

ngrep 抓包工具初体验

作者: [flowaters](#)

原文链接: <https://ld246.com/article/1532404227266>

来源网站: [链滴](#)

许可协议: [署名-相同方式共享 4.0 国际 \(CC BY-SA 4.0\)](#)

背景

linux/mac下调试http请求是很常见的需求，而且常常需要定位是客户端还是服务端的问题。

这时候，我们就需要一个抓包工具。

常见的抓包工具有wireshark, tcpflow等。

对于抓http请求，有没有更方便的工具呢？

根据我们运维同学的推荐，还真有一个工具，就是ngrep。

安装

mac下安装

```
brew install ngrep
```

linux下安装

```
wget http://rpmfind.net/linux/dag/redhat/el6/en/x86_64/dag/RPMS/ngrep-1.45-2.el6.rf.x86_64.rpm  
rpm -ivh ngrep-1.45-2.el6.rf.x86_64.rpm
```

或者

```
wget "https://rpmfind.net/linux/epel/7/x86_64/Packages/n/ngrep-1.47-0.1.a39256b.el7.x86_64.rpm"  
rpm -ivh ngrep-1.47-0.1.a39256b.el7.x86_64.rpm
```

简单使用

抓80端口的包

抓包语句： **ngrep port 80**

模拟发送请求

```
[note@abeffect ~]$ curl -s "www.hacpai.com"  
<html>  
<head><title>301 Moved Permanently</title></head>  
<body bgcolor="white">  
<center><h1>301 Moved Permanently</h1></center>  
<hr><center>nginx/1.13.12</center>  
</body>  
</html>
```

抓包结果：

```
####
```

```
T 30.30.140.17:54351 -> 118.31.188.179:80 [AP]
GET / HTTP/1.1..Host: www.hacpai.com..User-Agent: curl/7.54.0..Accept: */*....
##
T 118.31.188.179:80 -> 30.30.140.17:54351 [AP]
HTTP/1.1 301 Moved Permanently..Server: nginx/1.13.12..Date: Tue, 24 Jul 2018 02:45:35 GM
..Content-Type: text/html..Content-Length: 186..Connection: keep-alive..Location: https://hacp
i.com/....<html>..
```

可以看到，结果是抓到了，但是内容没有完整显示出来。

支持换行符

内容要完整显示，其示就是把换行符展示出来。

```
ngrep -Wbyline port 80
```

结果

```
#####
T 30.30.140.17:55286 -> 118.31.188.179:80 [AP]
GET / HTTP/1.1.
Host: www.hacpai.com.
User-Agent: curl/7.54.0.
Accept: */*.
.

##
T 118.31.188.179:80 -> 30.30.140.17:55286 [AP]
HTTP/1.1 301 Moved Permanently.
Server: nginx/1.13.12.
Date: Tue, 24 Jul 2018 03:04:13 GMT.
Content-Type: text/html.
Content-Length: 186.
Connection: keep-alive.
Location: https://hacpai.com/.
.
<html>.
<head><title>301 Moved Permanently</title></head>.
<body bgcolor="white">.
<center><h1>301 Moved Permanently</h1></center>.
<hr><center>nginx/1.13.12</center>.
</body>.
</html>.
```

支持正则

包其实太多了，怎么只抓hacpai的包呢，通过-q参数

```
ngrep -Wbyline -q hacpai port 80
```

```
ngrep -Wbyline 'GET /' port 80
```

结果

```
T 30.30.140.17:55294 -> 118.31.188.179:80 [AP]
GET / HTTP/1.1.
Host: www.hacpai.com.
User-Agent: curl/7.54.0.
Accept: */*.
.
```

```
T 118.31.188.179:80 -> 30.30.140.17:55294 [AP]
HTTP/1.1 301 Moved Permanently.
Server: nginx/1.13.12.
Date: Tue, 24 Jul 2018 03:04:45 GMT.
Content-Type: text/html.
Content-Length: 186.
Connection: keep-alive.
Location: https://hacpai.com/.
.
<html>.
<head><title>301 Moved Permanently</title></head>.
<body bgcolor="white">.
<center><h1>301 Moved Permanently</h1></center>.
<hr><center>nginx/1.13.12</center>.
</body>.
</html>.
```

十六进制显示

如果需要具体调试包中的bytes，想看到16进制的数，怎么办呢？

```
ngrep -x -q hacpai port 80
```

结果

```
T 30.30.140.17:55588 -> 118.31.188.179:80 [AP]
47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31 0d 0a GET / HTTP/1.1..
48 6f 73 74 3a 20 77 77 77 2e 68 61 63 70 61 69 Host: www.hacpai
2e 63 6f 6d 0d 0a 55 73 65 72 2d 41 67 65 6e 74 .com..User-Agent
3a 20 63 75 72 6c 2f 37 2e 35 34 2e 30 0d 0a 41 : curl/7.54.0..A
63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 0d 0a ccept: */*....

T 118.31.188.179:80 -> 30.30.140.17:55588 [AP]
48 54 54 50 2f 31 2e 31 20 33 30 31 20 4d 6f 76 HTTP/1.1 301 Mov
65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a ed Permanently..
53 65 72 76 65 72 3a 20 6e 67 69 6e 78 2f 31 2e Server: nginx/1.
31 33 2e 31 32 0d 0a 44 61 74 65 3a 20 54 75 65 13.12..Date: Tue
2c 20 32 34 20 4a 75 6c 20 32 30 31 38 20 30 33 , 24 Jul 2018 03
3a 32 30 3a 34 38 20 47 4d 54 0d 0a 43 6f 6e 74 :20:48 GMT..Cont
65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 68 ent-Type: text/h
74 6d 6c 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e tml..Content-Len
67 74 68 3a 20 31 38 36 0d 0a 43 6f 6e 6e 65 63 gth: 186..Connec
74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 tion: keep-alive
0d 0a 4c 6f 63 61 74 69 6f 6e 3a 20 68 74 74 70 ..Location: http
```

```
73 3a 2f 2f 68 61 63 70 61 69 2e 63 6f 6d 2f 0d s://hacpai.com/.
0a 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 ...<html>..<head
3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 ><title>301 Move
64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 d Permanently</t
69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 itle></head>..<b
6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 ody bgcolor="whi
74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 te">..<center><h
31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 1>301 Moved Perm
61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 anently</h1></ce
6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 nter>..<hr><cent
65 72 3e 6e 67 69 6e 78 2f 31 2e 31 33 2e 31 32 er>nginx/1.13.12
3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 </center>..</bod
79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a y>..</html>..
```

完整文档

请自行查看manual。

参考

- [ngrep使用方法](#)
- [linux命令之ngrep\(网络抓包工具的使用\)](#)