How I created 10 mln of viruses

„Viruses”

- V1 / V2 – simple downloader
  - Two flavors
- V3 – different hashes
  - random data added to the exe
- V4 – trolling at its finest
  - ~~So far…~~
- V5 – better, faster, more reliable.
- V6 – stay tuned…

V4

- Polymorphism made easy
  - Random string in printf
  - Random URL (both host, and file parts)
  - Randomly included pieces of code
    - = randomly imported functions
    - SNMP
  - Immutable parts
    - Domain name!

TCC

- FAST!
- And simple
- No optimizations
- Small output
- Can work as EXE and DLL
- In-memory compilation
- ONE INSTANCE AT A TIME ☹

Connecting dots

- IIS
    - ISAPI/CGI
- Folder for “viruses”
- 404 compiles new exe and serves it

Optimizations

- Hostname
- Block some IP addresses
- Compile from DLL
  - No TCC process creation
  - No 32bit anymore 😭
- RAMDisk?
- Header files (120kLoC → 27kLoC)
- CPU Affinity
- Timeouts
- Recycling
- Manual deletions

V5

- Load balancer
  - Scaling wide
  - No more “only one instance” limitations
  - Less downtime
- SNMP → BCrypt
- Urlmon → WinINet
  - Referer
  - User-Agent
- Telemetry

Staying safe

- Separate IP Address
- Burner domain with random name
- HTTPS? What about certificate?
- Random hostname
  - And what my registrar thinks about it
- Throttling (403 502)

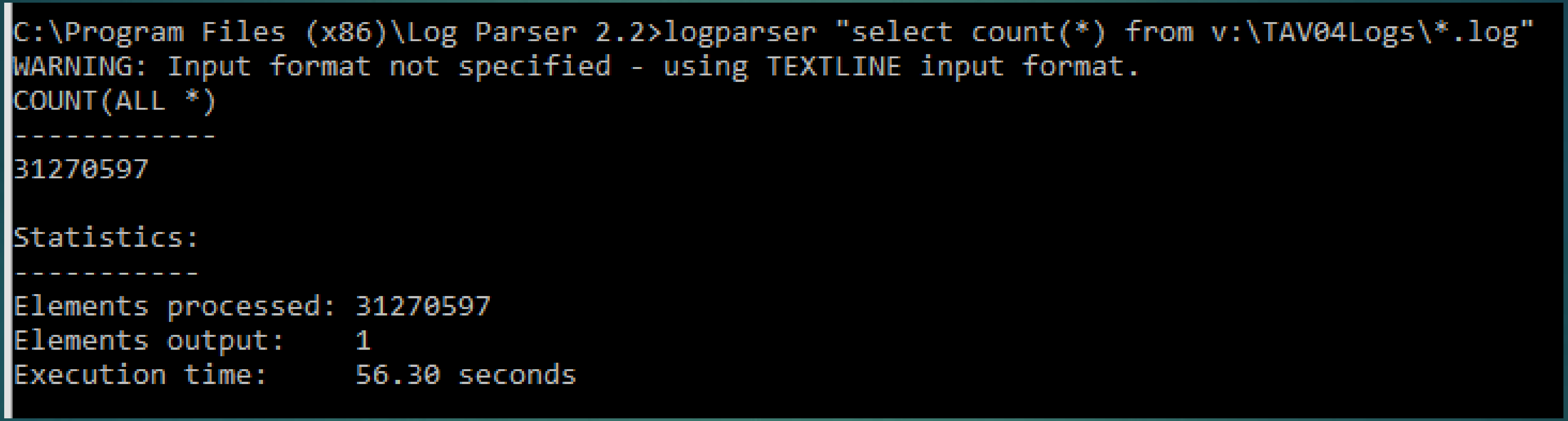
Antivirus

- Theory: Heuristics
  - Freshly registered domain
  - Fresh certificate
  - Creating exe files on a disk
  - No referrer
  - Child processes
  - x64/Win32
- Practice:
  - Well known domain string
  - Compiler

LogParser FTW!

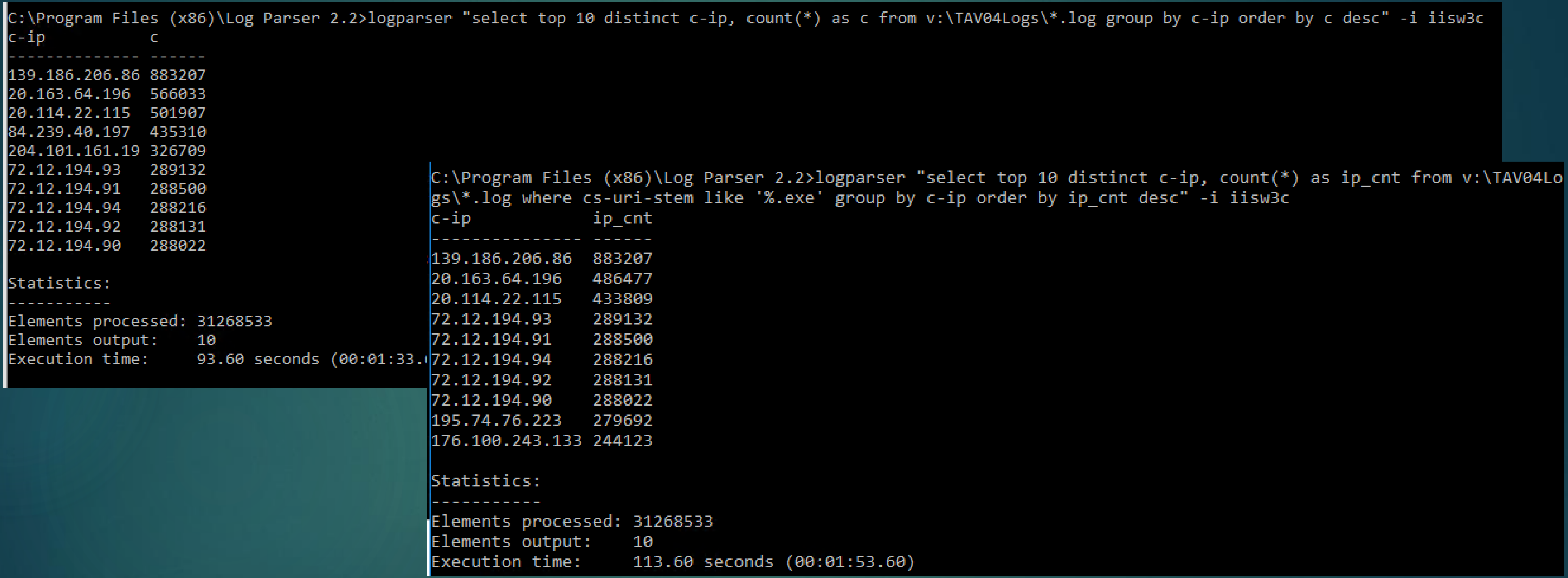
- https://www.microsoft.com/en-us/download/details.aspx?id=24659
- Well known
- Powerful
- Command line only, but some external helpers exist
- SQL-ish syntax
- Fast!
  - 100MB/s, 0.5Mqueries/s
  - Unless you have 30M+ entries in 7GB of logs...
  - 60-90s/query

Total queries



```
C:\Program Files (x86)\Log Parser 2.2>logparser "select count(*) from v:\TAV04Logs\*.log"
WARNING: Input format not specified - using TEXTLINE input format.
COUNT(ALL *)
------------
31270597

Statistics:
-----------
Elements processed: 31270597
Elements output:    1
Execution time:     56.30 seconds
```

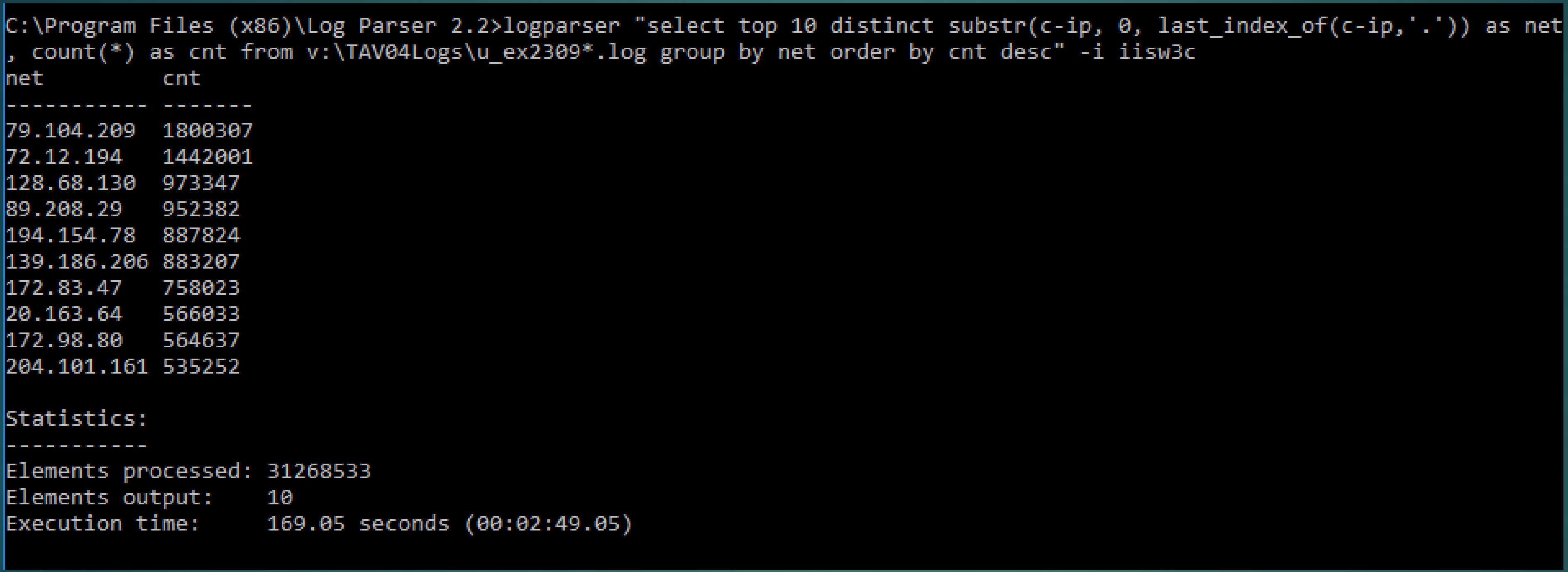
IPs



```
C:\Program Files (x86)\Log Parser 2.2>logparser "select top 10 distinct c-ip, count(*) as c from v:\TAV04Logs\*.log group by c-ip order by c desc" -i iisw3c
c-ip           c
-------------- ------
139.186.206.86 883207
20.163.64.196  566033
20.114.22.115  501907
84.239.40.197  435310
204.101.161.19 326709
72.12.194.93   289132
72.12.194.91   288500
72.12.194.94   288216
72.12.194.92   288131
72.12.194.90   288022

Statistics:
-----------
Elements processed: 31268533
Elements output:    10
Execution time:     93.60 seconds (00:01:33.
```

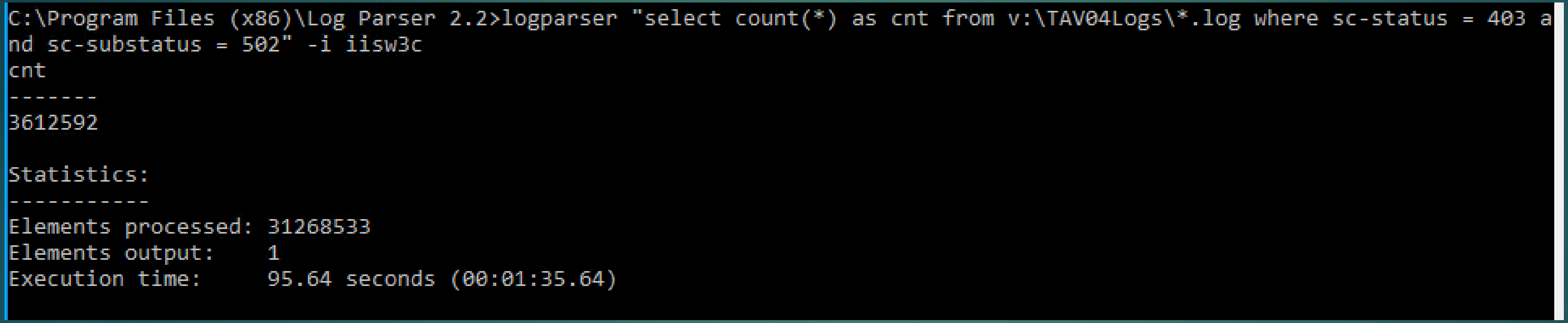
```
C:\Program Files (x86)\Log Parser 2.2>logparser "select top 10 distinct c-ip, count(*) as ip_cnt from v:\TAV04Lo
gs\*.log where cs-uri-stem like '%.exe' group by c-ip order by ip_cnt desc" -i iisw3c
c-ip            ip_cnt
--------------- ------
139.186.206.86  883207
20.163.64.196   486477
20.114.22.115   433809
72.12.194.93    289132
72.12.194.91    288500
72.12.194.94    288216
72.12.194.92    288131
72.12.194.90    288022
195.74.76.223   279692
176.100.243.133 244123

Statistics:
-----------
Elements processed: 31268533
Elements output:    10
Execution time:     113.60 seconds (00:01:53.60)
```

Networks



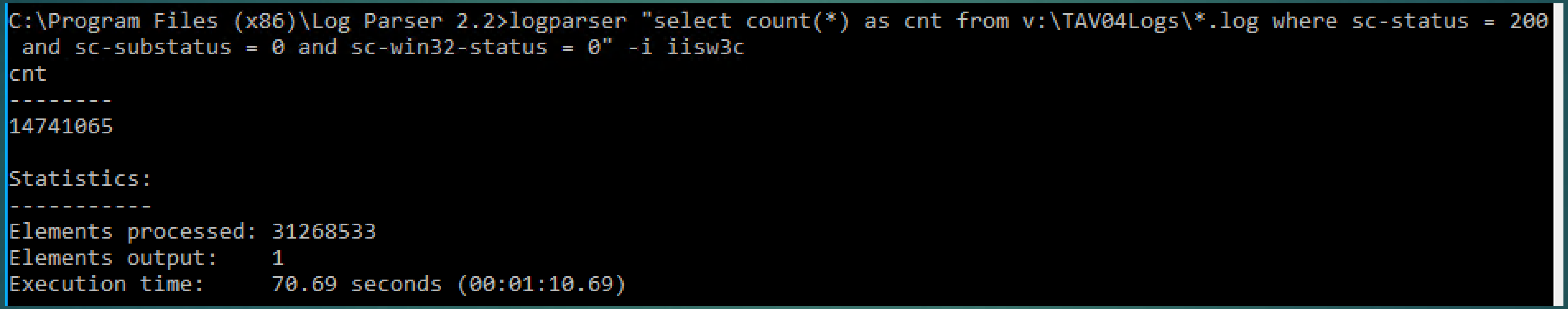
```
C:\Program Files (x86)\Log Parser 2.2>logparser "select top 10 distinct substr(c-ip, 0, last_index_of(c-ip,'.')) as net
, count(*) as cnt from v:\TAV04Logs\u_ex2309*.log group by net order by cnt desc" -i iisw3c
net         cnt
----------- -------
79.104.209  1800307
72.12.194   1442001
128.68.130  973347
89.208.29   952382
194.154.78  887824
139.186.206 883207
172.83.47   758023
20.163.64   566033
172.98.80   564637
204.101.161 535252

Statistics:
-----------
Elements processed: 31268533
Elements output:    10
Execution time:     169.05 seconds (00:02:49.05)
```

Excessive rate



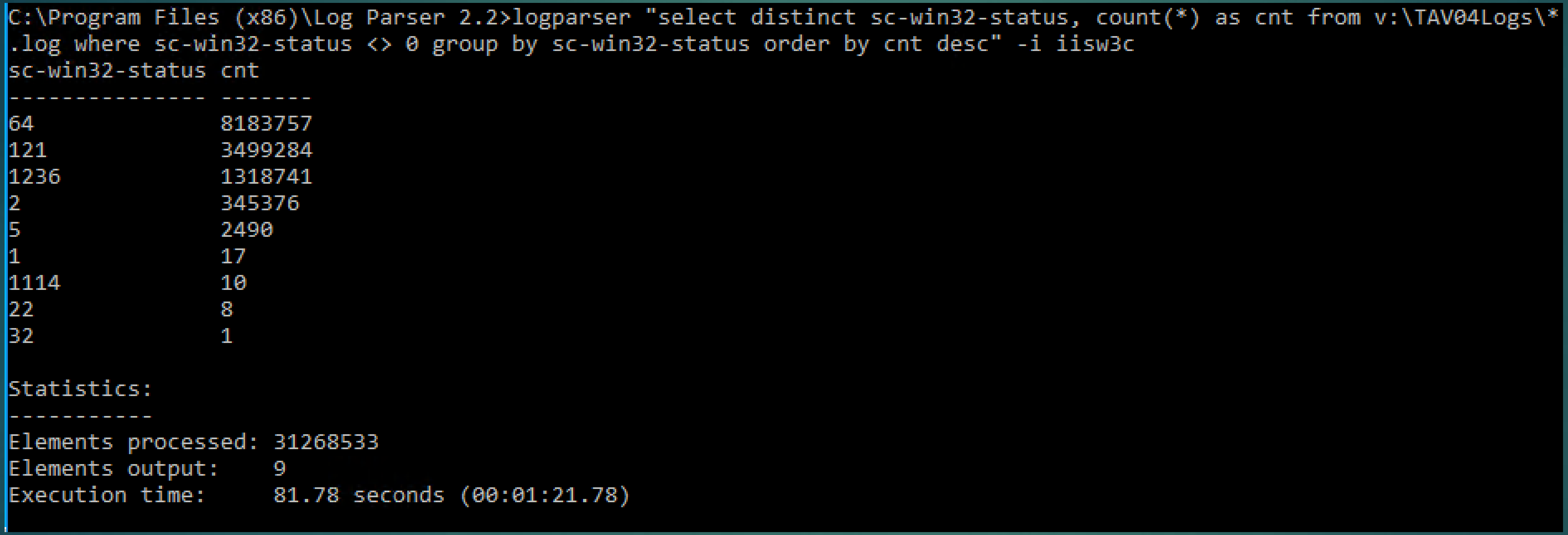
```
C:\Program Files (x86)\Log Parser 2.2>logparser "select count(*) as cnt from v:\TAV04Logs\*.log where sc-status = 403 a
nd sc-substatus = 502" -i iisw3c
cnt
-------
3612592

Statistics:
-----------
Elements processed: 31268533
Elements output:    1
Execution time:     95.64 seconds (00:01:35.64)
```

Successful responses



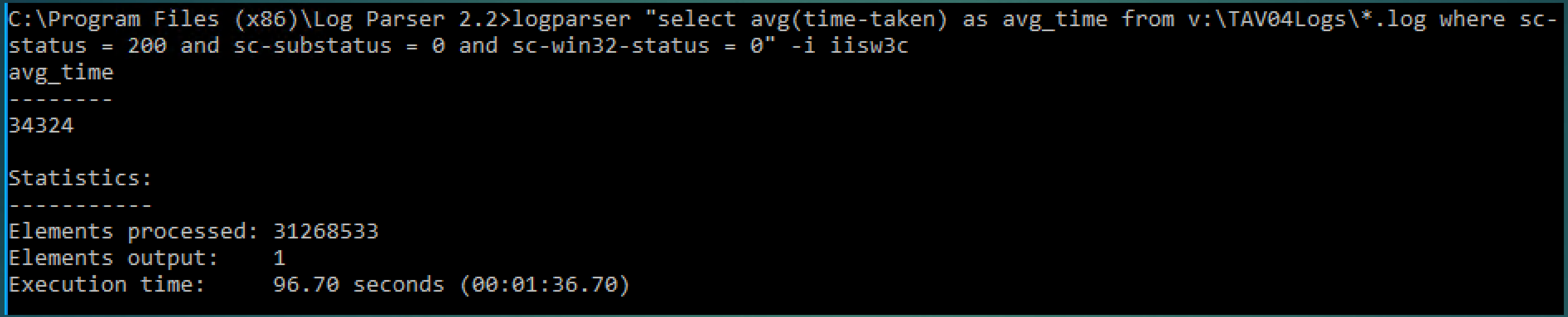
```
C:\Program Files (x86)\Log Parser 2.2>logparser "select count(*) as cnt from v:\TAV04Logs\*.log where sc-status = 200
 and sc-substatus = 0 and sc-win32-status = 0" -i iisw3c
cnt
--------
14741065

Statistics:
-----------
Elements processed: 31268533
Elements output:    1
Execution time:     70.69 seconds (00:01:10.69)
```

Win32 errors



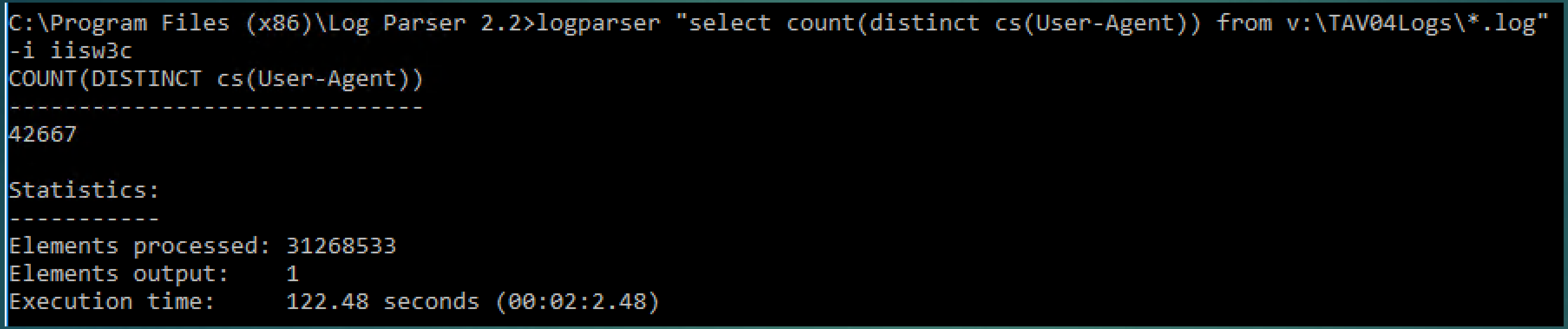
```
C:\Program Files (x86)\Log Parser 2.2>logparser "select distinct sc-win32-status, count(*) as cnt from v:\TAV04Logs\*
.log where sc-win32-status <> 0 group by sc-win32-status order by cnt desc" -i iisw3c
sc-win32-status cnt
--------------- -------
64              8183757
121             3499284
1236            1318741
2               345376
5               2490
1               17
1114            10
22              8
32              1

Statistics:
-----------
Elements processed: 31268533
Elements output:    9
Execution time:     81.78 seconds (00:01:21.78)
```

Performance



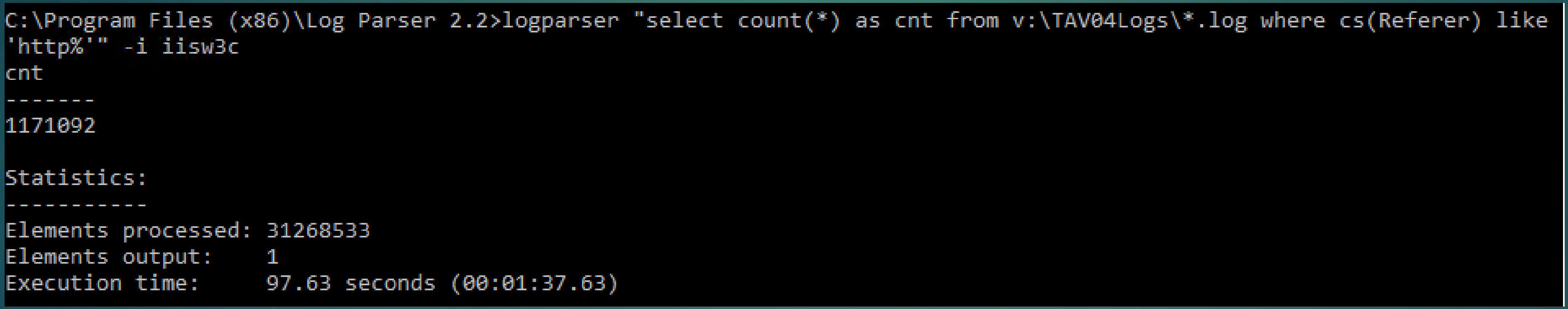
```
C:\Program Files (x86)\Log Parser 2.2>logparser "select avg(time-taken) as avg_time from v:\TAV04Logs\*.log where sc-
status = 200 and sc-substatus = 0 and sc-win32-status = 0" -i iisw3c
avg_time
--------
34324

Statistics:
-----------
Elements processed: 31268533
Elements output:    1
Execution time:     96.70 seconds (00:01:36.70)
```

User-Agents



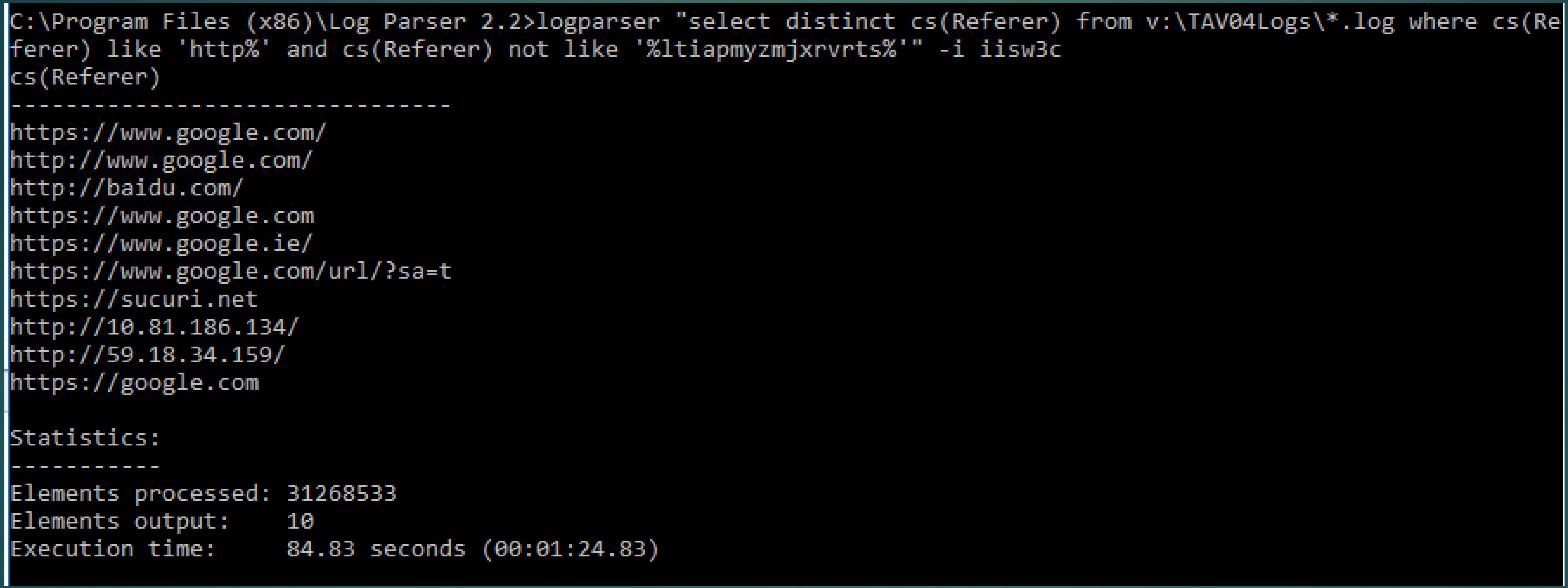
```
C:\Program Files (x86)\Log Parser 2.2>logparser "select count(distinct cs(User-Agent)) from v:\TAV04Logs\*.log"
-i iisw3c
COUNT(DISTINCT cs(User-Agent))
------------------------------
42667

Statistics:
-----------
Elements processed: 31268533
Elements output:    1
Execution time:     122.48 seconds (00:02:2.48)
```

Referrers?



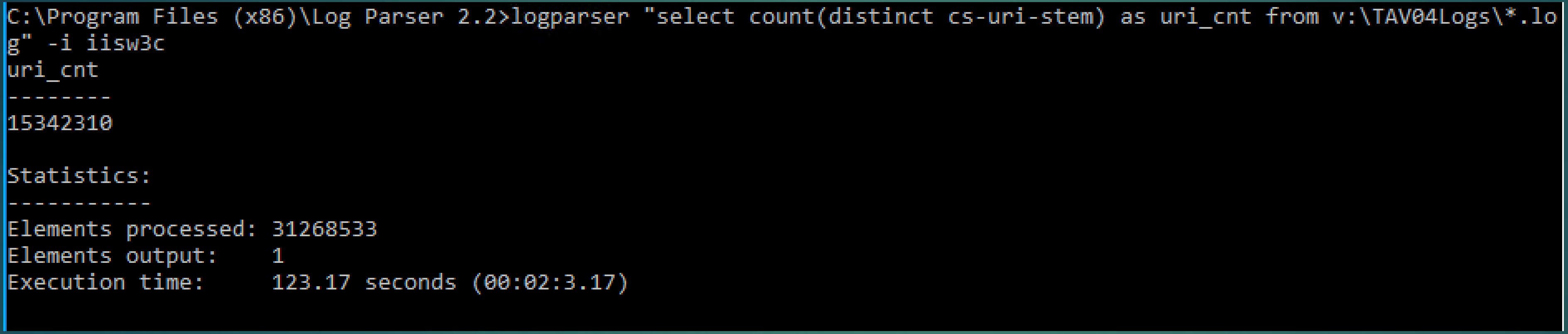
```
C:\Program Files (x86)\Log Parser 2.2>logparser "select count(*) as cnt from v:\TAV04Logs\*.log where cs(Referer) like
'http%'" -i iisw3c
cnt
-------
1171092

Statistics:
-----------
Elements processed: 31268533
Elements output:    1
Execution time:     97.63 seconds (00:01:37.63)
```

Referers



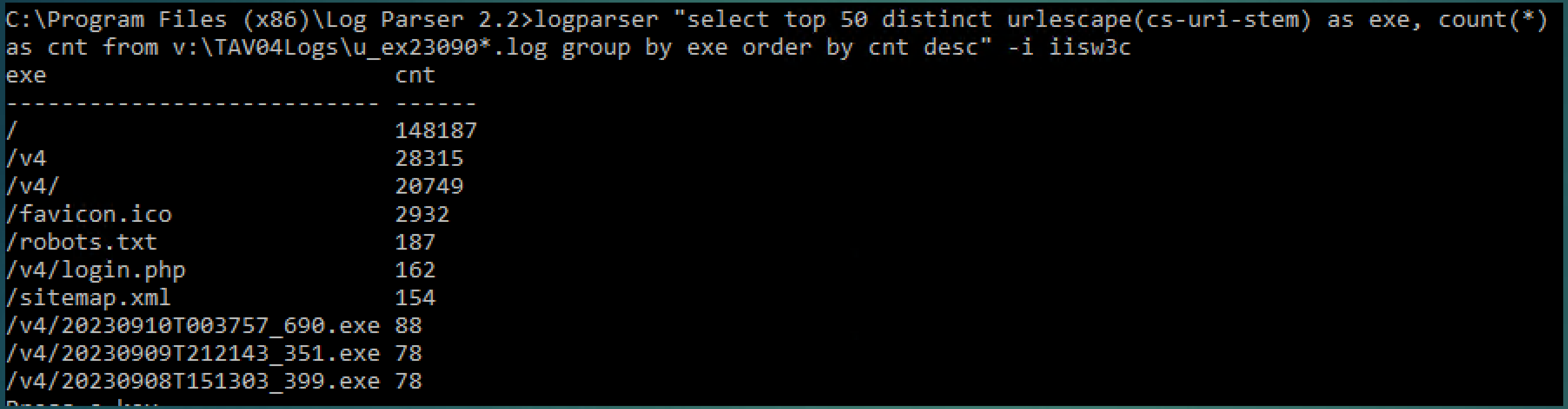
```
C:\Program Files (x86)\Log Parser 2.2>logparser "select distinct cs(Referer) from v:\TAV04Logs\*.log where cs(Re
ferer) like 'http%' and cs(Referer) not like '%ltiapmyzmjxrvrts%'" -i iisw3c
cs(Referer)
--------------------------------
https://www.google.com/
http://www.google.com/
http://baidu.com/
https://www.google.com
https://www.google.ie/
https://www.google.com/url/?sa=t
https://sucuri.net
http://10.81.186.134/
http://59.18.34.159/
https://google.com

Statistics:
-----------
Elements processed: 31268533
Elements output:    10
Execution time:     84.83 seconds (00:01:24.83)
```

URIs



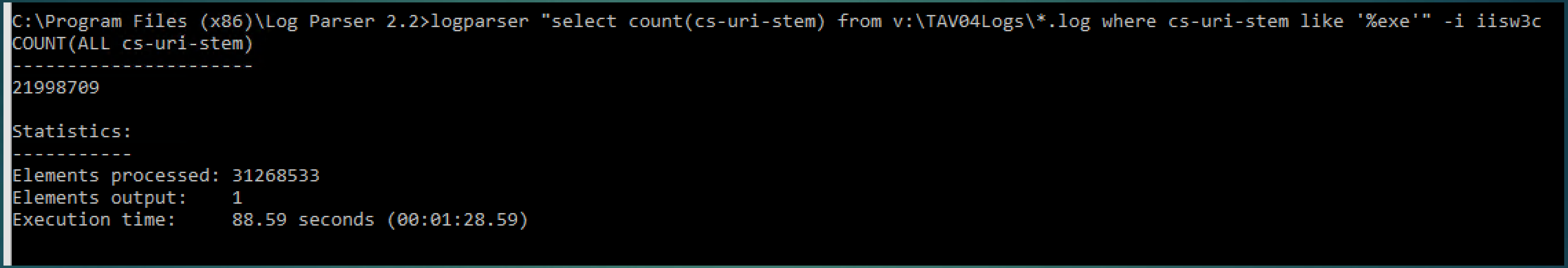
```
C:\Program Files (x86)\Log Parser 2.2>logparser "select count(distinct cs-uri-stem) as uri_cnt from v:\TAV04Logs\*.lo
g" -i iisw3c
uri_cnt
--------
15342310

Statistics:
-----------
Elements processed: 31268533
Elements output:    1
Execution time:     123.17 seconds (00:02:3.17)
```

Common URIs



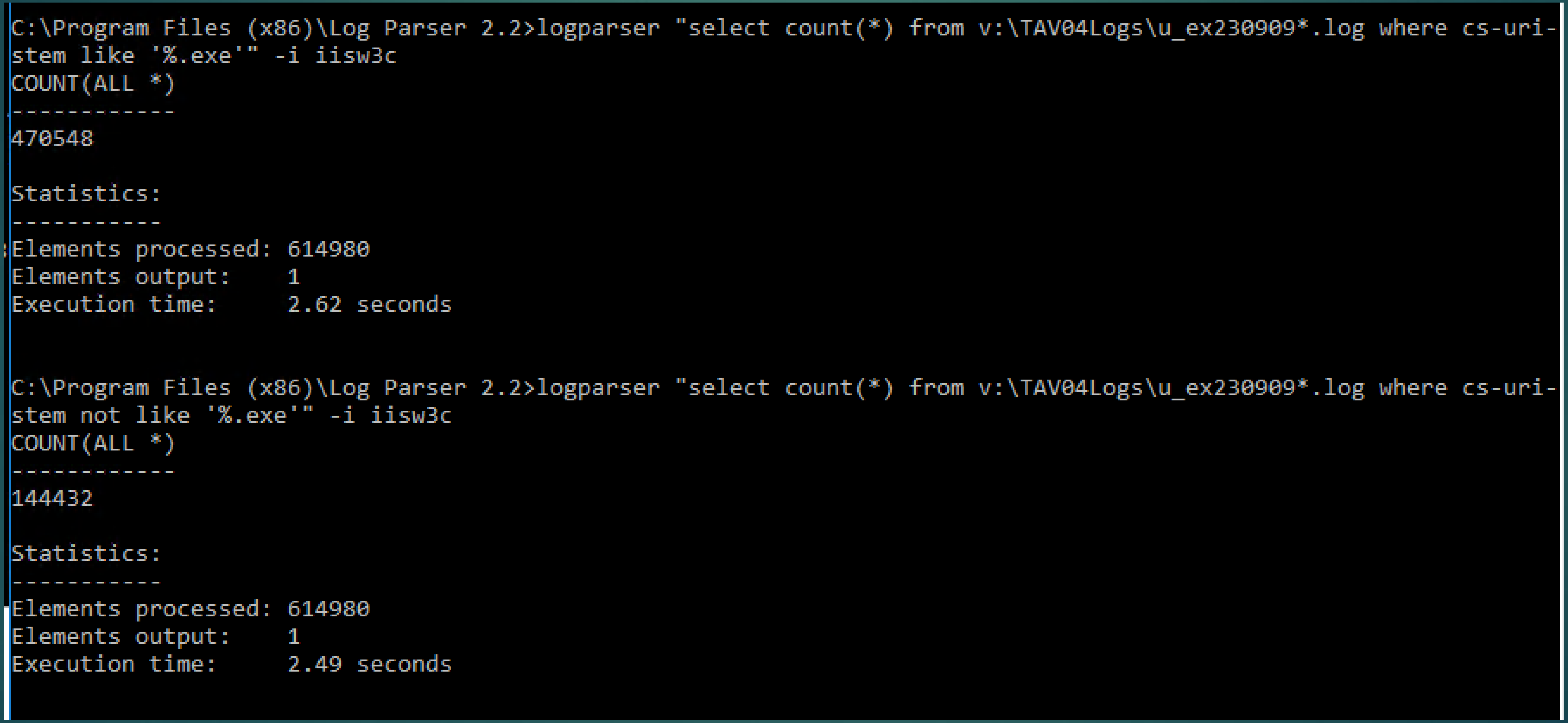
```
C:\Program Files (x86)\Log Parser 2.2>logparser "select top 50 distinct urlescape(cs-uri-stem) as exe, count(*)
as cnt from v:\TAV04Logs\u_ex23090*.log group by exe order by cnt desc" -i iisw3c
exe                          cnt
---------------------------- ------
/                            148187
/v4                          28315
/v4/                         20749
/favicon.ico                 2932
/robots.txt                  187
/v4/login.php                162
/sitemap.xml                 154
/v4/20230910T003757_690.exe 88
/v4/20230909T212143_351.exe 78
/v4/20230908T151303_399.exe 78
```

EXE



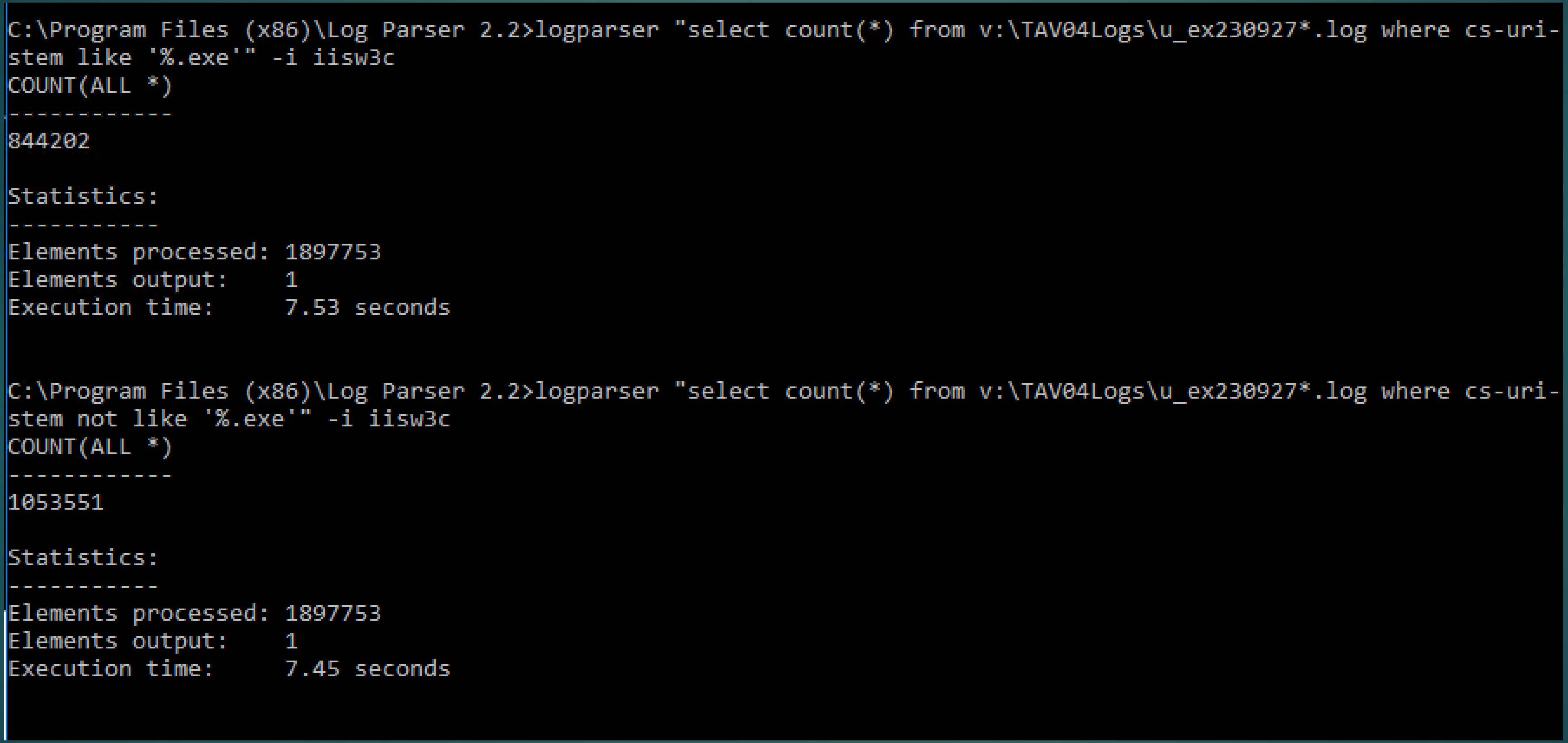
```
C:\Program Files (x86)\Log Parser 2.2>logparser "select count(cs-uri-stem) from v:\TAV04Logs\*.log where cs-uri-stem like '%exe'" -i iisw3c
COUNT(ALL cs-uri-stem)
----------------------
21998709

Statistics:
-----------
Elements processed: 31268533
Elements output:    1
Execution time:     88.59 seconds (00:01:28.59)
```

EXE vs others 9.09



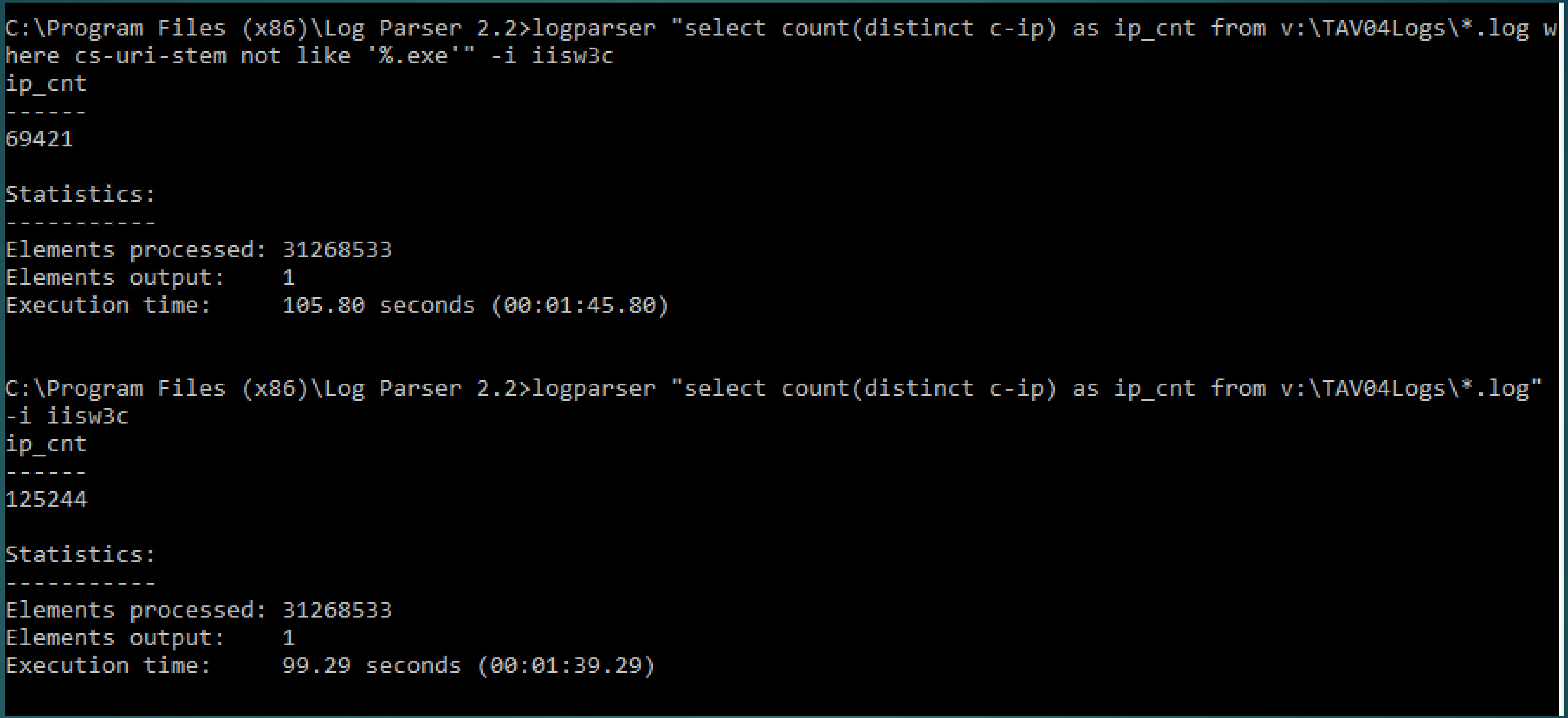
```
C:\Program Files (x86)\Log Parser 2.2>logparser "select count(*) from v:\TAV04Logs\u_ex230909*.log where cs-uri-
stem like '%.exe'" -i iisw3c
COUNT(ALL *)
------------
470548

Statistics:
-----------
Elements processed: 614980
Elements output:    1
Execution time:     2.62 seconds


C:\Program Files (x86)\Log Parser 2.2>logparser "select count(*) from v:\TAV04Logs\u_ex230909*.log where cs-uri-
stem not like '%.exe'" -i iisw3c
COUNT(ALL *)
------------
144432

Statistics:
-----------
Elements processed: 614980
Elements output:    1
Execution time:     2.49 seconds
```

EXE vs Others 27.09



```
C:\Program Files (x86)\Log Parser 2.2>logparser "select count(*) from v:\TAV04Logs\u_ex230927*.log where cs-uri-
stem like '%.exe'" -i iisw3c
COUNT(ALL *)
------------
844202

Statistics:
-----------
Elements processed: 1897753
Elements output:    1
Execution time:     7.53 seconds


C:\Program Files (x86)\Log Parser 2.2>logparser "select count(*) from v:\TAV04Logs\u_ex230927*.log where cs-uri-
stem not like '%.exe'" -i iisw3c
COUNT(ALL *)
------------
1053551

Statistics:
-----------
Elements processed: 1897753
Elements output:    1
Execution time:     7.45 seconds
```

Number of scanning IPs



```
C:\Program Files (x86)\Log Parser 2.2>logparser "select count(distinct c-ip) as ip_cnt from v:\TAV04Logs\*.log w
here cs-uri-stem not like '%.exe'" -i iisw3c
ip_cnt
------
69421

Statistics:
-----------
Elements processed: 31268533
Elements output:    1
Execution time:     105.80 seconds (00:01:45.80)


C:\Program Files (x86)\Log Parser 2.2>logparser "select count(distinct c-ip) as ip_cnt from v:\TAV04Logs\*.log"
-i iisw3c
ip_cnt
------
125244

Statistics:
-----------
Elements processed: 31268533
Elements output:    1
Execution time:     99.29 seconds (00:01:39.29)
```

Future (a.k.a. v6)

- GCC?
- (Even) more data in queries
- CreateProcess()
- Generate non-PE format(?)
- Put some misleading strings into a file
- Better Sleep()