tcpflow: invalid option -- '-'

tcpflow[5517]: error: unrecognized switch '?'

TCPFLOW version 1.4.5

usage: tcpflow [-aBcCDhJpsvVZ] [-b max\_bytes] [-d debug\_level]

[-[eE] scanner] [-f max\_fds] [-F[ctTXMkmg]] [-i iface] [-L semlock]

[-m min\_bytes] [-o outdir] [-r file] [-R file]

[-S name=value] [-T template] [-w file] [-x scanner] [-X xmlfile]

[expression]

-a: 做所有的后处理。

-b max\_bytes: 每流保存的最大字节数

-d debug\_level:调试级别；默认为1

-f: 使用的文件描述符的最大数量

-h:打印帮助信息（- HH更多的帮助）

-H: 打印每一个扫描仪的详细信息

-i:网络接口上的听

-I: 产生时间分组->字节索引文件的每一个流程（。Findex）

-g: 输出每个流交替的颜色（请注意更改！）

-l: 治疗非标志参数作为输入文件而不是一个pcap的表达

-L semlock -指定写入使用命名信号量锁定

-p:不要使用混杂模式

-q: 静音模式-不打印警告

-r file:阅读从tcpdump PCAP文件包（可重复）

-R file: 阅读从tcpdump PCAP文件完成连接包

-v: 详细的操作相当于D 10

-V: 打印版本号和退出

-w file: 写入未处理到文件的数据包

-o outdir :指定输出目录（默认值）。

-X filename :dfxml输出文件名

-m bytes : 指定启动一个新的流的跳过（默认为16777216）。

-F{p} : 文件名前缀/后缀（- HH选项）

-T{t} : 文件名模板(-hh for options; default %A.%a-%B.%b%V%v%C%c)

-Z: 不要解压缩gzip压缩HTTP事务

控制扫描仪:

-E scanner - 关闭所有扫描仪，除了扫描仪

-S name=value 配置参数设置（- HH信息）

可设置的选项（和他们的默认值）：

-S enable\_report=YES 生成 report.xml ()

-S http\_cmd= 命令对每个HTTP连接的执行（HTTP）

-S http\_alert\_fd=-1 文件描述符发送信息完成HTTP连接（HTTP）

-S netviz\_histogram\_dump=0 将直方图（netViz）

-S netviz\_histogram\_size=1000 最大尺寸（netViz）直方图

-S tcp\_timeout=0 TCP连接超时（tcpdemux）

-S check\_fcs=YES 需要有效的帧校验和（FCS）（wifiviz）

-e http - enable scanner http

-e md5 - enable scanner md5

-e netviz - enable scanner netviz

-e wifiviz - enable scanner wifiviz

-x tcpdemux - disable scanner tcpdemux

Console output options:

-B: 二进制输出，即使用C或C（通常是C或C关闭它）

-c: 控制台打印只（不创建文件）

-C: 控制台打印，但没有源/ dest标题显示

-0: 不打印换行后打印到控制台时，包

-s: 带非打印字符（改为“。”）

-D: 在十六进制输出（有用的结合- C或C）

表达：tcpdump像过滤的表达

查看更多信息的人页。

文件名前缀:

-Fc : 在所有的文件连接计数器

-Ft : 在time\_t时间戳的文件名

-FT : 在时间戳的ISO8601的所有文件名

-FX : 不输出任何文件（其他比报告文件）

-FM : 计算每个流的MD5（店dfxml）

-Fk :以1k目录本输出

-Fm : 在1M的目录本输出（2级）

-Fg :1g目录本输出（3级）

文件名模板格式:

%A/%a - source IP address/port; %B/%b - dest IP address/port

%E/%e - source/dest Ethernet Mac address

%V/%v - VLAN number, '--' if no vlan/'' if no vlan

%T/%t - Timestamp in ISO8601 format/unix time\_t

%c - connection\_count for connections>0 / %# for all connections; %C - 'c' if connection\_count >0

%N - (connection\_number ) % 1000

%K - (connection\_number / 1000) % 1000

%M - (connection\_number / 1000000) % 1000

%G - (connection\_number / 1000000000) % 1000

%% - Output a '%'

-S name=value options:

tdelta=0 秒时间三角洲

DEBUG Levels (specify with -dNN):

get\_max\_fds() = 1024

NUM\_RESERVED\_FDS = 6