CYBR472 Lab 01: Creating a Forensic Image
greenthom – 300536064

Assessment Overview

This assessment evaluates your understanding of forensic imaging techniques based on Lab 01. You will demonstrate your ability to create forensic images, compare acquisition methods, and analyze forensic reports for evidence integrity. Each lab is worth 6% and there are five labs making a total of 30% for all the lab work.

Submission Requirements

- Screenshots as indicated (no writing required)
- Write no more than a couple of paragraphs when answering each part of a questions
- There are 13 questions
- Submit as a single PDF document

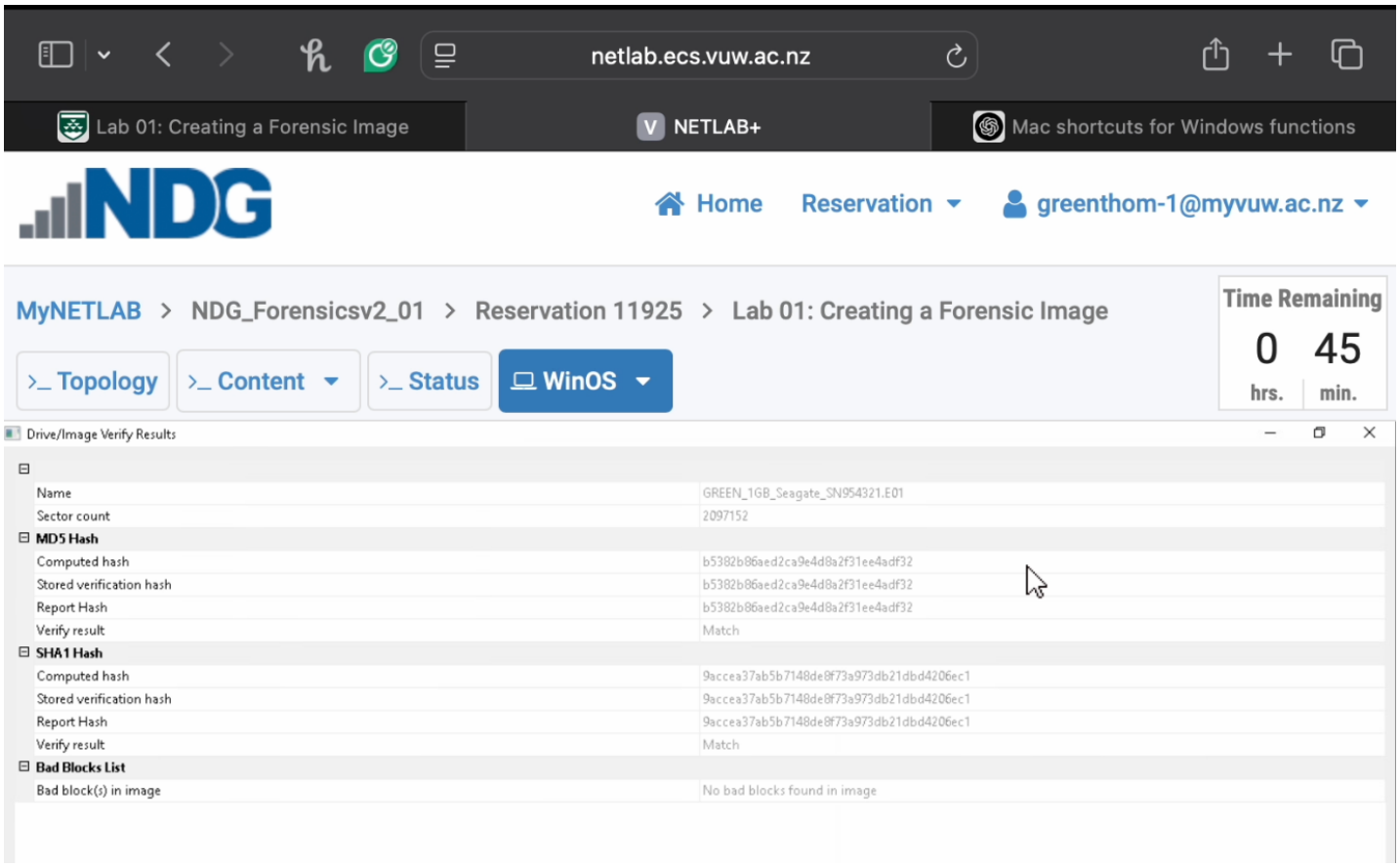
1.1. Create a Physical Forensics Image (20 marks)

Complete the lab but when creating your images please:

- Use your name as the examiner in the Evidence Information window, e.g. Ian Welch
- Include your last name in the image filename, e.g. WELCH_1GB_Seagate_SN54121

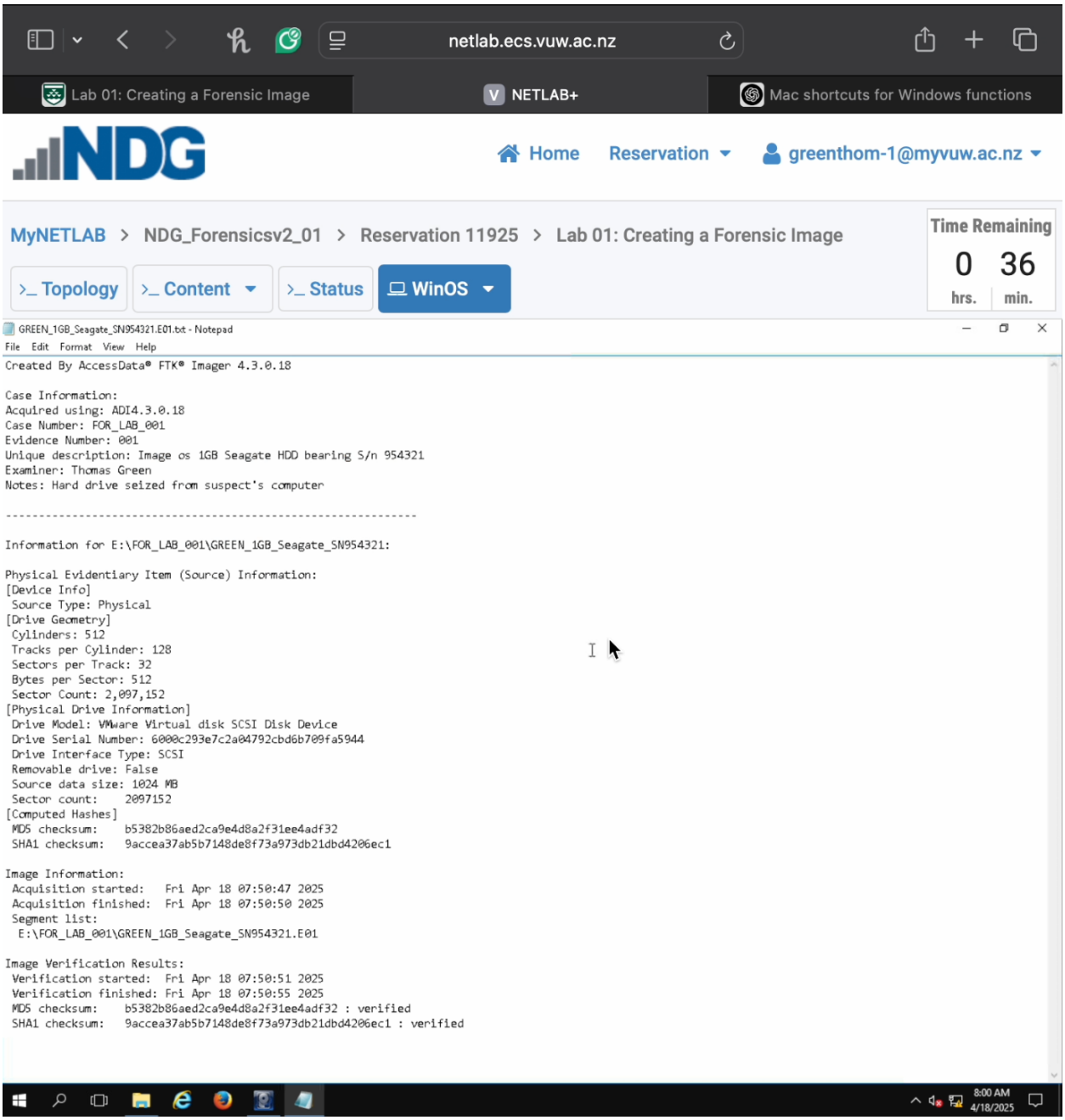
Document your process by providing screenshots for the physical acquisition (you do not need to write anything underneath the screenshot):

1) Screenshot showing your verification of the image integrity (5 marks)

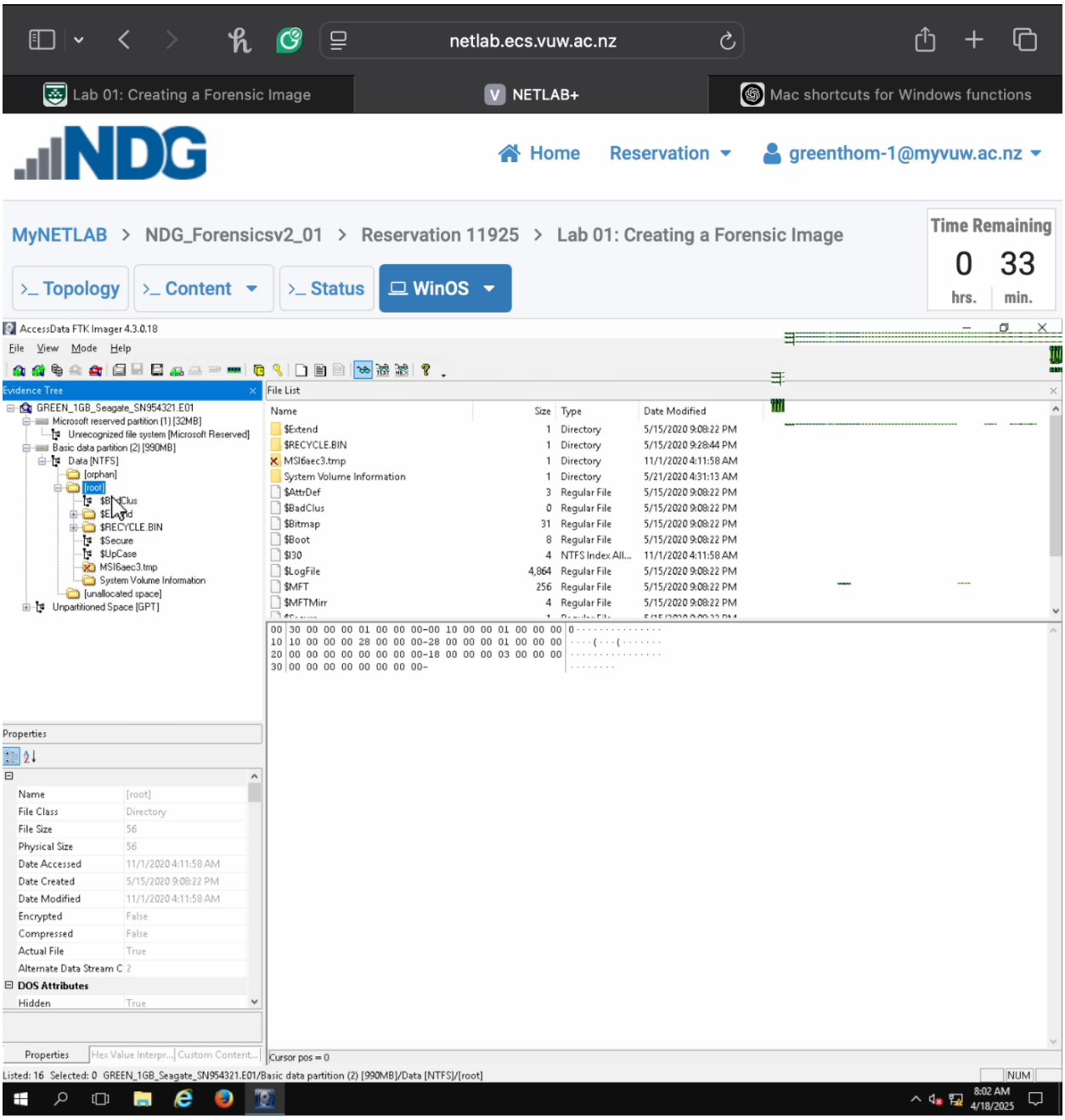


2) Screenshot of the FTK Imager's image report with the following information (10 marks):

- **Case number**
- **Evidence description**
- **Acquisition date/time**
- **Image format selected**
- **Hash values (MD5 and SHA1)**



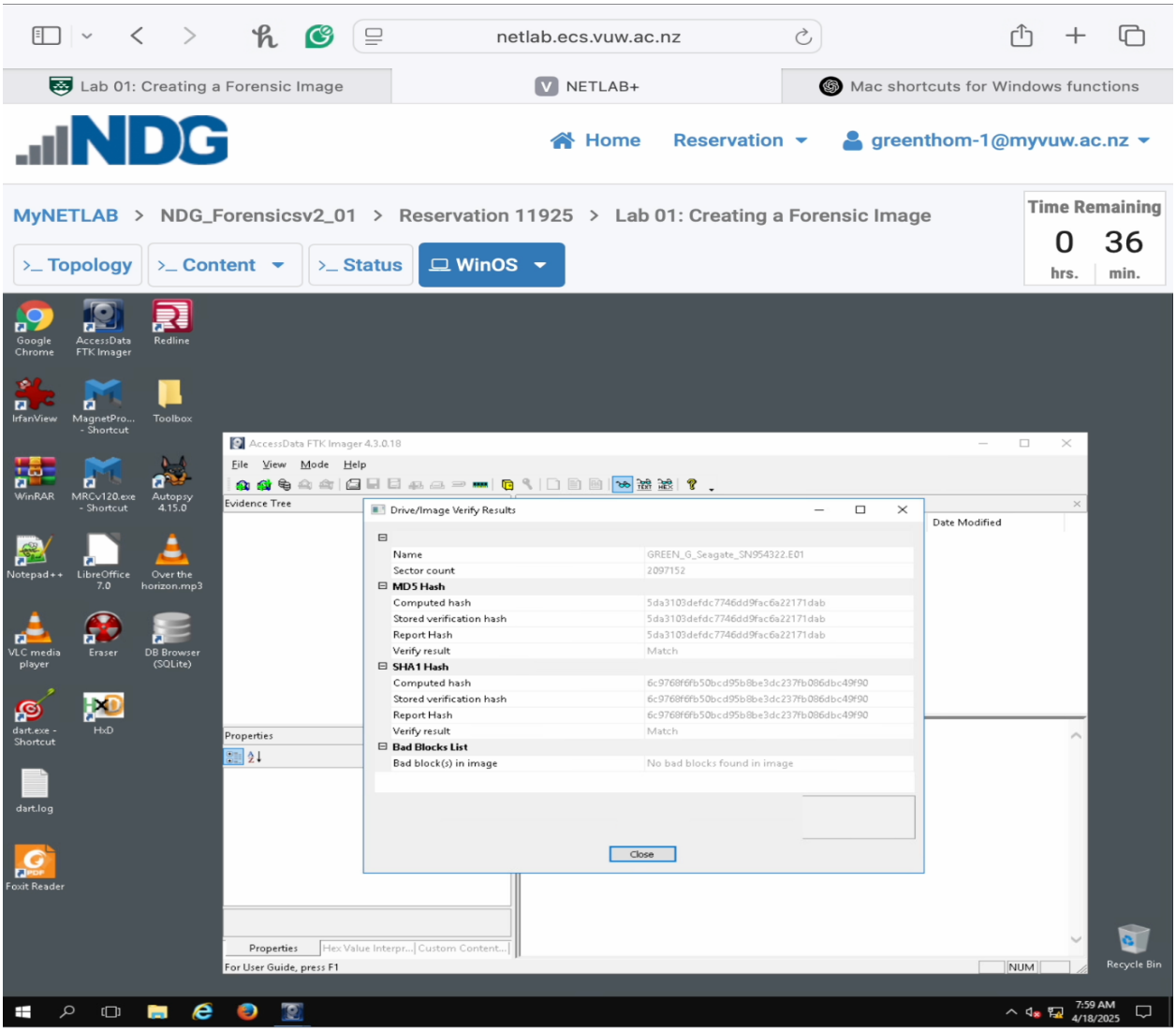
3) A screenshot showing you've successfully mounted the image and can view its contents (5 marks)



1.2. Create a Logical Forensics Image (20 marks)

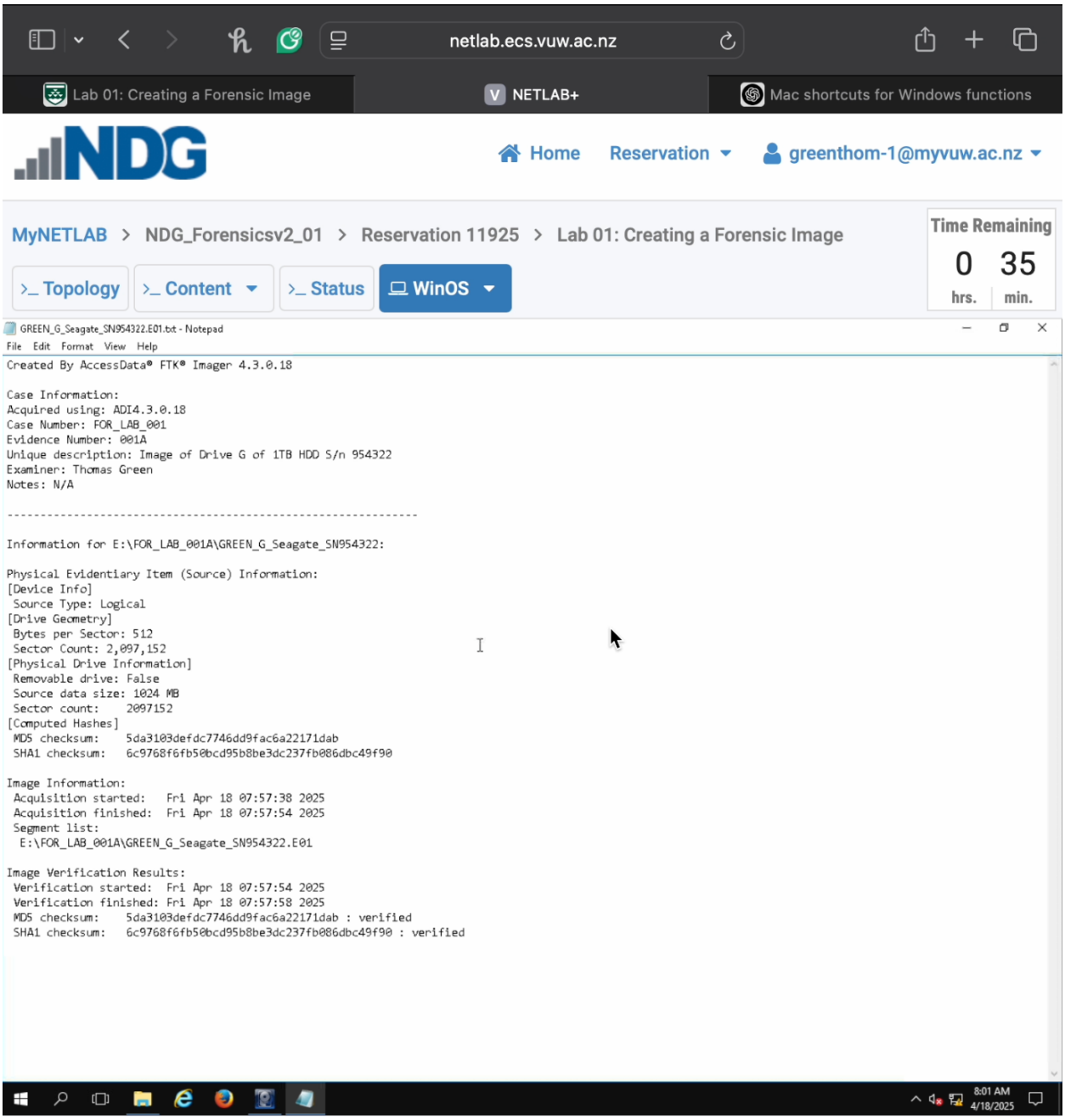
Document your process by providing the following screenshots for the logical acquisition:

4) Screenshot showing your verification of the image integrity (5 marks)

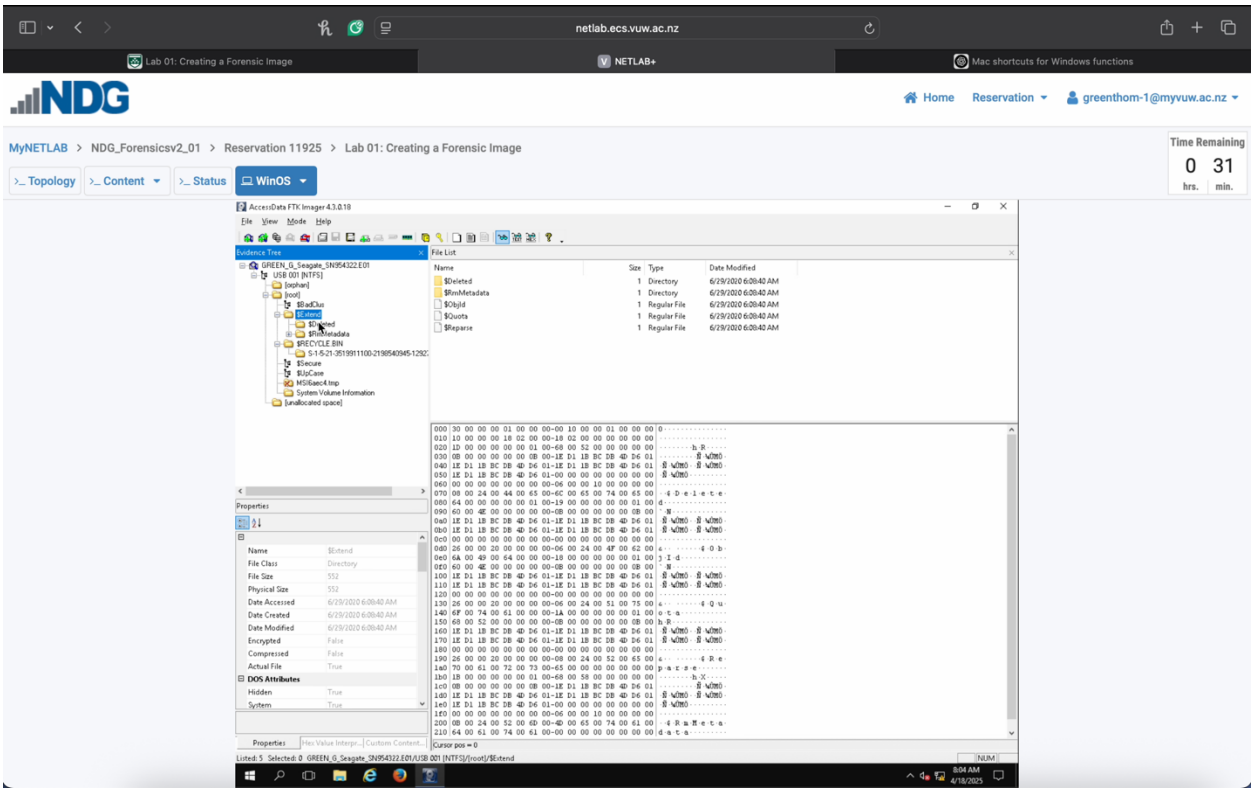


5) Screenshots of the FTK Imager's image report with the following information (10 marks)

- **Case number**
- **Evidence description**
- **Acquisition date/time**
- **Image format selected**
- **Hash values (MD5 and SHA1)**



6) A screenshot showing you've successfully mounted the image and can view its contents (5 marks)



1.3. Forensic Imaging Knowledge Check (40 marks)

Answer the following questions:

7) Explain the purpose of hashing in the forensic imaging process. Why are two different hash algorithms often used? (5 marks)

Hashing in forensic imaging is used to ensure the integrity and authenticity of the data being captured. When an image is created a hash value is generated based on the original data. After the image is made, the same hashing algorithm is run again on the image file, and if the two hash values match it proves that no data was altered during the imaging process.

The two different hash algorithms, MD5 and SHA1, are often used to provide redundancy and stronger verification. Using two algorithms helps mitigate the risk of hash collisions and increases the court admissibility of evidence by demonstrating through validation using independently trusted algorithms.

8) Identify four key pieces of information that should be found in a forensic image report and explain why each is important. (8 marks)

1. Case and Evidence Metadata ("Case Number: FOR_LAB_001, Evidence Number: E01A"): This information links the image to a specific investigation and helps maintain proper documentation and chain-of-custody. It ensures traceability and accountability in court.
2. Hash Values (MD5 and SHA1): These hashes are used to verify the integrity of the image. Matching pre- and post- acquisition hashes confirm that the data has not been altered, which is essential for admissibility in court.
3. Device Information (Removable Drive: False, Sector Count: 2,097,152, Size: 1024 MB): Provides technical details about the source device. Knowing the size, type, and layout of the disk helps verify that the full scope of evidence was captured and that no data was missed.
4. Acquisition and Verification Timestamps (Acquisition started: Fri Apr 18 07:57.38 2025): Timestamps document when the imaging took place and help establish a timeline. This can be critical for corroborating evidence and confirming that imaging occurred before any possible tampering.

9) Describe four specific steps necessary to maintain chain of custody when creating a forensic image and why these steps are necessary. (2 marks per step and explanation, 8 marks)

1. Record every action performed during imaging, including date, time, tools used (e.g. FTK Imager), and responsible person. This provides an audit trail showing the evidence was handled correctly and helps prove its authenticity in legal proceedings.
2. Utilize a hardware or software write-blocker when imaging the original media to prevent any modification. Ensures the original evidence remains untouched, preserving its integrity and making the image legally admissible.
3. Label physical media and image files clearly (e.g. case number, examiner, date) and store them securely. Prevents misidentification or unauthorized access, reducing the risk of contamination or tampering.
4. Calculate MD5 and SHA1 hash values before and after imaging and include them in the documentation. Confirms that the forensic image is an exact replica of the original, verifying integrity and protecting against accusations of evidence tampering.

10) Describe three key differences between physical and logical acquisition methods. (9 marks)

Review the image verification report provided below:

```
Image Information:
Acquisition started:  Mon Mar 11 09:15:22 2025
Acquisition finished: Mon Mar 11 09:37:14 2025
Image hash values:
MD5:    a8b42f651c97e3a8d9b2c710f24d3a12
SHA1:   6f87120d942480176bb6452cd9281e173cd

Image Verification Results:
Verification started:  Mon Mar 11 09:37:15 2025
Verification finished: Mon Mar 11 09:42:36 2025
MD5:    a8b42f651c97e3a8d9b2c710f24d3a12 : verified
SHA1:   6f87120d942480176bb6452cd9281e173cf : NOT VERIFIED
Bad Blocks List:
Bad block(s) in image: sectors 1052-1078
```

1. Physical acquisition captures the entire storage device, including active files, deleted files, slack space, unallocated space, and file system metadata. Logical acquisition captures only active files and folders that are visible to the operating system. Physical imaging is more thorough and allows recovery of deleted or hidden data, making it preferred for full forensic analysis.
2. Physical acquisition works independently of the file system as it copies all raw sectors from the disk regardless of format. Logical acquisition is dependent on the file system structure and mounts it to access files. If the file system is corrupted or intentionally manipulated, logical imaging might fail or miss data.
3. Physical acquisition takes longer and consumes more storage space since it includes everything on the disk. Logical acquisition is faster and more storage-efficient, since only selected files/folder are imaged. Logical imaging is sometimes the only option when time or storage resources are limited, or when you only need specific files.

11) Identify all issues present in this report. (4 marks)

1. The SHA1 hash result is marked as “NOT VERIFIED” indicating a possible mismatch between the original and verification hash values
2. The report lists bad blocks in sectors 1052-1078, which indicates physical damage or read errors during acquisition.
3. Because of the unverified SHA1 and bad sectors, the image may be incomplete or corrupted.
4. The MD5 hash is verified while the SHA1 is not, leading to an inconsistency in integrity checks.

12) Explain the potential causes of these issues. (4 marks)

1. This could be due to data corruption during acquisition or write errors when creating the image. It may also be from bad sectors affecting how data is interpreted for hashing.
2. These sectors may be physically damaged on the source drive, leading to incomplete reads or substituted data in the image.
3. A failing hard drive or unstable imaging hardware (e.g. faulty cable, overheating) could introduce errors.
4. FTK Imager or the system it runs on might have encountered a bug or memory fault during hashing or image writing.

13) Determine if this image would be admissible as evidence. Justify your answer. (2 marks)

No, the image would likely not be admissible in court without further validation. The SHA1 hash failed to verify, and bad blocks were detected, which raises questions about the image's integrity. In legal contexts, both hashes are expected to verify, and any data less must be explained and accounted for. Additional steps (e.g. re-imaging, testimony) would be needed to justify its use as evidence.