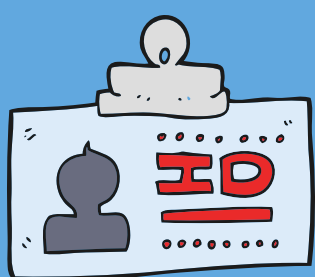METASPIKE

EMAIL AUTHENTICATION
CHECKLIST ✓

Forensic examiners review hundreds of data points when authenticating email messages. But which ones are the most common clues that indicate an email message may be fraudulent?
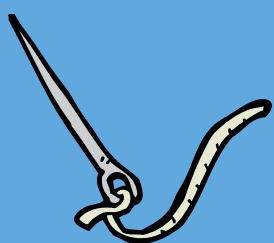
We have compiled them in a short checklist that you can focus on immediately.

DUPLICATE IDS

Email messages and threads have identifiers such as Message ID and Conversation Index that are designed to be unique. If the suspect message has an identifier that is a duplicate of another seemingly unrelated message, you should take a close look.

THREAD INDEX ISSUES

An email's Thread Index includes information such as the sent date of the first email in the thread, and the number and dates of subsequent child messages. If the data found in the Thread Index looks nothing like what the message reflects, you might have a red flag.

IMPOSSIBLE DATE
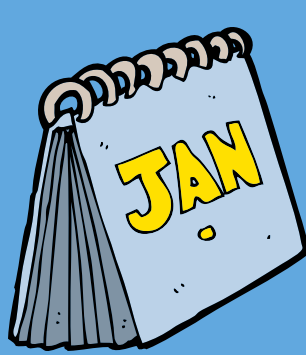
Believe it or not, fraudsters sometimes forget to check that a date they manipulated is valid. So, if you are suspecting a date such as Friday, December 13, 2014, it is worth verifying if that day really was a Friday.

ATTACHMENTS FROM FUTURE
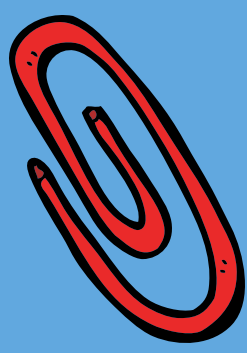
Dates of attachments are often retained in an email message. If the suspect message appears to have been sent in 2013, but contains attachments dated 2016, there is likely something wrong with that email, its attachments, or both.

ALIEN TECHNOLOGY USED
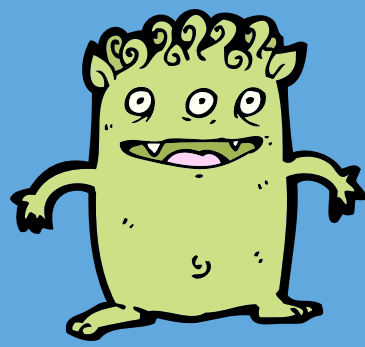
It is often possible to determine the email client that was used to send the email message. If the suspect message appears to have been sent in 2011, but was sent using Outlook 2016, you have a red flag.

TOO PUNCTUAL

Email sent dates can often be very precise. If you find two emails from the same sender sent within the same microsecond, at least one of them may be fraudulent.

DISTINCT BODIES
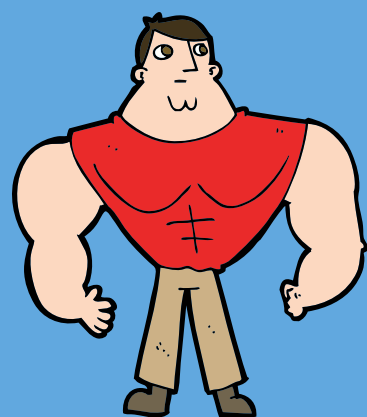
Email messages often contain multiple copies of the message body (e.g., plain text and HTML version). Contents of these message bodies should generally be in agreement aside from formatting differences. If you see any discrepancies, one of the message bodies may have been altered.

FONT ISSUES

Use of fonts that were not available when the email message appears to have been sent, and fonts in text blocks where they do not belong can be potential indicators of foul play.

METASPIKE