| Name | Type | 描述 | 備註 |
| --- | --- | --- | --- |
| srcip | nominal | Src IP address | Header |
| sport | integer | Src port number | Header |
| dstip | nominal | Dst IP address | Header |
| dsport | integer | Dst port number | Header |
| proto | nominal | Transaction protocol | Header |
| state | nominal | State (ex: TCP 有 SYN/ACK) | Header |
| dur | Float | Record total duration | flow裡最後一筆資料的時間 - 第一筆資料的時間 |
| sbytes | Integer | 在這個flow， src總共傳了多少東西給dst | 從Header拿到每個pkt的byte 再加總 |
| dbytes | Integer | 在這個flow， dst總共傳了多少東西給src | 從Header拿到每個pkt的byte 再加總 |
| sttl | Integer | Src TTL (還能被轉傳幾次) | flow裡每個pkt的ttl加總取平均 |
| dttl | Integer | Dst TTL | flow裡每個pkt的ttl加總取平均 |
| sloss | Integer | Src pkt 重傳或丟掉的次數 | flow裡每個pkt的loss加總 (看TCP的sequence num) |
| dloss | Integer | Dst pkt 重傳或丟掉的次數 | flow裡每個pkt的loss加總 (看TCP的sequence num) |
| service | nominal | http, ftp, smtp, ssh, dns, ftp-data ,irc and (-) if not much used service | Header |
| Sload | Float | Src bits per second | Header(Rate) -> 從wireshirk |
| Dload | Float | Dst bits per second | Header(Rate) -> 從wireshirk |
| Spkts | integer | Src to destination packet count | flow裡的pkt數 |
| Dpkts | integer | Dst to source packet count | flow裡的pkt數 |
| swin | integer | Src TCP windows size | Header(TCP) |
| dwin | integer | Dst TCP windows size | Header(TCP) |
| stcpb | integer | Src TCP base seq num | Header(TCP) |
| dtcpb | integer | Dst TCP base seq num | Header(TCP) |
| smeansz | integer | Mean of Flow pkt size | Header 取平均 |
| dmeansz | integer | Mean of Flow pkt size | Header 取平均 |
| trans\_depth | integer | the pipelined depth into the connection of http request/response transaction | 每次能平行傳輸的數目？ |
| res\_bdy\_len | integer | Actual uncompressed content size of the data transferred from the server?s http service. |  |
| Sjit | Float | Src jitter (mSec) | 拿不到 |
| Djit | Float | Dst jitter (mSec) | 拿不到 |
| Stime | Timestamp | record start time | flow裡第一個pkt的timestamp |
| Ltime | Timestamp | record last time | flow裡最後一個pkt的timestamp |
| Sintpkt | Float | Source interpacket arrival time (mSec) |  |
| Dintpkt | Float | Destination interpacket arrival time (mSec) |  |
| tcprtt | Float | synack + ackdat |  |
| synack | Float | TCP SYN跟SYN\_ACK之間的時間 |  |
| ackdat | Float | TCP SYN\_ACK 跟 ACK之間的時間 |  |
| is\_sm\_ips\_ports | Binary | 1 -> flow裡Src IP == Dst IP 且 Src Port == Dst Port (或Port == 0)  0 -> 不是1 |  |
| ct\_state\_ttl | Integer | No. for each state (6) according to specific range of values for source/destination time to live (10) (11). |  |
| ct\_flw\_http\_mthd | Integer | No. of flows that has methods such as Get and Post in http service. |  |
| is\_ftp\_login | Binary | If the ftp session is accessed by user and password then 1 else 0. | 看FTP Header |
| ct\_ftp\_cmd | integer | No of flows that has a command in ftp session. | 看FTP Header |
| ct\_srv\_src | integer | No. of connections that contain the same service (14) and source address (1) in 100 connections according to the last time (26). | 為什麼是100? |
| ct\_srv\_dst | integer | No. of connections that contain the same service (14) and destination address (3) in 100 connections according to the last time (26). |  |
| ct\_dst\_ltm | integer | No. of connections of the same destination address (3) in 100 connections according to the last time (26). |  |
| ct\_src\_ ltm | integer | No. of connections of the same source address (1) in 100 connections according to the last time (26). |  |
| ct\_src\_dport\_ltm | integer | No of connections of the same source address (1) and the destination port (4) in 100 connections according to the last time (26). |  |
| ct\_dst\_sport\_ltm | integer | No of connections of the same destination address (3) and the source port (2) in 100 connections according to the last time (26). |  |
| ct\_dst\_src\_ltm | integer | No of connections of the same source (1) and the destination (3) address in in 100 connections according to the last time (26). |  |
| attack\_cat | nominal | 攻擊的種類 | 9種 |
| Label | binary | 0 -> 非攻擊  1 -> 攻擊 |  |