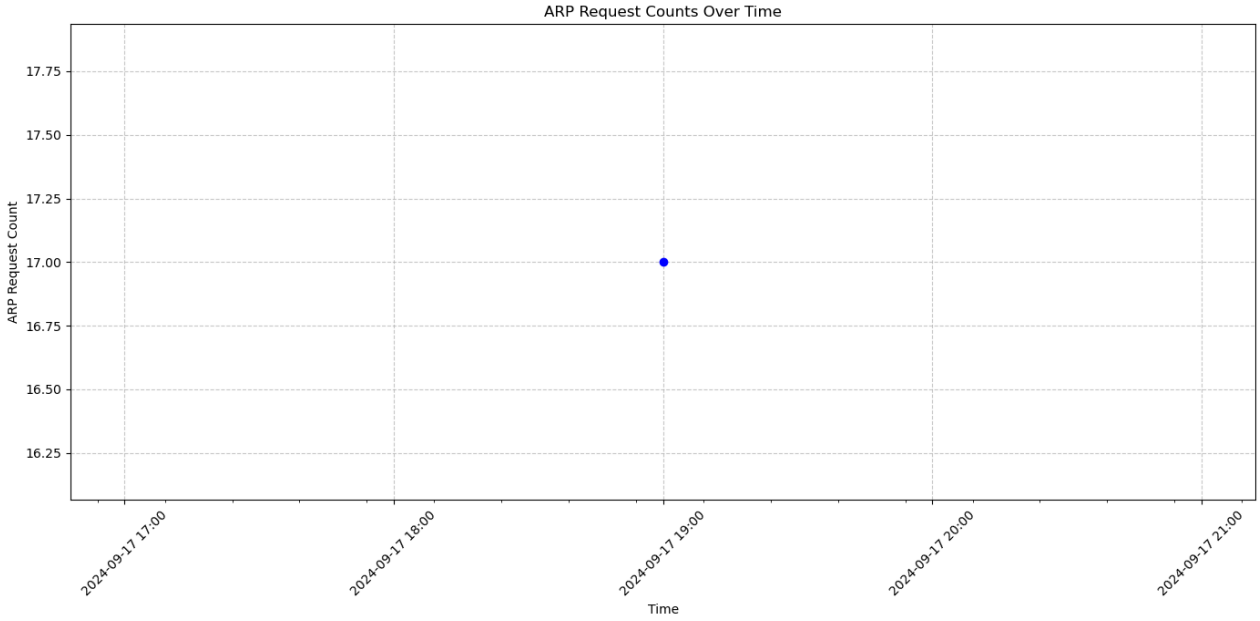
Analyze Ethernet Types

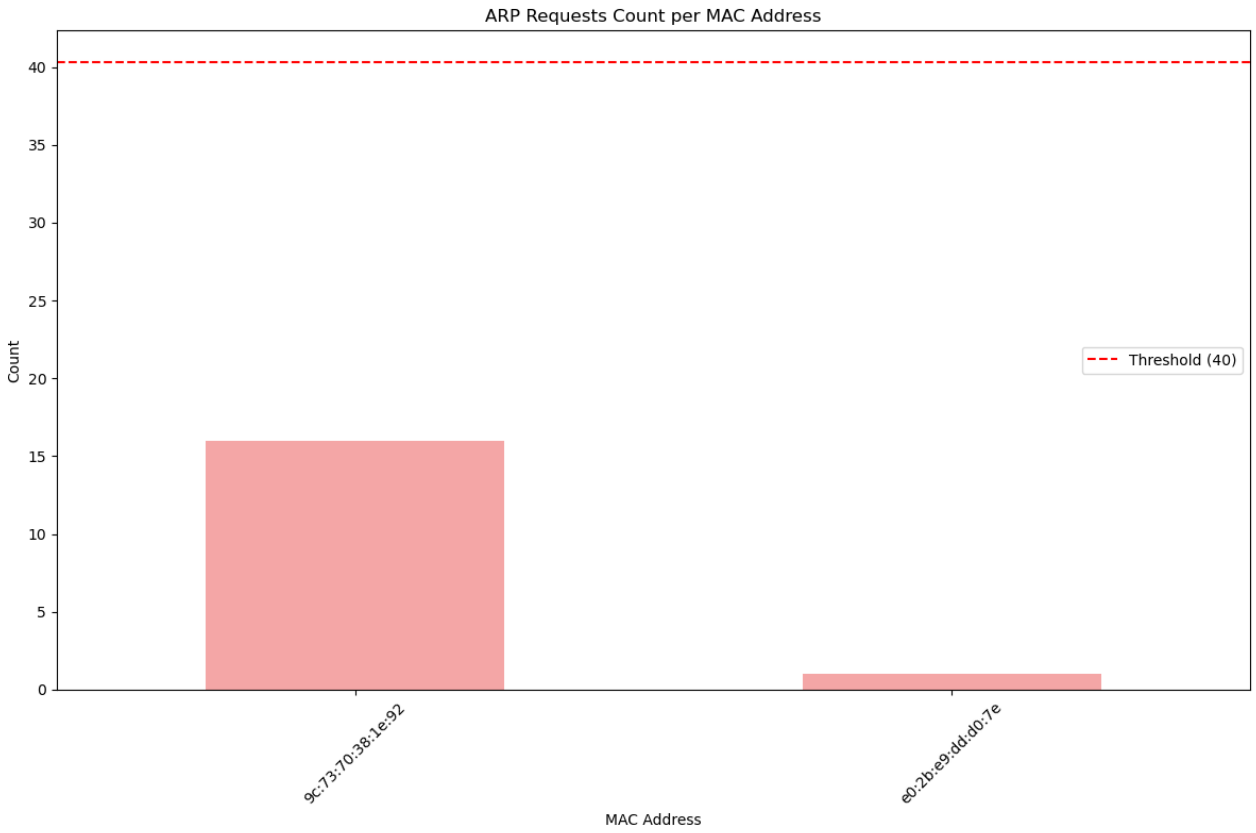
Classifie les trames Ethernet par type (par exemple, ARP, IP) pour comprendre les types de trafic sur le réseau.



Detect ARP Scanning

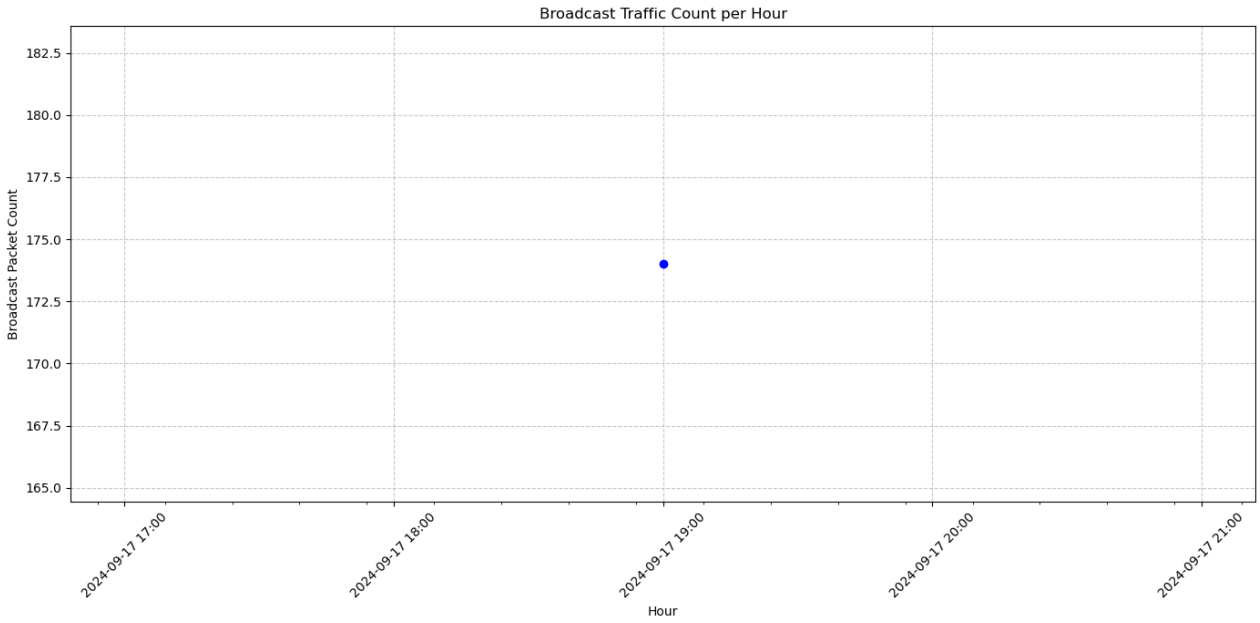
Identifie les modèles de requêtes ARP qui pourraient indiquer un balayage ARP, utilisé pour cartographier les adresses IP à MAC.





Broadcast Traffic Analysis

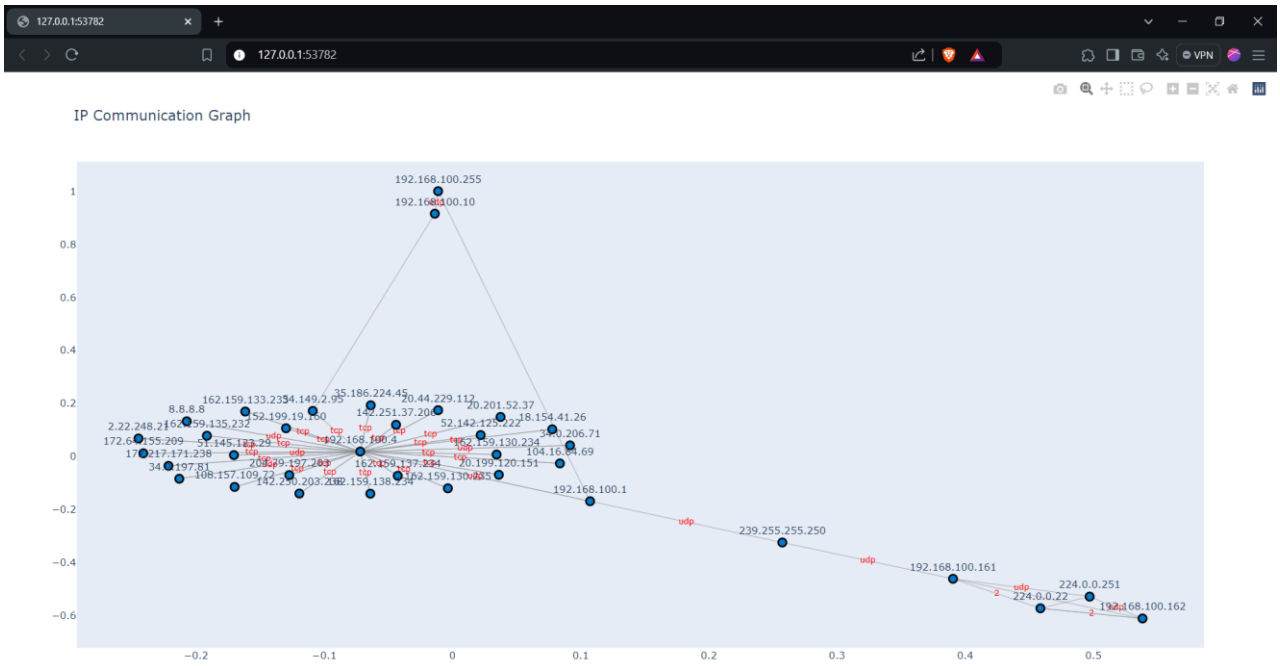
Examine le volume de paquets de diffusion au fil du temps pour détecter les anomalies.



Analyse IP

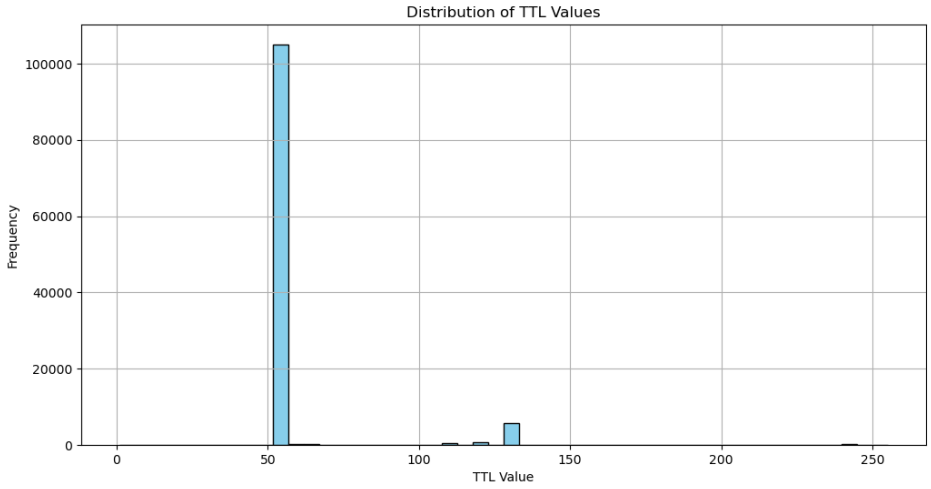
IP Communication Graph

Crée un graphe montrant les connexions entre différentes adresses IP, facilitant l'identification des interactions entre les hôtes.



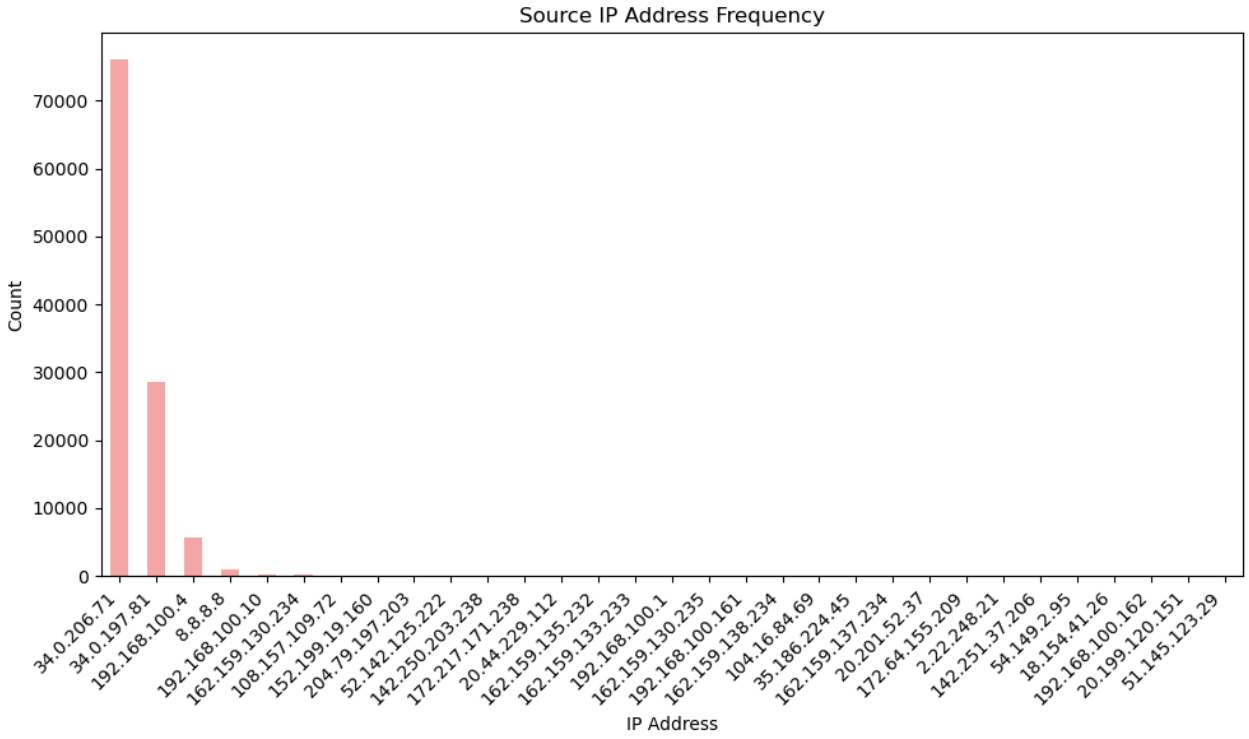
Analyze TTL

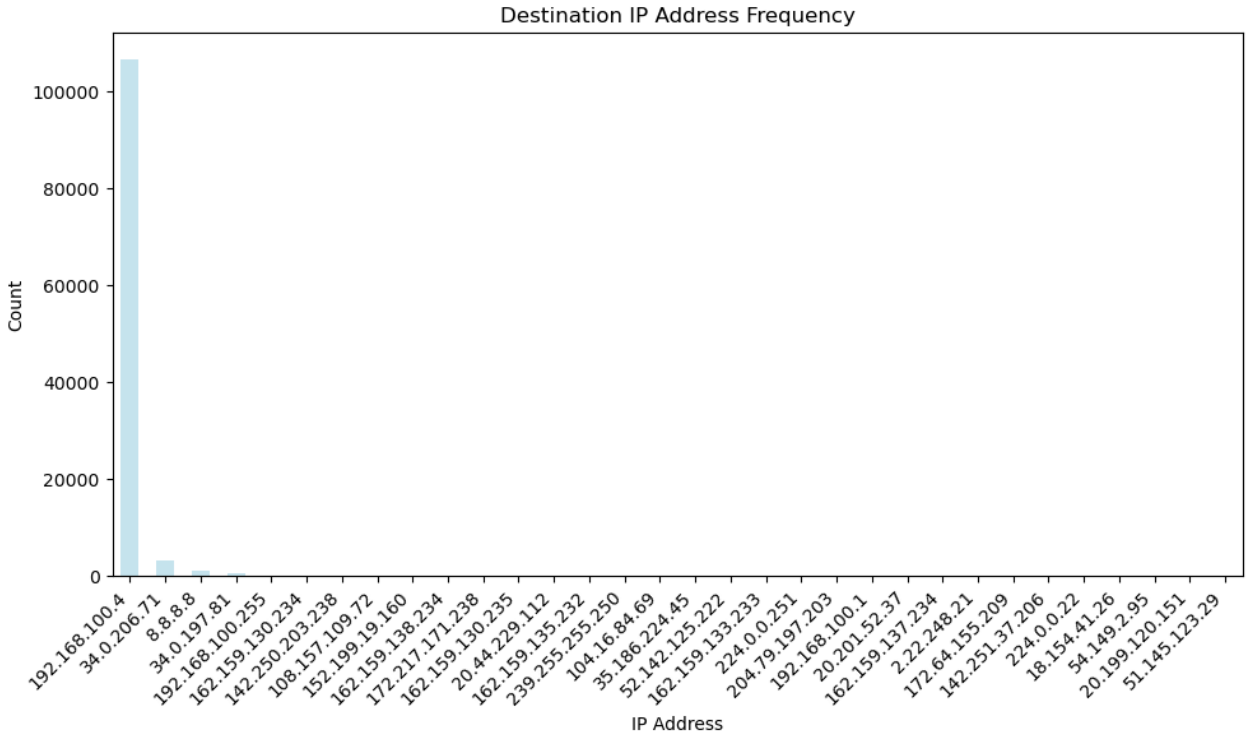
Examine les valeurs TTL pour détecter des anomalies



IP Frequency Analysis

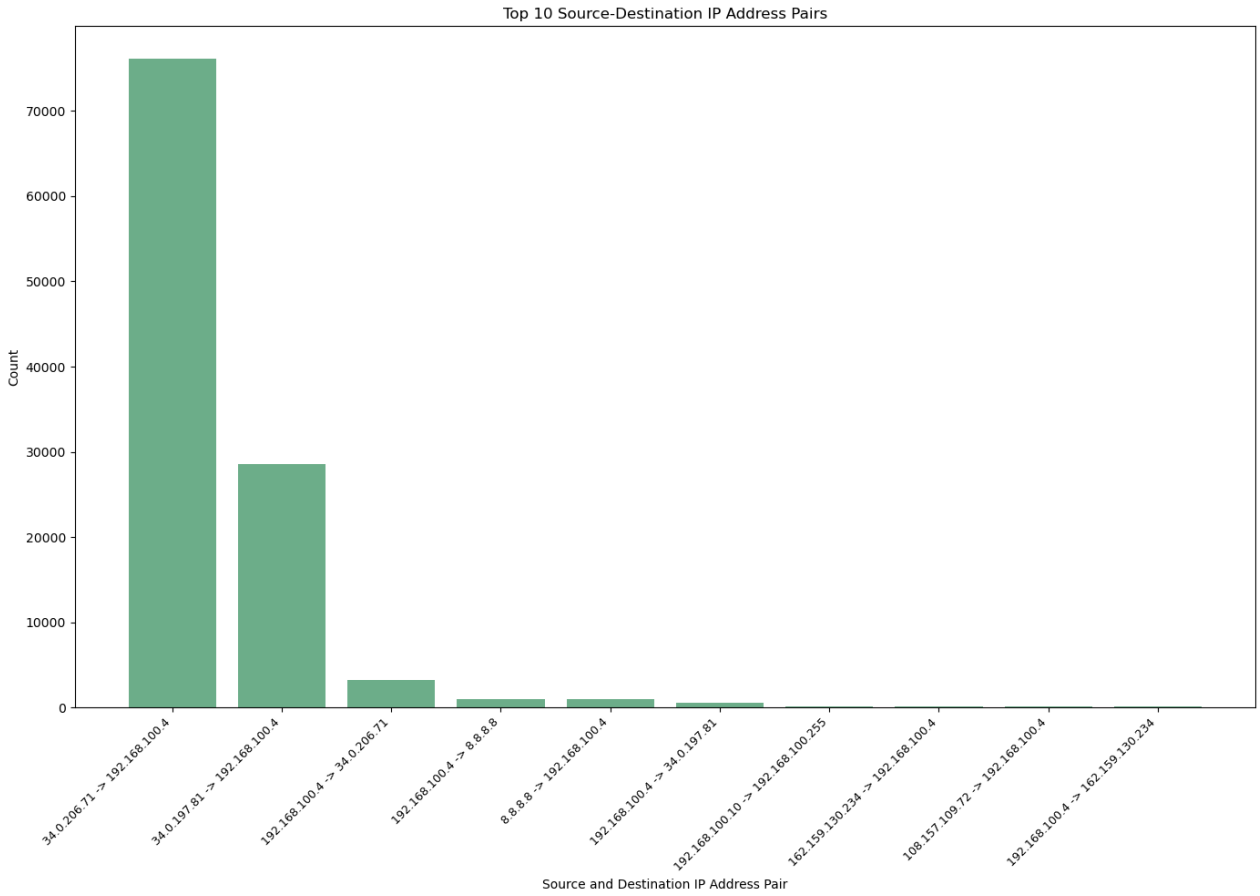
Compte combien de fois chaque adresse IP source et destination apparaît dans les paquets capturés.





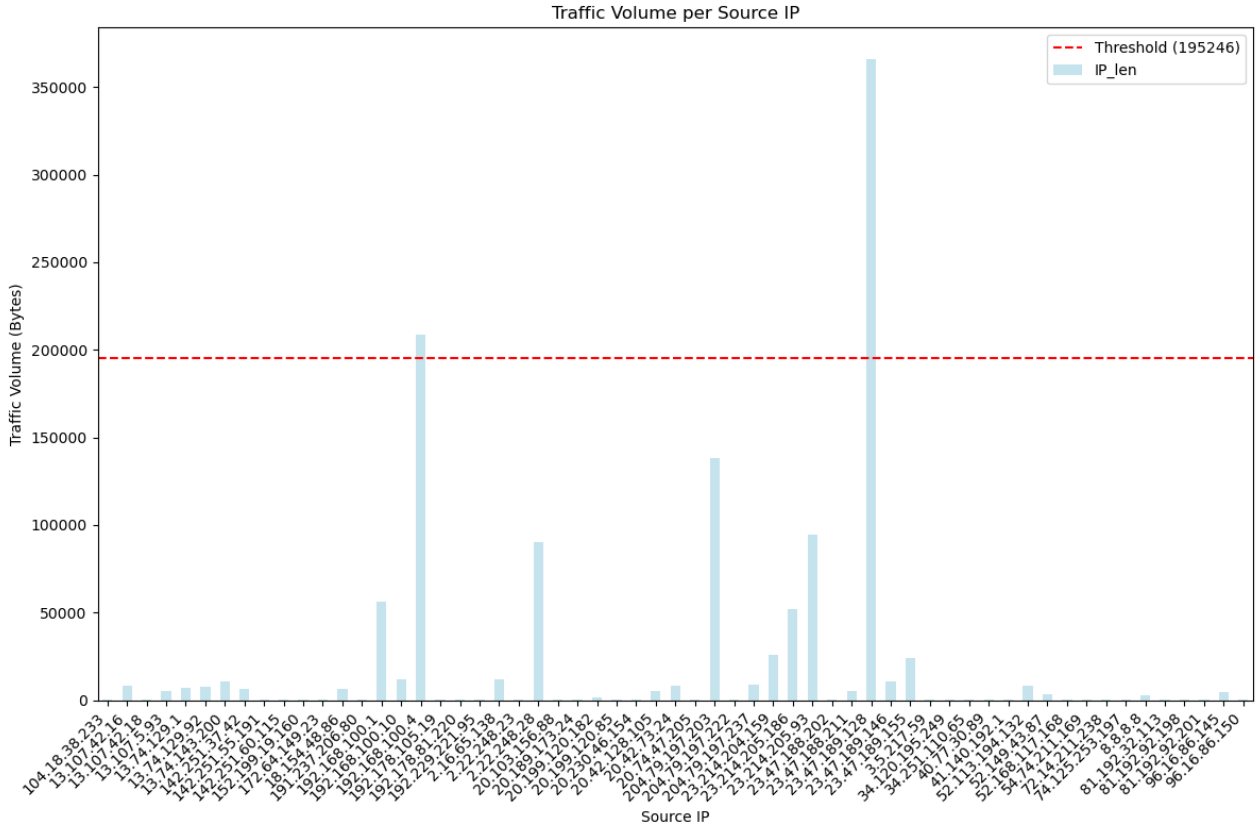
IP Pair Analysis

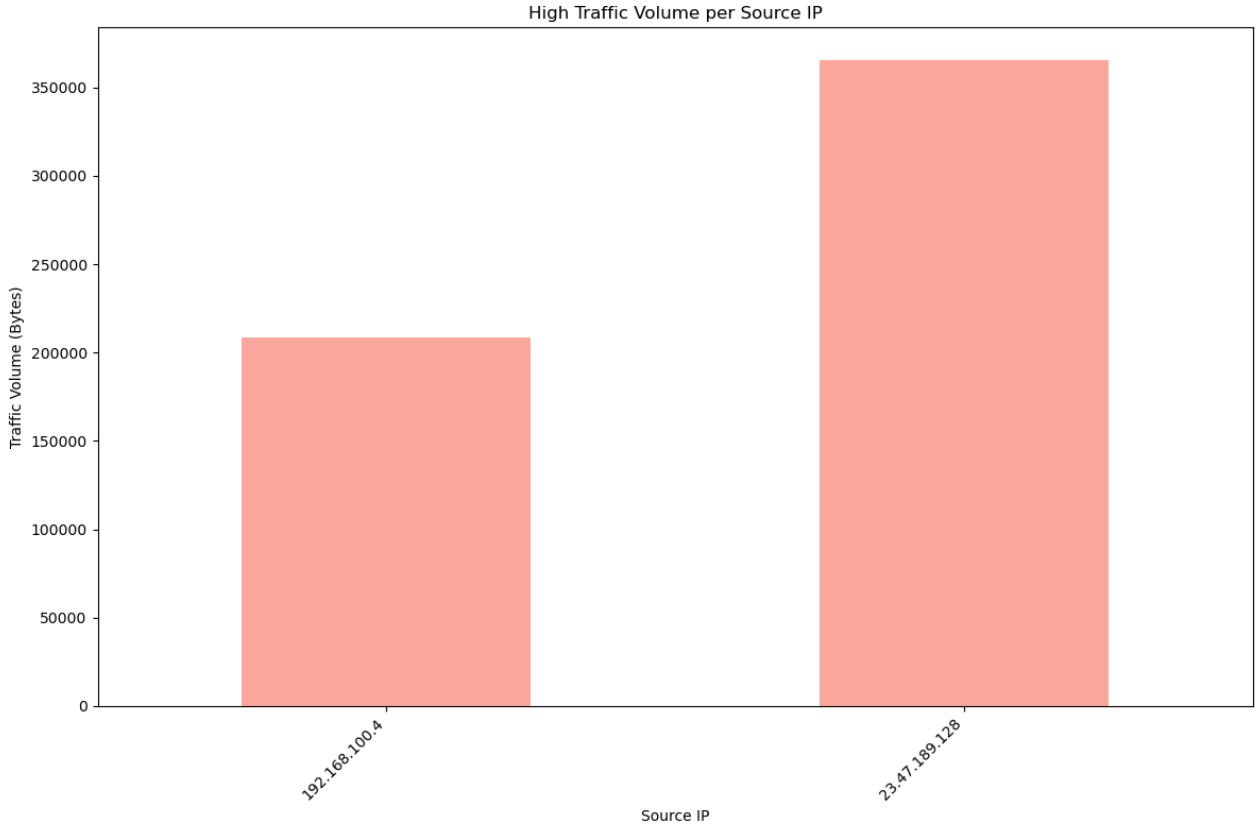
Examine les interactions entre les paires d'adresses IP pour détecter des schémas de communication ou des anomalies.



High Traffic IPs

Détecte les adresses IP qui envoient ou reçoivent des volumes de trafic anormalement élevés, ce qui peut indiquer des activités suspectes.

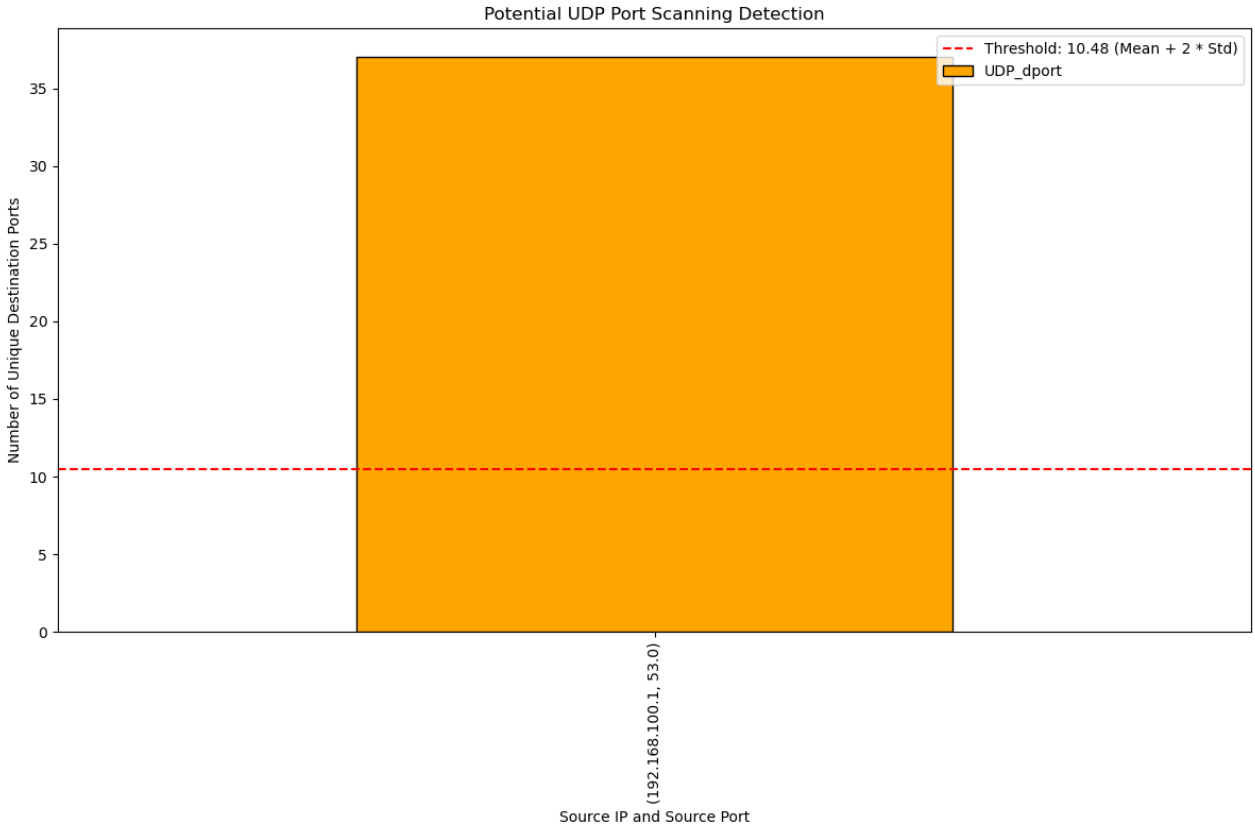

Traffic Volume per Source IP
Threshold (195246)
IP_len
Traffic Volume (Bytes)
Source IP


High Traffic Volume per Source IP
Traffic Volume (Bytes)
192.168.100.4
23.47.189.128
Source IP

Analyse de la couche de transport :

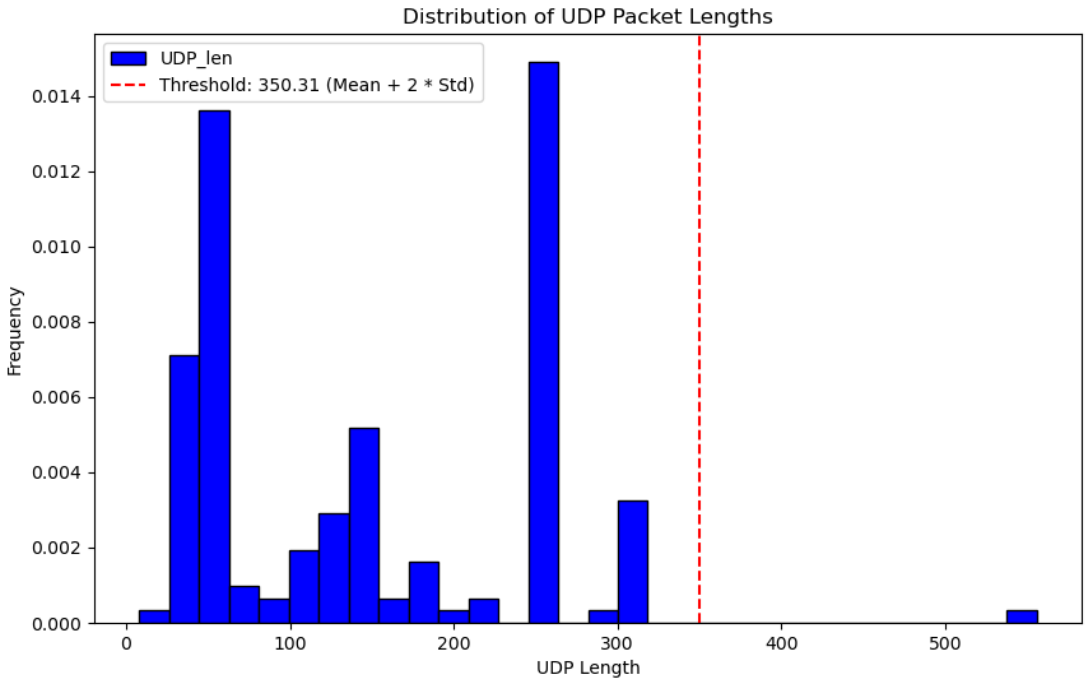
Detect UDP Port Scanning

Identifie les tentatives de balayage de ports UDP, souvent utilisées pour découvrir des services ouverts sur des ports UDP.



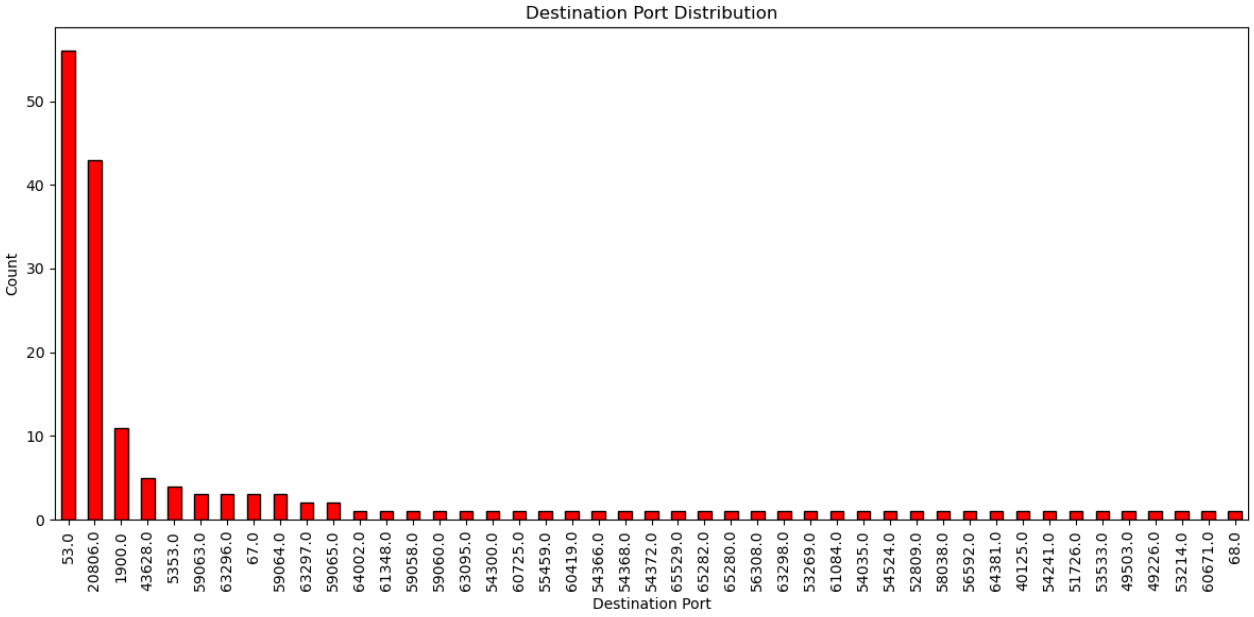
Analyze UDP Length

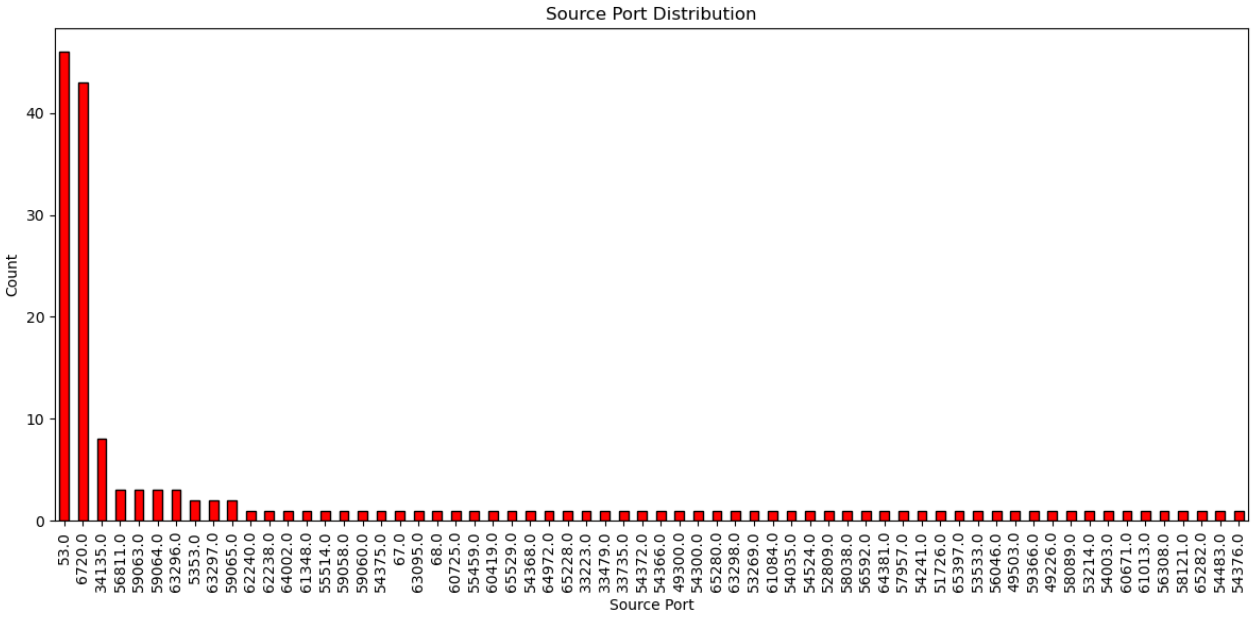
Examine la taille des paquets UDP pour détecter des anomalies .



UDP Port Distribution

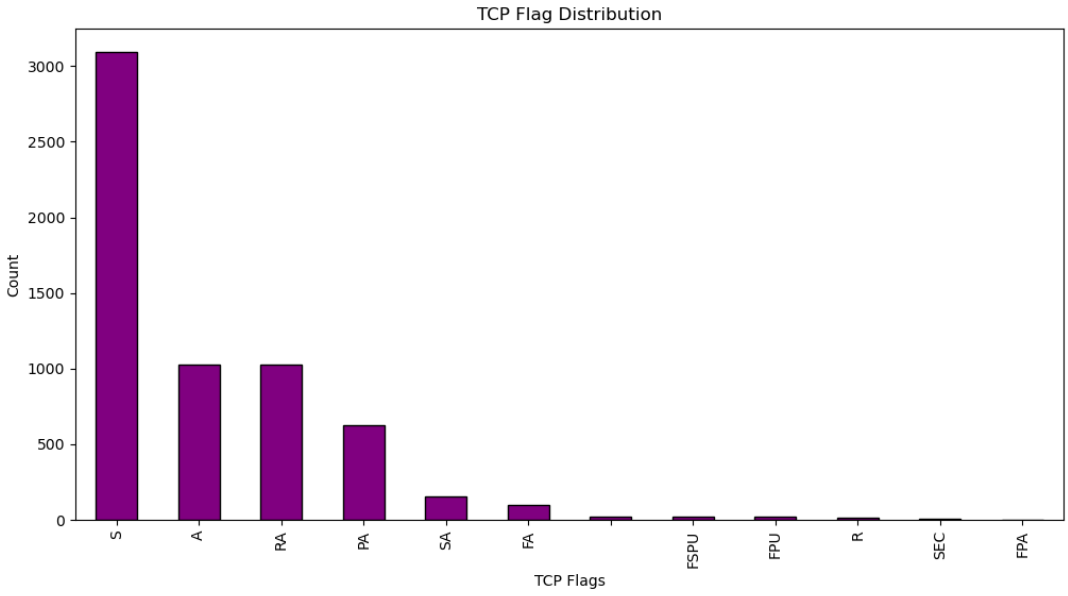
Analyse la répartition des ports UDP utilisés dans les paquets capturés, offrant une vue d'ensemble des ports UDP les plus actifs.





TCP Flags Distribution

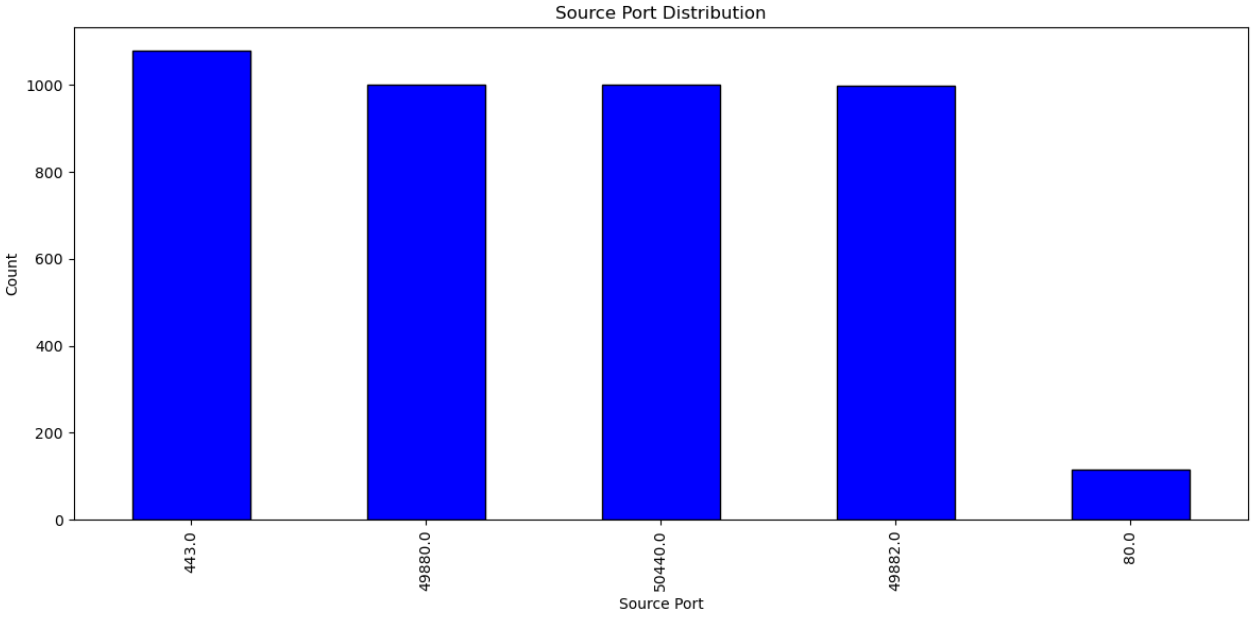
Examine les différents indicateurs TCP (SYN, ACK, FIN, etc.) pour comprendre les types de connexions et les comportements du réseau.

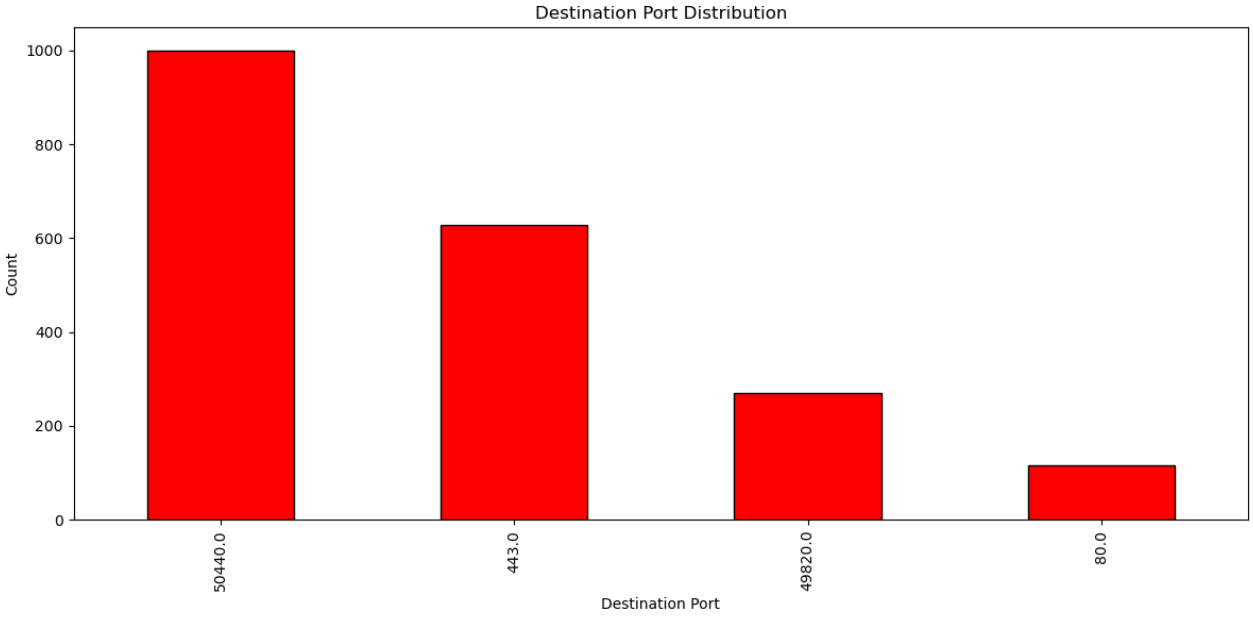


TCP Port Distribution

Analyse la répartition des ports TCP utilisés dans les paquets capturés, offrant une

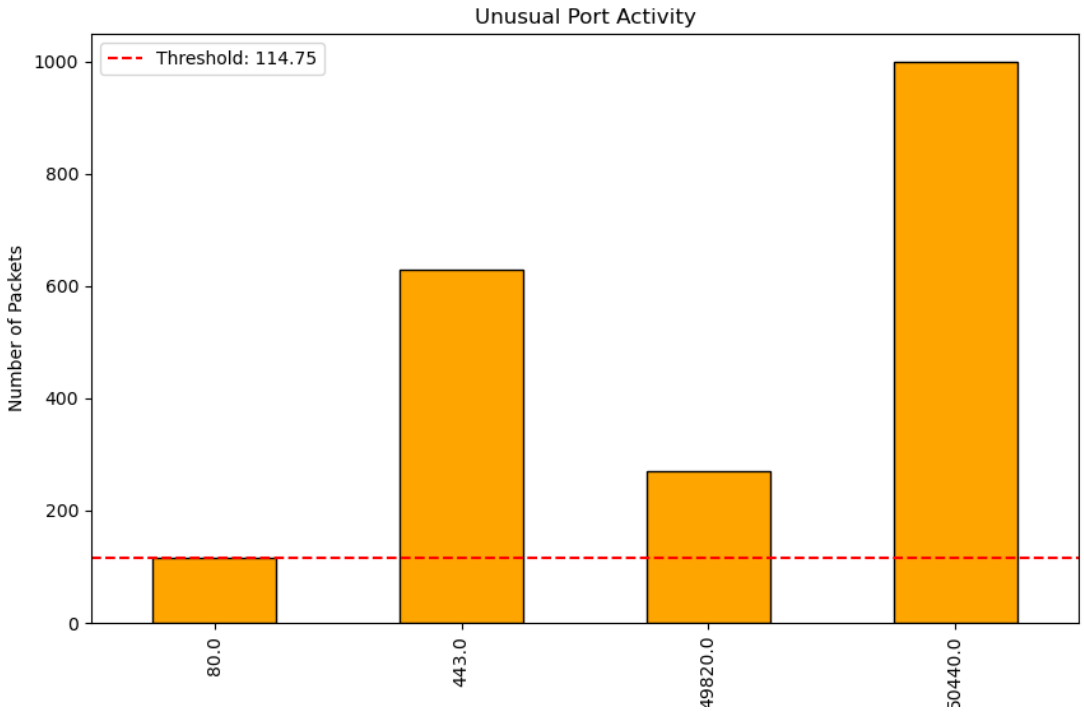
vue d'ensemble des ports TCP les plus actifs.





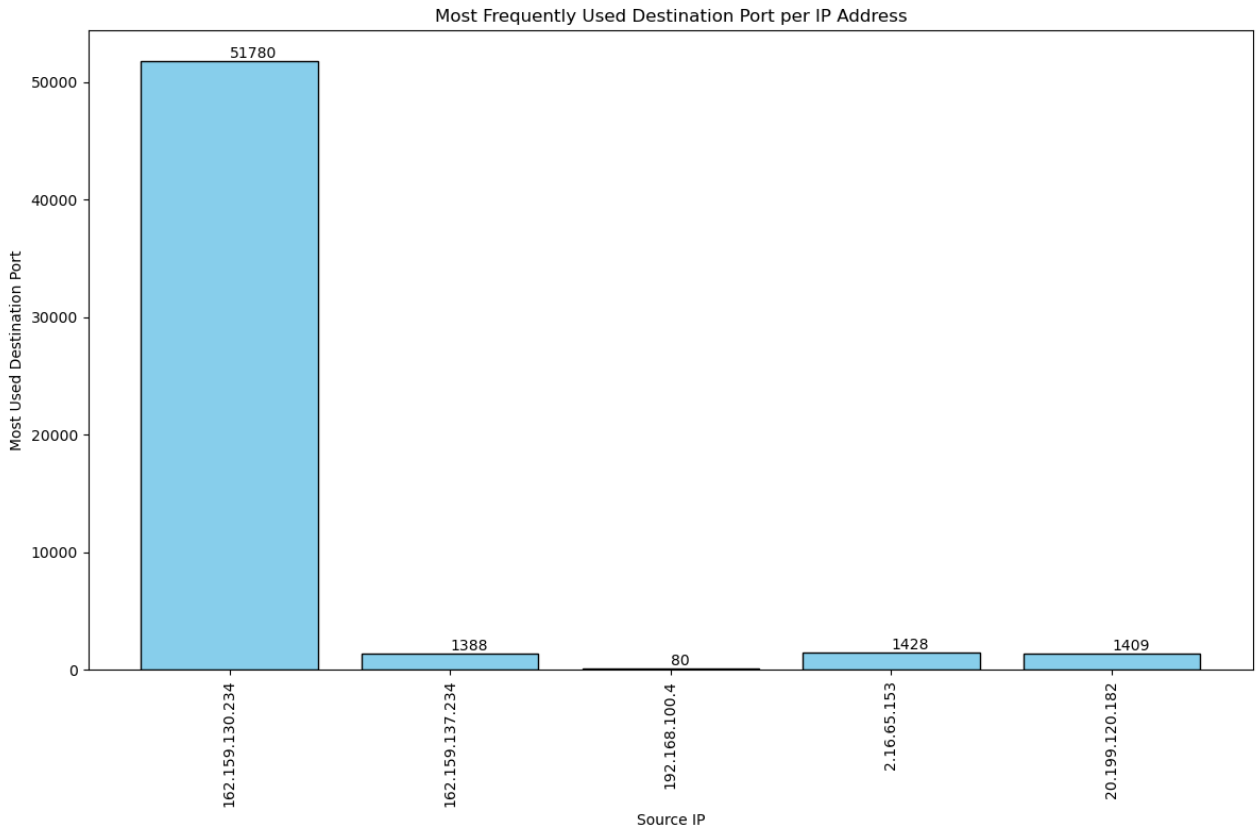
Unusual TCP Port Activity

Identifie les modèles de trafic TCP inhabituels ou inattendus, ce qui peut indiquer des activités suspectes.



IP / Port Distribution

Examine la répartition des adresses IP et des ports dans les paquets capturés pour détecter des schémas d'utilisation ou des anomalies.



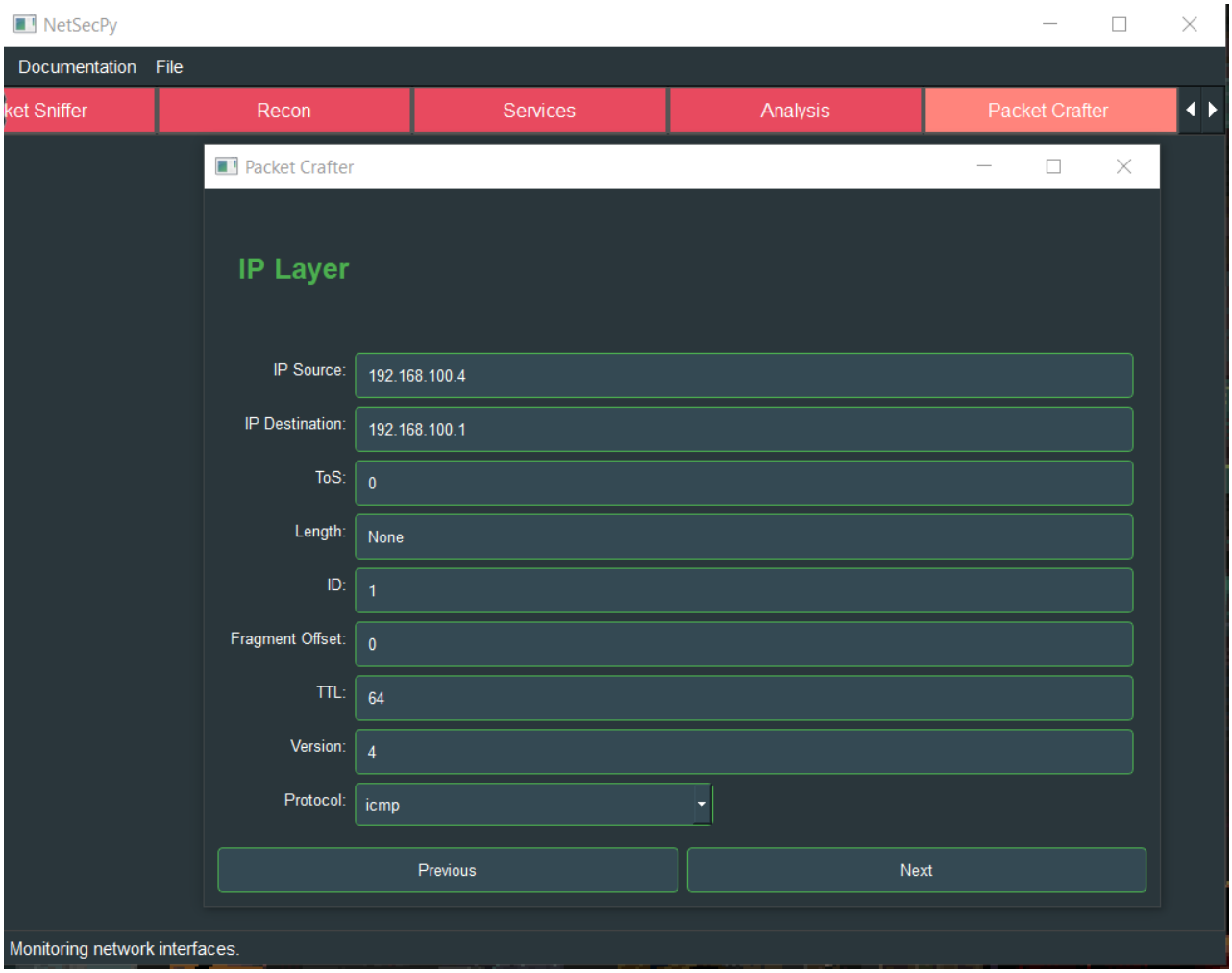
Onglet Packet Crafter

L'onglet "Packet Crafter" de NetSecPy est un outil polyvalent conçu pour la création et la manipulation de paquets réseau. Cet onglet permet aux utilisateurs de concevoir des paquets personnalisés en ajustant chaque couche du paquet, y compris la couche Ethernet, IP, Transport, et Data. Avec cette fonctionnalité, les utilisateurs peuvent :

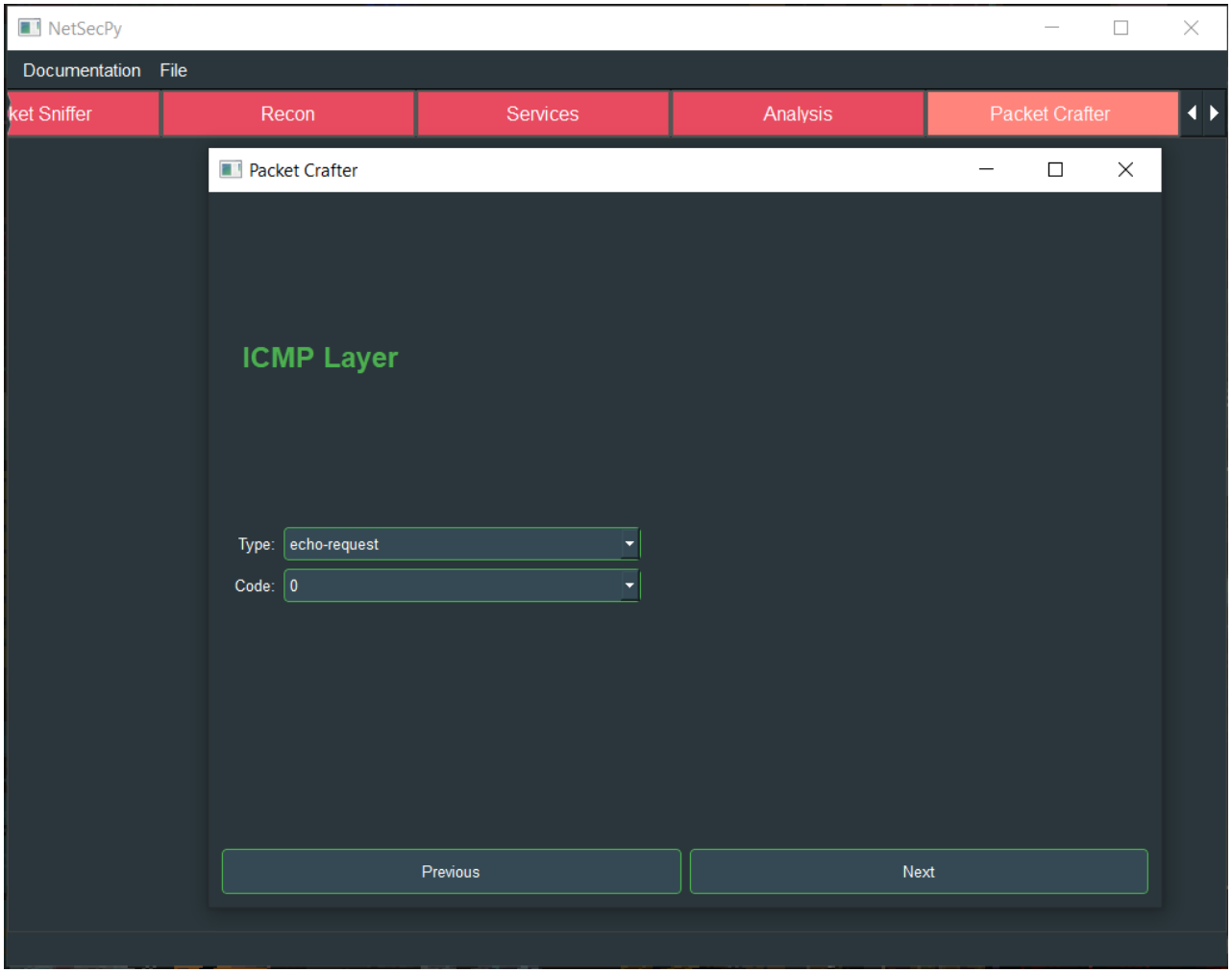
- **Créer des Paquets Personnalisés** : Définir et ajuster les paramètres de chaque couche du paquet, offrant une flexibilité pour la création de paquets sur mesure.
- **Visualiser les Paquets** : Observer la structure et le contenu des paquets pour une validation approfondie avant l'envoi.
- **Envoyer les Paquets** : Tester les paquets directement sur le réseau pour évaluer leur comportement et leur impact en conditions réelle

Exemple (ICMP packet) :

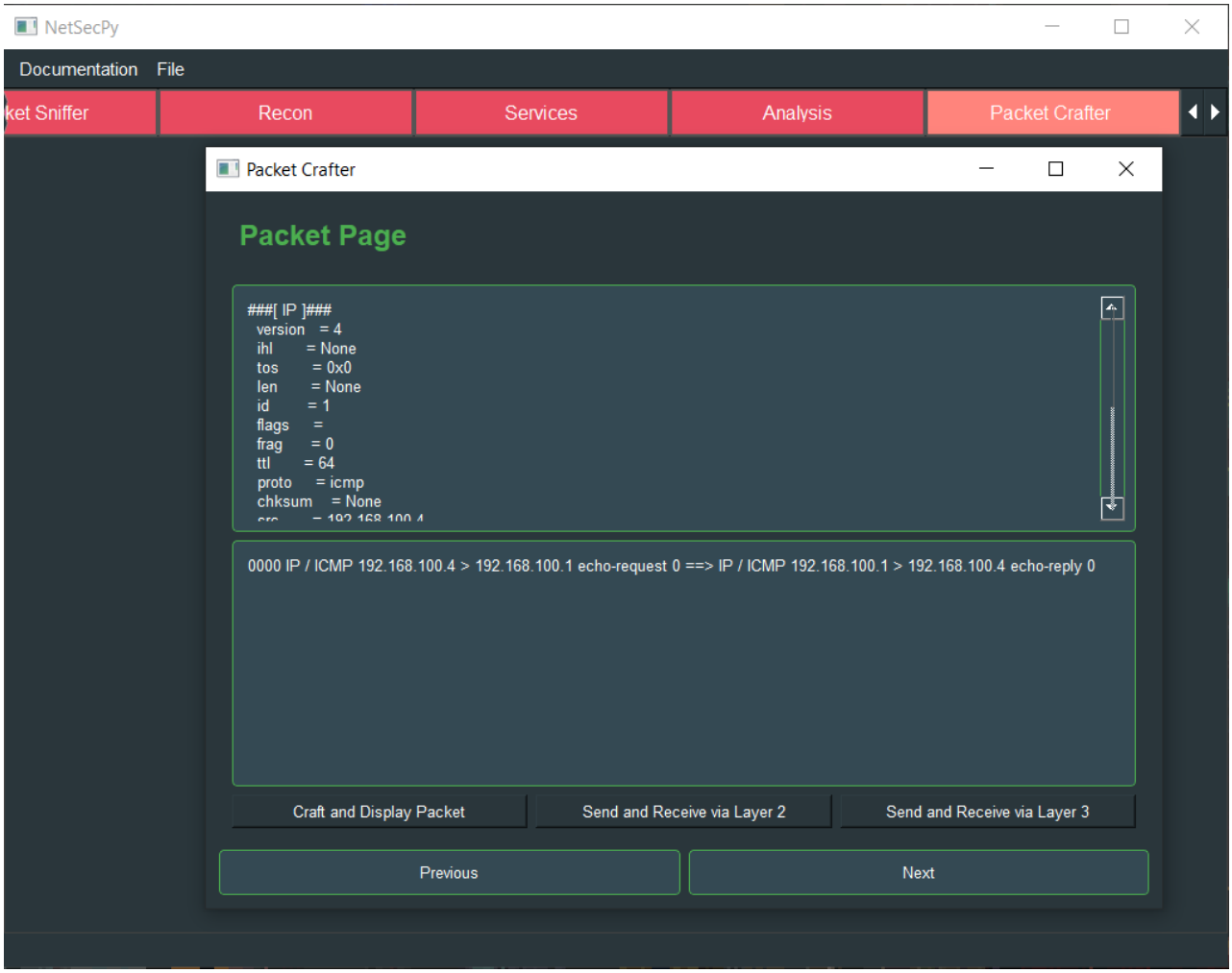
Couche IP :



Couche ICMP :

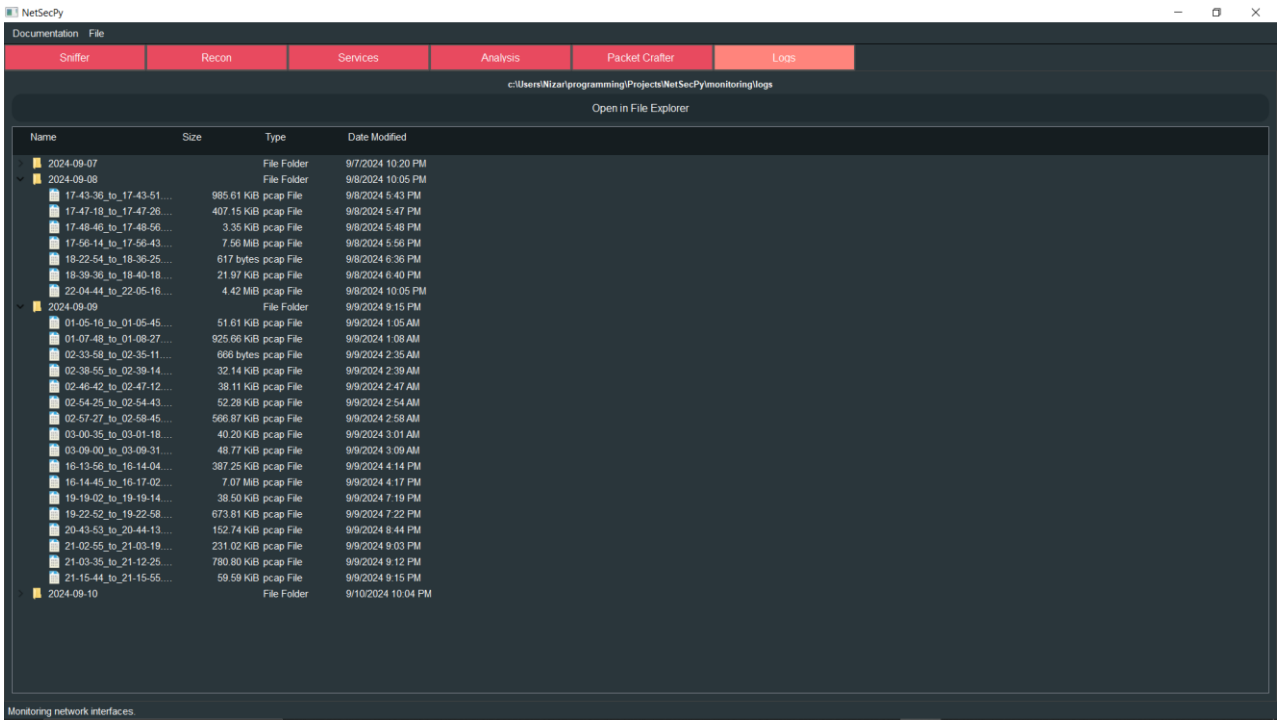

NetSecPy
Documentation
File
ket Sniffer
Recon
Services
Analysis
Packet Crafter
Packet Crafter
ICMP Layer
Type:
echo-request
Code:
0
Previous
Next

Création et Envoi du Packet :



Onglet Logs

L'onglet Logs de NetSecPy est conçu pour faciliter l'accès et la gestion des fichiers journaux générés par l'application. Il offre une interface utilisateur intuitive qui permet aux utilisateurs de visualiser la structure des fichiers journaux, d'ouvrir le répertoire des journaux directement dans l'explorateur de fichiers de leur système, et de naviguer facilement à travers les dossiers et fichiers. Cet onglet est particulièrement utile pour consulter et organiser les données collectées pendant les opérations de reconnaissance et de capture réseau, permettant ainsi une gestion efficace des informations critiques.



Note : Lorsque vous quittez l'application ,les logs (fichiers pcap) sont automatiquement enregistrés dans un répertoire spécifié

Conclusion

En conclusion, ce projet vise à développer une application robuste et polyvalente pour l'analyse de trafic réseau, combinant à la fois des fonctionnalités de capture en direct et l'analyse de fichiers pcap.

L'application est divisée en plusieurs onglets et sections dédiées, chacun axé sur des aspects essentiels de l'analyse réseau, tels que la détection des services, la reconnaissance réseau, et l'exploration approfondie des couches de communication Ethernet, IP et Transport et la création de paquets.