ITMS 538 Assignment 03a_s

Alan Palayil

Due Date: 09/26/2022

      In this lab, we are presented on how the corrupted file can be checked using WinHex. We use a sample corrupted file called ClownFish to practice how to look over and repair the file. After the practice we use the resources given in Assign03a_s.pdf to start repairing Assign03b_rds and these are the following steps I used to identify and repair the Assign03b_rds.

Step 1: The assignment Assign03b_rds is a corrupted file which we open in WinHex.
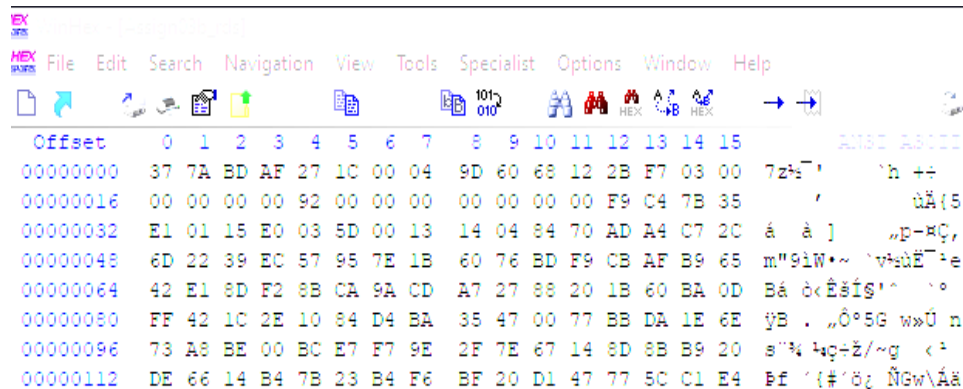

Figure 1: Hexadecimal of original file Assign03_rds

Step 2: As we can see in the ANSI ASCII that 7z is there, we can look up the file signature of 7z on the wikipedia list.

Step 3: We can edit the 3rd offset which appears to be wrong from BD to BC and then save the file as Assign03b_rds-clean.7z
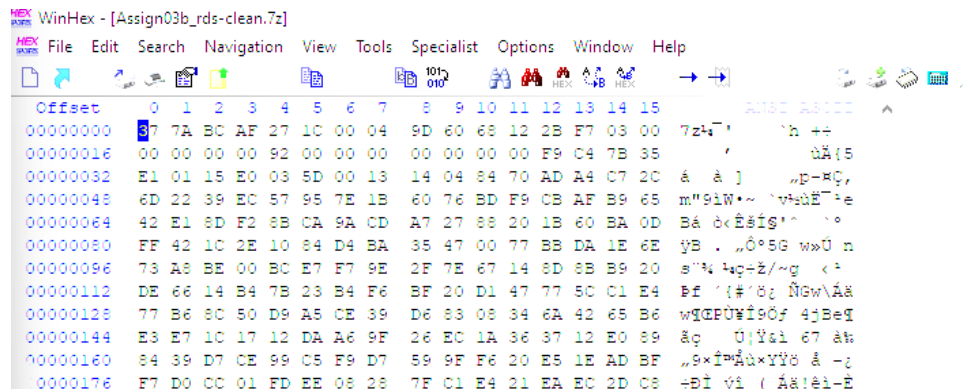

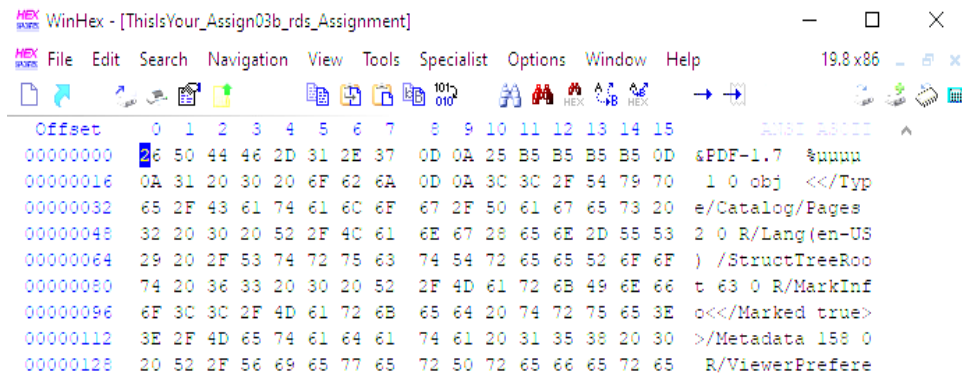Figure 2: Hexadecimal of new file Assign03_rds-clean.7z

Step 4: We can access the file and after opening the .7z file we are shown with the "ThisIsYour_Assign03b_rds_Assignment" which also appears to be corrupted.

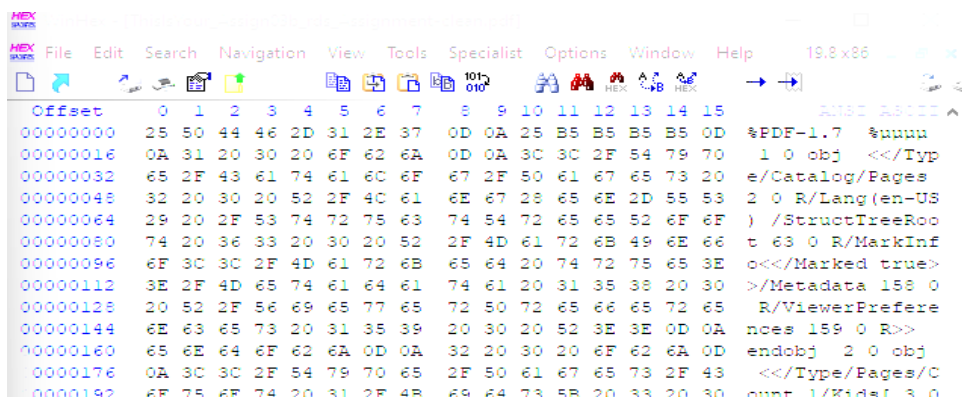Step 5: We open this file in WinHex.

Alan Palayil

Due Date: 09/26/2022

Figure 3: Hexadecimal of original file ThisIsYour_Assign03b_rds_Assignment

Step 6: As we can see in the ANSI ASCII that PDF is there, we can look up the file signature of PDF on the wikipedia list.

25 50 44 46 2D		%PDF-		0	pdf	PDF document[29]

Step 7: We can edit the 0 offset which appears to be wrong from 26 to 25 and then save the file as ThisIsYour_Assign03b_rds_Assignment -clean.pdf

Figure 4: Hexadecimal of new file ThisIsYour_Assign03b_rds_Assignment -clean.pdf

Step 8: Thus, we can access our Assign03b_rds_Assignment-clean.pdf and a screenshot of the assignment is added.

ITMS 538 Assignment 03a_s

Alan Palayil

Due Date: 09/26/2022

Assignment 03b_rds (Reading and Submittal)

Due: Sunday, October 2, 2022 @ 11:59pm (US Central)

Assignment Objectives

- **Submittal:**
  - *Nelson* text: Submit answers to Review Questions 1-10 from Chapter 1
  - Submit answers to the Special Problems (see below)
  - *Nelson* text: Submit answers to the following Review Questions from Chapter 2:
    - 4, 5, 8, 9, 11, 13, 14, 15, 17

Special Problems

SP01.1

1. Define *Carrier's* 3 phases of a digital crime scene investigation.
2. For a hard disk, what are *Carrier's* 4 phases of analysis?
3. Discuss how your responses to (1) and (2) above compare with the *Nelson* text.

SP01.2

For a country other than the United States, identify the part of that country's constitution or laws that are as close to the U.S. Constitution's 4th amendment.

If you are originally from a country other than the U.S., use your country of origin's constitution or laws.

Write a description of the above that includes:

- An identification of the part of the constitution or laws
- A direct, relevant quotation in English of the constitution or laws.

You must not use the examples given in the *Nelson* text or in my lecture slides.

Submittal Instructions

- Submit ALL parts of Assign03b_rds as a single submission with clearly marked and separated parts.
- Submit as a single compressed archive in PDF format.
- Observe the homework guidelines provided during the Class 01 lecture.
- Recall that this must be submitted by the due date (Sunday, 2 October, US Central).

No late submissions will be accepted

September 14, 2022   D. Nelson © 2022   Page | 1
                           Illinois Tech

Figure 5: Assign03b_rds_Assignment-clean.pdf