Name : Challenge 2

Domain : Forensics

Author: Kaushik Aduri

Description :
Digital forensics is the application of analysis techniques to gather evidence from a particular computing device in a way that is suitable for presentation in a court of law.
The goal of forensics is to perform a structured investigation and maintain a documented chain of evidence.
Cryptographic hashing is the practice of transforming plain text into cipher text, for the purpose of security.
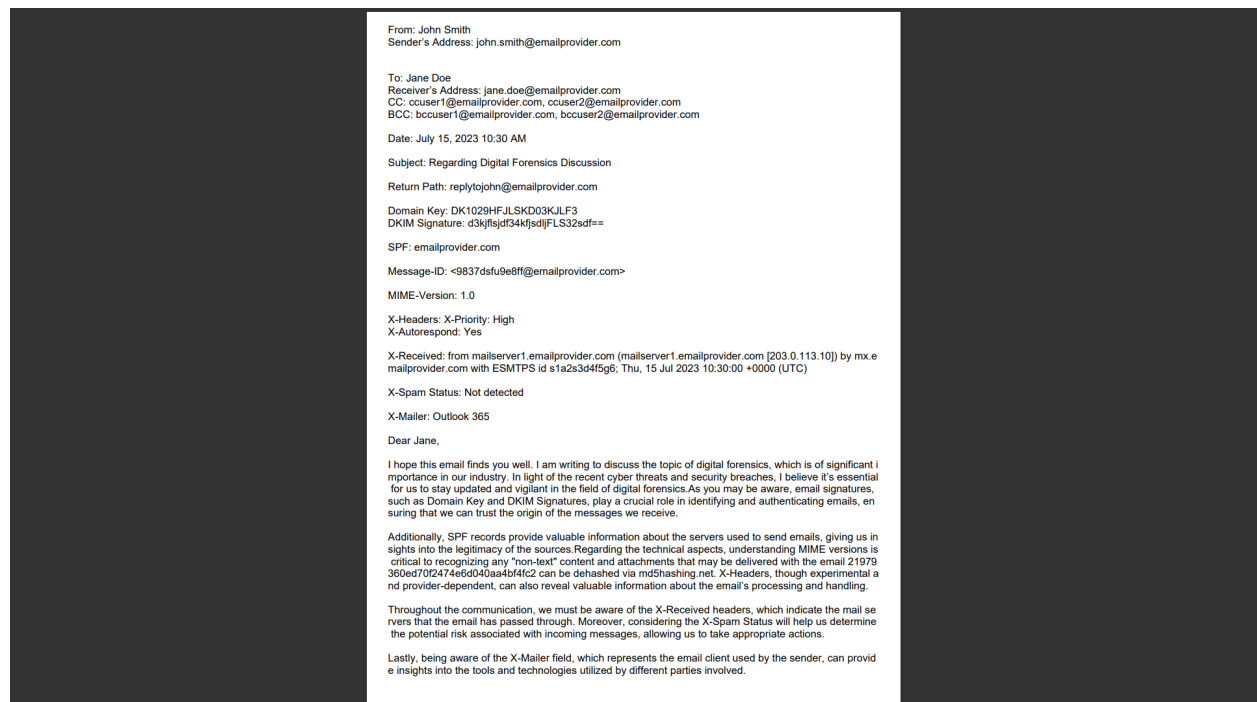A Hash Value (also called as Hashes or Checksum) is a string value (of specific length), which is the result of calculation of a Hashing Algorithm. Hash Values have different uses. One of the main uses of Hash Values is to determine the Integrity of any Data.

Files Given: Digi_Forensics_Challenge2.pdf

Writeup:
This challenge is basically related to email forensics .So this email consists of a cryptographed hash value that needs to be decoded by the user.
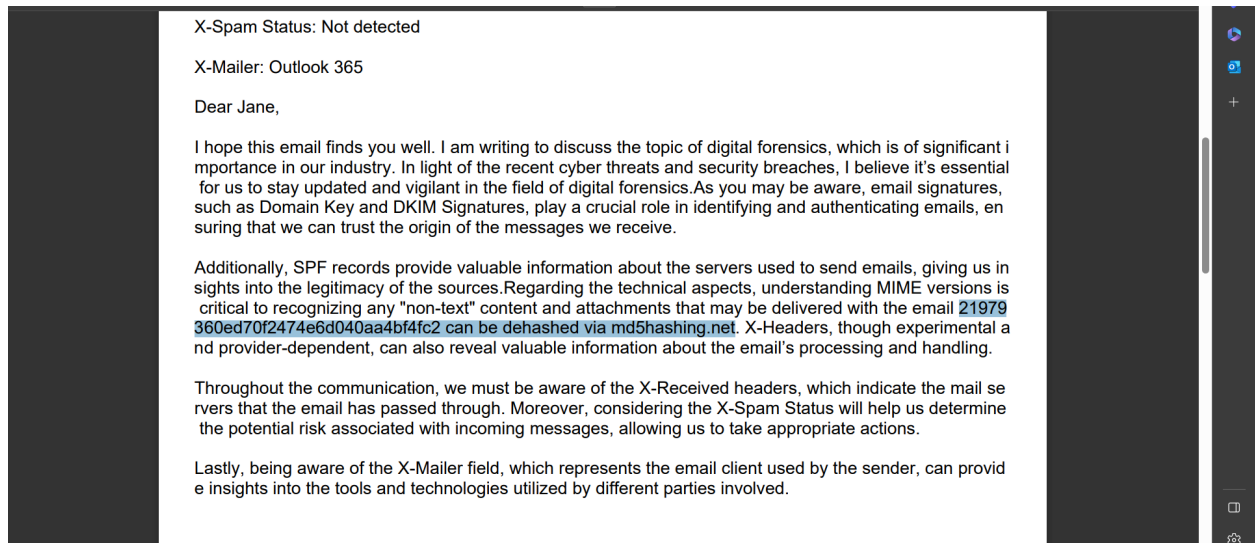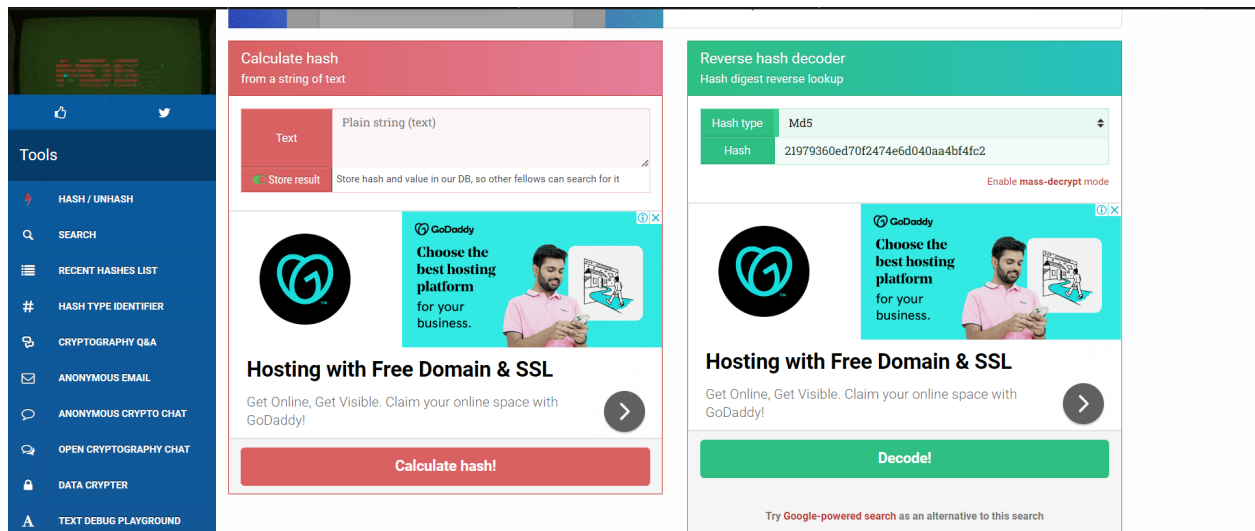Email in the given file

From: John Smith
Sender's Address: john.smith@emailprovider.com

To: Jane Doe
Receiver's Address: jane.doe@emailprovider.com
CC: ccuser1@emailprovider.com, ccuser2@emailprovider.com
BCC: bccuser1@emailprovider.com, bccuser2@emailprovider.com

Date: July 15, 2023 10:30 AM

Subject: Regarding Digital Forensics Discussion

Return Path: replytojohn@emailprovider.com

Domain Key: DK1029HFJLSKD03KJLF3
DKIM Signature: d3kjflsjdf34kfjsdljFLS32sdf==

SPF: emailprovider.com

Message-ID: <9837dsfu9e8ff@emailprovider.com>

MIME-Version: 1.0

X-Headers: X-Priority: High
X-Autorespond: Yes

X-Received: from mailserver1.emailprovider.com (mailserver1.emailprovider.com [203.0.113.10]) by mx.e
mailprovider.com with ESMTPS id s1a2s3d4f5g6; Thu, 15 Jul 2023 10:30:00 +0000 (UTC)

X-Spam Status: Not detected

X-Mailer: Outlook 365

Dear Jane,

I hope this email finds you well. I am writing to discuss the topic of digital forensics, which is of significant i
mportance in our industry. In light of the recent cyber threats and security breaches, I believe it's essential
for us to stay updated and vigilant in the field of digital forensics.As you may be aware, email signatures,
such as Domain Key and DKIM Signatures, play a crucial role in identifying and authenticating emails, en
suring that we can trust the origin of the messages we receive.

Additionally, SPF records provide valuable information about the servers used to send emails, giving us in
sights into the legitimacy of the sources.Regarding the technical aspects, understanding MIME versions is
critical to recognizing any "non-text" content and attachments that may be delivered with the email 21979
360ed70f2474e6d040aa4bf4fc2 can be dehashed via md5hashing.net. X-Headers, though experimental a
nd provider-dependent, can also reveal valuable information about the email's processing and handling.

Throughout the communication, we must be aware of the X-Received headers, which indicate the mail se
rvers that the email has passed through. Moreover, considering the X-Spam Status will help us determine
the potential risk associated with incoming messages, allowing us to take appropriate actions.

Lastly, being aware of the X-Mailer field, which represents the email client used by the sender, can provid
e insights into the tools and technologies utilized by different parties involved.

In the mail hash and website to decode is given.
Hash :21979360ed70f2474e6d040aa4bf4fc2
Website: https://md5hashing.net

Visit the given website and enter the hash and click on "Decode!"

Reversed hash value is the required flag

Flag is : PCC{T@$k_2_F0re%$1sc}