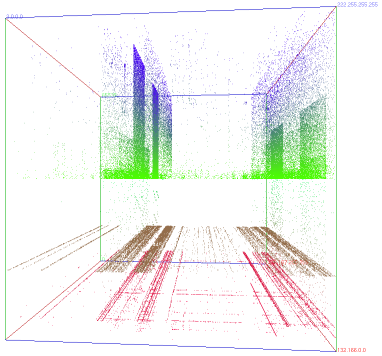
Visualisation d'attaques en temps réel: le Cube

Jean-Philip Guichard – Christian Perez
Groupe SSI – (CEA/DCS)

SSTIC 2008 (Rump Session)

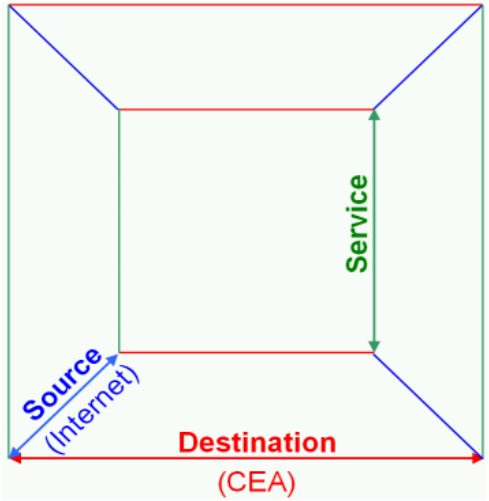


Flux réseau - Collecte

- A partir de sondes d'écoute, positionnées à l'extérieur de nos moyens de protection
- Collecte des flux par le logiciel Argus.
  - Donne le sens de la communication
  - Enregistrement unique pour une communication client-serveur :
    - @IP source, @ip destination, Port source, Port destination, informations horaires, informations volumétriques.

Présentation du Cube

- Développement interne
- Les **Axes**:
  - Axe rouge: Adressage IP CEA => destination;
  - Axe Bleue: Adressage IP Internet => source;
  - Axe Vert: Services.



- Les données:
  - Un flux est représenté par un point dans le cube (**IP Source x IP Destination** x **Service);**

- Accumulation de points sur deux heures d'activité

Applications du Cube

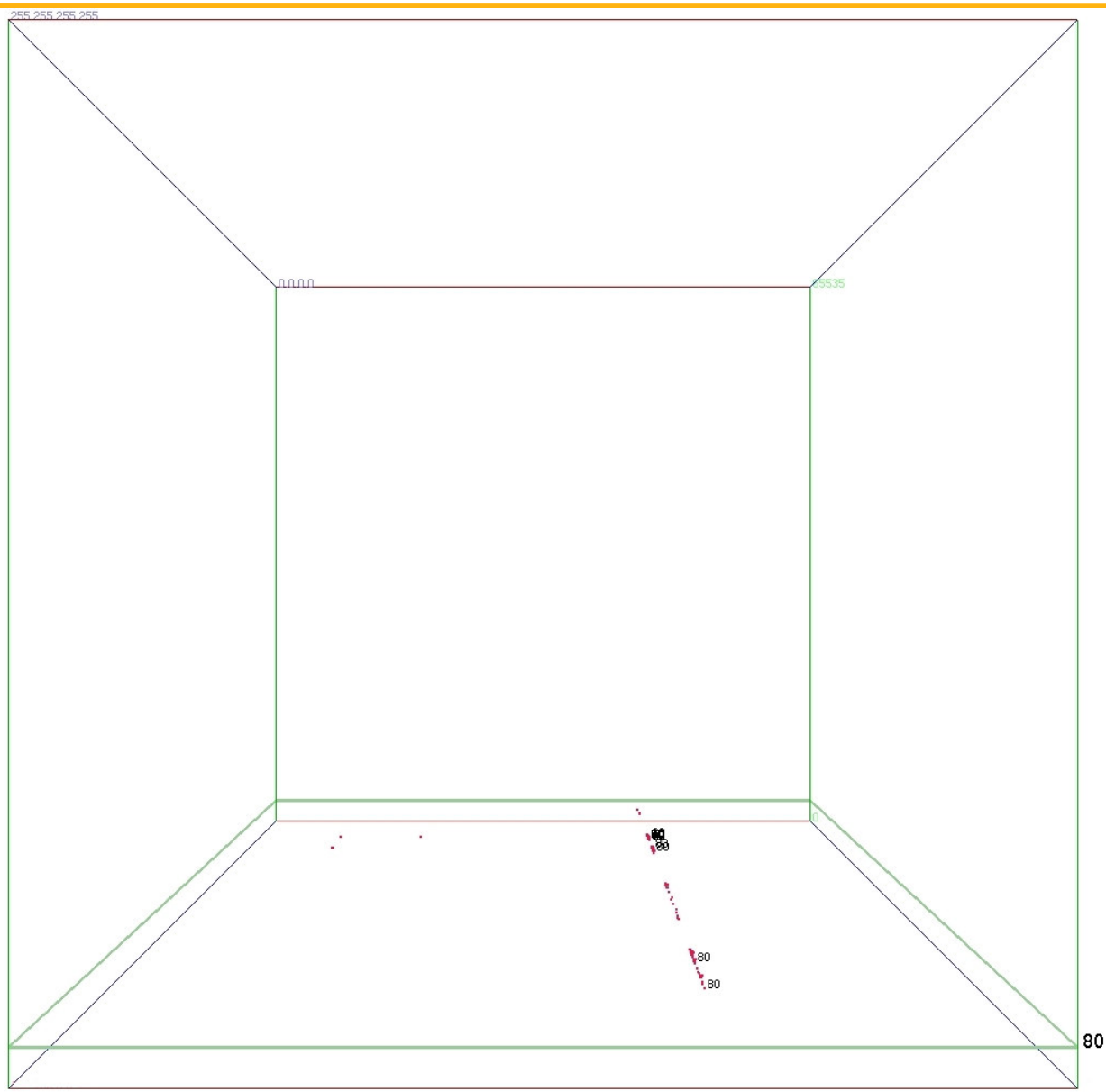
- Visualiser en un coup d'œil les tendances d'activité malveillante.
- Valider globalement que les flux autorisés correspondent à des services autorisés par la Politique de filtrage (Web, SSH,..) depuis Internet.
- Sensibiliser les utilisateurs aux dangers d'Internet (97% des flux entrants sont illégitimes du point de vue de la politique de filtrage)

Publication

- Le Labo SSI a publié un article sur le sujet dans le magazine MISC n°35 de janvier/février 2008, intitulé « Supervision et sécurité par analyse de flux ».

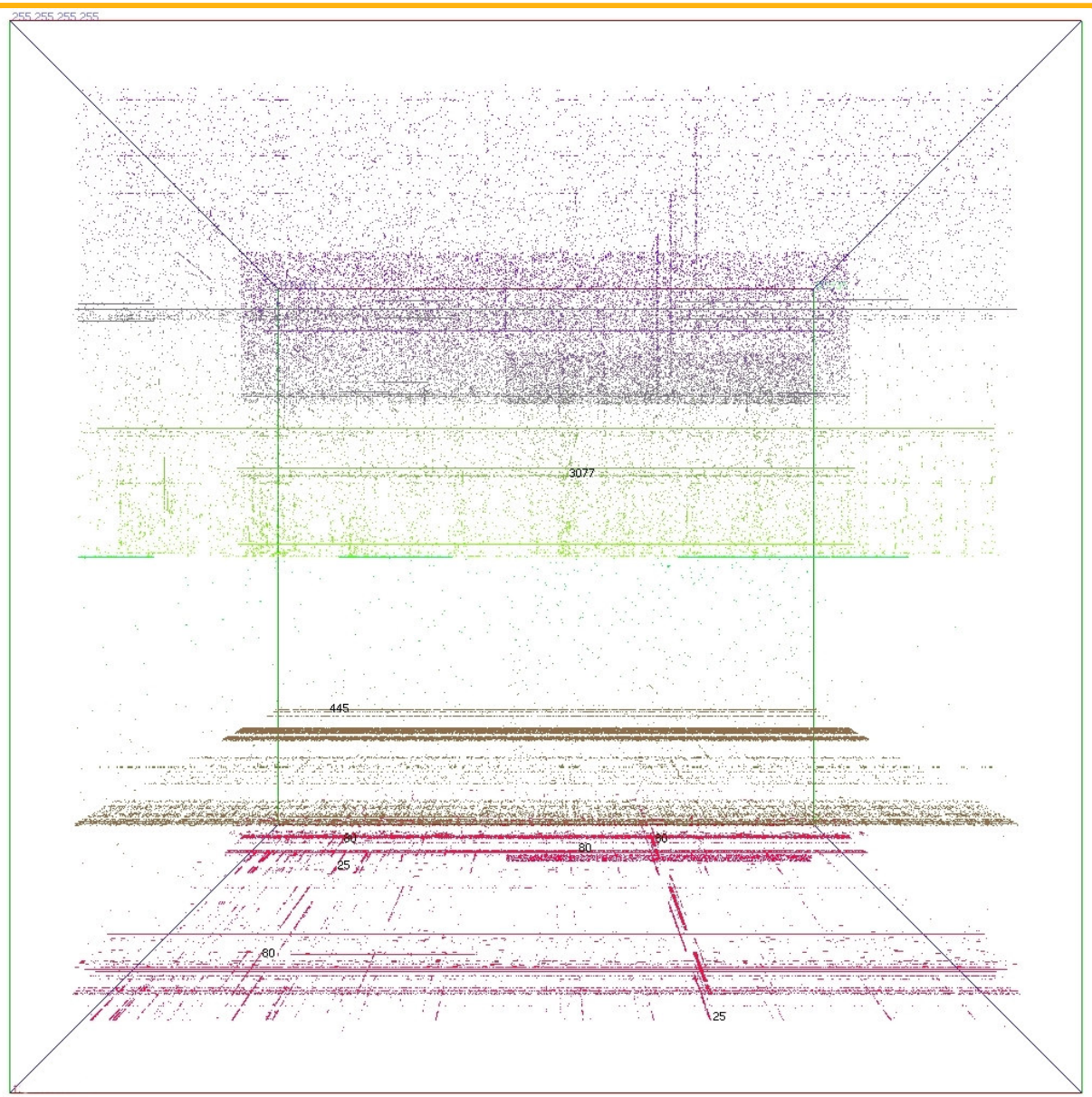
Annexes

Flux autorisés : HTTP

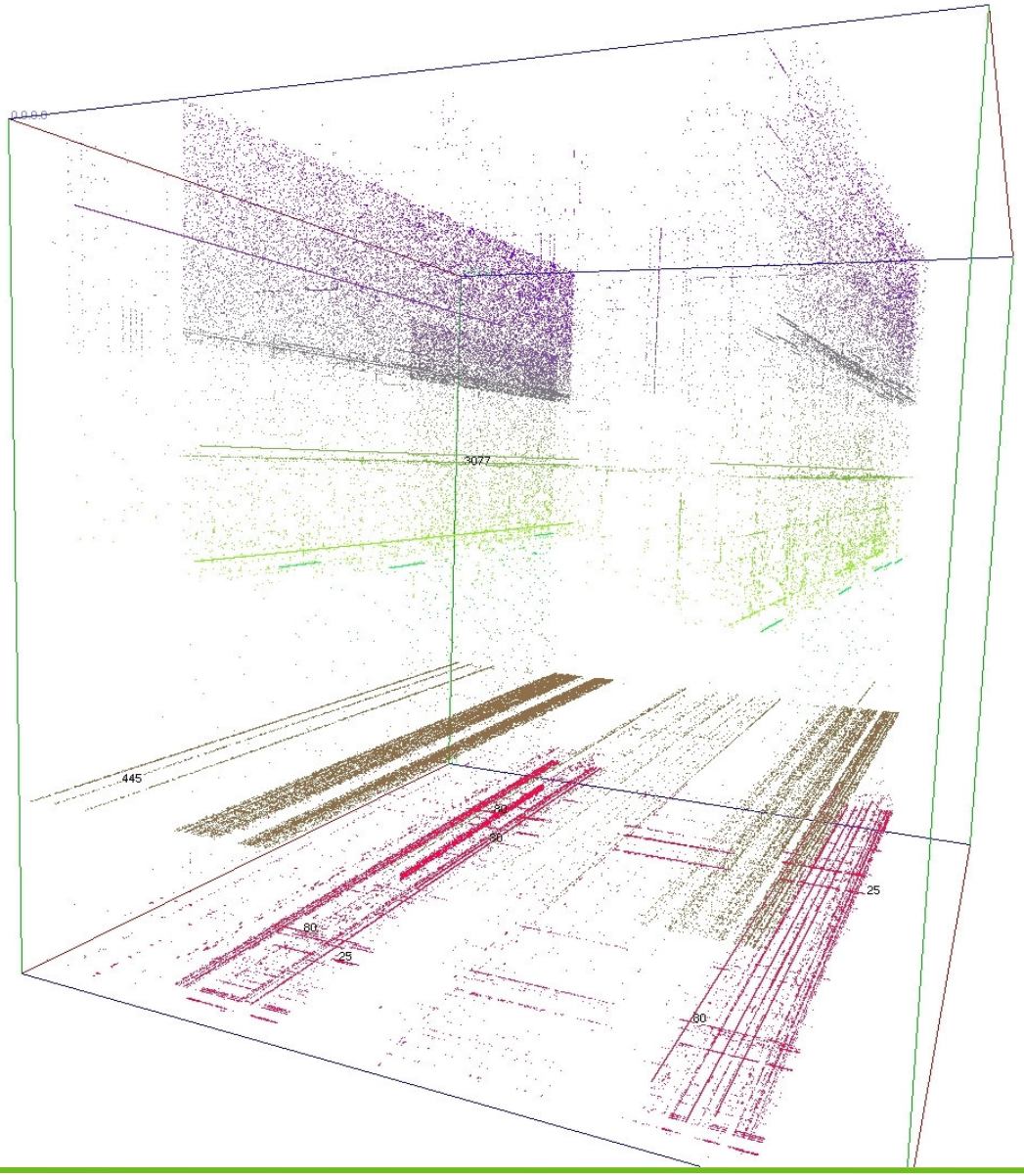


Visualisation des services : HTTP

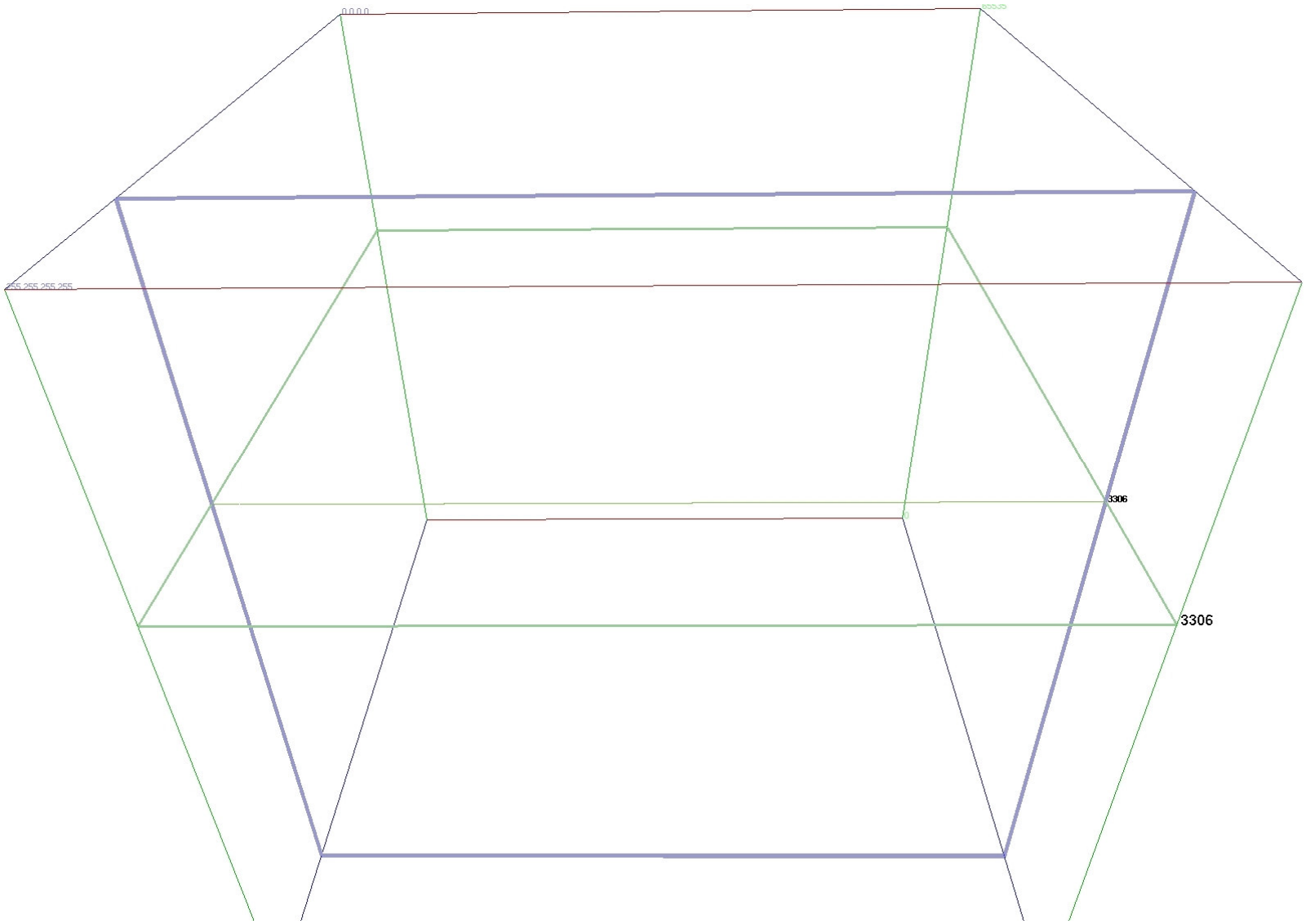
Intégralité des flux collectés



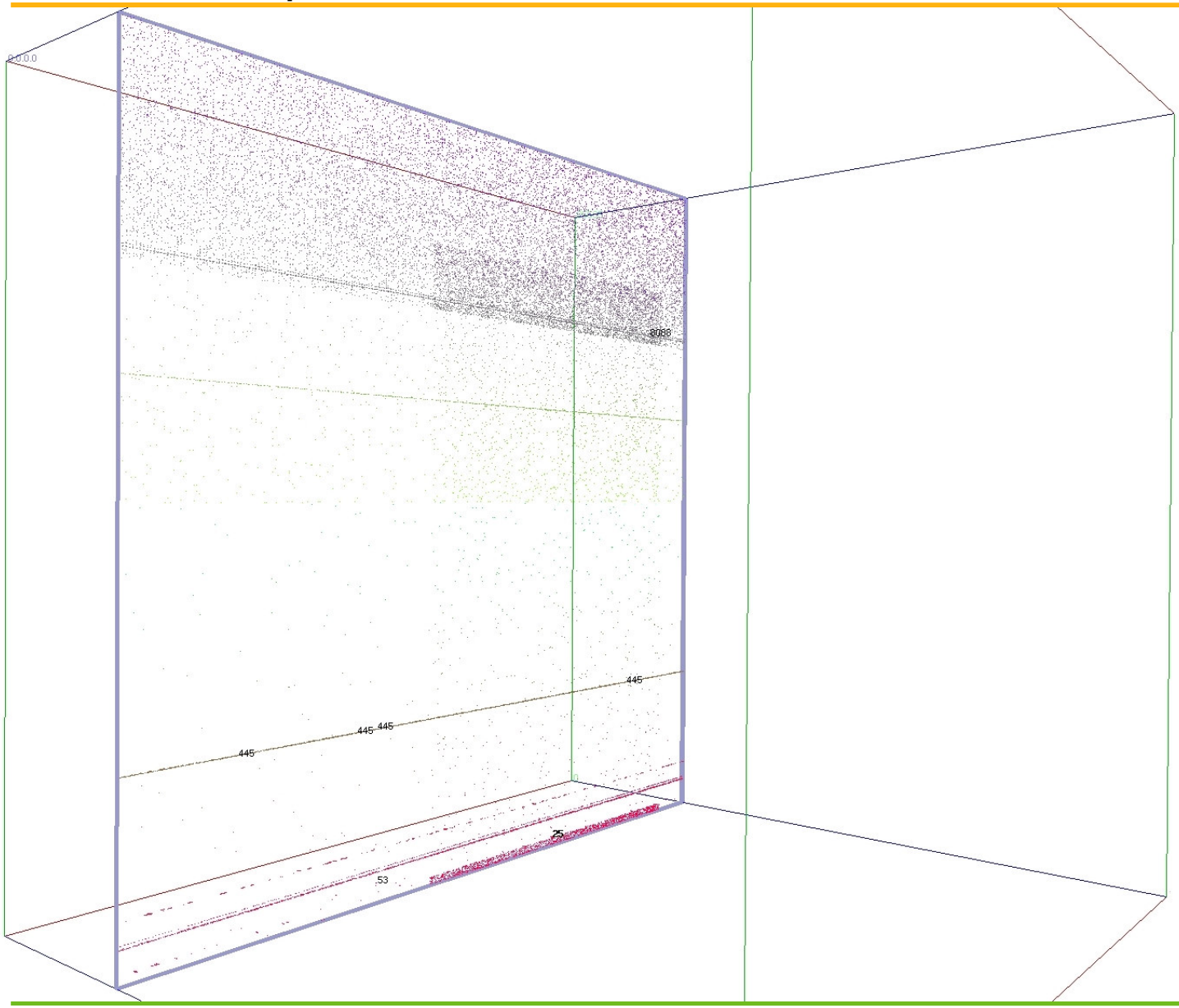
Intégralité des flux collectés



Motif d'attaque: le scan horizontal



Motif d'attaque: la muraille



Motif d'attaque: le plateau