Suricata - Bug #5133
DCERP: master - logs not created
02/19/2022 02:41 PM - Peter Manev

Status: New
Priority: Normal
Assignee: OISF Dev
Category: TBD
Target version: TBD
Affected Versions: git master
Effort: TBD

Description
Using midstream (due to the pcap nature)

7.0.0-dev (b1c09369a 2022-02-17)

with the following pcap
the DCERP events are not created, even though the flow has app_proto set as dcerpc (example)

```
{
    "timestamp": "2020-07-19T20:26:24.971636+0200",
    "flow_id": 1011604658379232,
    "event_type": "flow",
    "src_ip": "172.16.66.36",
    "src_port": 49683,
    "dest_ip": "172.16.66.1",
    "dest_port": 50059,
    "proto": "TCP",
    "app_proto": "dcerpc",
    "flow": {
        "pkts_toserver": 14,
        "pkts_toclient": 16,
        "bytes_toserver": 2312,
        "bytes_toclient": 3824,
        "start": "2020-07-19T20:26:24.973280+0200",
        "end": "2020-07-19T20:26:36.004852+0200",
        "age": 12,
        "state": "established",
        "reason": "shutdown",
        "alerted": false
    },
    "tcp": {
        "tcp_flags": "19",
        "tcp_flags_ts": "19",
        "tcp_flags_tc": "18",
        "fin": true,
        "psh": true,
        "ack": true,
        "state": "established"
    }
}
```

History
#1 - 02/19/2022 02:42 PM - Peter Manev

to reproduce

```
```