**Homework task**

**Introduction**

Create a console application to parse a log csv file and print out logs based on a custom query. Use the attached csv file to work with.

**Getting Started**

TODO:

1. Build solution that is able to search any column by full or partial text string. Example: "signatureId=’Microsoft-Windows-Security-Auditing:4608’“ or "signatureId=’*4608*’“ should return all the logs from the file. This functionality should work with all columns. if column is not found return "column not found. Query should be provided by user input. Query syntax can be in free form. Example:  
   [column\_name = ‘search\_string’] or [select FROM collum\_name WHERE text=’search\_string’]
2. Results from the query should be combined and returned in JSON format. Example see bellow.
3. Submit your code to a github repository.

Bonus points:

* Add Boolean logical operator support in the queries;
* Add multiple file support;
* Add log count value in the resulting JSON output;

Extra bonus points:

* Improvements are welcome 😊. For example: Deal with duplicates, combine results in a more readable format.
* Implement database layer. Save results in a database of your choice.
* Implement options to send alerts based on the severity of the log. No need to actually send the notification, you can use Console.WriteLine().

**JSON Example**

{

         "searchQuery": "deviceVendor='Microsoft'",

         "result": [{

                          "deviceVendor": "Microsoft",

                          "deviceProduct": "Windows Vista",

                          "deviceVersion": 1,

                          "signatureId": "Microsoft-Windows-Security-Auditing:4896",

                          "severity": 5,

                          "name": "One or more rows have been deleted from the certificate database.",

                          "start": "2022-05-29T04:53:43.560000Z",

                          "rt": "1653800023.56",

                          "msg": "One or more rows have been deleted from the certificate database.",

                          "shost": "DESKTOP-FQYFQMDY9RGD",

                          "smac": "60:6C:66:8a:4c:a5",

                          "dhost": "w2019r2008-srv",

                          "dmac": "38:00:25:b4:b0:3f",

                          "suser": "RIesa",

                          "suid": null,

                          "externalId": 4896,

                          "cs1Label": "payload",

                          "cs1": "",

                          "sproc": ""

                 },

                 {

                          "deviceVendor": "Microsoft",

                          "deviceProduct": "Windows Vista",

                          "deviceVersion": 1,

                          "signatureId": "Microsoft-Windows-Security-Auditing:4624",

                          "severity": 3,

                          "name": "An account was successfully logged on.",

                          "start": "2022-05-29T04:54:16.359000Z",

                          "rt": "1653800056.359",

                          "msg": "This event is generated when a logon session is created.",

                          "shost": "LENOVO-TZJUVSD7H",

                          "smac": "E4:A7:A0:65:60:dd",

                          "dhost": "w2014r2010-srv",

                          "dmac": "D8:3B:BF:0d:02:5a",

                          "suser": "LENOVO-TZJUVSD7H$",

                          "suid": 5e+188,

                          "externalId": 4624,

                          "cs1Label": "payload",

                          "cs1": "",

                          "sproc": ""

                 }

         ]

}