# TP-wireshark

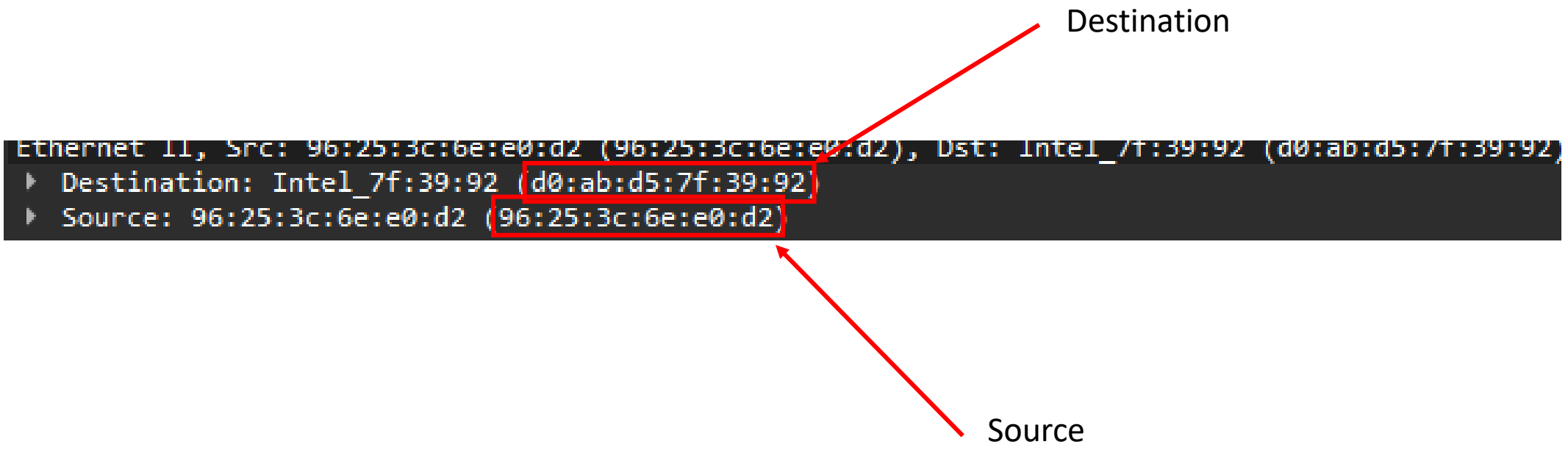
KALETA Maxime

# Utilisation de Wireshark

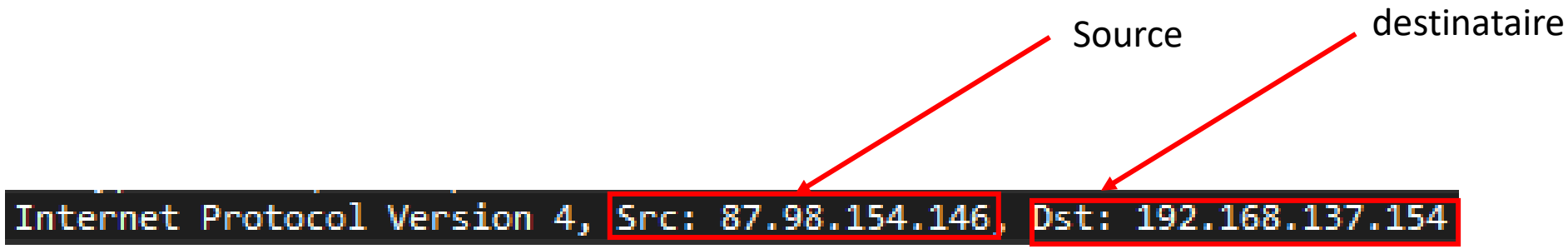
Analyse d’une trame :

- Adresse mac source et destinataire
- Adresse IP source et destinataire
- Time to live
- Numéro de frame
- Taille de trame et taille des données

# Adresse MAC


Destination
Source
Destination: Intel_7f:39:92 (d0:ab:d5:7f:39:92)
Source: 96:25:3c:6e:e0:d2 (96:25:3c:6e:e0:d2)

# Adresse IP source et destinataire:



# Time to live

```
Time to Live: 128
```

# Numéro de frame:

```
Frame 3879:
```

# Taille de trame et taille des données

```
Frame 3879: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
```

# ICMP (Internet Control Message Protocol)

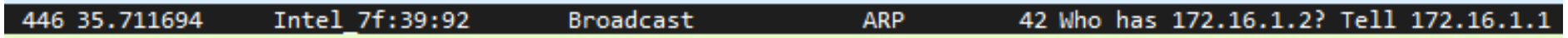
Après application d'un filtre ICMP, nous avons une partie de la trame destinée au ICMP

```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x45fe [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 1885 (0x075d)
    Sequence Number (LE): 23815 (0x5d07)
    [Response frame: 25]
```

# Modification des paramètres IP

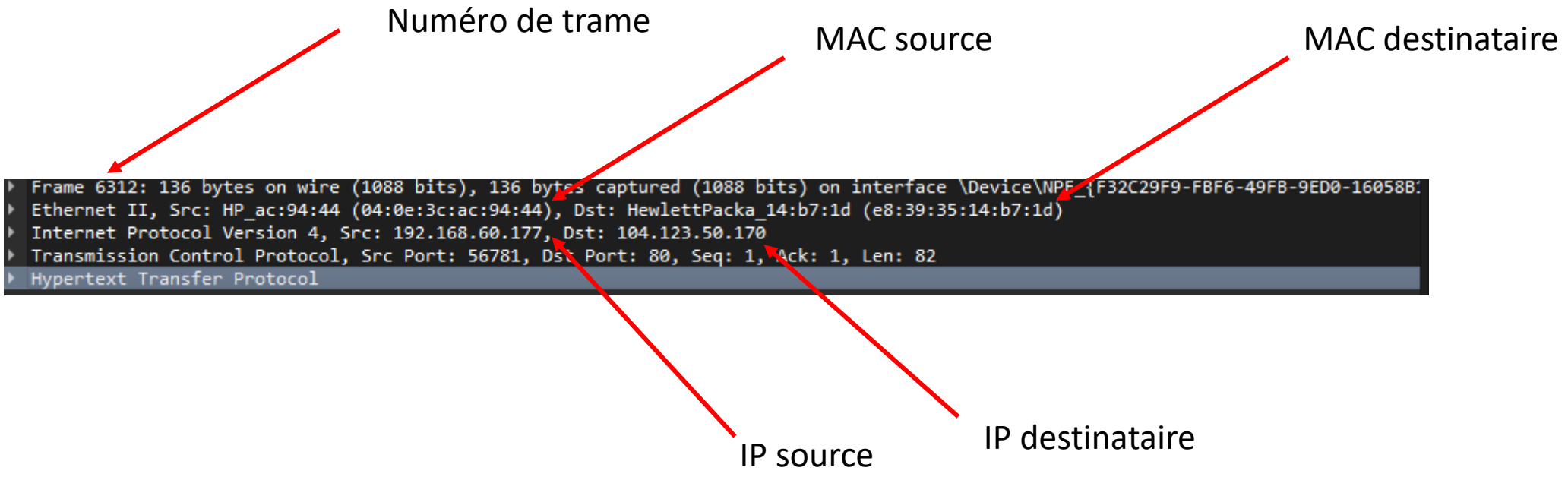
Après changement d'adresse IP pour une adresse 172.16.x.y celui-ci me demande automatiquement de saisir un masque soit 255.255.0.0.

Suite au ping ma machine physique (172.16.1.1) envoie un signal pour demander qui a 172.16.1.2 qui elle est ma machine virtuelle




On peut donc voir que grâce à la commande « ping » ma machine physique demande sur le réseau qui est 172.16.1.2 et donc elle attends la réponse de ma machine virtuelle

# Analyse du protocole http et https



# Analyse du protocole FTP

Nous pouvons voir que lors de la connexion nous voyons le user et le password dans les trames.
Pour le sécuriser il faudrait mettre en place un sftpd (Secure File Transfer Protocol)