

Content Forensics

What's on your network?

Most service providers offer their subscribers anti-virus and anti-spam protection on their own email platform. However, the problem of viruses and spam in non-platform SMTP email traffic grows daily.

The causes include botnets/spam Zombie infected subscribers and professional spammers/criminals abusing the service provider's network. The impact can be enormous:

- The service provider can be black-listed by other providers and third party email systems.
- Identifying professional spammers and infected users on the network can be both resource intensive and time consuming.
- Valuable network bandwidth is wasted by unwanted spam and virus-infected traffic.
- Call centre costs and subscriber churn rises as subscribers experience service degradation and problems caused by their botnet-infected PCs.
- The service provider's network can be used to launch denial of service attacks, phishing attacks and other malicious activities.

We have developed a powerful solution, called Content Forensics™, which gives the service provider's abuse and network operations teams management and control over SMTP email traffic on the network.

Key capabilities

- » Content Forensics/Monitor: Monitors SMTP email traffic on the network. Shows the breakdown of normal and spam email traffic on the network. Lists the top N spammers in real-time. Reports each subscriber's email activity by time of day. Reveals how much bandwidth is wasted by unwanted or harmful traffic.
- » Content Forensics/Record: Optional facility to record header information for all SMTP emails on the network. Can be used for long-term trend analysis, evidence collection for abusive users and regulatory purposes.
- » Content Forensics/Action: Automated facilities to quarantine and control infected botnet subscribers.

Read our Content Forensics Solution Overview document opposite to find out more and check out our free trial offer.