# MICT1 – Exercise Week 6

Exercise for week 6:

1. Investigate the provided file 'file6' and recover the message hidden

somewhere inside it

2. See if you can find some usable files that could have been in either RAM-

and/or Disk-slack.

3. Make a small report describing:

- What you found

- Where you found it (locations, spans, etc.)

- How you found it. What tools? Include source, screenshots, howto's, etc.

Put the report in the /exercises/week6/yourgroupname directory in the repo

and send it in as a Pull Request on Github.

Good luck!

# What we found

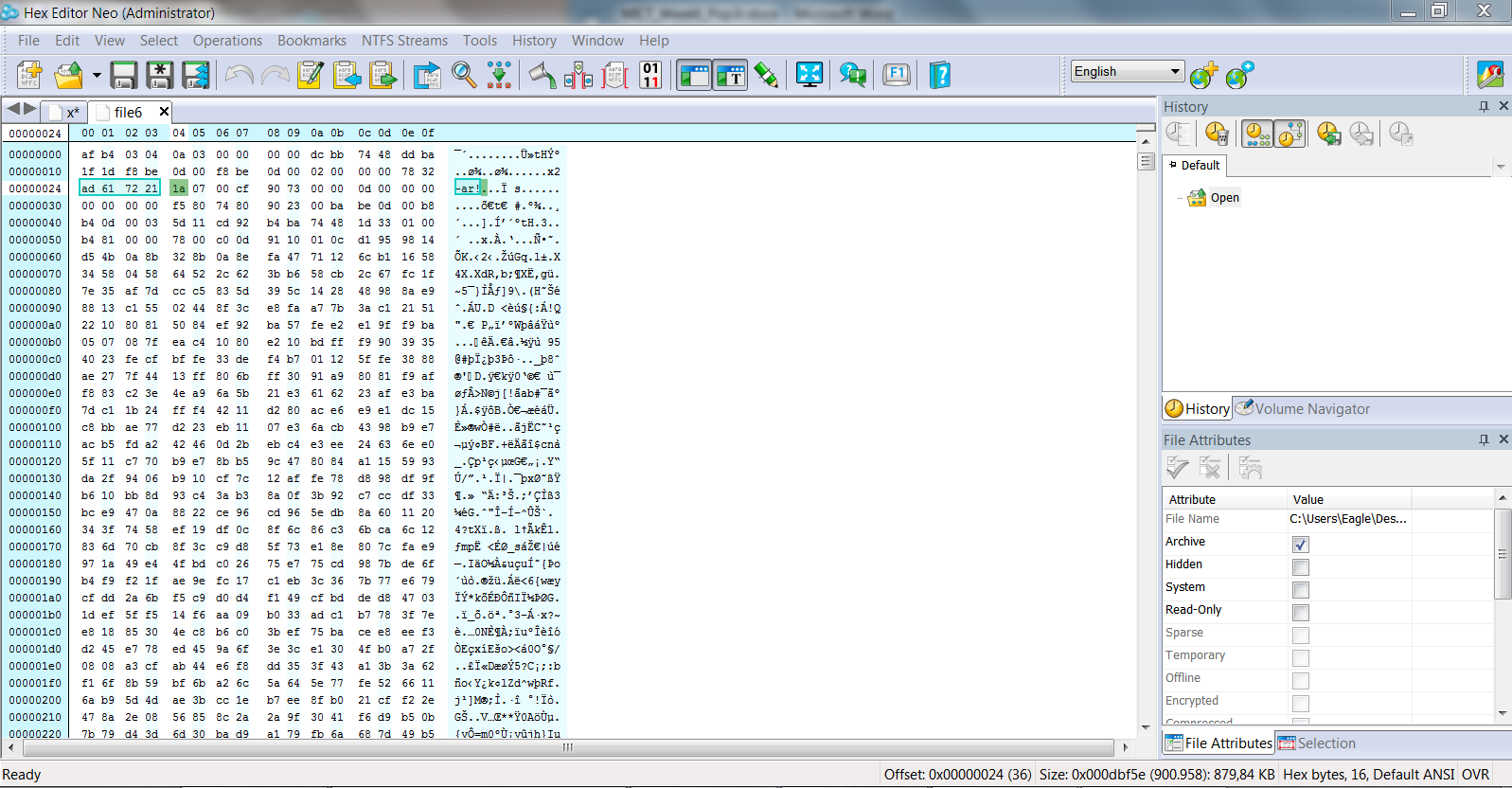
Het file6 bestand is als eerst geanalyseerd d.m.v. foremost en Digital Forensics Framework. Deze tools analyseren file6 op bekende data structuren en headers van afbeeldingen, containers (rar,zip), documenten en andere media. Deze tool heeft 8 bmp files gevonden op basis van header informatie, echter zijn deze files corrupted of incompleet. De data gevonden met deze tools waren voor het onderzoek niet interessant of concluderend. De files hebben de volgende offsets:

|  |  |
| --- | --- |
| Begin | Eind |
| 0x4cba7 | 0x65247 |
| 0x28a72 | 0x41112 |
| 0x358f5 | 0x4df95 |
| 0x720ae | 0x8a74e |
| 0x954cf | 0xadb6f |
| 0x1661c | 0x2ecbc |
| 0x7440f | 0x8caaf |
| 0xb6244 | 0xce8e4 |

We hebben file6 geopend in HexEditor Neo. Na het openen van deze file viel het op dat er geen bekende header in stond, maar wel “-ar!” (0x00000020-0x00000023). Vervolgens hebben we op internet naar bekende headers gezocht en vonden we de header “Rar!”.

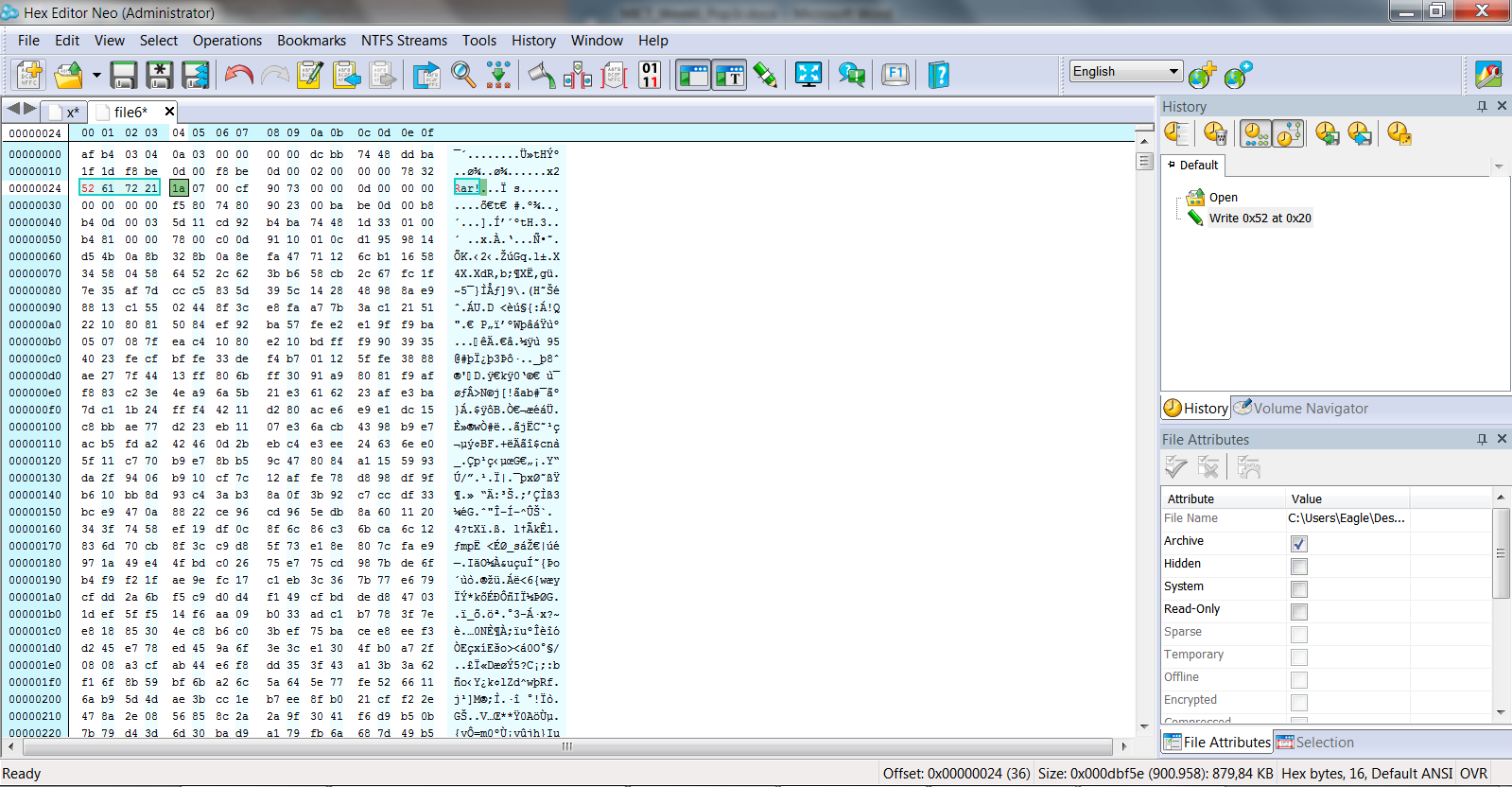
“-ar!” is in hex:

AD 61 72 21

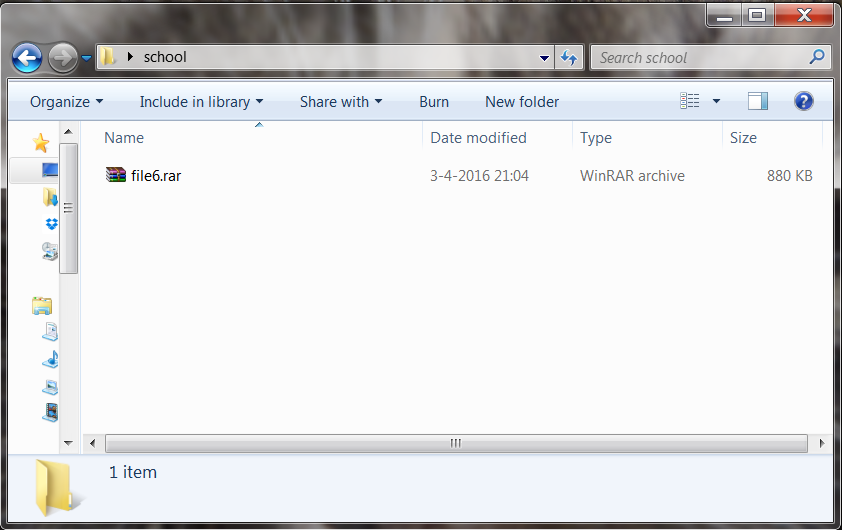


“Rar!” is in hex:

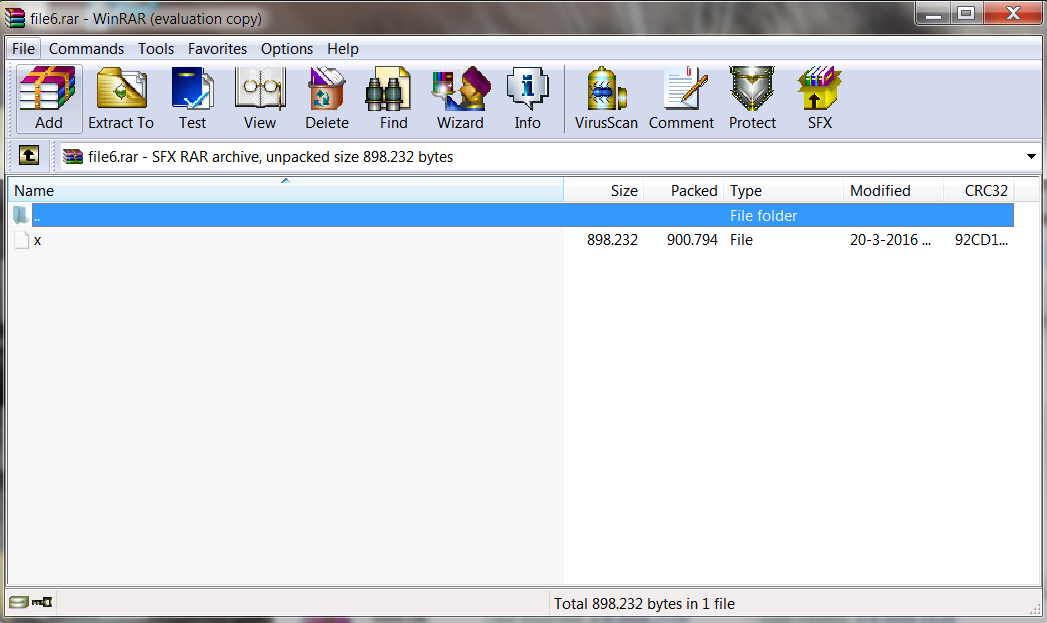
52 61 72 21



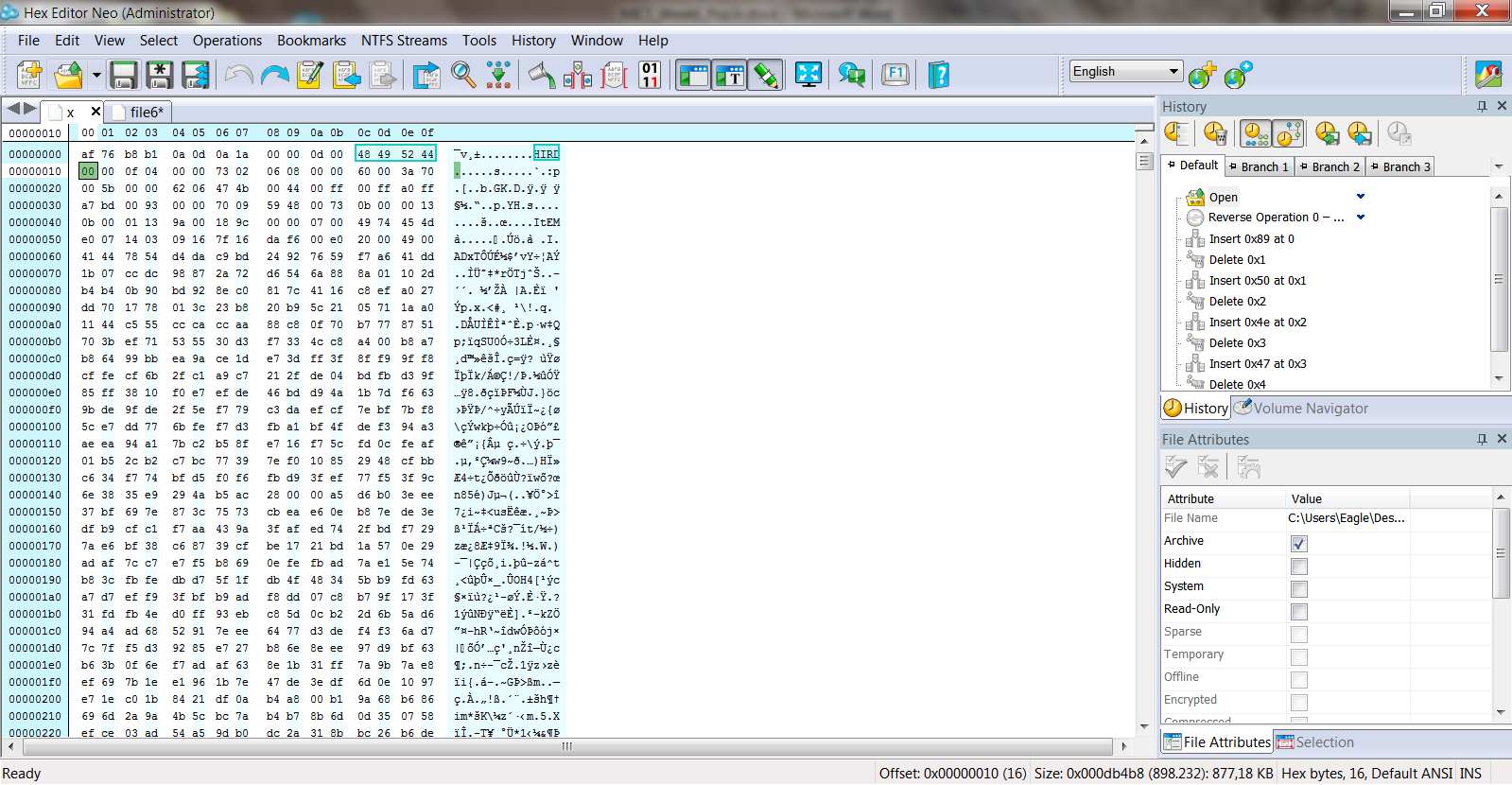
Vervolgens hebben we “AD” veranderd in “52” en het bestand opgeslagen als “file6.rar”. Dit is een non-corrupted bestand geworden wat we konden openen met Winrar.



De .rar bevat de file “x”.

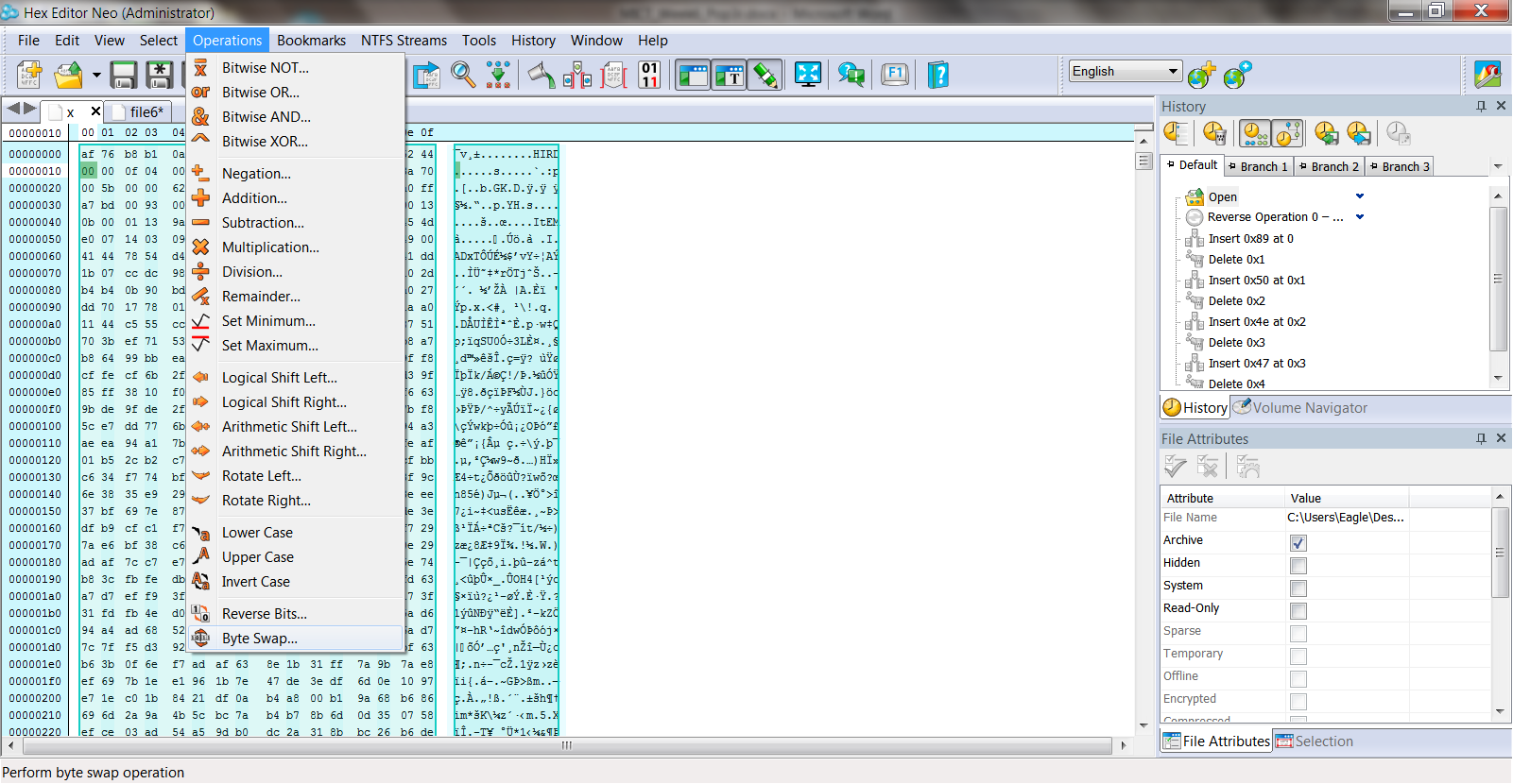


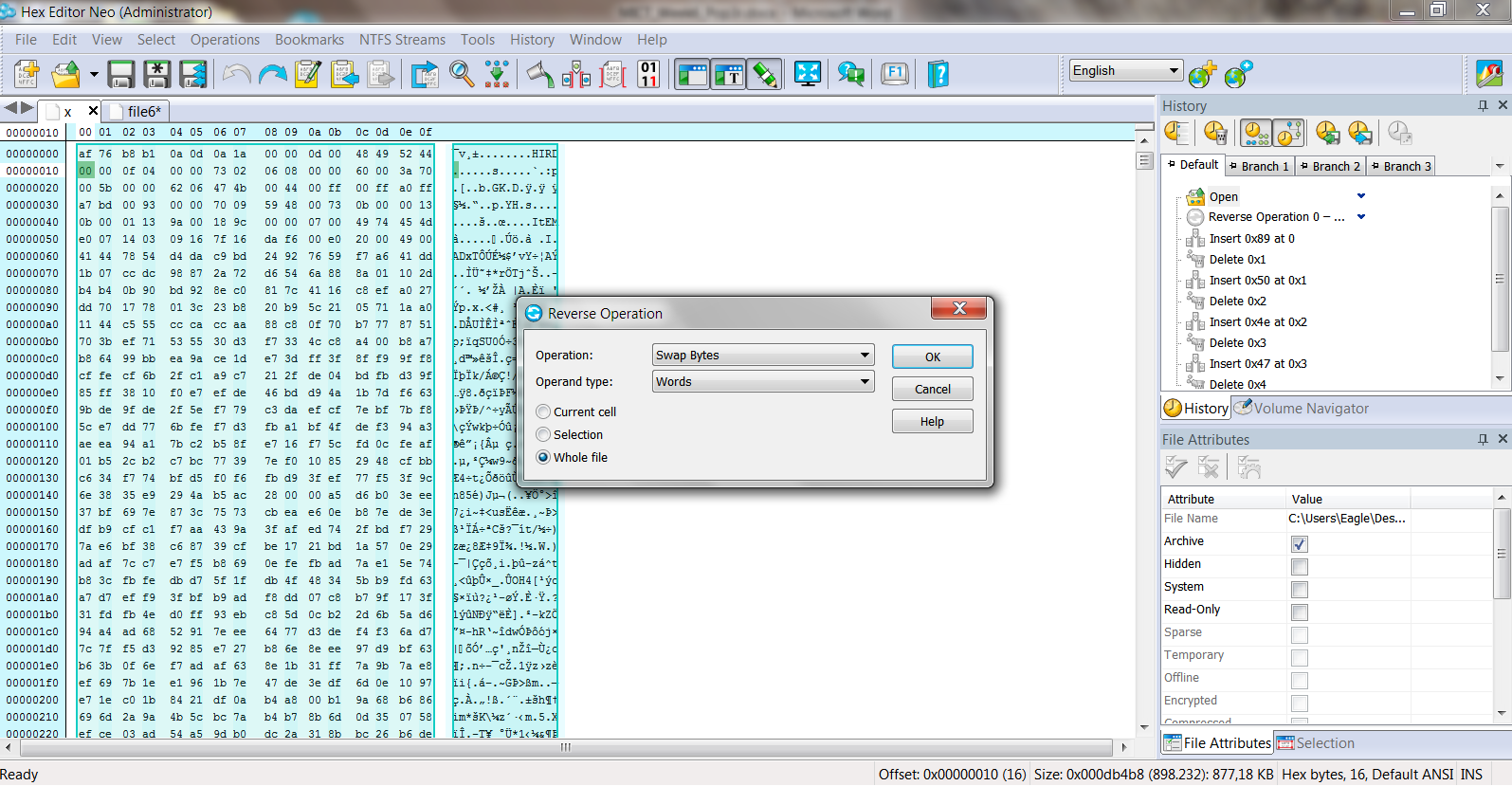
Bestand “x” hebben we wederom geopend in HexEditor Neo.



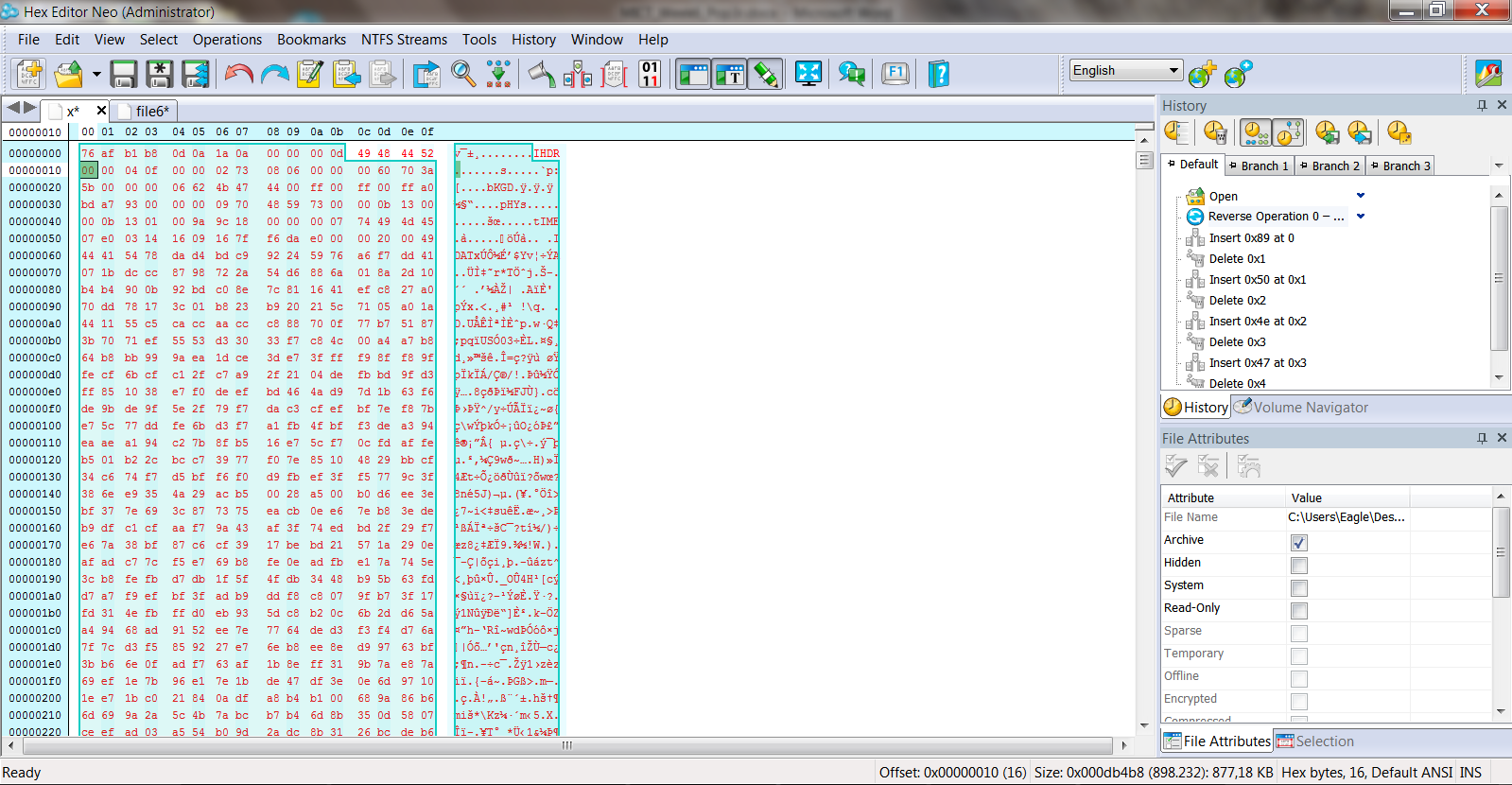
Hier viel op dat de file geen header bevatte, maar wel “HIRD”, “pYH” en “ItEM”. Vanuit eerdere opdrachten hebben we geleerd dat “HIRD” geen correcte header is, maar “IHDR” wel. Na het opzoeken van deze header, vonden we dat dit onderdeel is van een .PNG bestand.

Om de header van “HIRD” naar “IHDR” te krijgen, moeten in groepjes van twee, iedere tweede bit met iedere eerste bit verwisseld worden. Om dit voor elkaar te krijgen hebben we gebruik gemaakt van de “Byte Swap” functie binnen HexEditor Neo. Deze is te openen via Operations > Byte Swap.





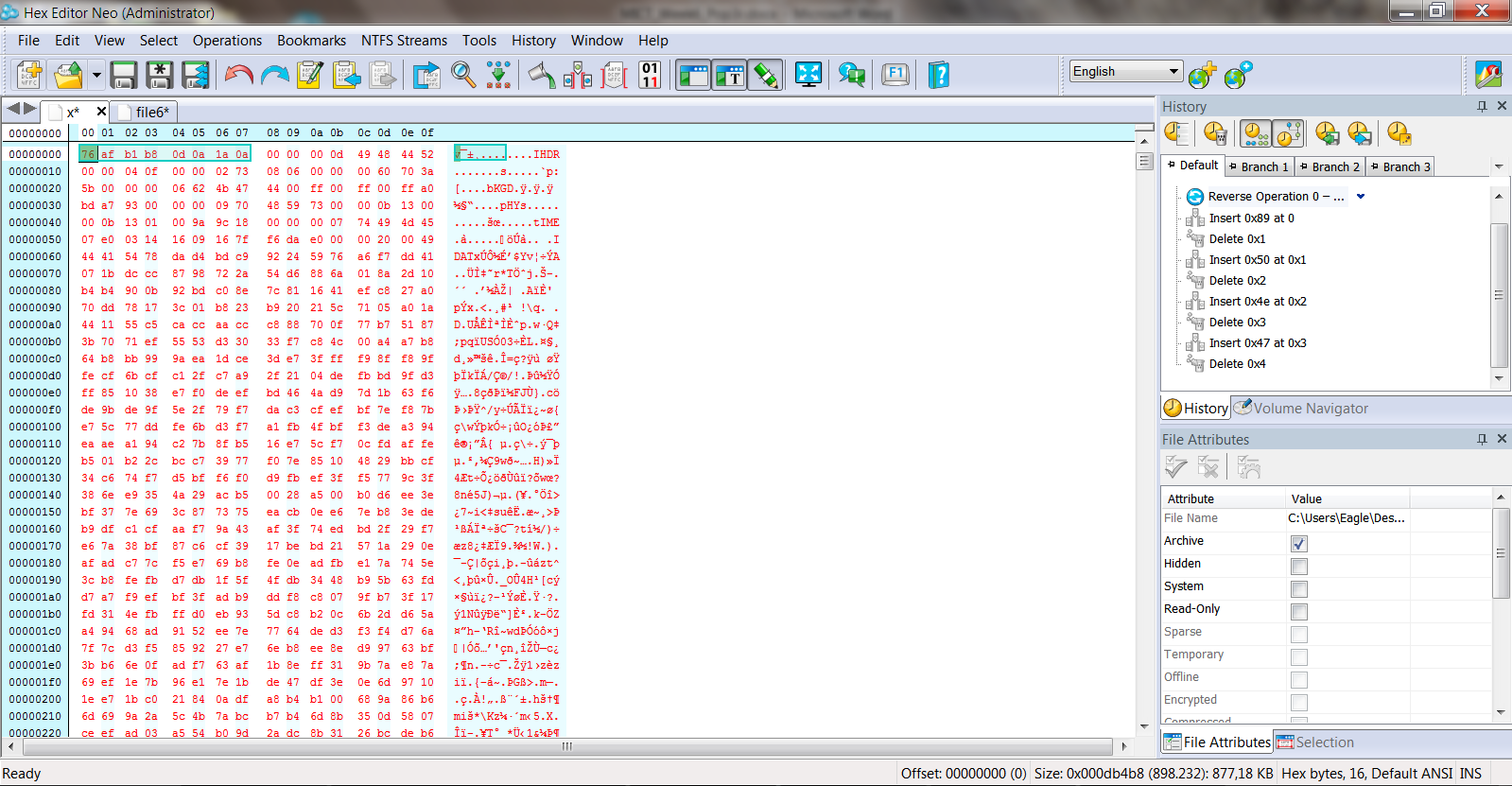
De “byte swap” hebben we uitgevoerd over de gehele file, waarna de headers zichtbaar waren als “IHDR”, “pHY” en “tIME”.

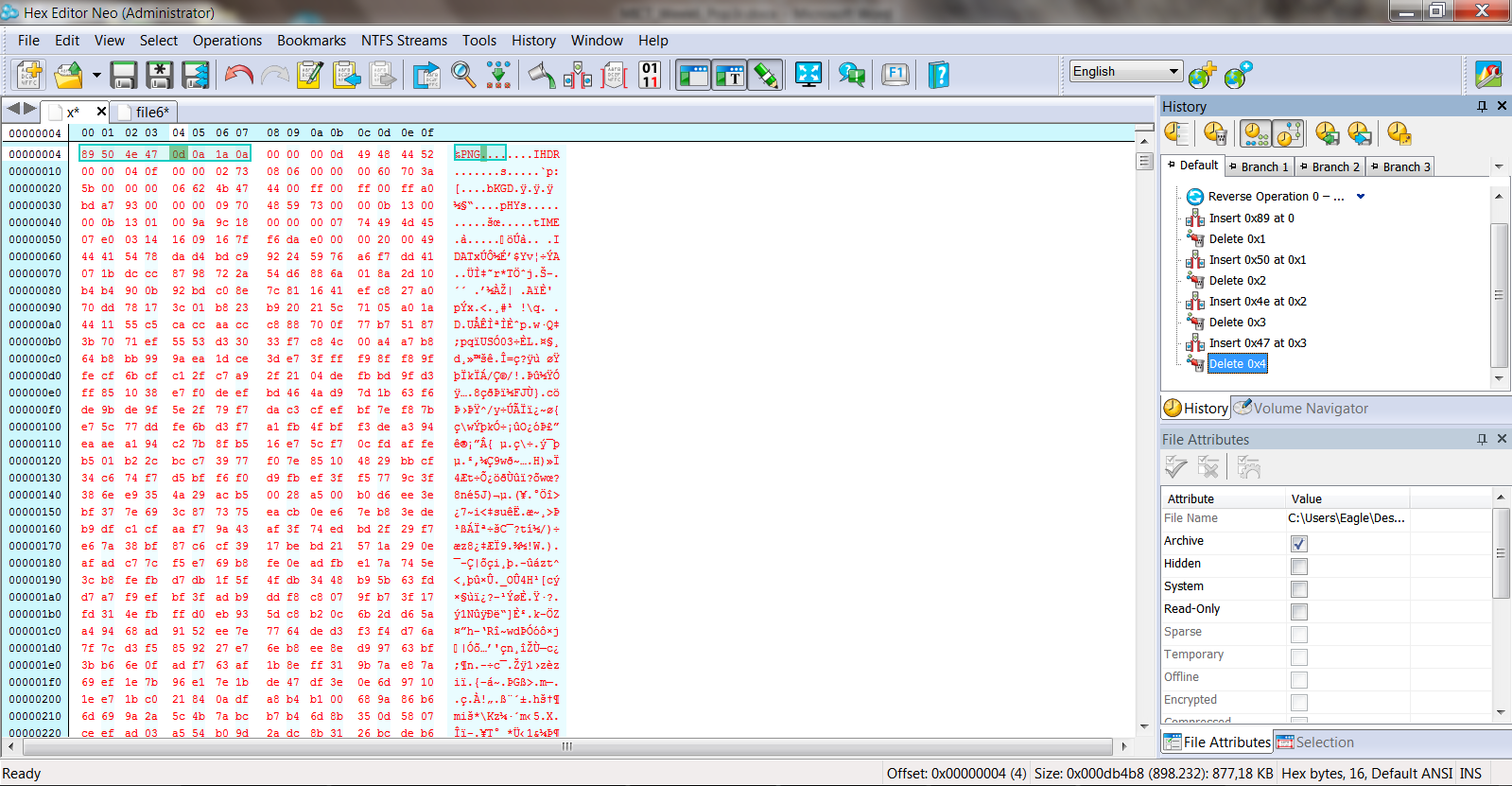


Na het uitvoeren van deze functie hebben we het bestand opgeslagen als x.png en geprobeerd te openen. Hierbij kregen we de melding dat het bestand corrupted was en niet geopend kon worden.

Vervolgens x.png geopend in HexEditor Neo en nogmaals de header bestudeerd. Hier stond in plaintext geen “png”. Na het opzoeken van de PNG specificaties hebben we de volgende hex-values aangepast naar de juiste waarden van de png header:

“76 af b1 b8 0d 0a 1a 0a” naar “89 50 4e 47 0d 0a 1a 0a”.





Vervolgens het bestand opgeslagen als “x2.png”.

Dit bestand konden we vervolgens wel openen en hierin vonden we het verborgen bericht:

“It’s true. All of it.”



Vervolgens hebben we file6 gecarved met foremost om overige bestanden uit file6 te halen. Deze tool heeft 8 bmp files gevonden op basis van header informatie, echter zijn deze files corrupted of incomplete. De files hebben de volgende offsets:

# Tools

HHD Software Hex Editor Neo (Adminsitrator) (x64 edition) Ultimate Edition. Version 6.10.02.5330

<http://www.hhdsoftware.com/Downloads>

Foremost en Digital Forensics Framework, beide tools zijn beschikbaar in het Kali linux distributie.

<https://www.kali.org/>

# Bronnen

<http://www.forensicswiki.org/wiki/RAR>

<http://www.libpng.org/pub/png/spec/1.2/PNG-Structure.html>

<https://en.wikipedia.org/wiki/Hexadecimal>

<http://www.scadacore.com/field-applications/programming-calculators/online-hex-converter/>

<http://www.garykessler.net/library/file_sigs.html>