

Email Header Forensic Report

Generated by Automated Analyzer

==== BASIC METADATA ====

From: SecureMail Alerts <alerts@securemail-demo.com>
To: user@example.com
Subject: Important Notice: Login Attempt Detected
Date: Tue, 18 Feb 2025 06:11:58 +0000
Message-ID: <f9923af3b21\$e8b92340\$9a2b69c0\$@securemail-demo.com>

==== HOP TIMELINE (origin → destination) ===

Hop 1:

Timestamp: Tue, 18 Feb 2025 06:11:59 +0000 (UTC)
HELO : host-22-11-77.isp-unknown.net
IPs : 10.8.44.29
PTR : N/A
WHOIS : N/A

Hop 2:

Timestamp: Tue, 18 Feb 2025 06:12:10 +0000 (UTC)
HELO : smtp.securemail-demo.com
IPs : 203.0.113.45
PTR : N/A
WHOIS : N/A

Hop 3:

Timestamp: Tue, 18 Feb 2025 11:42:13 +0530 (IST)
HELO : mailout04.securemail-demo.com
IPs : 198.51.100.24
PTR : N/A
WHOIS : N/A

==== AUTH CHECKS (SPF / DKIM / DMARC) ===

Domain: securemail-demo.com
SPF TXT: N/A
DMARC TXT: N/A
DKIM selector: dk2024
DKIM TXT: N/A

==== END ===