IPCopper™

Network and Data Security Solutions

IPCopper USC1030

forensic packet capture appliance

Deploy IPCopper packet capture appliances anywhere on your network, either at the perimeter to monitor all traffic in and out of your network or at core nodes to monitor crucial equipment. Without affecting network topology, netflow or speed, IPCopper continuously records all Ethernet-based communications, giving you the information you need to protect against advanced persistent threats, insider misuse and run-of-the-mill hack attacks — even custom-tailored attacks that antiviruses and firewalls cannot detect.

IPCopper™ USC1030 provides a capture rate of up to 1Gbps, 1TB onboard storage, dual 20Kb encryption and continuous network recording. Using neither an IP nor MAC address, stealthy operation hides its presence from electronic snoopers, while the sealed 12 ga. enclosure provides a measure of physical security.

IPCopper appliances "plug-and-play" anywhere on your network, connecting inline on any Cat-5 cable, via a mirror/span port or via a network tap. IPCopper requires no configuration; once powered up, the units operate autonomously, capturing all IP network activity, including packet headers and payloads.

Peak Capture Rate: 1 Gbps

Memory Capacity: 1 TB

Network Interface: 2 x RJ-45

Processor: Intel dual core

Supported Protocols: TCP/IP, UDP, ARP, POP3, SMTP and others that use underlying Ethernet or Ethernet framing as transport

Weight: 4 lbs

Dimensions: 3" x 9" x 7.5"

Comprehensive, reliable, long-term packet capture

The IPCopper USC1030 delivers reliable packet capture and netflow monitoring capabilities. Combining gigabit-speed data capture, encrypted recording and easy installation in a small footprint, the USC1030 is a nimble and effective surveillance appliance for any network.

- Detect intrusions, unauthorized access and other threats to your data and network structure.
- Gather detailed and comprehensive evidence that can be used in court to prevent and prosecute cyber-attacks, corporate espionage and internal misuse.
- Reduce incident response time to suspicious network events by conducting effective and efficient network forensics based on accurate, comprehensive data and historical, deep-packet analysis.
- Prevent false positives; know definitively whether data was compromised or stolen.
- Demonstrate compliance with network security regulations related to HIPAA, SOX, PCI and other.
- Collect information to better detect and prevent intrusions, identify and troubleshoot network problems, benchmark servers and bolster network security and data integrity.
- Create carbon copies of emails, IM chats and other IP-based communications.
- Record VoIP calls and SIP sessions.
- Unobtrusively record and monitor the activities of specific employees and workgroups or log server access.

No Electronic Footprint, Dual Data Encryption

Stealthy operation hides IPCopper's presence from electronic snoopers. The USC1030 does not announce itself on the network or require an IP address, making its presence on your network invisible to hackers and other potential observers. IPCopper further protects your data with dual encryption using a 20Kb key and technique that "mates" the data to the unit's hard drive itself, protecting you even in the unlikely event that someone manages to mechanically duplicate the hard drive. Illicit copies of the data would be useless even with the correct key — data is only retrievable from the original hard drive *and* with the correct key.

continuous network and ip traffic recorders for network forensics, troubleshooting and network event analysis

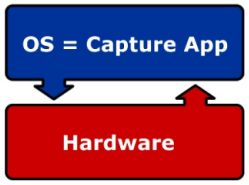
IPCopper's Strengths

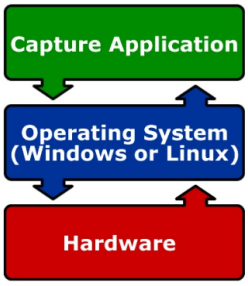
- Compact
- Affordable
- Stealthy, electronically invisible
- Robust, with sealed, tamper-resistant case
- All data encrypted, 20Kb key
- Dedicated, proprietary operating system

Vs. The Competition

- Bulky
- Expensive
- Visible on network, announces itself
- Not suitable for undercover deployment
- Usually no encryption
- Usually Windows- or Linux-based OS*

Comparative Hardware/ Software Structure





- No configuration required
- Made in USA

- Complex installation & configuration

** And adding yet another Windows/Linux-based network device creates yet another point of attack*

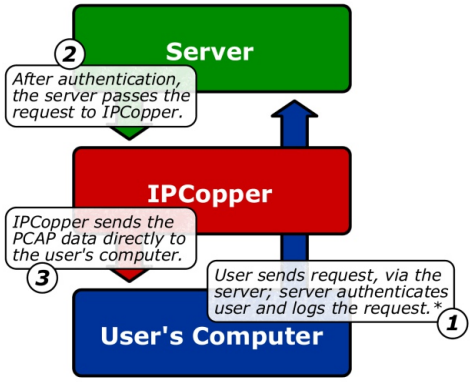
The IPCopper USC1030 is compact, fast, stealthy, cost-effective and easy to install. And, backing up one IPCopper unit is as simple as daisychaining another unit right next to it. Unlike the competition, which uses RAID systems that can be rendered ineffective by a simple power supply or other hardware malfunction, if one IPCopper in a daisychain fails, it won't affect the integrity of the next. With IPCopper, the magnitude of redundancy is entirely in your hands. Due to its low cost, it is feasible and practical to backup one IPCopper unit with another, and even a third, if the data is crucial.

Customized versions of IPCopper are available with a variety of options, including battery backup, redundant capture and record, filtering capabilities, specialized enclosures and features for secure, remote access using a protocol that evades detection and maintains IPCopper's stealthy profile.

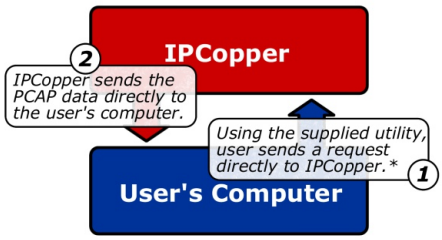
Retrieving data from IPCopper is as easy as selecting a date and time. Data downloads to your workstation into PCAP-formatted files for backup or analysis with PCAP-capable utilities.

IPCopper packet capture appliances allow users two ways to retrieve data, both of which incorporate a process for user authentication and create access logs, detailing data download requests. Use our Windows-based utility to directly connect to IPCopper, and IPCopper will keep a record of such connections. Or, authenticate the data through our server, which creates a second access log. Users who utilize the server may choose to disable the option for direct access.

Two Methods for Data Retrieval and User Authentication



*To avoid spoofing attacks, IPCopper must be located in between the user's computer and the server for authentication to be successful.



*The utility provided will be for use with a specific IPCopper unit and cannot be used to communicate with any other IPCopper unit.

Contact Us for More Information

IPCopper™ is designed and manufactured in the USA by IPCopper, Inc. For more information on our packet capture appliances, visit us online at www.ipcopper.com or call us at 855-347-8074. Sales email: sales@ipcopper.com.

IPCopper, Inc.
7180 SW Fir Loop #100 • Portland, Oregon 97223
855-347-8074 (toll free) • 503-290-0110 (tel) • 503-290-0111 (fax)
Email: sales@ipcopper.com • Web: www.ipcopper.com

IPCopper™
Network and Data Security Solutions