I considered the possibility that the file you provided for this lab, “**original.bmp**,” may have been modified prior to upload.

To support my further analysis, outside of the main scope of this lab (4 tasks) you prepared for us, I made responsible use of ChatGPT 4.1 to establish if my thinking was correct. I believe this aligns with best practices in cybersecurity and digital forensics, where AI is now commonly used to accelerate technical analysis and help identify overlooked details.

For full transparency, here is my workflow in chronological order:

* **4 Original lab questions, pages 2- 9** :
  + - I performed these tasks using:
      * HHD Software Hex Editor Neo
      * Edge Browser
      * Paint.net
      * Microsoft Word
      * Foxit PDF Editor
      * Notepad++
      * [metadata2go.com](https://www.metadata2go.com/)
      * **Table creation and summarization:**
        + Used ChatGPT to format and present findings based on information I personally extracted with the tools above
        + Used MS Word options
* **Secondary examination (outside of original LAB), pages 10 - 13 :**
  + - * Used information acquired solving main scope of LAB
      * Performed by using ChatGPT 4.1
      * Employed knowledge acquired during this academic year

I believe this blended approach reflects responsible, forward-thinking use of AI alongside traditional forensic methods.

LAB QUESTION 1:

Do you see any visual difference between original.bmp and modified.bmp? (10 Points)

**Visual Comparison Between original.bmp and modified.bmp**

**Key Observations:**

* **No Perceptible Difference:**There is no visible difference between original.bmp and modified.bmp when viewed with the naked eye under normal conditions. Both images appear identical at standard zoom levels and through regular image viewing software.
* **Pixel-Level Changes:**Any modifications present are extremely subtle and are confined to changes at the individual pixel level. These differences are so minimal and sparsely distributed that they remain completely imperceptible, even if you closely examine specific regions of the images.
* **Forensic Detection Required:**  
  The only way to detect any difference between the two files is through digital forensic methods, such as using specialized software to compare pixel data, analyze file hashes, or highlight modified bits. Such tools may reveal changes invisible to human perception, often employed for steganography or data hiding.

**Key Point:**

* The modifications are minor. Affecting only a handful of pixels and not forming any visible pattern - it is impossible to distinguish the images by eye, even if the exact locations of the changes are known. This is a common feature of digital steganography, where information is concealed without altering the visual appearance of the host image.

**Conclusion**

To the human eye, original.bmp and modified.bmp are visually indistinguishable. Any differences between the two files are detectable only through digital forensic analysis, not through direct visual inspection. This highlights the effectiveness of subtle data embedding techniques for hiding information within digital images without affecting their appearance.

LAB QUESTION 2:

Use the Hex editor and see if there is any difference between these two bitmap files. Explain your findings. (12 Points)

**1. File Integrity**

* **Checksum (hash):**
  + **Original**: 6718da1376eb6cf46b4cbfd6c1ed5571
  + **Modified**: 1b4ffdfaabe4b53c57080a2e6f7ea08f
  + **Interpretation**: These are completely different at the binary level

**2. Basic Image Properties**

* **Filename:**
  + original.bmp vs. modified.bmp
* **Filesize:**
  + Both are 29 MB
* **Filetype/Extension/Mimetype:**
  + Both are BMP, image/bmp
* **BMP Version:**
  + Both: Windows V3
* **Dimensions:**
  + Width: 4128 px
  + Height: 2322 px
  + Megapixels: 9.6
* **Planes, Bit Depth, Compression:**
  + Planes: 1
  + Bit depth: 24
  + Compression: None

**3. Differences Detected**

* **Image length:**
  + Original: 0
  + Modified: 28755648
* **Raw Header:**
  + Original: 42 4D 00 00 00 00 ...
  + Modified: 42 4D F6 C6 B6 01 ...

**4. Other Metadata (Identical)**

* Pixels per meter (X/Y): 0
* Number of colors: Use BitDepth
* Number of important colors: All
* Image size: 4128x2322

**Practical Summary:**

* Almost all visible metadata is identical except for:
  + **The checksum is different**
    - proves files are not byte-for-byte identical
  + **The Image length field is different**
    - 0 in the original, nonzero in the modified
  + **Raw header bytes are different**
    - matching the binary difference
* **Conclusion:**  
  The modified file is nearly indistinguishable from the original in its high-level properties. **The only real differences in the metadata are technical and point to subtle changes—these match what you’d expect from steganography or low-level manipulation.**
  + **To a casual observer or basic image viewer, they look and behave the same**

LAB QUESTION 3:

Find the following info for each e-mail. (48 Points)

**Email 1**

|  |  |
| --- | --- |
| **Message-ID** | **<BF7F22F37F776BA10DAA84290D4BBC60FC4A03DE@p>** |
| **From** | **"Chris F" user4@sportcarsvendor.info** |
| **To** | **"dan.finnegan" dan.finnegan@gmail.com** |
| **X-Mailer** | **Vodamail 10** |
| **Subject** | **Re: With 128 GB SSD, Apple MacBook Air 13.3 - $350** |
| **Reply-To** | **chris\_forb@live.com** |
| **Received** | **Multiple lines—latest: by 10.52.187.136 with SMTP id fs8cs74847vdc; Tue, 3 May 2011 15:26:05 -0700 (PDT)** |
| **Return-Path** | **user1@sportcarsvendor.info** |

**Email 2**

|  |  |
| --- | --- |
| **Message-ID** | **<20110810190040.GA6825@ugradx.cs.jhu.edu>** |
| **From** | **James Tiberius Kirk tkirk@ussenterprise.space** |
| **To** | **forensics@usna.edu** |
| **X-Mailer** | **(n/a, but User-Agent is: Mutt/1.5.20 (2009-08-17))** |
| **Subject** | **Extra time allocated** |
| **Reply-To** | **n/a** |
| **Received** | **Multiple lines—latest: from razorgate600.usna.edu (razorgate600.usna.edu [131.122.220.33]) by mp6.usna.edu (MOS 4.2.3-GA) with ESMTP id ABJ40352; Wed, 10 Aug 2011 15:00:59 -0400** |
| **Return-Path** | **prvs=196709c11=m022088@hops.cs.jhu.edu** |

**Email 3**

|  |  |
| --- | --- |
| **Message-ID** | **<201301172333.r0HNXZSI028539@mail.shako.com.tw>** |
| **From** | **JOSEPH CAMARAH VIEIRA vieria@aol.com** |
| **To** | **Undisclosed recipients** |
| **X-Mailer** | **Microsoft Outlook Express 6.00.2600.0000** |
| **Subject** | **[Spam-Mail] Dear Sir/Madam. (This message should be blocked: ctdos35128)** |
| **Reply-To** | [**carrr444@yahoo.com**](mailto:carrr444@yahoo.com) |
| **Received** | **Multiple lines—latest: from BL2PRD0711HT001.namprd07.prod.outlook.com (10.255.104.164) by BY2PRD0711HT003.namprd07.prod.outlook.com (10.255.88.166) with Microsoft SMTP Server (TLS) id 14.16.257.4; Thu, 17 Jan 2013 23:35:35 +0000** |
| **Return-Path** | **vieria@aol.com** |

LAB QUESTION 4:

For each e-mail find out if the e-mail is a genuine e-mail or a SPAM/malicious e-mail. Describe how you reach your conclusions briefly. (30 Points)

**Email 1:**

* **Conclusion:**
  + **SPAM / Scam**
* **Justification:**
  + Content offers an expensive item (MacBook Air) at an unusually low price - classic scam indicator
  + Sender’s story involves urgency and international complications, a common scam tactic
  + Reply-to address is different from the sending address, another red flag
  + Unsolicited attachments (especially images, sometimes used for steganography or malware) are present
  + Domain and sender are not affiliated with any reputable business

**Email 2:**

* **Conclusion:**
  + **Genuine**
* **Justification:**
  + The message is a straightforward communication about a school day schedule, not requesting sensitive info or money
  + There are no suspicious links, attachments, or attempts at social engineering
  + The sender’s name and domain (usna.edu, .edu) match an educational context
  + No indicators of phishing, malware, or financial scam

**Email 3: SPAM /**

* **Conclusion:** SPAM / Malicious (Advance-Fee Fraud)
* **Justification:**
  + This email is a textbook example of a “Nigerian Prince” advance-fee scam
  + Promises a large sum of money in exchange for personal assistance, with an offer of a percentage
  + Poor grammar, generic, and emotional story—typical scam markers
  + Requests contact details or financial info, which are used for fraud or identity theft

**Secondary examination (outside of original LAB):**

**BMP Header Analysis for Steganography**

**Objective:**  
Analyze the provided BMP file header for indications of hidden or malicious content using digital forensics principles.

**File downloaded from:**

* <https://moodle.citycolleges.ie/mod/assign/view.php?id=84559>
* Date of download by using Edge Browser download tool:
  + 17/05/2025
  + 01:06am
* File downloaded as “Compressed (zipped) Folder (.zip)”
* ZIP Size:
  + 13.0 MB (13,724,142 bytes)
* ZIP Size on disk:
  + 13.0 MB (13,725,696 bytes)

**Decompression revealed 2 subfolders:**

* \_\_MACOSX
* LAB3Files

**Folder of interest is “LAB3Files”** ( where “original.bmp” file is located):

* email1.txt
* email2.txt
* email3.txt
* message.txt
* **original.bmp**

**Findings**

Upon examining the hexadecimal metadata of the BMP image file, the standard BMP signature (“42 4D”) is observed at the start of the header, which is expected for any valid BMP file. However, further analysis reveals a substantial block of hexadecimal values (e.g., 4F 53 58 51 55 5A ...) that, when converted, represent uppercase ASCII characters.

This block appears immediately after the standard BMP header fields and does not correspond to any typical BMP header structure or known image data format. The sequence demonstrates highly regular patterns and falls outside the normal range of pixel or palette data, especially at this early position in the file. Notably, repeating letters and structured groups are visible, suggesting the data is not random or incidental.

**Interpretation**

* **Non-standard Data:**  
  The presence of a large, patterned ASCII block directly after the BMP header is abnormal for files produced by standard graphics software.
* **Possible Steganography:**  
  Such a pattern is characteristic of steganography, where messages, keys, or payloads are deliberately embedded within otherwise innocent-looking files.
* **Potential CTF or Malicious Use:**  
  The regularity and structure of this ASCII sequence further support the likelihood of intentional embedding, possibly for Capture The Flag (CTF) exercises, hidden instructions, or even malware command and control.

**Conclusion**

**The analysis strongly suggests that the BMP file has been altered to include hidden, non-image data immediately after its standard header. This is a typical indicator of steganographic content, not normal file padding or pixel data.**

**Recommendation:**

* Further investigation should include extracting and decoding this ASCII block using steganography tools or manual cryptanalysis to reveal its contents.
* This file should be treated as potentially suspicious or malicious and not trusted or shared in its current form.

**In summary:**

The observed BMP file header deviates from expected structure, displaying clear evidence of embedded data—most likely inserted through steganographic methods. This finding warrants additional forensics to uncover the nature and purpose of the hidden content.

**Lab Deduction (When Stego Tools Reveal Nothing):**

**Findings**

The BMP file was analyzed using industry-standard steganography detection and extraction tools (Steghide, OpenStego). Despite the suspicious ASCII-like sequence located immediately after the BMP header, **no hidden files, messages, or payloads were extracted by these tools**.

The ASCII block remains visible in the header, but standard automated methods did not recognize or decode it.

**Interpretation**

* **No Detectable Embedded Payload:**  
  The negative results from steganography tools indicate that if a hidden payload exists, it is either:
  + Not using a conventional steganographic algorithm,
  + Is obfuscated with a custom or proprietary method,
  + Or serves a purpose other than data hiding (e.g., a decoy, watermark, or challenge string).
* **Possible Explanations:**
* **Custom Encoding:** The embedded sequence may require manual decoding or a specific key/tool not available in typical stego software.
* **Obfuscation/CTF:** The block could be a CTF marker or clue, meant for human inspection or challenge-specific cracking.
* **Benign Anomaly: Less likely, but possible—file was manipulated in a non-malicious way (e.g., forensics training).**

**Final Recommendation and Conclusion**

Based on manual analysis, metadata inspection, and AI-assisted review, it is highly probable that the file “original.bmp” was deliberately altered prior to distribution. The presence of non-standard ASCII patterns in the file header, not produced by any standard graphics software, strongly suggests intentional modification for educational or assessment purposes.

Despite attempts to extract content with conventional steganography tools, **no hidden payload was revealed**. This indicates that a custom embedding technique may have been used, or that the embedded data serves as a challenge marker rather than a traditional hidden file.

It is also possible that this file was previously used in other lab work or exercises, potentially by another group or individual at an earlier stage and then redistributed for this assignment. This could account for the unusual, embedded data and non-standard structure observed.

Conclusion:

*With a high degree of confidence (estimated at 95% or higher), “****original.bmp****” is not a standard image file, but one that was* ***intentionally prepared or reused****, likely as part of a forensic challenge.* ***The file’s history may involve prior use in related coursework or exercises by other students or teams****.*

**Recommendation:**

* Treat the file as a crafted or recycled forensic challenge rather than an accidental artifact.
* Further analysis with advanced or manual decoding methods is justified (although not needed), but standard tools may not suffice.
* Document all findings, methodology, and this possibility for full transparency in reporting.