1. filebeat의 zeek 모듈 활성화

```
sudo filebeat modules enable zeek
```

2. Elasticsearch와 Kibana 실행

```
sudo ./start.sh
```

3. zeek.yml 파일 수정

```
sudo vim /etc/filebeat/modules.d/zeek.yml
```

```
# Module: zeek
# Docs: https://www.elastic.co/guide/en/beats/filebeat/main/filebeat-module-zeek.html

- module: zeek
  capture_loss:
    enabled: false
  connection:
    enabled: true
    var.paths: ["/home/remnux/Downloads/conn.log"]
  dce_rpc:
    enabled: true
    var.paths: ["/home/remnux/Downloads/dce_rpc.log"]
  dhcp:
    enabled: true
    var.paths: ["/home/remnux/Downloads/dhcp.log"]
  dnp3:
    enabled: false
  dns:
    enabled: true
```

```
  var.paths: ["/home/remnux/Downloads/dns.log"]
dpd:
  enabled: false
files:
  enabled: true
  var.paths: ["/home/remnux/Downloads/files.log"]
ftp:
  enabled: false
http:
  enabled: true
  var.paths: ["/home/remnux/Downloads/http.log"]
intel:
  enabled: false
irc:
  enabled: false
kerberos:
  enabled: true
  var.paths: ["/home/remnux/Downloads/kerberos.log"]
modbus:
  enabled: false
mysql:
  enabled: false
notice:
  enabled: false
ntp:
  enabled: true
  var.paths: ["/home/remnux/Downloads/ntp.log"]
ntlm:
  enabled: false
ocsp:
  enabled: true
  var.paths: ["/home/remnux/Downloads/ocsp.log"]
pe:
  enabled: false
radius:
  enabled: false
rdp:
```

```
  enabled: false
rfb:
  enabled: false
signature:
  enabled: false
sip:
  enabled: false
smb_cmd:
  enabled: false
smb_files:
  enabled: true
  var.paths: ["/home/remnux/Downloads/smb_files.log"]
smb_mapping:
  enabled: true
  var.paths: ["/home/remnux/Downloads/smb_mapping.log"]
smtp:
  enabled: false
snmp:
  enabled: false
socks:
  enabled: false
ssh:
  enabled: false
ssl:
  enabled: true
  var.paths: ["/home/remnux/Downloads/ssl.log"]
stats:
  enabled: false
syslog:
  enabled: false
traceroute:
  enabled: false
tunnel:
  enabled: false
weird:
  enabled: true
  var.paths: ["/home/remnux/Downloads/weird.log"]
```

```
x509:
  enabled: true
  var.paths: ["/home/remnux/Downloads/x509.log"]

  # Set custom paths for the log files. If left empty,
  # Filebeat will choose the paths depending on your OS.
  #var.paths:
```

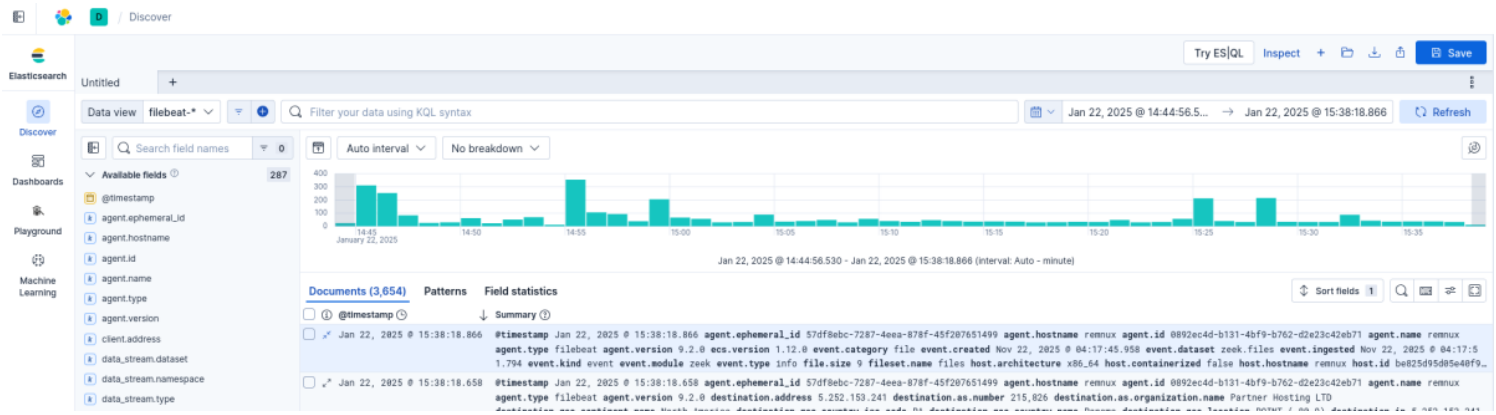
4. filebeat 대시보드 세팅 후 시작

```
sudo filebeat setup --dashboards
sudo systemctl start filebeat
sudo systemctl enable filebeat
```

5. zeek를 실행해서 json 형태로 로그 생성

```
echo "redef LogAscii::use_json=T;" > json-config.zeek
sudo docker run -it --rm -v $(pwd):/pcaps -w /pcaps zeek/zeek:lts \
  zeek -C -r 2025-01-22-traffic-analysis-exercise.pcap json-
config.zeek
```

6. 브라우저로 Kibana 접속해서 정상 작동 확인



# zeek.files.depth	0
# zeek.files.duration	0
k zeek.files.fuid	FhzZLM2k0cflHt4VY2
k zeek.files.id.orig_h	10.1.17.215
# zeek.files.id.orig_p	49,689
k zeek.files.id.resp_h	5.252.153.241
# zeek.files.id.resp_p	80
zeek.files.is_orig	false
zeek.files.local_orig	false
# zeek.files.missing_bytes	0
# zeek.files.overflow_bytes	0
# zeek.files.seen_bytes	9
k zeek.files.source	HTTP
zeek.files.timedout	false
# zeek.files.total_bytes	9
k zeek.files.uid	CdNdP91QAftg1×6XYc