This is a readme file and I provide some guideline to run my program:

(1) Put the program into your workspace of Eclipse
(2) Make sure input file is at the same directory with src
(3) Add the external Jar dependencies
(4) Input the running parameters
(5) Get the result from local
(6) Get the result from Internet, currently it only supports https://isc.sans.edu/api/search

Next I will offer more details about the parameters
(1) The format of parameters is like : “XXX:XXXX”

(2) The program can support multiple parameter-constrained search. For example, if you wanna search a record with ip:192.168.1.1 and port:8080, the parameter is like:
“ip:192.168.1.1,port:8080”

(3) The && logic is represented as a comma (,) and || logic is represented as a whitespace. For example if you wanna search records either with a port:28 or port:29. The parameter is shown as:
“ip:28 ip:29”

(4) If you wanna specify another local file, you need you add a parameter “file:filename”

(5) Overall parameter type:

```
        [filename, pattern, request_raw, time, source, request_url]
        [date, destination_ip, signature, proto, header, sensor, classification, priority,                source_ip]
        [date, destination_ip, signature, destination_port, proto, source_port, header,             sensor, classification, priority, source_ip]
        [attackerIP, victimIP, victimPort, attackerPort, connectionType]
        [attackerIP, victimIP, shellcodeName, downloadMethod, victimPort, attackerPort,                connectionType, attackerID, vulnName, timestamp]
        e.g attackerip:xxx.xxx.xxx.xxx,attackerport:xxxx
                victimip:xxx.xxx.xxx.xxx
                attackerport:xxxx
                destination_ip:xxx.xxx.xxx.xxx
```

(6) It support “Blur Search” which means if you do not specify attackerip or victimip, you can just search “ip:XXX.XXX.XXX.XXX”. Blur Search also supports other parameters.

Next I will provide a running example:

```
Parameters input: file:honeypot.json  attackerip:
71.6.167.142,attackerport:48241  attackerPort:57230  attackerPort:
44621

Result:

*******************     Analyse from local file
*******************

Infomation for attackerport:57230 :
Source : Honeypot
{
        attackerIP : 162.197.24.67
        victimIP : 172.31.13.124
        victimPort : 80
        attackerPort : 57230
        connectionType : initial
        timestamp : 2014-09-28T04:55:17.147+0000
}

Infomation for attackerport:44621 :
Source : Honeypot
{
        attackerIP : 71.6.167.142
        victimIP : 172.31.13.124
        victimPort : 80
        attackerPort : 44621
        connectionType : initial
        timestamp : 2014-09-28T05:05:28.994+0000
}

Infomation for attackerip:71.6.167.142,attackerport:48241 :
Source : Honeypot
{
        attackerIP : 71.6.167.142
        victimIP : 172.31.13.124
        victimPort : 80
        attackerPort : 48241
        connectionType : initial
        timestamp : 2014-09-30T15:46:58.395+0000
}

Infomation for attackerport:44621 :
Source : Honeypot
{
        attackerIP : 54.169.100.200
        victimIP : 172.31.14.66
        victimPort : 443
        attackerPort : 44621
        connectionType : initial
        timestamp : 2014-10-18T00:50:10.187+0000
}

Infomation for attackerport:57230 :
Source : Honeypot
{
        attackerIP : 54.169.105.234
        victimIP : 172.31.14.66
        victimPort : 443
        attackerPort : 57230
        connectionType : initial
        timestamp : 2014-11-11T07:05:17.832+0000
}

Infomation for attackerport:57230 :
Source : Honeypot
{
        attackerIP : 199.115.117.65
        victimIP : 172.31.14.66
        victimPort : 3389
        attackerPort : 57230
        connectionType : initial
        timestamp : 2014-11-12T17:20:47.460+0000
}

Infomation for attackerport:44621 :
Source : Honeypot
{
        attackerIP : 104.171.112.125
        victimIP : 172.31.13.124
        victimPort : 110
        attackerPort : 44621
        connectionType : initial
        timestamp : 2014-11-21T14:45:52.562+0000
}

Infomation for attackerport:57230 :
Source : Honeypot
{
        attackerIP : 54.169.174.46
        victimIP : 172.31.14.66
        victimPort : 443
        attackerPort : 57230
        connectionType : initial
        timestamp : 2014-12-02T07:30:56.208+0000
}

Infomation for attackerport:44621 :
Source : Honeypot
{
        attackerIP : 14.35.234.212
        victimIP : 172.31.14.66
        victimPort : 80
        attackerPort : 44621
        connectionType : initial
        timestamp : 2014-12-07T14:49:19.319+0000
}

Infomation for attackerport:57230 :
Source : Honeypot
{
        attackerIP : 58.240.232.58
        victimIP : 172.31.14.66
        victimPort : 8080
        attackerPort : 57230
        connectionType : initial
        timestamp : 2014-12-28T16:37:06.630+0000
}

Infomation for attackerport:57230 :
Source : Honeypot
{
        attackerIP : 66.240.236.119
        victimIP : 172.31.14.66
        victimPort : 9999
        attackerPort : 57230
        connectionType : initial
        timestamp : 2015-01-14T14:30:31.086+0000
}


***********************     Analysis from API
***********************

Analysis for ip-71.6.167.142 for PARAM-< attackerip:
71.6.167.142,attackerport:48241 > :
Source : https://isc.sans.edu/api/
{
        IP : {
                assize : 106491
                maxdate : 2016-03-04
                count : 114756
                ascountry : US
                maxrisk : 10
                network : 71.6.128.0/17
                number : 71.6.167.142
                mindate : 2015-10-08
                asabusecontact : complaints@cari.net
                as : 10439
                asname : CARINET - CariNet, Inc.
                attacks : 10998
                threatfeeds : {
                        openbl_ftp :
{"lastseen":"2016-03-03","firstseen":"2015-09-04"}
                        ciarmy :
{"lastseen":"2016-03-03","firstseen":"2015-09-19"}
                        shodan :
{"lastseen":"2016-03-04","firstseen":"2015-11-02"}
                },
                comment : Used by ShodanHQ to perform Internet Wide
scans
                updated : 2016-03-04 03:36:26
                opendnsresolver : no
        }
}

Analysis for port-48241 for PARAM-< attackerip:
71.6.167.142,attackerport:48241 > :
Source : https://isc.sans.edu/api/
{
        number : 48241
        data : {
                datein : 2016-03-04
                portin : 48241
        },
        services : {
                udp : {
                        service : 0
                        name : 0
                },
                tcp : {
                        service : 0
                        name : 0
                }
        }
}

Analysis for port-57230 for PARAM-< attackerport:57230 > :
Source : https://isc.sans.edu/api/
{
        number : 57230
        data : {
                datein : 2016-03-04
                portin : 57230
        },
        services : {
                udp : {
                        service : 0
                        name : 0
                },
                tcp : {
                        service : 0
                        name : 0
                }
        }
}

Analysis for port-44621 for PARAM-< attackerport:44621 > :
Source : https://isc.sans.edu/api/
{
        number : 44621
        data : {
                datein : 2016-03-04
                portin : 44621
        },
        services : {
                udp : {
                        service : 0
                        name : 0
                },
                tcp : {
                        service : 0
                        name : 0
                }
        }
}


******************************     END
******************************
```