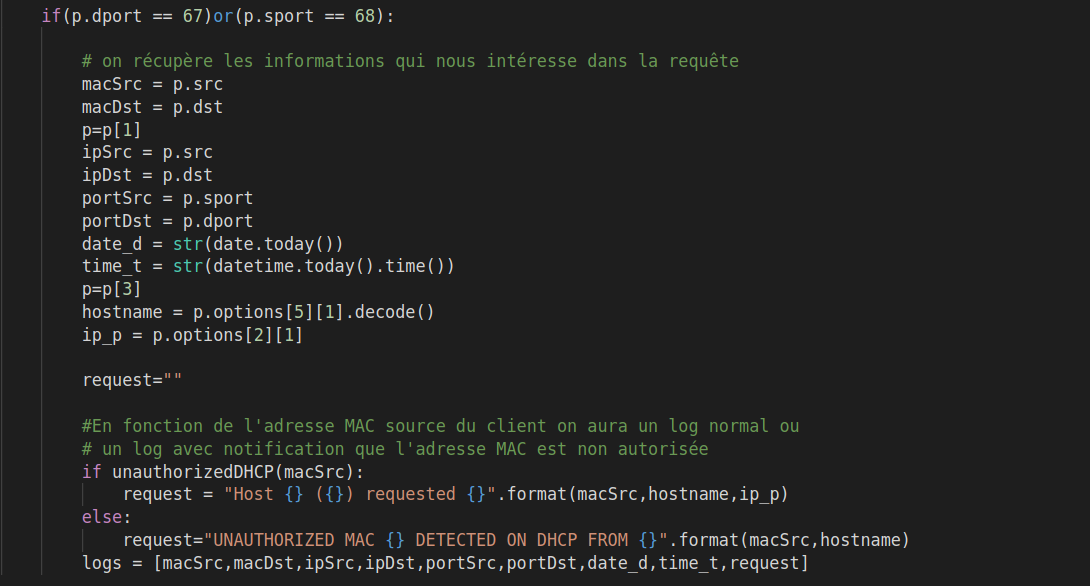
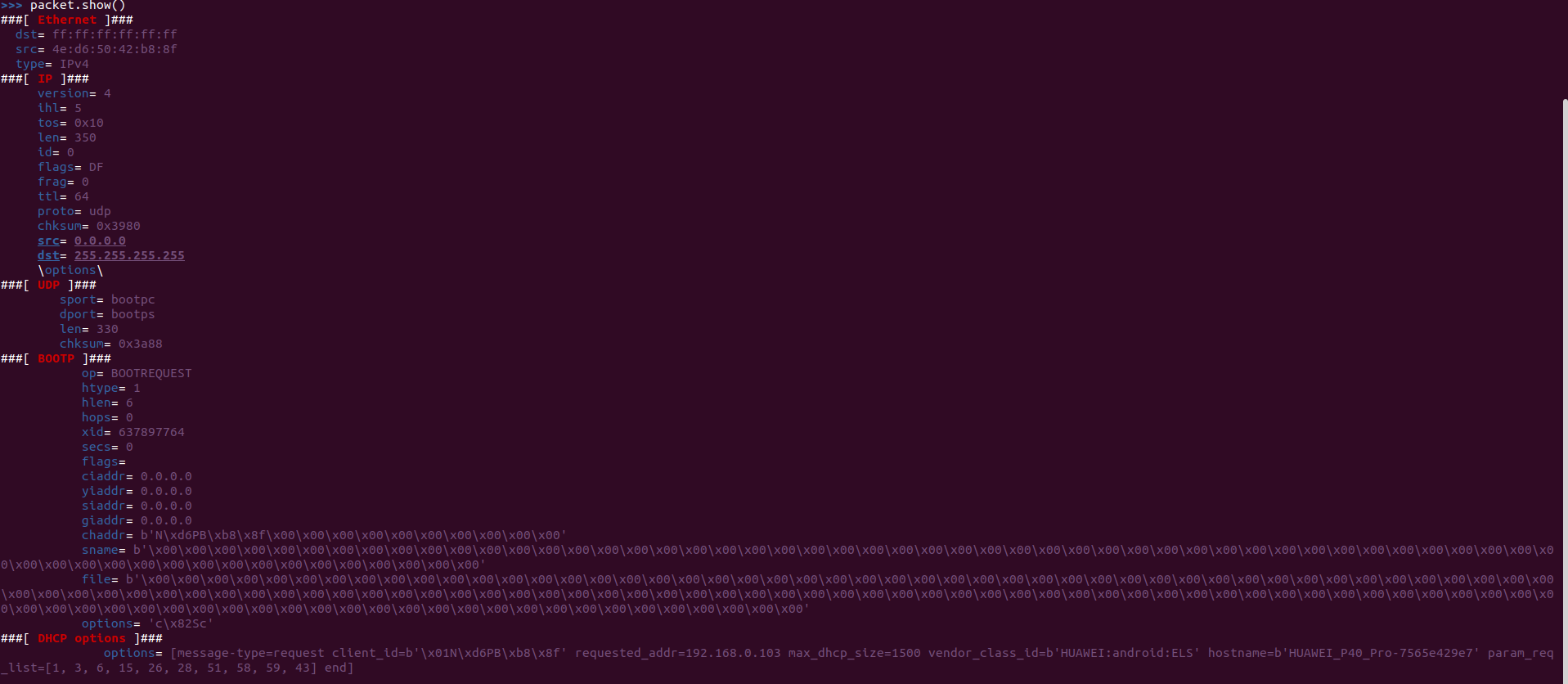
**Traitement des paquets DHCP avec Scapy**

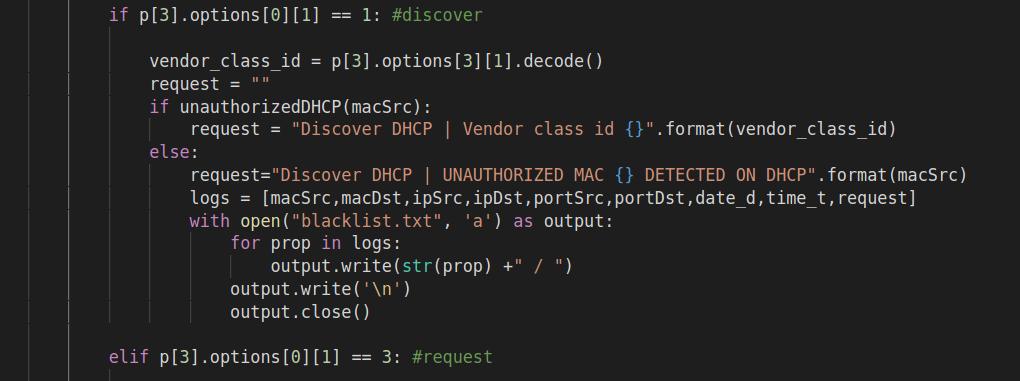
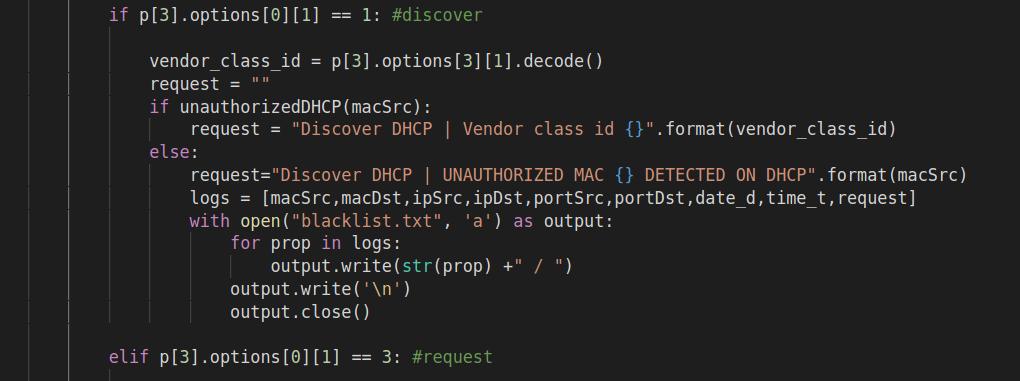
Comme nous le savons, le DHCP est un protocole qui permet à un ordinateur qui se connecte sur un réseau local d’obtenir dynamiquement et automatiquement sa configuration IP. On pourrait croire qu’un seul aller-retour peut suffire à la bonne marche du protocole mais il existe plusieurs messages DHCP qui permettent de compléter une configuration, la renouveler… Ces messages sont susceptibles d’être émis soit par le client pour le ou les serveurs, soit par le serveur vers un client : DHCP Discovery, DHCP Offer, DHCP Request, DHCP Ack etc.

Ici nous nous intéresserons aux requêtes DHCP Discovery et DHCP Request, l’une permet à un client de trouver le serveur puis lui demander une réponse et l'autre de demander au serveur de lui attribuer une IP choisie parmi celle proposées.

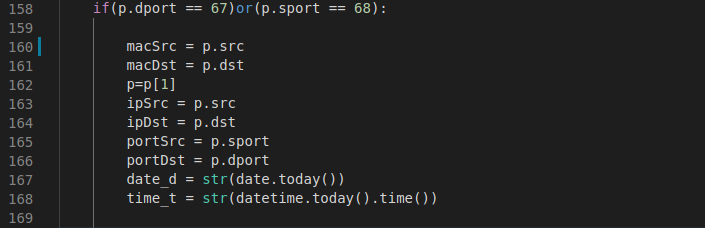
Pour différencier les paquets DHCP des paquets DNS capturés par Scapy, on vérifiera les ports source et destination du paquet capturé. Un paquet DHCPutilise le port 67 et 68, 68 sur la source et 67 sur le destinataire. On a aura juste une condition if à rajouter dans le code :  
Ensuite pour différencier les paquets les DHCP Discovery et Request des autres paquets DHCP il faudra s’intéresser à la structure d’un paquet DHCP. Globalement la structure des deux paquets qui nous intéresse est presque la même. Comme nous le savons, un paquet est structuré sous forme de couche. On a dans un paquet DHCP 5 couches (Ether, IP, UDP, BOOTP et DHCP options) comme montré sur la photo ci-dessous :

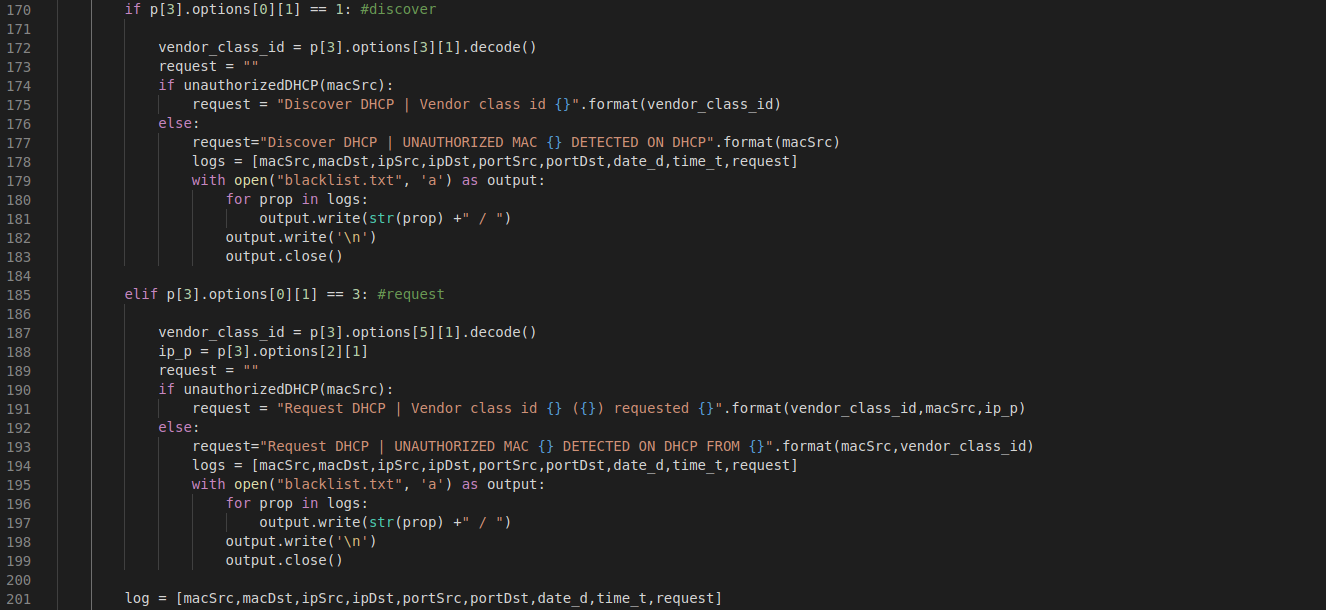


L’information qui permet de différencier les deux paquets se trouve dans la liste **options** dans la couche 5 **[DHCP options]**, c’est le “**message-type = request**”. S’il est égal à 1 le paquet est un Discovery, s’il est égal à 3 c’est un Request. Donc encore une fois on rajoutera une condition **if** pour traiter les informations qui diffèrent entre les deux paquets.



Une fois qu’on connait la structure d’un paquet DHCP il est facile d’en récupérer les informations qui nous intéresse. Les adresses MAC, IP et les ports source et destination des paquets sont au même endroit.



Mais c’est pour le traitement de l’enregistrement du type de la requête que va nous servir les conditions du dessus. 

Pour un paquet DHCP Discovery on aura un type de requête différent de celui d’un paquet DHCP Request. Dans les deux cas on rajoutera une condition pour notifier le client lorsque l’on détectera une adresse MAC source dans un paquet qui correspond à une adresse MAC non autorisée de notre base de données.

Une fois toutes les informations nécessaires récupérées on les enregistre dans la liste **log**, et on insérera cette liste dans la base de données grâce à la fonction **insertLog()**.