

# Qe-Packets

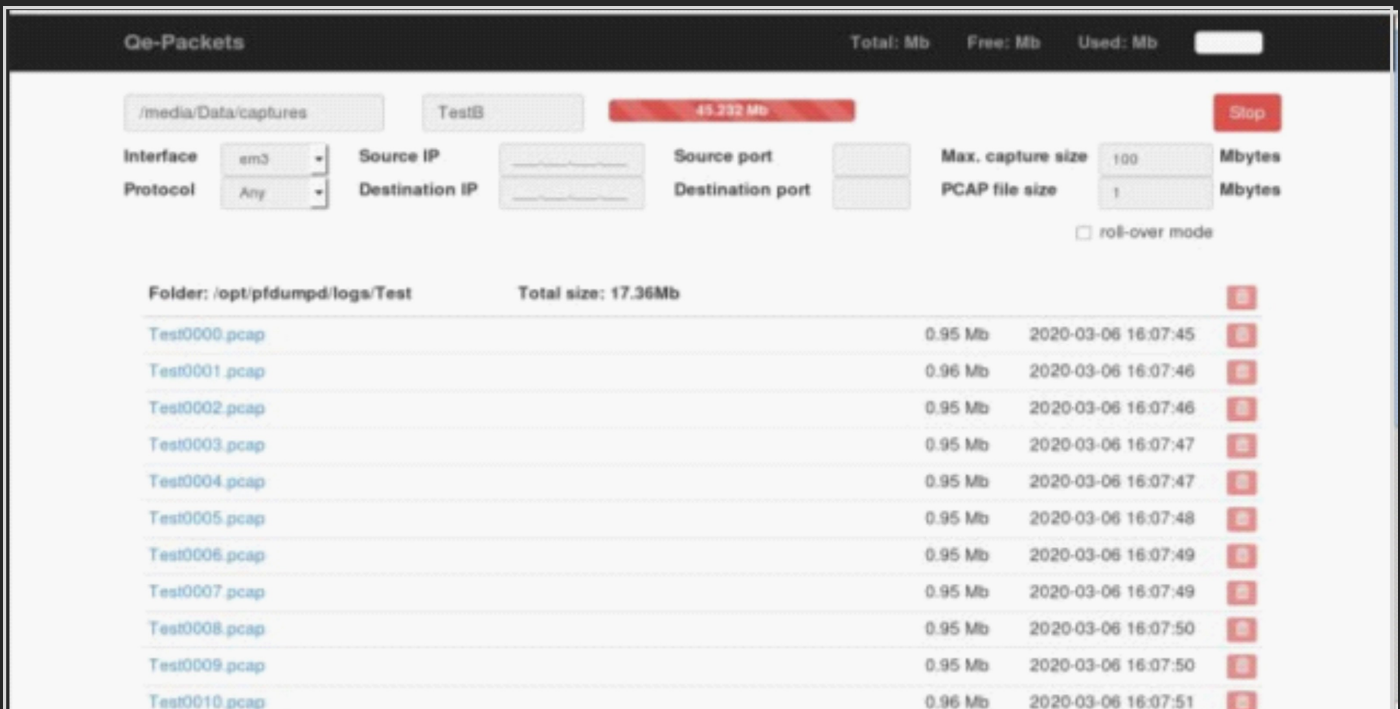
## Appliance for full packet capture within IP networks



Qe-Packets is the full packet capture system from Allentis. This platform works in combination with the Qe-Streams solution, the allentis flow analytics solution for the analysis and performance of exchanges on large IP networks. It is an appliance for acquiring streams and all the packets exchanged on the links on which it is positioned up to a speed of 20 Gbps (10 Gbps full duplex). It guarantees a high retention period by clustered 96TB storage modules.

### Stand-alone solution

Qe-Packets copies and stores all traffic exchanged on monitored links. The user decides the overall volume of data retention. The storage space is configured in a circular or linear manner in order to guarantee a retention period in line with production constraints. To facilitate rereading and access to data, the size of the *pcap* files can be configured. For example, for a global storage of 1 TB of data in circular mode, the creation of 1,000 files of 1 GB may be requested. This approach guarantees rapid data extraction. Filtering functions are available in order to retain only the data which appears to be the most relevant. The data produced can be read directly on the appliance or with all the products on the market allowing the reading of network frames.



The screenshot shows the Qe-Packets web interface. At the top, there are status indicators for 'Total: Mb', 'Free: Mb', and 'Used: Mb'. Below this, there are configuration fields for 'Interface' (set to 'em3'), 'Protocol' (set to 'Any'), 'Source IP', 'Destination IP', 'Source port', 'Destination port', 'Max. capture size' (set to '100 Mbytes'), and 'PCAP file size' (set to '1 Mbytes'). A 'roll-over mode' checkbox is also present. A 'Stop' button is visible in the top right. The main section displays a folder path '/opt/pfdumpd/logs/Test' with a total size of 17.36Mb. Below this is a table listing individual PCAP files.

File Name	Size	Timestamp
Test0000.pcap	0.95 Mb	2020-03-06 16:07:45
Test0001.pcap	0.96 Mb	2020-03-06 16:07:46
Test0002.pcap	0.95 Mb	2020-03-06 16:07:46
Test0003.pcap	0.95 Mb	2020-03-06 16:07:47
Test0004.pcap	0.95 Mb	2020-03-06 16:07:47
Test0005.pcap	0.95 Mb	2020-03-06 16:07:48
Test0006.pcap	0.95 Mb	2020-03-06 16:07:49
Test0007.pcap	0.95 Mb	2020-03-06 16:07:49
Test0008.pcap	0.95 Mb	2020-03-06 16:07:50
Test0009.pcap	0.95 Mb	2020-03-06 16:07:50
Test0010.pcap	0.96 Mb	2020-03-06 16:07:51

Illustration : Storage files of all traffic by Qe-Packets

### Access to capture data from the Qe-Streams interface

In the architecture of Qe solutions, Qe-Packets represents the access module to network frames in exchanges requiring advanced investigation by analysis of the frame of the packets involved in the flows on which an in-depth analysis appears necessary.

This combined approach with the indicators highlighted by Qe-Streams makes it easy to obtain details on the transactions involved in a given problem. With a unique workflow, the exchanges identified on Qe-Streams can therefore easily be accessed on Qe-Packets to extract the network frames exchanged and thus obtain detailed information on the exchanges hitherto unavailable elsewhere on standard analytical solutions. .

Positioned at strategic concentration points, the Qe-Packets appliance allows the analysis of specific fields available in the frames.

### InceptRack® mobile bays integration

Qe-Packets responds to full packet capture issues. Also, the solution contributes to the overall objective of InceptRack® racks. Integrated into the bays, Qe-Packets provides users of these systems with all the functionalities expected by experts dedicated to the copying of flows on IP networks for the purpose of dedicated data processing.

With InceptRack®, a synthesis of all of Allentis' businesses in flow copying and data analysis architectures for large organizations, Qe-Packets completes the system to deliver integrated solutions ready to process all topics related to the capture and analysis of exchanges encountered on the networks

For needs in environments with strong environmental constraints, Qe-Packets exists in a hardened version allowing its integration in bays intended for more specific applications such as for example in the context of military applications.

InceptRack® racks are mobile for moving to concentration points requiring, in the case of those carrying Qe-Packets, massive data capture for specific applications in the field of network flow monitoring.



**Illustration** : InceptRack® by embedded Qe-Packets

### Order references

QEPACK-10-96	Qe-Packets full packet capture appliance, 2U long chassis, 1 x 10 GbE full duplex data acquisition, 96 TB clustered storage capacity
QEPACK-10-40	Qe-Packets full packet capture appliance, 2U long chassis, 1 x 10 GbE data acquisition, 40 TB storage capacity
QEPACK-10-20	Qe-Packets full packet capture appliance, 2U long chassis, 1 x 10 GbE data acquisition, 20 TB storage capacity
QEPACK-4-20-M	Qe-Packets full packet capture appliance, 1U short chassis, 4 x 1 GbE data acquisition, 20 TB storage capacity. Rugged equipment.

### About allentis

allentis is a French company specializing in systems for monitoring the performance and security of data flow network exchanges. It has designed and manufactures QE flow analysis systems (Qe-Secure for threat detection, Qe-Streams and Qe-Flows for performance analysis and mapping of WAN, SD-WAN and LAN flows, Qe -Packets for massive data capture, Qualevent for business hypervision), and the TAPICS range of network components for traffic replication and isolation