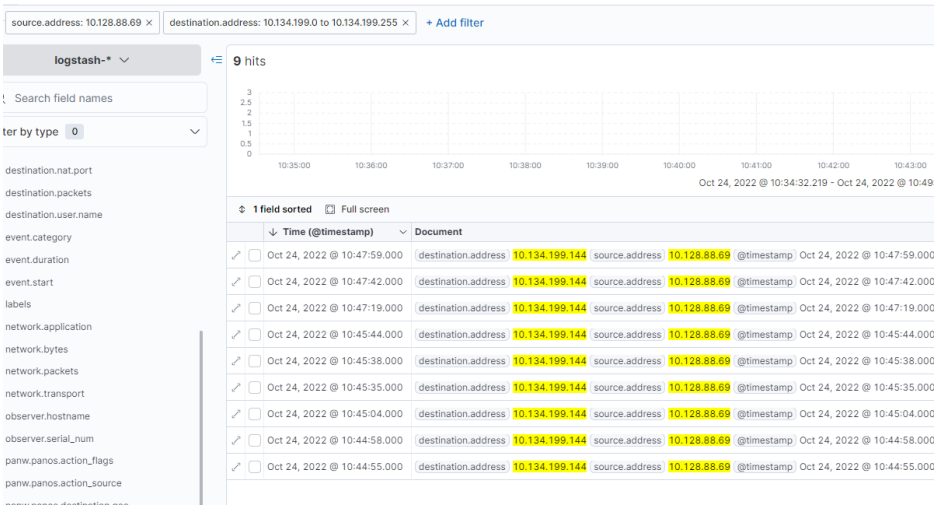
Kibana Tips

Subnet search

To filter a subnet for any variable for PA logs:

```
Add Filter -> Edit as Query DSL

{
  "query": {
    "range": {
      "<variable>": {
        "gte": "<first_subnet_ip>",
        "lt": "<last_subnet_ip>"
      }
    }
  }
}
```



Filter by Vsys:

Traffic logs are duplicated potentially so you can add the following +filter to a query to make sure you're searching the right firewall vsys!

- Datacenter Primary - panw.panos.vsys_name : SMPH-DDN (vsys14)
- Animal-Primary - panw.panos.vsys_name : SMPH-ANIMAL (vsys2)
- CSSC-Primary - panw.panos.vsys_name : SMPH-CSSC (vsys2)
- 432NM-Primary - panw.panos.vsys_name : SMPH-432NM (vsys38)