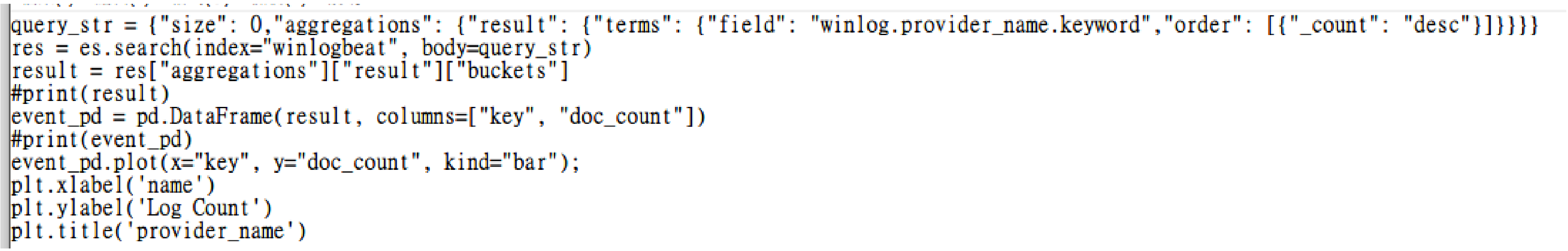
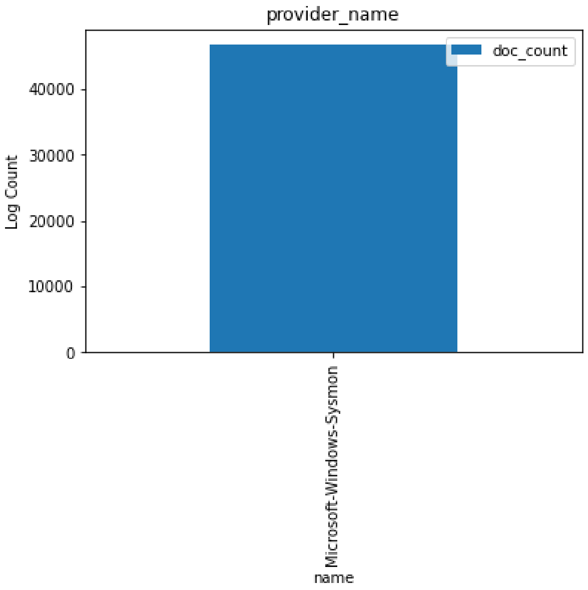
姓名：許魁珍

學號：108AB0748

班級：資財三乙



```
query_str = {"size": 0,"aggregations": {"result": {"terms": {"field": "winlog.provider_name.keyword","order": [{"_count": "desc"}]}}}}
res = es.search(index="winlogbeat", body=query_str)
result = res["aggregations"]["result"]["buckets"]
#print(result)
event_pd = pd.DataFrame(result, columns=["key", "doc_count"])
#print(event_pd)
event_pd.plot(x="key", y="doc_count", kind="bar");
plt.xlabel('name')
plt.ylabel('Log Count')
plt.title('provider_name')
```


provider_name
doc_count
Log Count
Microsoft-Windows-Sysmon
name