



# Ensuring Permissible Packet Capture for Digital Legal Evidence

**Industry:** Law Enforcement, Entertainment, Media

**Related Cases:** Copyright Infringement, Piracy, Content Protection

## Key Issues:

Real time tracking and analysis of big data to provide IT Forensics that include packet captures that are permissible for legal evidence in criminal trials.

## Solution:

Deployment of a reliable and secure turnkey solution consisting of Savvius and Garland Technology products. Garland network TAPs provide a reliable network test access solution (TAP) for packet capture and mirroring. Savvius Omnipliance provides network forensics that allows for business intelligence and if warranted, definitive legal action.

## The Garland + Savvius Solution Ensures:

- Real time network access using passive network TAPs
- Reliable mirroring of the network traffic with network TAPs
- Reliable 100% packet capture with network TAPs and Savvius Omnipliance
- PTP timestamp with Savvius Omnipliance
- Network forensics with Savvius Omnipliance
- Capture of evidence with Savvius Omnipliance

## Benefits:

Reliable data is tracked and analyzed providing the customer with packet capture evidence that can be used in a criminal trial as digital evidence.

## Tools Deployed:

[Garland Passive Fiber TAPs](#)

[Savvius Omnipliance](#)

**“90% of organizations say they have been breached, 43% say in the last year. 46% of breaches led to data loss.”**

-KASPERSKY LAB

This document is for informational purposes only. The information in this document, believed by Garland Technology to be accurate as of the date of publication, is subject to change without notice. Garland Technology assumes no responsibility for any errors or omissions in this document and shall have no obligation to you as a result of having made this document available to you or based upon the information it contains. ©2017 Garland Technology LLC. All Rights Reserved