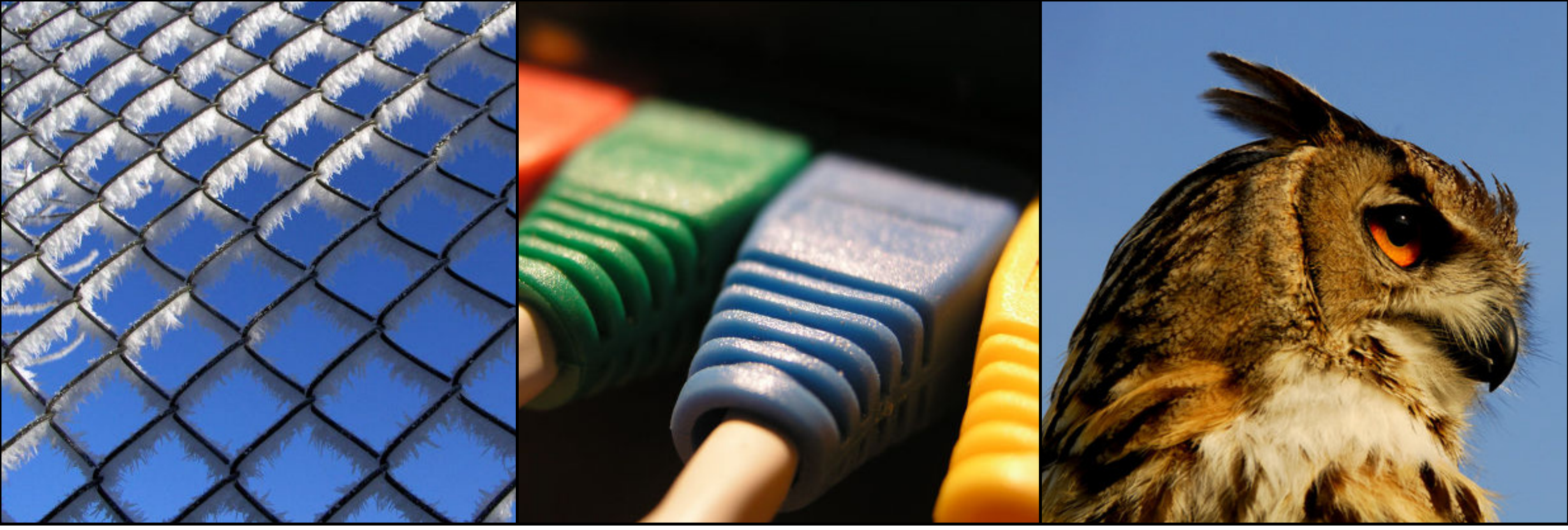


NETHUNTER

Net.Hunter a Tireless Packet Capture

the Path to Excellence

Net.Hunter is a stream-to-disk appliance capable of monitoring live traffic to capture selected TCP/IP flows at wirespeed. Interestingly, it includes an embedded tap with triggers and programmable filter conditions. Suspicious packets can either be saved in real-time into an internal disk or tapped to a LAN.

Hand-held unit

Net.Hunter is a compact and independent device that includes screen, keyboard and batteries to operate everywhere. It captures and records by hardware therefore at full wirespeed in full duplex Consequently is ready to assist those who need to monitor and capture critical data, protocols and VoIP conversations, everything transparently without disturbing live traffic. Net.Hunter satisfies the need of packet capture that are not well served by probes, testers and analyzers unable to capture, tap and save in real-time.

Focused Traffic Analysis

This appliance manages the traffic using switch-like technology to aggregate the traffic allowing monitoring of both sides of a full duplex conversation making the analysis much easier to lawful experts and telecom engineers. Monitoring ports include SFP, RJ45 and Wi-Fi, while captured packets can be either recorded in PCAP format with NTP synchronization or tapped to a LAN in real time.

Undetectable

Net.Hunter is comprehensive and small; does not have IP or MAC addresses, and works at full bit rate without generating any delay, jitter or loss, therefore it is total and absolutely invisible.

> **“Seamless packet capture for troubleshooting, security and lawful interception”**

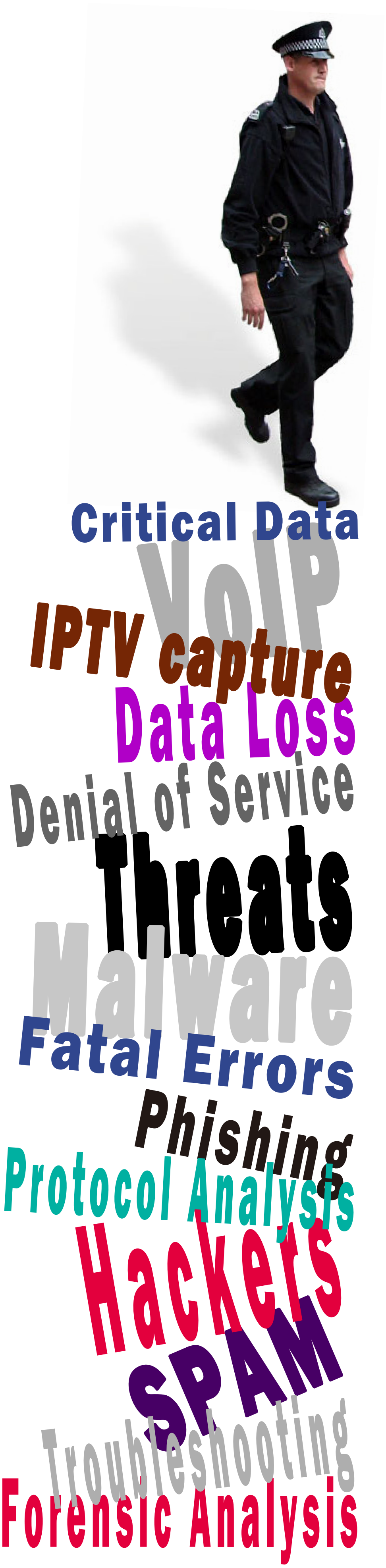
Embedded Tap included: smart record

Net.Hunter includes a tap to filter traffic before *recording* which means that only IP flows, compliant with any of the 32 programmable filters, are captured reducing on this way the need of disk capacity.

Hardware Captures means Full bit rate

Malware, hackers, cyber-attacks have moved to a new dimension able to infiltrate mission critical systems. Responsible security requires advanced and portable tools to monitor and face all the threats. Net.Hunter can be easily integrated with existing infrastructures such as firewalls and management systems to gain awareness while helping to define mitigation policies.

ALBEDO
Telecom



Bread & Butter

Packet sniffing of live traffic has become a common practice for a number of professionals. The problem is that most of commercial products find the lack of capacity to filter and capture packets in real time without disturbing the stream and this is the case for all software based solution, because this challenge can only be solve at hardware and firmware layer.

How it all works

Net.Hunter is able to monitor at wirespeed full duplex lines in order to captures complete IP flows. The whole content is analysed including headers and payloads then, if compliant with any of the programmable conditions, they can either be tapped to a LAN or recorded into the internal hard disk. Recorded flows from different sources can be correlated thanks to PCAP time stamp synchronized by NTP.

> **“Compact, cost-effective solution to manage quality, troubleshooting threats, incidents, hackers and malware”**

Fault Tolerant

Batteries not only gives autonomy but also guarantees that 100% tap function is completely passive and won’t disrupt the network even if AC power is lost. Power glitches and failures no longer mean dropped packets and lengthy renegotiation sequences.

Transparent as a fibre strip

Net.Hunter operates in two modes:
(a) connected to a mirror point, or
(b) in pass through mode, and in this case the link is setup as it was (speed, duplex mode, pause, etc) by means of auto-negotiation or manual configuration.

In both case the tap does not use IP or MAC addresses, therefore cannot be detected under any circumstance because it has no exposure to attacks, being as transparent as a piece of cable.

Smart Recording

In order to capture only those flows with interest Net.Hunter supports up to 32 programmable filters to facilitate the exact analysis and quick capture in real time. Simple and complex set of rules can be defined to capture packets based on multiple criteria (MAC, IP, VLAN, IP, MPLS, TOS, TCP, UDP, Port, Protocol, Pattern, Arbitrary, User Defined...) to allow you the capture of complete flows that can either be recorded or tapped.

Capture, record & analysis

Net.Hunter takes advantages of both open source software and other analysis suites to reconstruct sessions that will allow you to discover what occurred. Experts may then analyse the protocols, reassemble a conversation or identify malware in order to get a clear picture of what occurred with the traffic. Saved packets with PCAP can be correlated and reconstruct traffic from several sources. Post-event incident analysis is the most common use of network forensics, but proactive situational awareness can deliver higher value. For this use, capturing data at high rates and indexing to speed access are critical.

Local or Remote

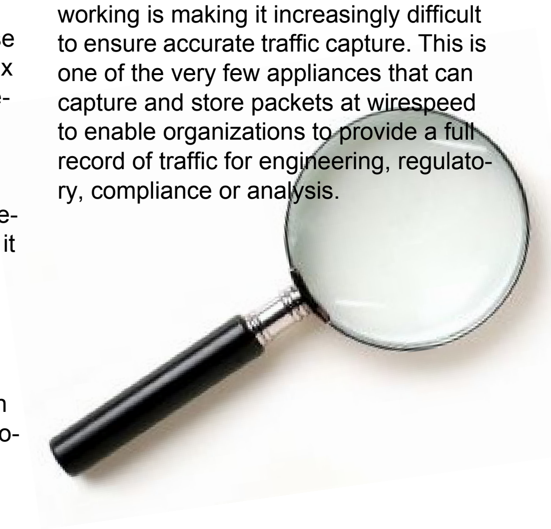
Net.Hunter can be deployed as part of a centrally managed monitoring system because any VNC client, such as a PC or an iPad, can gain full control or, if preferred, the keyboard and screen allows on-site operation as a stand-alone to tap specific points.

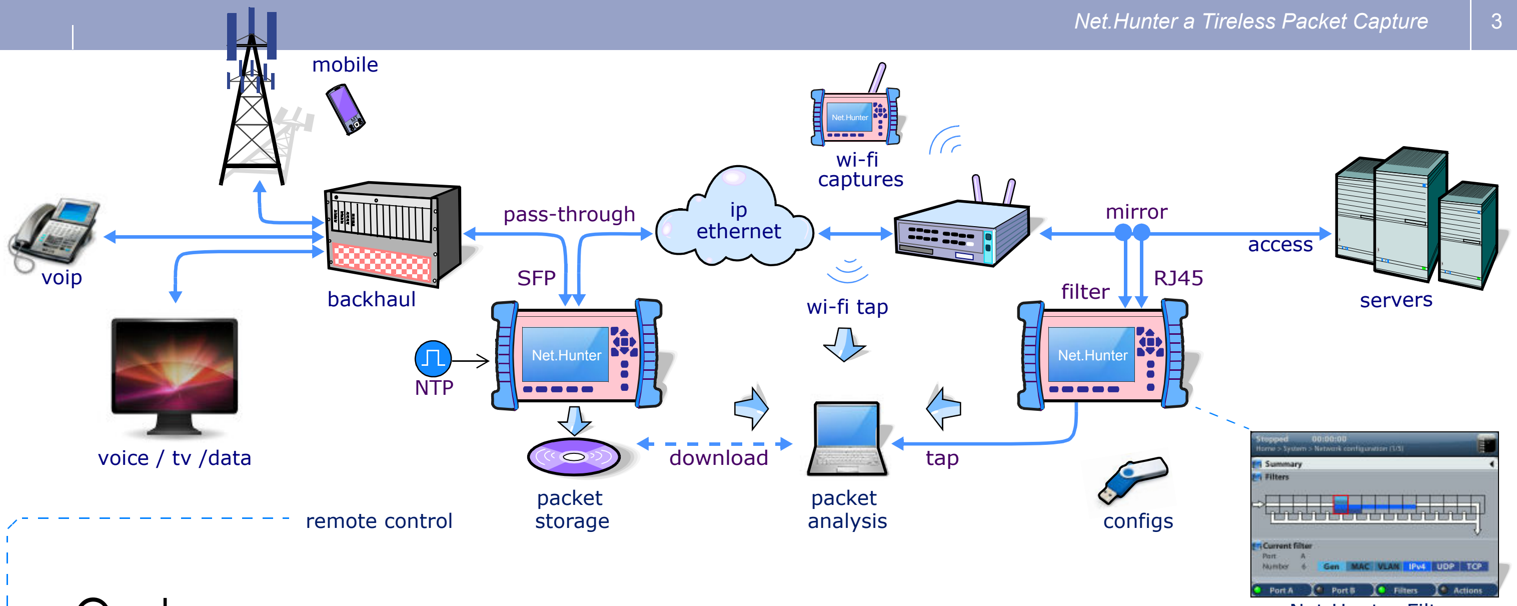
Scalable solution

Net.Hunter enables analysis of the full network traffic by deploying several units across the access points. Captured traffic can be correlated thanks to NTP synchronization, which could be aggregated in a server for deeper analysis with your preferred application.

Wireless / Optical / Electrical

The adoption of wireless and optical networking is making it increasingly difficult to ensure accurate traffic capture. This is one of the very few appliances that can capture and store packets at wirespeed to enable organizations to provide a full record of traffic for engineering, regulatory, compliance or analysis.





Net.Hunter Filters

Customers

As networks grow, customers have to face on a daily basis issues that require traffic capture and analysis. With Net.Hunter you now have a stream-to-disk Tap that satisfies enterprise capture needs, field portability and autonomous operation.

IP Service Providers

Net.Hunter is ideal for enterprises looking to ensure their networks are robust, scalable and able to meet or even exceed customer QoE expectations.

VoIP and IPTV Operators

Net.Hunter provides proactive monitoring of Voice and Video services based on IP facilitating the analysis and reproduction of the sessions recorded on the disk.

Traffic Analysis

Net.Hunter provides proactive monitoring of Voice and Video services based on IP facilitating the analysis and reproduction of the sessions recorded on the disk.

Security & Forensic

Intelligence Captures

Although Net.Hunter is not detectable on the network as it does not have a physical or logical address, it still captures full-duplex traffic simultaneously.

Lawful Interception

Legal access to private communications such as email, VoIP calls or Internet is one of the Net.Hunter most popular applications available to law enforcement officials when requested.

Threat Awareness

Attackers use several methods such as social media phishing linked to malware. When attacks occur, network security teams need to know who did it, how they did it and what systems were impacted.

Incident Response

Enterprises may respond using Net.Hunter integrated with contents analytic tools to mitigate security breaches.

Threat Detection

Investigators will have the capability to reconstruct web sessions, emails and 'chat line' conversations in a chronological order to investigate data loss incidents.

Intrusion Detection System (IDS)

Net.Hunter monitors network and/or networks for malicious activities or policy violations and can forward suspicious traffic to the Management Station.

FEATURES

- Pass-through and Mirror
- Hardware filter & capture
- No Delay, Zero Packet Loss
- NTP synchronisation
- PCAP format support
- VNC remote control
- Hand-held tap
- 4.5h on batteries, 2.6 lbs
- 60 or 120 GB hard disk
- IPv4 and IPv6

APPLICATIONS

- Intelligent collection
- IPTV Multistream captures
- VoIP surveillance
- SIP troubleshooting
- Protocol Analysis
- Legal Interception
- Forensic Analysis
- Firewall Enhancement
- Cyber-security
- 24/365 Access Monitoring
- Data Loss Analysis

BENEFITS

- Compact and Autonomous
- Multicast captures for IPTV
- Record at full wirespeed
- Scalable to dozens of units
- AC power Fault tolerant
- Invisible and undetectable
- Risk-less traffic control
- Stream-to-disk LAN & Wi-Fi

Net.Hunter Specification

Networking Features	
Formats and Protocols	• 10, 100, 1000 Mbit/s Ethernet • IP, TCP/UDP, IEEE 802.3 • Ethernet frame: IEEE 802.3, IEEE 802.1Q, IEEE 802.1ad (Q-in-Q) • IP packet: IPv4 and IPv6 • Jumbo frames: up to 10 kB MTU (Maximum Transmission Unit) • Configurable MTU size • Throughput between measurement LINE ports: 2x1 Gbit/s or 2x1,500,000 frames/s • Autonegotiation parameters including bit rate (10, 100, and 1000 Mbit/s) and duplex mode • Autonegotiation Full Setup by user • Autonegotiation Disabled by user
Ports and Interfaces	• LINE Ports: SFPs based 1 Gbit/s, SFP interfaces including: 10BASE-T, 100BASE-TX, 100BASE-FX, 1000BASE-T, 1000BASE-SX, 1000BASE-LX • MIRROR Ports: Dual RJ-45 port for electrical connection 10/100/1000BASE-T • Local Storage: 60 / 120 GBytes in PCAP format NTP synchronized
Operation	• LINE ports: GbE SFP interfaces are used to connect -in pass thought- to the network Host A and Host B • MIRROR Ports: GbE RJ45 interfaces to forward captured packets to the protocol analyzer device (i.e. Wireshark) • All frames coming to Net.Hunter are forwarded to destination without delay or lost • Frames compliant with filtering conditions and copied to Wireshark device • Operation is based on 16 filters per LINE port • Filtered frames can be aggregated in one drop port • The Filtering process is executed sequentially • When a packet satisfies a filter is sent to the Drop Port and immediately forwarded to the output (No more filters are processed) • Each packet may modify only the statistics of one filter • Customizable filters defined by field contents on Ethernet, IP, UDP and TCP headers • Agnostics filters defined by 16 bits masks and user defined offset • Lawful filter: 64 byte pattern match at any place in the frame payload • Length filters applied to the full packet • Pattern filters to be applied on payload fields
Ethernet Filters	• Ethernet Flow: Source and destination MAC addresses (Selection of MAC address sets with masks) • Ethertype value with selection mask • VLAN-VID with selection mask, VLAN-CoS value with selection mask • S-VLAN / C-VLAN with selection mask, S-VLAN / C-VLAN CoS value with selection mask, DEI
IP Filters	• IPv4 / IPv6 address: source, destination, and source-and-destination • IP address group: subset of addresses filtered by masks • Protocol encapsulated in the IP packet (TCP, UDP, Telnet, FTP, etc.) • DSCP field, single value and range • TCP/UDP port, single value and range
Results	• Autonegotiation results including current bit rate, duplex mode, Ethernet interface • SFP presence, vendor, and part number • Traffic statistics per each of the Four Ports • Statistics for both transmit and receive directions • Frame counts: Ethernet, and IEEE 802.1Q • Frame counts: unicast, multicast and broadcast • Basic error analysis: FCS errors, undersized frames, oversized frames, fragments, jabbers, collisions • Frame size counts: 64, 65-127, 128-255, 256-511, 512-1023, and 1024-1518 bytes • Four byte counts: Port A (Tx / Rx) and Port B (Tx / Rx) • All traffic counters follow RFC 2819 • Counters and statistics per filter (up to 16)

Design	
Performance	• Full Duplex operation at 1 Gbit/s or 1,5 Mframes/s • Accuracy better than 10^{-6} secs. at 1 Gbit/s • Performance and accuracy 100% independent of the line bit rate • Jitter-less captures in solid state hard disk and full wirespeed (full Gbit/s at Tx & Rx simultaneously)
GUI	• Configuration and management on web browser • Configuration and management on CLI thought SSH and Telnet
Operating System	• Linux operating system

Ergonomics	
Hand-held Tap	• Display 480 x 272 TFT full color screen • Dimensions: 223 mm x 144 mm x 65 mm • Weight: 1.2 kg (with rubber boot, one battery pack) • USB and Ethernet ports, Serial Port RS-232C • Rechargeable Batteries continuous working for 5 hours. Fast recharging time • AC Power Adapter Input: 100 ~ 240 V AC, 50/60 Hz, • Operating Temperature 0ºC ~ 50º C Storage Temperature -20ºC ~ 70ºC Humidity 5% ~ 95% • All events at a glance: 2xLEDS executing logical OR and Multiple Soft LEDS in screen

ALBEDO Telecom

the Path to Excellence