**Session**:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| direction | timestamp | IP header | TCP header | data + padding |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **域名** | **注释** | **映射值** | **说明** |
| direction | 包的方向  [C→S, S→C] | [1,0]  [0,1] | 2 item |
| timestamp | 包时间戳 | relative time | 1 item |
| **IP header** | IP 层头部字段 | **IP-header-map** | 4 items |
| **TCP header** | TCP层头部字段 | **TCP-header-map** | 5 items |
| data | 应用层数据 | data + padding | 数据+填充 |

|  |  |  |  |
| --- | --- | --- | --- |
| **IP header map** | | | |
| **域名** | **注释** | **映射值** | **说明** |
| ip\_v | ip\_hl | 版本和首部长度 | None | 需剔除信息 |
| ip\_tos | 服务类型 | None | 需剔除信息 |
| ip\_len | 全长 | ip\_len | 1 item |
| ip\_id | 标识符 | None | 需剔除信息 |
| ip\_off | 标志和分片偏移 | 2位标识|偏移 | 2 items |
| ip\_ttl | 生存时间 | ip\_ttl | 1 item |
| ip\_p | 传输层协议 | None | 需剔除信息 |
| ip\_cksum | 首部校验和 | None | 需剔除信息 |
| ip\_src | 源IP地址 | None | 需剔除信息 |
| ip\_dst | 目的IP地址 | None | 需剔除信息 |

|  |  |  |  |
| --- | --- | --- | --- |
| **TCP-header-map** | | | |
| **域名** | **注释** | **映射值** | **说明** |
| th\_sport | 源端口号 | None | 需剔除信息 |
| th\_dport | 目的端口号 | None | 需剔除信息 |
| th\_seq | 序列号 | relative seq | 1 item |
| th\_ack | 确认号 | None | 需剔除信息 |
| th\_off | 首部长度 | None | 需剔除信息 |
| th\_x2 | 保留域 | None | 需剔除信息 |
| URG | 紧急指针有效标志 | 0|1 | 1 item |
| ACK | 确认序号有效标志 | None | 需剔除信息 |
| PSH | push数据标志 | 0|1 | 1item |
| RST | 重建连接 | None | 需剔除信息 |
| SYN | 同步序号发起连接 | None | 需剔除信息 |
| FIN | 完成发送任务标志 | None | 需剔除信息 |
| th\_win | 窗口大小 | th\_win | 1 item |
| th\_sum | 校验和 | None | 需剔除信息 |
| th\_urp | 紧急指针 | th\_urp | 1item |

数据段以128字节截断，每个流截取前128个包

（12 + 128）\* 128 = 140 \* 128

UDP数据包的表示