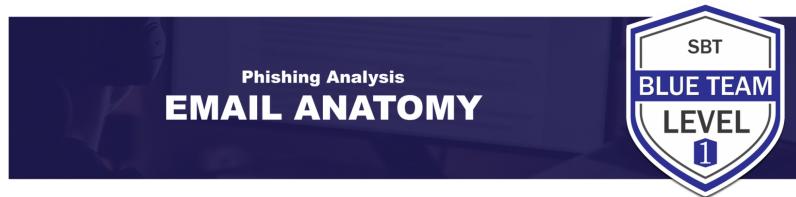


Blue Team Level 1 Certification (Standard)	
Introduction to BT1	
<input checked="" type="checkbox"/> Welcome to Blue Team Level 1!	
● 4 Topics	
<input checked="" type="checkbox"/> Lab and Forum Access	
SECURITY FUNDAMENTALS DOMAIN	
<input checked="" type="checkbox"/> Introduction to Security Fundamentals	
● 1 Topic	
<input checked="" type="checkbox"/> Soft Skills	
● 7 Topics	
<input checked="" type="checkbox"/> Security Controls	
● 5 Topics   1 Quiz	
<input checked="" type="checkbox"/> Networking 101	
● 6 Topics   1 Quiz	
<input checked="" type="checkbox"/> Management Principles	
● 4 Topics   1 Quiz	
PHISHING ANALYSIS DOMAIN	
<input checked="" type="checkbox"/> PA1) Introduction to Emails and Phishing	
● 7 Topics   1 Quiz	
<input checked="" type="checkbox"/> Section Introduction: Emails and Phishing	
<input checked="" type="checkbox"/> How Electronic Mail Works	
<input checked="" type="checkbox"/> Anatomy of an Email	
<input checked="" type="checkbox"/> What Is Phishing?	
<input checked="" type="checkbox"/> Impact of Phishing	
<input checked="" type="checkbox"/> Further Reading Material: Phishing Analysis	
<input checked="" type="checkbox"/> Phishing Analysis Glossary	
<input type="checkbox"/> Activity) End of Section Review: Emails and Phishing	
<input checked="" type="checkbox"/> PA2) Types of Phishing Emails	
● 10 Topics   2 Quizzes	
<input checked="" type="checkbox"/> PA3) Tactics and Techniques Used	
● 12 Topics   2 Quizzes	
<input checked="" type="checkbox"/> PA4) Investigating a Phishing Email	
● 8 Topics   2 Quizzes	
<input type="checkbox"/> PA5) Analysing URLs, Attachments, and Artifacts	
● 8 Topics   1 Quiz	
<input type="checkbox"/> PA6) Taking Defensive Actions	
● 12 Topics   1 Quiz	
<input type="checkbox"/> PA7) Report Writing	
● 7 Topics   1 Quiz	
<input type="checkbox"/> PA8) Phishing Response Challenge	
● 3 Topics   1 Quiz	
THREAT INTELLIGENCE DOMAIN	
<input type="checkbox"/> TI1) Introduction to Threat Intelligence	
● 7 Topics	
<input type="checkbox"/> TI2) Threat Actors & APTs	
● 6 Topics   2 Quizzes	

# Anatomy of an Email

Blue Team Level 1 Certification (Standard) > PA1) Introduction to Emails and Phishing > Anatomy ...

COMPLETE



Ever wondered what actually makes an email? Electronic mail messages are comprised of two parts; a **header** and a **body**. We'll cover both of these parts as it will make it more straightforward when conducting artifact retrieval and analysis in later lessons.

## EMAIL HEADER

A header is a set of lines containing information about the message's transportation, such as the sender's address, the recipient's address, or timestamps showing when the message was sent by intermediary servers to the transport agents (MTAs), which act as a mail sorting office. The header begins with the **From** line and is changed each time it passes through an intermediary server. Using headers, you can see the exact path taken by the email and how long it took each server to process.

### Header Fields

The **message** itself, made up of the two following elements: the **header fields**, a set of lines describing the message's settings, such as the sender, the recipient, the date, etc. An email includes at least the three following headers:

- **From**, showing the sender's email address
- **To**, showing the recipient's email address
- **Date**, showing the date when the email was sent.

### Optional Header Fields

It may also contain the following optional fields:

- **Received**, showing various information about the intermediary servers and the date when the message was processed
- **Reply-To**, showing a reply address
- **subject** showing the message's subject
- **message-ID**, showing a unique identification for the message
- **message body**, containing the message, separated from the header by a line break

### Custom X-Headers

It is important to note that header data is no guarantee of when the message was sent or who sent it, as values can be edited without any requirement for authorization, such as changing the From address to make it look like the email has come from "contact@amazon.co.uk" (We cover Sender Spoofing in more detail in PA3) Tactics and Techniques Used). Additional personalized headers (called **X-headers**) can be set in order to provide the appropriate information. X-headers are called such because their name must begin with X-. For example, some anti-spam software programs mark messages as unwanted using the following header: **X-Spam-Status: YES**.

- TI3) Operational Threat Intelligence
  - 7 Topics | 1 Quiz
- TI4) Tactical Threat Intelligence
  - 7 Topics | 2 Quizzes
- TI5) Strategic Threat Intelligence
  - 5 Topics | 1 Quiz
- TI6) Malware and Global Campaigns
  - 6 Topics | 1 Quiz

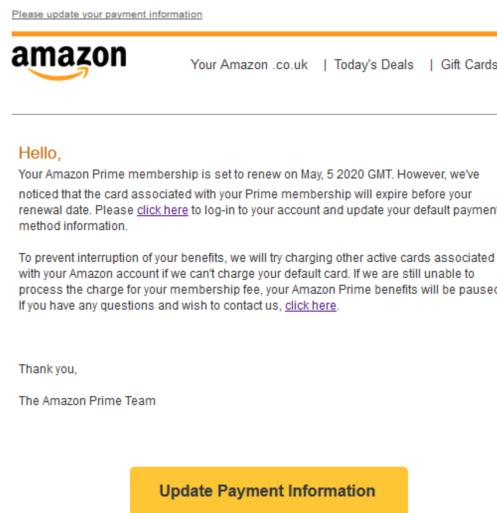
## DIGITAL FORENSICS DOMAIN

- DF1) Introduction to Digital Forensics
  - 5 Topics
- DF2) Forensics Fundamentals
  - 10 Topics | 5 Quizzes
- DF3) Digital Evidence Collection
  - 8 Topics | 1 Quiz
- DF4) Windows Investigations
  - 3 Topics | 3 Quizzes
- DF5) Linux Investigations

## EMAIL BODY

An email body is where the information written by the sender is displayed for the recipient. This can be purely text-based or it can include hyperlinks, images, and HTML styling.

This is the email we're going to walk you through, a fake Amazon email. This email looks genuine and uses Amazon colors and branding to effectively impersonate the brand. The email is structured nicely, and there are no spelling mistakes, improving its effectiveness.



It is fairly common for emails to use encoding for their contents, especially if they are using a lot of HTML styling, as this works to reduce the size of the email. In the below image you can see that we are told on the third line of this screenshot that the email content is encoded in base64. So let's decode it!

-alt=b28cf535948dcfd6189b1b38cb7aff0  
Content-Type: text/html; charset=urf-8  
Content-Transfer-Encoding: base64

PCTELVBTlRJQk9UUmFkZTMzF2l0MExDl1MjY1vJyAwUmQ5TY4M2JdLS0+PCFET0NUWVF  
IGHobWphGobWphG1hYQhDq0BwM5Yb0Sd0HrLwU1L2PSd2502W50LVR5cGUhGvnbr1  
bnQnInRleQhVaRtDhsyGvChknNld16lGyC1T+PPrhdGx1PktPT1RPTDwvG1bGuH+IdwvaGh  
ZD4KPGPrjd4pa1w11GrHgd1Ta17Wx20E8lPS1FSeHmC1hbg33+j5PdHrcwzvCo3ld3dyh  
bfWb2Fa4y28udwszvA2zv3c15odG1sP+9w9ykwuPmTf1UKTfJyVzHxbzAs7zL1Ts4N1VG1VOpVStEm  
Yw1Yw0009xJduYw0Jbptc2z6MjAyDaTzKtLwzJyUdVf17D1nqz0tLwHg0U2Y7JvN1Rl2h1  
Yw1DwCld5Zxh2b1Ja7y0jDwL0BLwvRkrdaMfDtpUwMv1Yw019Hw01He1l0K1h1Kz  
bfWfXNz7XuLzCm3c1nLw1Twd1lyhbfWb2Fa4y28ut1Kw1H2z1TzGryLyJyAxJ2Gh6m2T12  
dtJh1bwnLwmpd2zXh2b1Ja7y0jDwL0BLwvRkrdaMfDtpUwMv1Yw019Hw01He1l0K1h1Kz  
Xz2M7TnEfWdfTf0W1h01Kxx29pW5z1b1z3aHw0D1Si1gxwP2f0H5Si1jx4KPhG1lbn1lc1j4K  
PRHyrHym11Gn1bx2CgJfaw5n1St1Wb1jzKfcGkfLuzw1P1kg2lkd9g7jyAxJwC0Ug8o6V3  
ZhK+Cjx+4jKPHR1KfGf+sdw05j31S20zX11hngh1nJyid9gnw1b1z2nvG9yS1jz2mz1m2m  
I4jKPHR1yMx11Gn1bx2CgJfaw5n1St1Wb1jzKfcGkfLuzw1P1kg2lkd9g7jyAxJwC0Ug8o6V3  
ad01TQw1b1jbfGzc0v11q39aR0wD1M1C+jx9y8mke4TfKCHgryy8go4Gg012kdg91jy1w18h  
bn1bg1j0Y2Vdubg1j1bJg0zcc1f0e39aR0wD1w4J183Rk3gpd0g2lg1kG91jyUw1Ctg  
Z249im1zL0q1zHngh1bJn1g6l9w1b1jg2zC0fie39aR0wD1zC1+jxkaYwzv2xh3c91nHf  
ag1nLk215Grc35g629u1mzbvQntz1fMwz50kxyw1sLh1sL2h1GzJySxzW5Lx1mlm0yB250  
LxNpem16WTbdwes1p1zLwHg07twezdgyz9s2b1z16y2zN1y211n+jch1jHrmhd0b1  
X2j3Sm511bYy29w1m5b281bMy15yGvcmw3Mx2jY11GrhdgetyXw0d1wymz1aPw02j19G  
alldpmwbs33j5PdHrcwzvCo3ld3dyhbfWb2Fa4y28udwszvA2zv3c15odG1sP+9w9ykwuPmTf1K  
TUfJYfJyHxbzAs7zL1Ts4N1VG1VOpVStEmYw0009xJduYw0Jbptc2z6MjAyDaTzKtLwzJyUdVf  
ZD17D1nqz0tLwHg0U2Y7JvN1Rl2h1Jy1Wm1twCld5Zxh2b1Ja7y0jDwL0BLwvRkrdaMfDtpUw  
PUh1Wm1l0u1W09aR0hC1101y1Kj1K23dz1u1h3em1Lw1m1vLw1rTzJG23Al1Kwcm2z1tMwln1  
W1y1M2z0z5zURFvgrJy1j1z2yMfTzEgyFmV1y1TwWzQy1Qd104TfCvfyfbnf3c1z2y  
aXBoa0u1Qx6kvh1Ex3WzF6Gz02zXh2a75D502uMVFvTPRp0wMs1k1w08eySfZCk3c0B8Bm1t  
cdTy1WzFpx1Xb2z1TzWfDf1c0hJ1d0x3C5x12zX3N1yHf1y1w1g2d1w18s1W5J3F1rc1d  
dg1u1HnyX0p5D5pb1h1Ldn13z0nq1w11Z0Tdh10nJhcKtsfzdg1mz02q02nlpMcPnRqV1y  
NDM72f1VefExeGKFmN01000Dzjz1E13M107zqxtb1y1UvU0Rz1uPnUg1QzT0Lz1R2Pt1NxP  
zlw1Jew0nfDzU2nTzg1nxUyGz1r2z0sfNs1xj3z4C5yJN17DzGz1Np1vBp6gU6l1Ud1  
MvzxUv3NTBmkRmNzVsHaJ1gtRcrklyyJN17Dy1wTg91b1dHs1zT01z9s3b16z1z2y1J  
N1sJgdgdf4C1zLw1m1cm09aUw1UvGzbyGlu1zGux1Lx11b1c1RhGudwGe1Lw1tXz50

In the below GIF, we show how CyberChef can be used to quickly decode Base64 into readable text.



The screenshot shows a user interface for a hex dump tool. On the left, there's a sidebar with several options: 'To Hexdump', 'From Hexdump', 'URL Decode', 'Regular expression', 'Entropy', 'Fork', and 'Magic'. The 'Magic' option is currently selected, indicated by a blue background. In the center, there's a large input field containing the text 'STEP'. Below the input field are two buttons: a green 'BAKE!' button and a smaller 'Auto Bake' button with a checked checkbox. To the right of the input field is an 'Output' section with a status bar at the top showing 'time: 1ms', 'length: 14', and 'lines: 14'. Below the status bar are icons for copy, paste, and search. At the bottom of the interface are three navigation buttons: 'Previous Topic' (with a left arrow), 'Back to Lesson' (centered), and 'Next Topic' (with a right arrow).

To Hexdump  
From Hexdump  
URL Decode  
Regular expression  
Entropy  
Fork  
Magic

STEP

BAKE!

Auto Bake

Output

time: 1ms  
length: 14  
lines: 14

Previous Topic Back to Lesson Next Topic