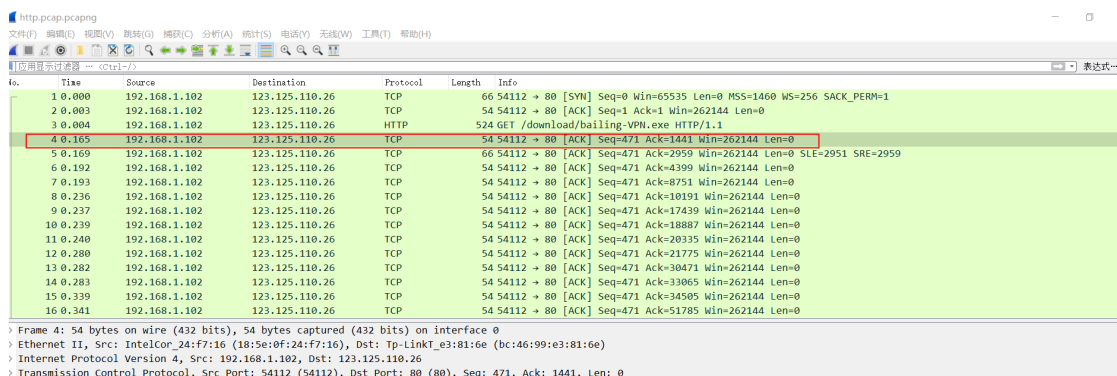


1. 需求：镜像数据转成 netflow

把网卡上的镜像数据以 netflow 的方式送出，（网卡上只有 http 的请求报文）具体要求如下：

1. 保证性能，用 c 语言实现，提供源码；
2. Flow 流开始报文是 http get 报文后的第一个 ack 报文，具体截图如下：



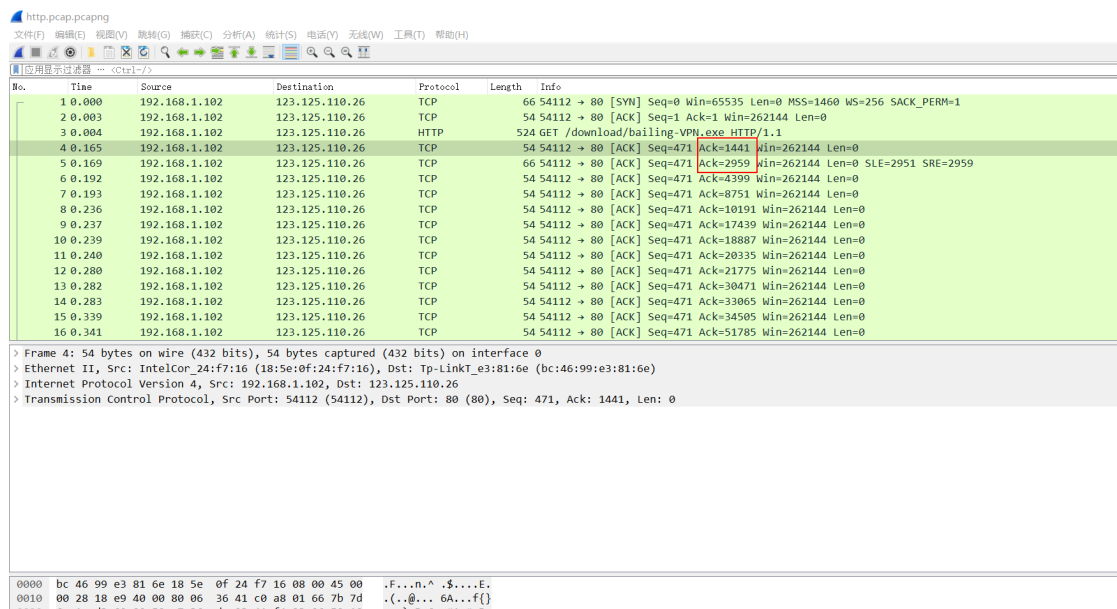
| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------|---------------|----------------|----------|--------|--|
| 1 | 0.000 | 192.168.1.102 | 123.125.110.26 | TCP | 66 | 54112 → 80 [SVN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 2 | 0.003 | 192.168.1.102 | 123.125.110.26 | TCP | 54 | 54112 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0 |
| 3 | 0.004 | 192.168.1.102 | 123.125.110.26 | HTTP | 524 | GET /download/bailing-VPN.exe HTTP/1.1 |
| 4 | 0.165 | 192.168.1.102 | 123.125.110.26 | TCP | 54 | 54112 → 80 [ACK] Seq=471 Ack=1441 Win=262144 Len=0 |
| 5 | 0.169 | 192.168.1.102 | 123.125.110.26 | TCP | 66 | 54112 → 80 [ACK] Seq=471 Ack=2959 Win=262144 Len=0 SLE=2951 SRE=2959 |
| 6 | 0.192 | 192.168.1.102 | 123.125.110.26 | TCP | 54 | 54112 → 80 [ACK] Seq=471 Ack=4399 Win=262144 Len=0 |
| 7 | 0.193 | 192.168.1.102 | 123.125.110.26 | TCP | 54 | 54112 → 80 [ACK] Seq=471 Ack=8751 Win=262144 Len=0 |
| 8 | 0.236 | 192.168.1.102 | 123.125.110.26 | TCP | 54 | 54112 → 80 [ACK] Seq=471 Ack=10191 Win=262144 Len=0 |
| 9 | 0.237 | 192.168.1.102 | 123.125.110.26 | TCP | 54 | 54112 → 80 [ACK] Seq=471 Ack=17439 Win=262144 Len=0 |
| 10 | 0.239 | 192.168.1.102 | 123.125.110.26 | TCP | 54 | 54112 → 80 [ACK] Seq=471 Ack=18887 Win=262144 Len=0 |
| 11 | 0.240 | 192.168.1.102 | 123.125.110.26 | TCP | 54 | 54112 → 80 [ACK] Seq=471 Ack=20335 Win=262144 Len=0 |
| 12 | 0.280 | 192.168.1.102 | 123.125.110.26 | TCP | 54 | 54112 → 80 [ACK] Seq=471 Ack=21775 Win=262144 Len=0 |
| 13 | 0.282 | 192.168.1.102 | 123.125.110.26 | TCP | 54 | 54112 → 80 [ACK] Seq=471 Ack=30471 Win=262144 Len=0 |
| 14 | 0.283 | 192.168.1.102 | 123.125.110.26 | TCP | 54 | 54112 → 80 [ACK] Seq=471 Ack=33065 Win=262144 Len=0 |
| 15 | 0.339 | 192.168.1.102 | 123.125.110.26 | TCP | 54 | 54112 → 80 [ACK] Seq=471 Ack=34505 Win=262144 Len=0 |
| 16 | 0.341 | 192.168.1.102 | 123.125.110.26 | TCP | 54 | 54112 → 80 [ACK] Seq=471 Ack=51785 Win=262144 Len=0 |

> Frame 4: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
> Ethernet II, Src: IntelCor_24:f7:16 (18:5e:0f:24:f7:16), Dst: Tp-LinkT_e3:81:6e (bc:46:99:e3:81:6e)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 123.125.110.26
> Transmission Control Protocol, Src Port: 54112 (54112), Dst Port: 80 (80), Seq: 471, Ack: 1441, Len: 0

该报文的时间戳作为 first switch；

需求更正：Flow 流开始的 sync 报文

3. Netflow 中的 bytes 以当前报文的 ack num 减去同一流中上一个报文的 ack num



| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------|---------------|----------------|----------|--------|--|
| 1 | 0.000 | 192.168.1.102 | 123.125.110.26 | TCP | 66 | 54112 → 80 [SVN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 2 | 0.003 | 192.168.1.102 | 123.125.110.26 | TCP | 54 | 54112 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0 |
| 3 | 0.004 | 192.168.1.102 | 123.125.110.26 | HTTP | 524 | GET /download/bailing-VPN.exe HTTP/1.1 |
| 4 | 0.165 | 192.168.1.102 | 123.125.110.26 | TCP | 54 | 54112 → 80 [ACK] Seq=471 Ack=1441 Win=262144 Len=0 |
| 5 | 0.169 | 192.168.1.102 | 123.125.110.26 | TCP | 66 | 54112 → 80 [ACK] Seq=471 Ack=2959 Win=262144 Len=0 SLE=2951 SRE=2959 |
| 6 | 0.192 | 192.168.1.102 | 123.125.110.26 | TCP | 54 | 54112 → 80 [ACK] Seq=471 Ack=4399 Win=262144 Len=0 |
| 7 | 0.193 | 192.168.1.102 | 123.125.110.26 | TCP | 54 | 54112 → 80 [ACK] Seq=471 Ack=8751 Win=262144 Len=0 |
| 8 | 0.236 | 192.168.1.102 | 123.125.110.26 | TCP | 54 | 54112 → 80 [ACK] Seq=471 Ack=10191 Win=262144 Len=0 |
| 9 | 0.237 | 192.168.1.102 | 123.125.110.26 | TCP | 54 | 54112 → 80 [ACK] Seq=471 Ack=17439 Win=262144 Len=0 |
| 10 | 0.239 | 192.168.1.102 | 123.125.110.26 | TCP | 54 | 54112 → 80 [ACK] Seq=471 Ack=18887 Win=262144 Len=0 |
| 11 | 0.240 | 192.168.1.102 | 123.125.110.26 | TCP | 54 | 54112 → 80 [ACK] Seq=471 Ack=20335 Win=262144 Len=0 |
| 12 | 0.280 | 192.168.1.102 | 123.125.110.26 | TCP | 54 | 54112 → 80 [ACK] Seq=471 Ack=21775 Win=262144 Len=0 |
| 13 | 0.282 | 192.168.1.102 | 123.125.110.26 | TCP | 54 | 54112 → 80 [ACK] Seq=471 Ack=30471 Win=262144 Len=0 |
| 14 | 0.283 | 192.168.1.102 | 123.125.110.26 | TCP | 54 | 54112 → 80 [ACK] Seq=471 Ack=33065 Win=262144 Len=0 |
| 15 | 0.339 | 192.168.1.102 | 123.125.110.26 | TCP | 54 | 54112 → 80 [ACK] Seq=471 Ack=34505 Win=262144 Len=0 |
| 16 | 0.341 | 192.168.1.102 | 123.125.110.26 | TCP | 54 | 54112 → 80 [ACK] Seq=471 Ack=51785 Win=262144 Len=0 |

> Frame 4: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
> Ethernet II, Src: IntelCor_24:f7:16 (18:5e:0f:24:f7:16), Dst: Tp-LinkT_e3:81:6e (bc:46:99:e3:81:6e)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 123.125.110.26
> Transmission Control Protocol, Src Port: 54112 (54112), Dst Port: 80 (80), Seq: 471, Ack: 1441, Len: 0

第 5 个包文作为 flow 流的第二个报文，该报文的 bytes 是红色框标出的相减。

需求更正：字节数属性：是同一个流中，最后一个报文的 ack num

4. Flow 流的结束，可以参考 fprobe, softflowd。
5. 封装三个字段分别用来存放 http 协议中的的 uri, host, referrer

2. 使用手册：

编译：

```
./configure  
make
```

启动：

```
sudo ./src/fprobe -i eth0 -S 1500 -f tcp localhost:6688
```

此处 eth0 为监听接口， 1500 为抓包大小， tcp 为监听数据包类型

默认情况下，netflow 输出接口与监听接口相同，如果需要把 netflow 输出到特定接口，例如：
输出到 eth2，启动参数追加 -o eth2，启动命令为：sudo ./src/fprobe -i eth0 -S 1500 -f tcp -o eth2 localhost:6688

数据包封装格式：

| 包格式： | MAC | IP | UDP | Netflow v5 Head | Netflow v5 pdu | Host | Referer | URI |
|------|-----|----|-----|-----------------|----------------|------|---------|-----|
| 字节数： | 14 | 20 | 8 | 24 | 48 | 64 | 256 | 384 |

封装后数据包总大小为 818 Bytes.