Why did I get an email when the To: line says it is to someone else? Also, how can I find out who really sent this email?

When trying to answer email questions like this, it is helpful to make an analogy between email and US Mail. If you get a letter via US Mail, your address will be on the envelope and your address may also appear on the letter inside the envelope (as would be the case with a formal business letter). The envelope address is used to get the letter to you but the address on the letter is not used during the actual delivery. So, the letter address can be totally incorrect and the letter will still get to you. Similarly, the sender’s address may appear in both places as well.

Likewise, email has two sets of addresses. The first, like the envelope address, is used during the actual delivery. This address is used by the programs (such as sendmail) that actually do the mail delivery. The second set of addresses is analogous to the addresses on the actual letter and these are the addresses you see in the To: and From: headers of the email message. Just as with the US Mail, these addresses need not be correct for you to get the letter. In fact, the sender can make these be anything they wish.

So, I could send out a spam mailing to thousand’s of addresses and put your email address in the From: line. As a result, the recipient may think you sent the spam and complain to you, even though you had nothing to do with it! See further information in the KB page Why do I get email returned as undeliverable for messages I didn't even send?

In order to determine the true sender of the email (ie. to see the envelope address) you have to dig deeper into the headers of the message. Unfortunately, many email programs try to hide this information from the user. If the mail program you are using gives you the option to see the full headers of the message, then you will see a series of Received: lines. Every time the email is handed off to another computer, it is stamped with a Received: header, which is similar to a postmark. The only way to find the true originator of the message is to look at the Received header with the earliest date. To confuse things even more, some older or misconfigured mail servers can be tricked into putting incorrect information in the Received: lines as well, so proceed with caution. In general, you will likely find at least the IP number of the machine on which the email originated, but you are likely not to find a username or real email address.

In order to see the actual recipient address (remembering that the To: line may be incorrect) you are likely to find this in the last Received: header (ie. the one with the oldest date). Note that when reading the headers from top to bottom, the Received headers show up in reverse chronological order.