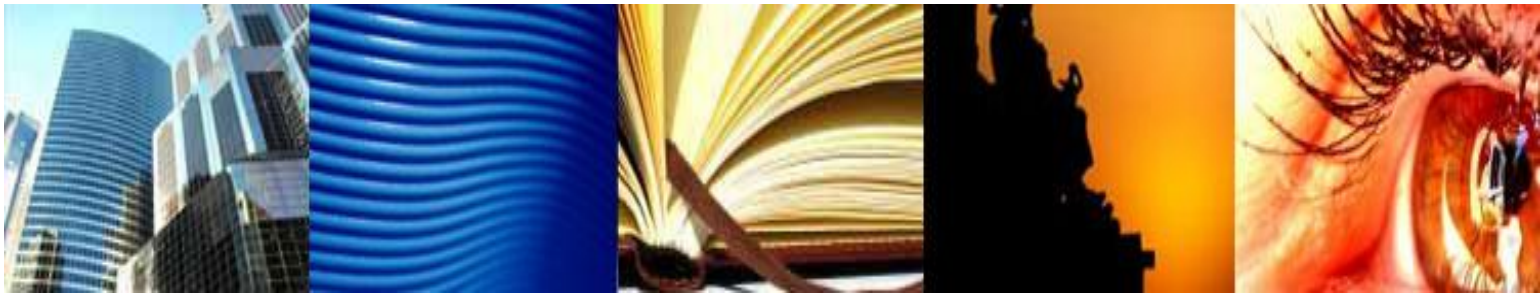
Net.Hunter Intelligence&Security



Forensic device: Filter , Record and Analyse at wirespeed in one unit

ALBEDO Telecom

the Path to Excellence

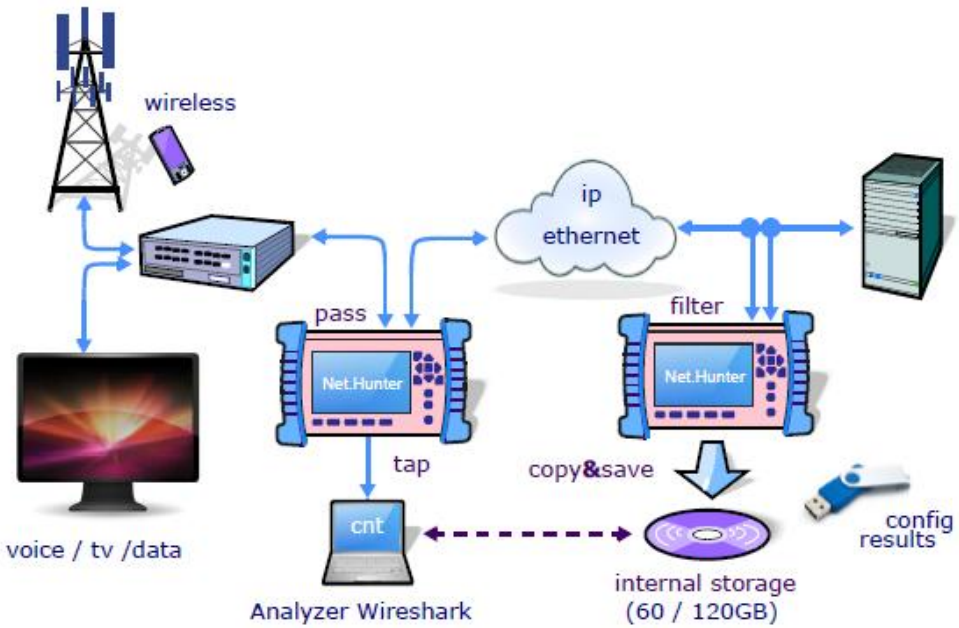
Unique Capture Device

Net.Hunter – Capture & Save live IP packets anywhere

Forget limitations in Packet Capture

1. Stream-to disc any point: self-contained keyboard, screen, etc.
2. Complete mobility: 1kg and battery for several hours
3. Smart recording to a disk-drive after filtering
4. Wirespeed operation: no packet delay or loss on the live traffic
5. Undetectable: as no MAC or IP address
6. Complete (100%) analysis of the whole stream
7. Embedded tap to 1000BASE-T

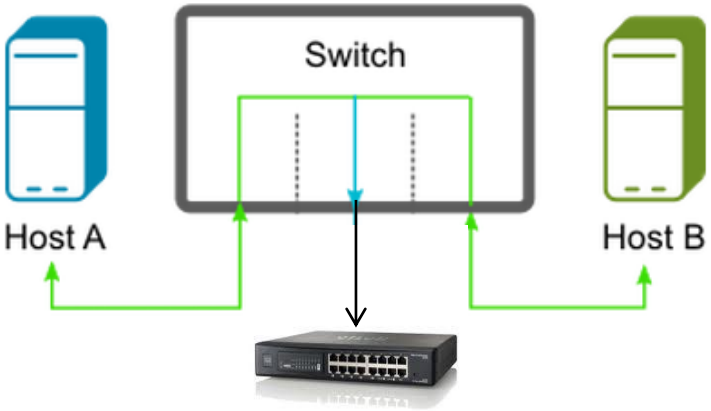
Security Requirements

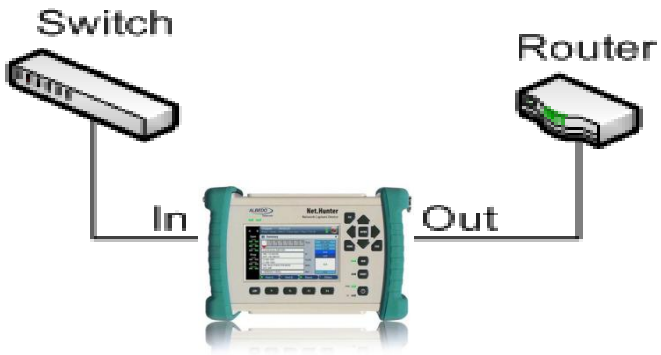


- Capture & Record the 100% suspicion packets is key for security analysis
- Apply filtering rules using embedded tap
- Record to the disk drive suspicion packets
- Alternatively you can tap all the suspition packet to a PC or a server
- Analyze with Wireshark or your favorite application to discover threats
- Assume the consequencies and take into account new security rules

ALBEDO Telecom

Net.Hunter also is a TAP





Other Appliances

- Only can connect at mirror ports, because are not poweful engough
- do not pass bad / long / short frames, or VLAN tags
- change timing – you can't do any timing studies, no jitter …
- MP / replication is low priority of a switch and thus issues

Consequently

- Monitor ports are NOT acceptable lawful enforcement surveillance
- Monitor ports are NOT acceptable for Compliance or Audit studies

>>> Net.Hunter works in mirror and pass-through mode too

ALBEDO Telecom

Handy & reliable at **full bit rate** (1+1GbE)

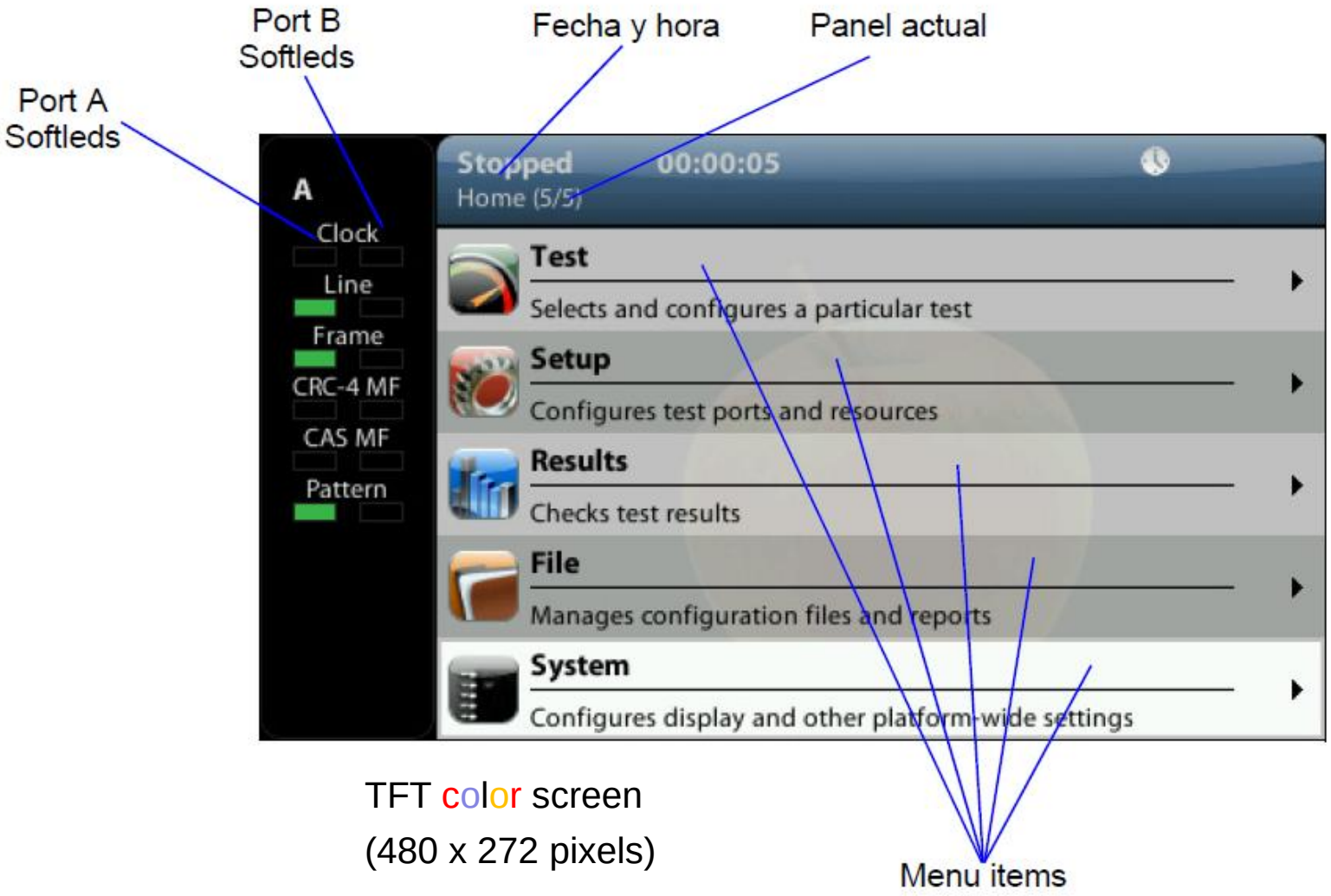
- 1,2 kg
- Batteries means
  - Fault tolerant
  - Operate everywhere
- Keyboard + Screen

- SFP - Span Ports
- Optical / Electrical
- Tap Ports

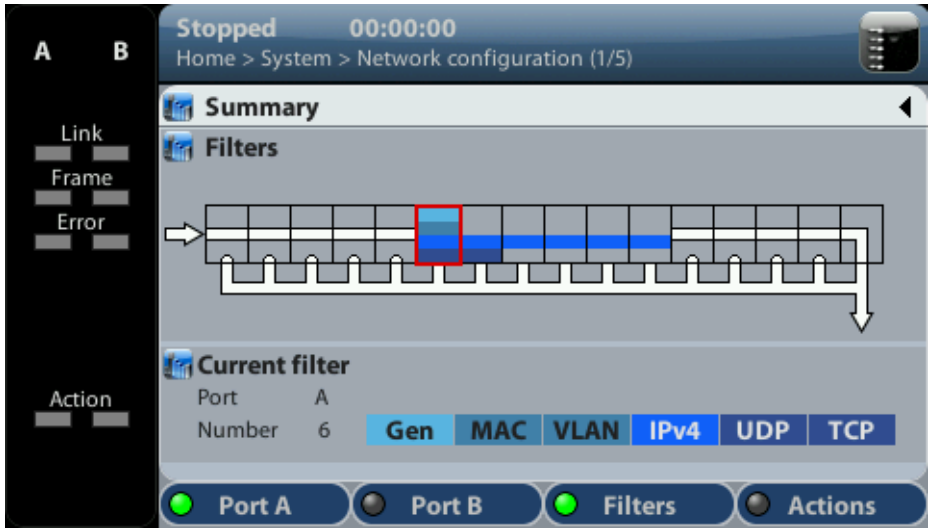
- Remote Control Port
- USB and Printer

ALBEDO Telecom

Screen+keyboard: in-site **GUI** for field engineers



Smart Recording: Filter and Save



Do not wate space: Only compliant packets should copied to disk

- Equipped with 16 filters to capture traffic in real time
- Full Dulex Operation means independent Up/Downstream filters
- All filters (16+16) can work simultaneouslly at wirespeed (1Gb/s + 1Gb/s)
- Multiplayer filters: MAC, VLAN, IP, UDP, TCP, etc.
- Up to 120GB disk drive
- Non-stop recording 24h / 365d
- Optionally Wraps around when full

Net.Hunter : Unique Tap & Store device

World **first** hand-held tool

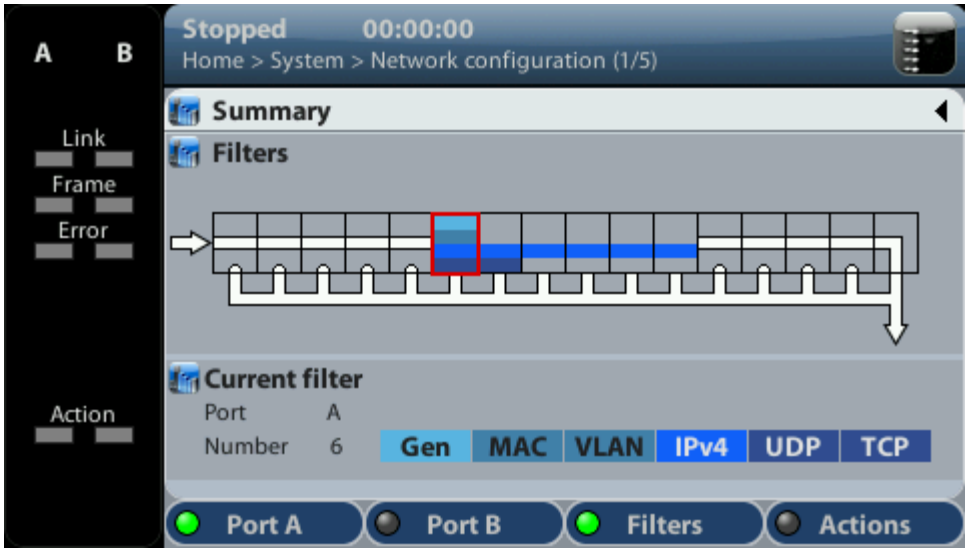
- **Captures** ALL **packets** that are
  - Compliant with a trigger condition
  - Compliant with any of the 16 programmable filter

- Caught packets --in full duplex GbE links– can be
  - **SAVED** in local hard-disk
  - **TAPED** to 1000BASE-T

All the operations at **wirespeed**

ALBEDO Telecom

Net.Hunter – **Tap** & **Filtering**



Net.Hunter is equipped with 16 filters to capture traffic in real time

Net.Hunter : Unique Tap & Store device

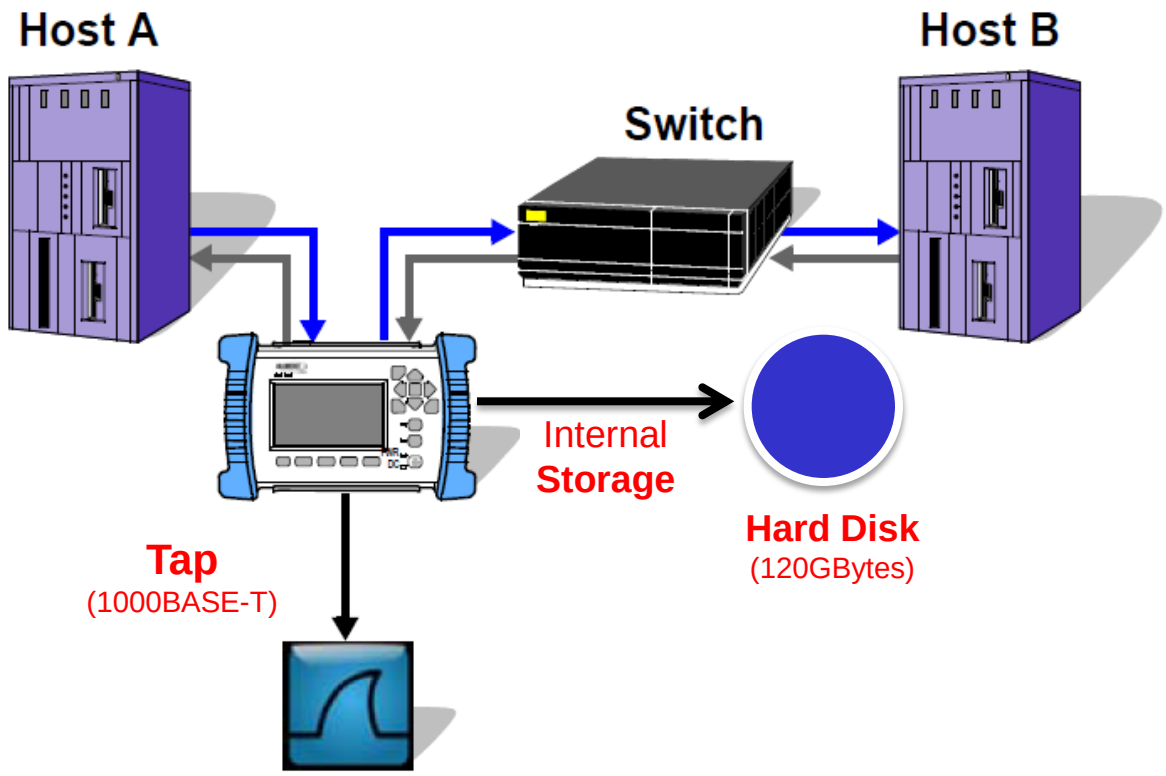
Ethernet filters 16 simultaneous filters can be applied to the traffic

- Customizable by Ethernet, IP, UDP and TCP
- Agnostics filters by 16 bits masks and offset
- Lawful filter: 64 byte pattern

- Ethernet filters 16 simultaneous filters can be applied to the traffic
  - By source and destination MAC addresses.
  - Selection of MAC address sets with masks
  - By Ethertype value with selection mask
  - By VLAN-VID with selection mask
  - By VLAN-CoS value with selection mask

- IP filters
  - IP address: source, destination, or both
  - IP address group: subset of addresses filtered by masks
  - Protocol encapsulated (TCP, UDP, Telnet, FTP, etc.)
  - DSCP field, single value and range
  - TCP/UDP port, single value and rangeCaptures ALL packets that are

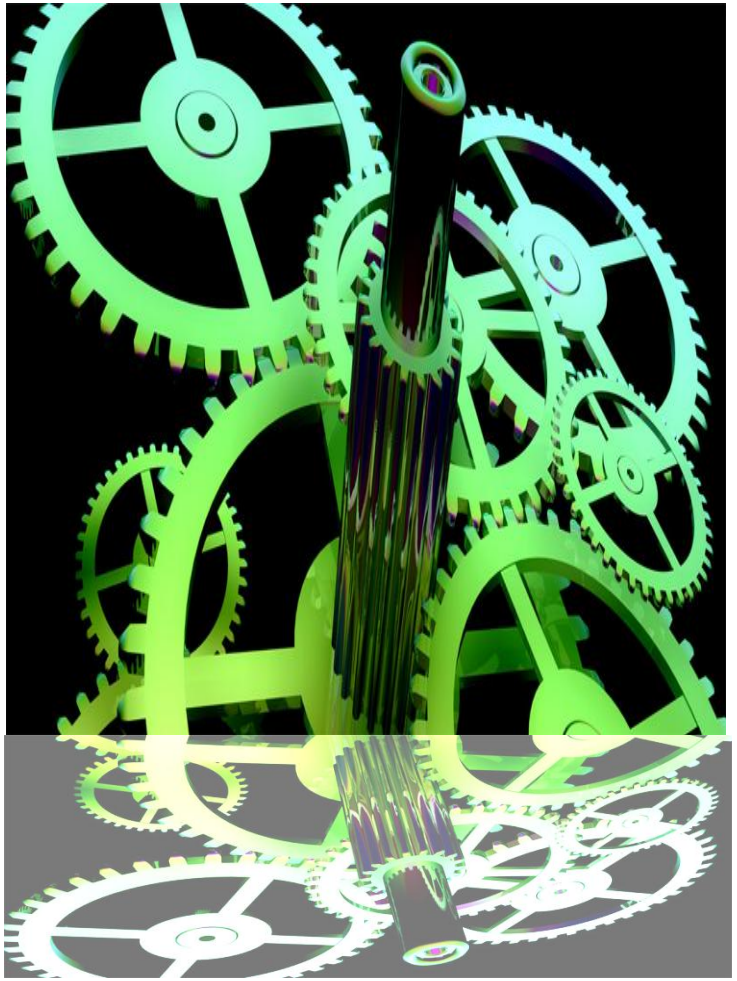
Net.Hunter in Operation



- 100% conformance packets with one filter are C&P
- The copy is Dropped to the LAN port or Saved in Memory
- **ALL** the operations are executed in real time: 1Gb/s throughput

Field Applications

- Forensic Applications
  - Filter, Record
  - Analysis
- Security
  - Internet analysis
  - 100% capture is a must
  - Intelligence agencies
- Enterprise
  - Protocol Analysis
  - Troubleshooting
- Protocol VoIP, IPTV
  - Wirespeed Captures



Competitors

Net.Hunter
ALBEDO

- Hand-held
- AC fault torerant
- SFP+RJ45 (o/e)
- Wirespeed (full)
- 24 / 365
- Tap
- Filter
- Mirror Mode
- Pass Mode
- Good Deal
- Device

CSN/NTM-EX3
Fluke

- Rack
- AC required
- SFP+RJ45 (o/e)
- 0.8 wirespeed
- 24 / 365
- no Tap
- no Filter
- Mirror Mode
- no Pass Mode
- Expensive
- Device

WA100-8D
NetWitness

- Rack
- AC required
- RJ45 (elect)
- 0.1 wirespeed
- 24 / 365
- no Tap
- no Filter
- Mirror Mode
- no Pass Mode
- More expensive
- System

DeepSee 2G
SOLERA

- Rack
- AC required
- RJ45 (elect)
- 0.5 wirespeed
- 24 / 365
- no Tap
- no Filter
- Mirror Mode
- no Pass Mode
- Most expensive
- System

USC4060
IP Copper

- Portable
- AC required
- RJ45 (elect)
- 0.3 wirespeed
- 24 / 365
- no Tap
- no Filter
- Mirror Mode
- Pass Mode
- Best price
- Device

Why Net.Hunter

- **4x4 OPERATION**: hand-held (4h. with batteries)
- **STORAGE CAPACITY**: up to 120 Gbytes captured packets
- **HARDWARE PERFORMANCE**: 100% lossless at GbE
- **FDX TIME STAMPS**: PCAP format
- **REMOTE CONTROL**: from any VNC platform
- **ACCURATE RECORDING**: for further analysis

ALBEDO Telecom

That's all

www.albedotelecom.com

ALBEDO
Telecom
the Path to Excellence