Table of Contents

The system allows to record the traffic for selected protocols in PCAP format. It can save metadata of HTTP requests in log files.

To record the data in PCAP format: please use the following parameters in configuration file /etc/dpi/fastdpi.conf:

```
ajb_save_udpi=1
ajb_save_udpi_proto=OSPFIGP:ospf-lite
ajb_udpi_path=/var/dump/dpi
ajb_save_ip=192.168.0.0/24
```

Here: ajb_save_udpi=1 - activate the traffic recording for a list of protocols
ajb_udpi_path=/var/dump/dpi - is a directory to place log files (/var/dump/dpi by default)
ajb_save_udpi_proto=OSPFIGP:ospf-lite - is a list of protocols to record as test or numerical identificators, . This is a hot parameter. It can be changed on the run by instruction **service fastdpi reload**
ajb_save_ip=192.168.0.0/24 - activate the traffic recording by IP or CIDR (0.0.0.0/0 - to record all the traffic)

To record HTTP requests' metadata: please use the following parameters in configuration file /etc/dpi/fastdpi.conf:

```
ajb_save_url=-1
ajb_save_url_format=ts:prg:login:ipsrc:ipdst:host:path:ref:uagent:cookie
ajb_url_path=/var/dump/dpi
```

Here:
ajb_save_url=-1 - activate recording of HTTP metadata
ajb_url_path=/var/dump/dpi - is the directory to place files with these records (/var/dump/dpi by default)
ajb_save_url_format=ts:prg:login:ipsrc:ipdst:host:path:ref:uagent:cookie - is the list of metadata to record:

```
ts - is a time stamp
prg - is: id of the active services at the moment of request
login - subscriber's login
ipsrc - subscriber's IP address
ipdst - host IP address (that of the request's addressee)
host - the host name (Host field)
path - the path to the requested resource (URI)
ref - from where (Referer field)
uagent - browser's type (User-Agent field)
cookie - Cookie
```

To record SIP requests' metadata: please use the following parameters in configuration file /etc/dpi/fastdpi.conf:

```
ajb_save_sip=1
ajb_sip_ftimeout=15
ajb_sip_path=/home/sip
```

```
ajb_save_sip_format=ts:ssid:ipsrc:ipdst:login:msg:scode:from:to:callid:uagen
t
```

here
ajb_save_sip=1 activate the SIP metadata recording in a file
ajb_sip_path==/home/sip directory for SIP metadata files (default /var/dump/dpi)
ajb_sip_ftimeout=15 record timeout between files
ajb_save_sip_format=ts:ssid:ipsrc:ipdst:login:msg:scode:from:to:callid:uagent list of SIP metadate fields, here

```
ts - time stamp
ssid - session identifier (it's used to link to Netflow/IPFIX data to get
bytes volume)
ipsrc - subscribers' IP
ipdst - server IP
login - subscribers' LOGIN (from RADIUS)
msg - message type
scode - status-code
from - phone/identifier of calling party
to - phone/identifier of called party
callid - call identifier
uagent - type of handset (User-Agent)
```

If you set the configuration parameter

```
ajb_reserved=1
```

the memory for a buffer is allocated in advance (on DPI start) and you can start and stop data recording on the run. You only need to change parameters ajb_save_url, ajb_save_udpi and ajb_save_ip.