# Week 3



## Opdracht

|  |
| --- |
| De opdracht gegeven van week 3 gegeven door dhr. J. van den Bos is te vinden op GitHub.  *Exercise for week 3:*  *1. Investigate the provided files 'f\_z.data' and 'e\_r.data'.*  *2. Extract and organize (part of) the provided data so that they can be interpreted as valid media files.*  *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/week3/yourgroupname directory in the repo and*  *send it in as a Pull Request on Github.* |

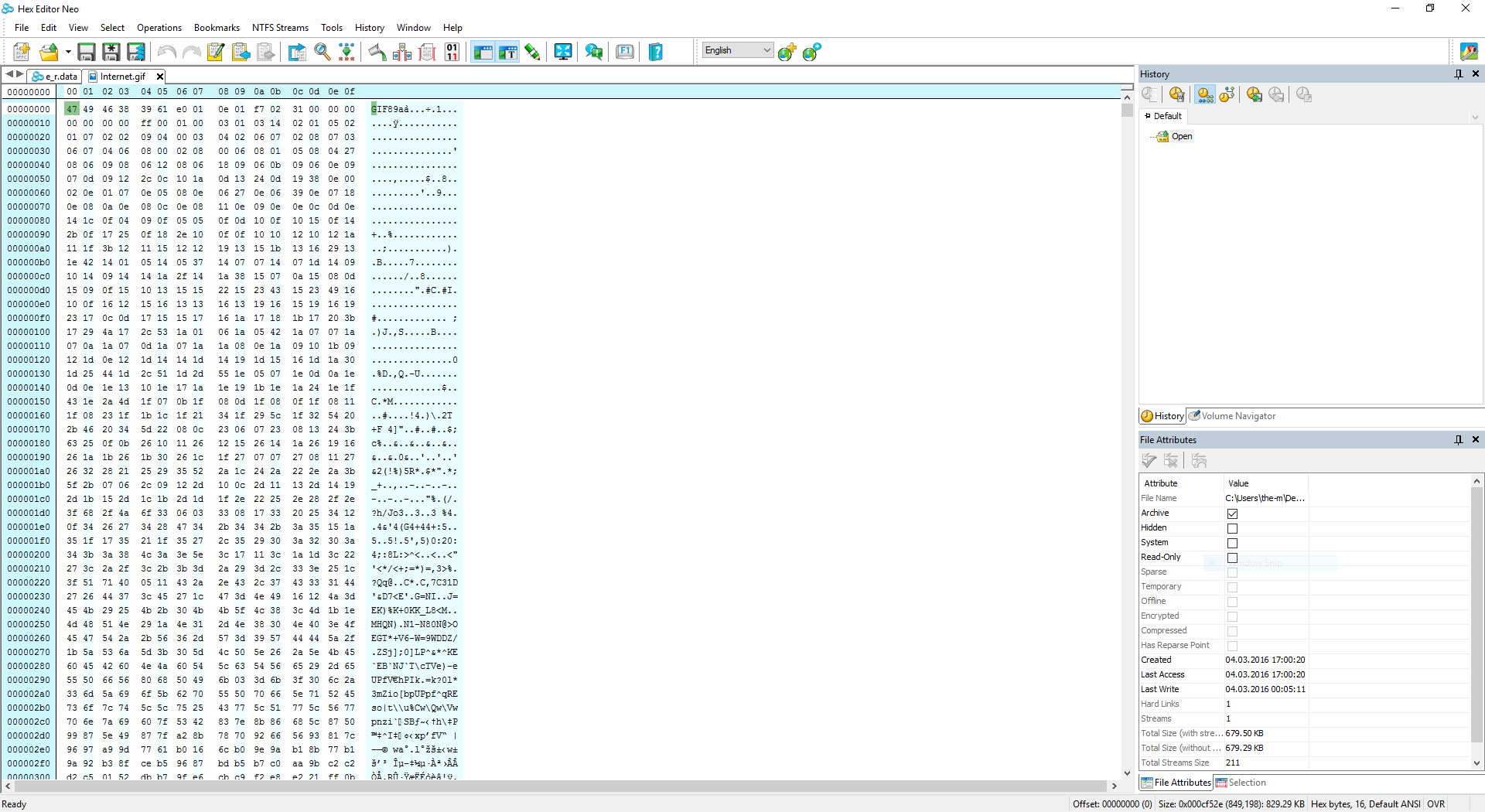
Bron:

https://github.com/pop3r/MICT1/blob/master/exercises/week3/week3.exercises

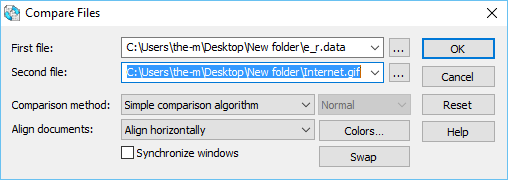
## Uitwerking

### E\_R.data

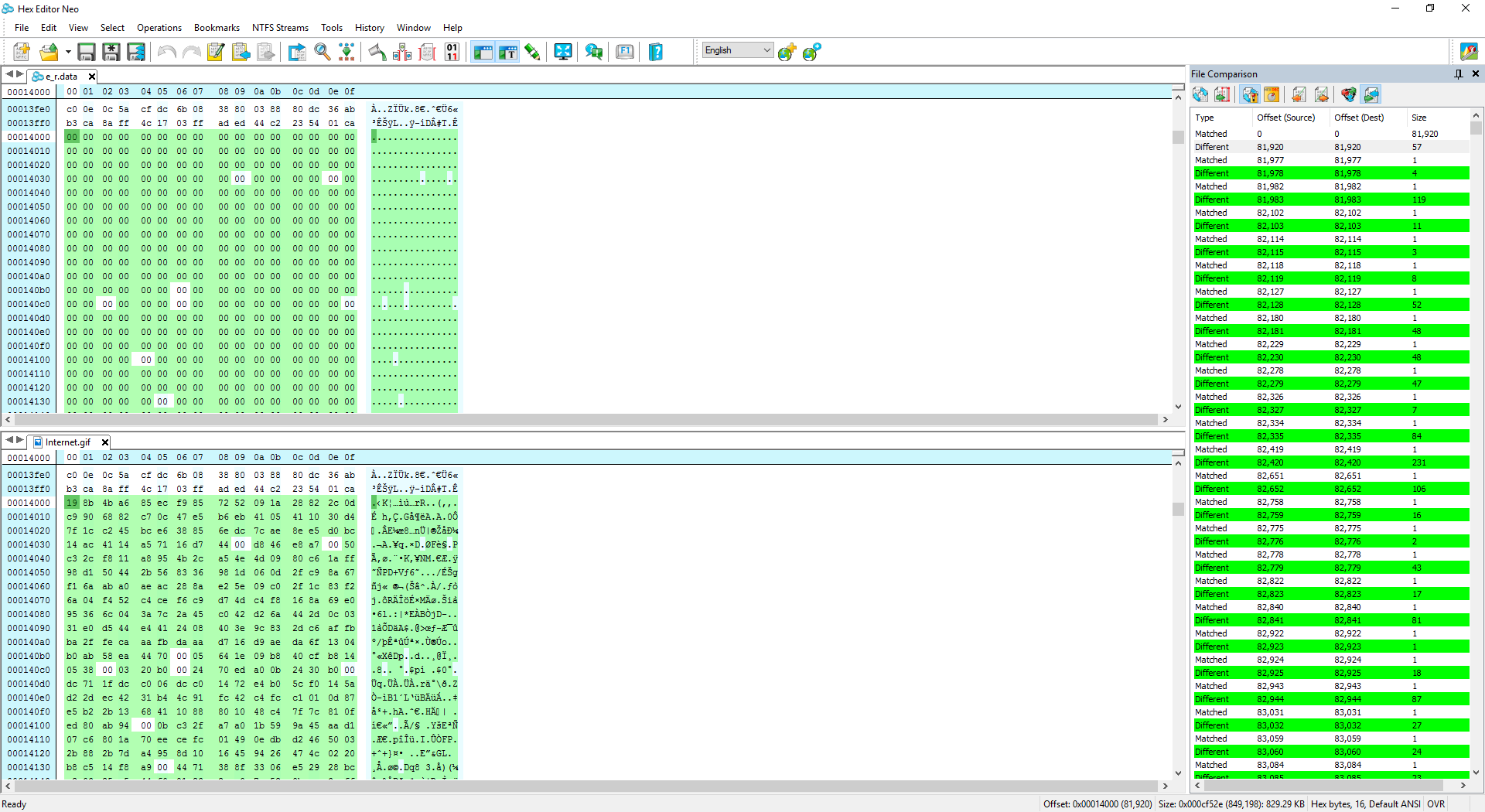
Beide bestanden geopend in Neo HexEditor.



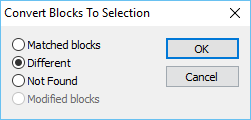
Via Tools > File comparison



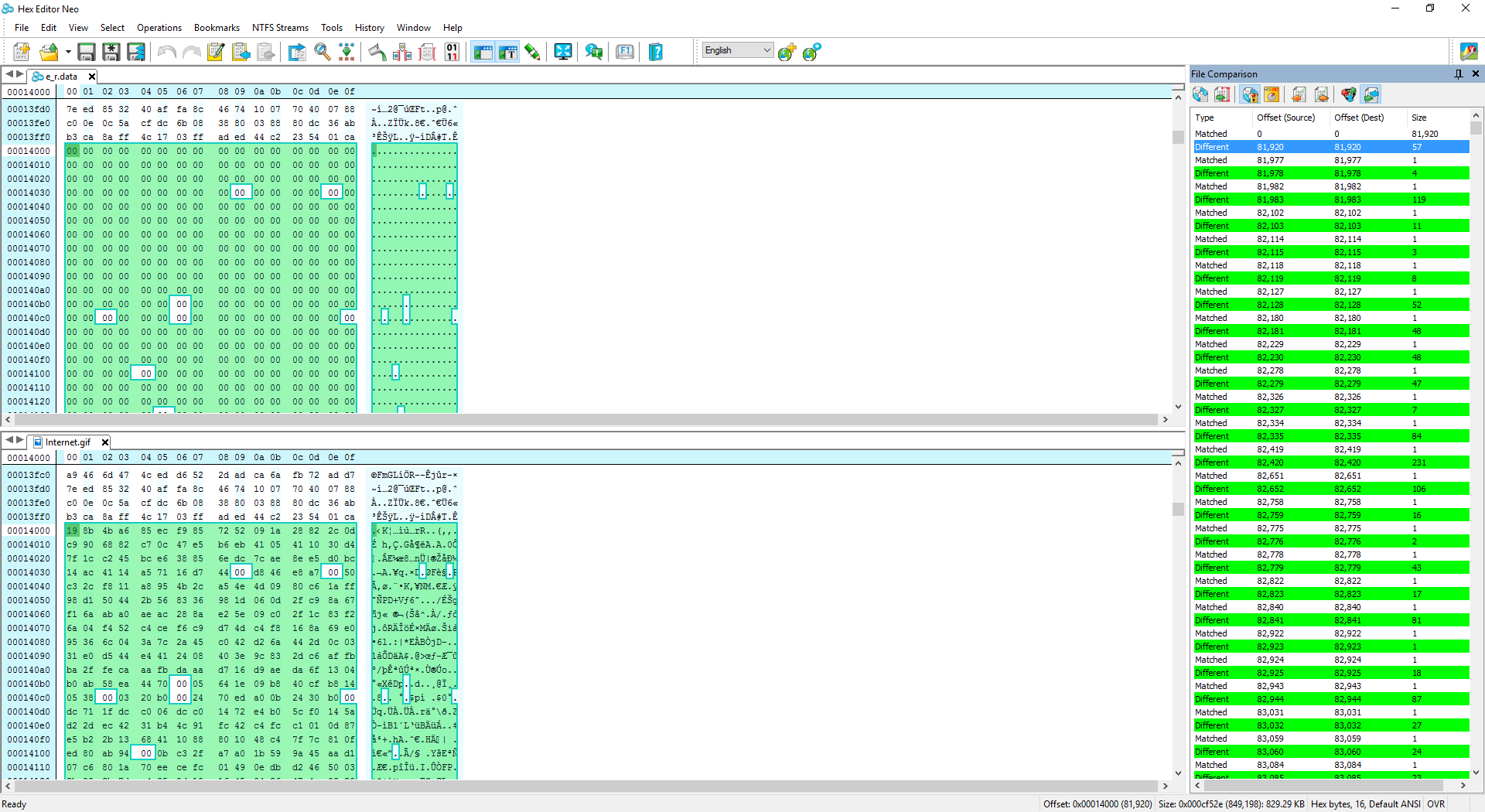
Links het eerste groene different block geselecteerd. Dit vergelijkt alle whitespace (corrupte/verwijderde data) in e\_r.data met de data in internet.gif



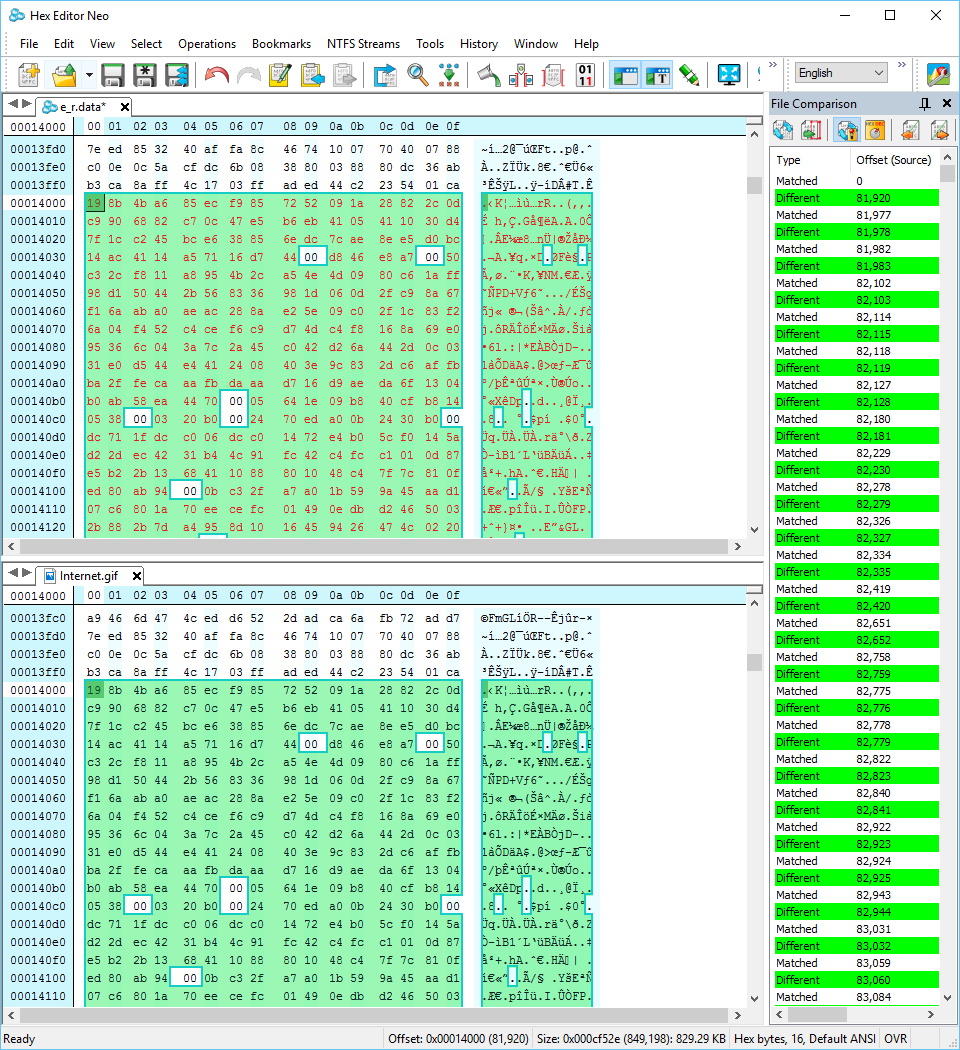
Vervolgens convert blocks to selection gekozen.



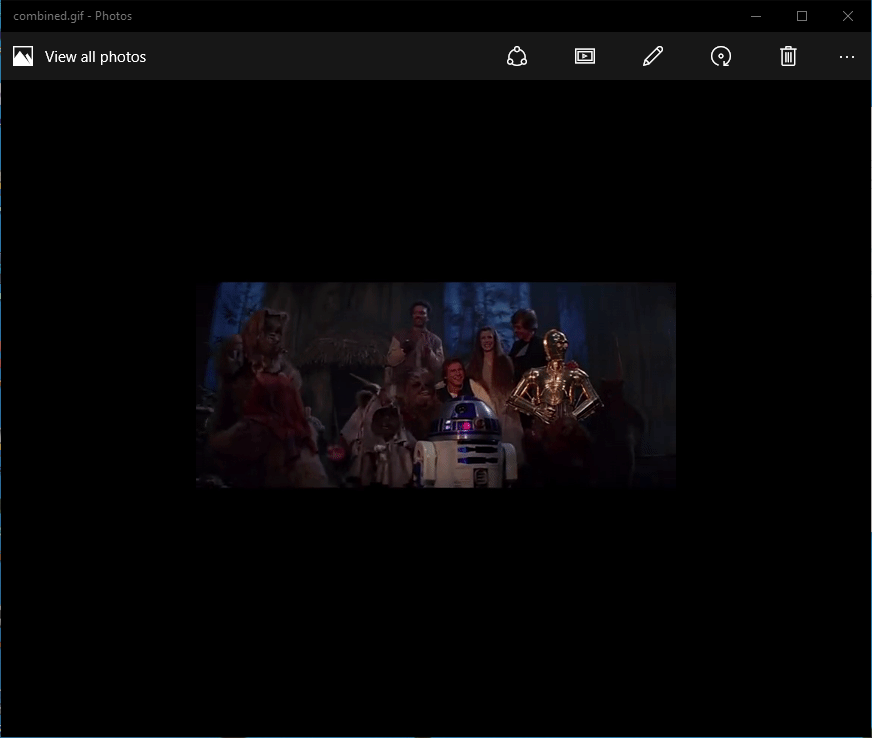
Resultaat hiervan is dat alle whitespace wordt geselecteerd.



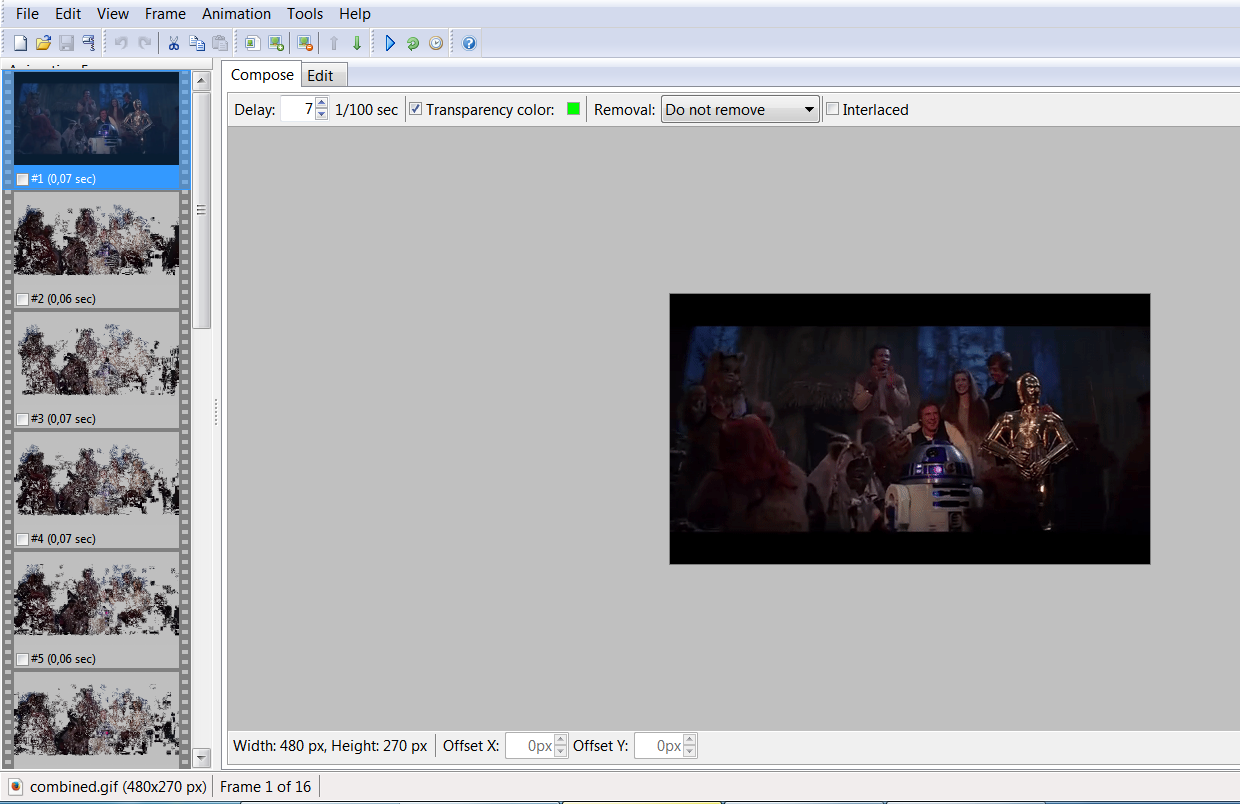
Vervolgens data van internet.gif naar e\_r.data gekopieerd.



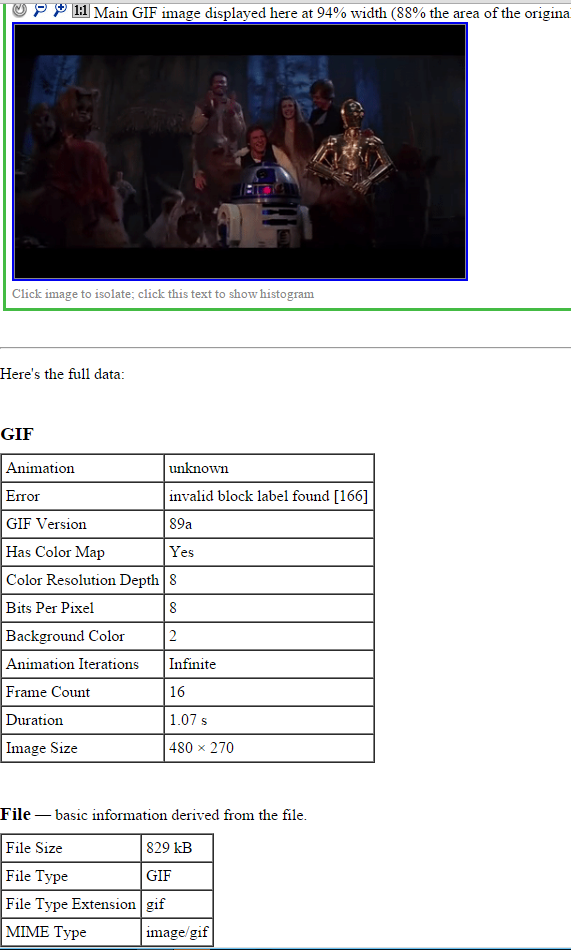
Vervolgens het bestand opgeslagen als combined.gif.



Met de tool Gif Animator is het mogelijk elke frame van een gif gesplitst weer te geven. In Gif Animator is te zien dat combined.gif bestaat uit 16 frames.



De website Jeffrey's Exif Viewer brengt fouten van afbeeldingen in kaart. Combined.gif is geaudit d.m.v. Jeffrey's Exif Viewer, deze rapporteerde een error in het bestand. Een screenshot met informatie van de audit is hieronder weergegeven.



### F\_Z.data

F\_Z.data is d.m.v. een andere methode onderzocht. Voor dit onderzoek is gebruik gemaakt van de tool Foremost op GNU/Linux.

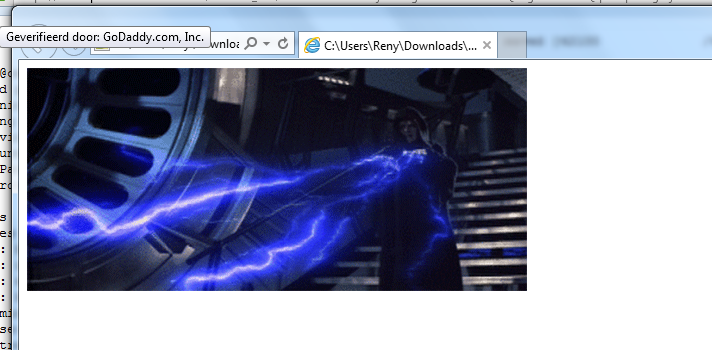
De commando’s uitgevoerd en de output gegenereerd op dit systeem is hieronder gedocumenteerd.

|  |
| --- |
| [root@centos-7-x64 usr]# cd MICT1/  [root@centos-7-x64 MICT1]# ls  e\_r.data f\_z.data  [root@centos-7-x64 MICT1]# foremost -h  foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus.  $ foremost [-v|-V|-h|-T|-Q|-q|-a|-w-d] [-t <type>] [-s <blocks>] [-k <size>]  [-b <size>] [-c <file>] [-o <dir>] [-i <file]  -V - display copyright information and exit  -t - specify file type. (-t jpeg,pdf ...)  -d - turn on indirect block detection (for UNIX file-systems)  -i - specify input file (default is stdin)  -a - Write all headers, perform no error detection (corrupted files)  -w - Only write the audit file, do not write any detected files to the disk  -o - set output directory (defaults to output)  -c - set configuration file to use (defaults to foremost.conf)  -q - enables quick mode. Search are performed on 512 byte boundaries.  -Q - enables quiet mode. Suppress output messages.  -v - verbose mode. Logs all messages to screen  [root@centos-7-x64 MICT1]# foremost -v -t all -o outputMICT -i e\_r.data  foremost: /usr/local/etc/foremost.conf: No such file or directory  Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus  Audit File  Foremost started at Tue Mar 1 14:50:23 2016  Invocation: foremost -v -t all -o outputMICT -i e\_r.data  Output directory: /usr/MICT1/outputMICT  Configuration file: /usr/local/etc/foremost.conf  Processing: e\_r.data  |------------------------------------------------------------------  File: e\_r.data  Start: Tue Mar 1 14:50:23 2016  Length: 829 KB (849198 bytes)  Num Name (bs=512) Size File Offset Comment  0: 00000000.gif 66 KB 0 (480 x 270)  \*|  Finish: Tue Mar 1 14:50:23 2016  1 FILES EXTRACTED  gif:= 1  ------------------------------------------------------------------  Foremost finished at Tue Mar 1 14:50:23 2016  [root@centos-7-x64 MICT1]# foremost -v -t all -o outputMICT -i f\_z.data  foremost: /usr/local/etc/foremost.conf: No such file or directory  ERROR: /usr/MICT1/outputMICT is not empty  Please specify another directory or run with -T.  [root@centos-7-x64 MICT1]# foremost -v -t all -o outputMICT1 -i f\_z.data  foremost: /usr/local/etc/foremost.conf: No such file or directory  Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus  Audit File  Foremost started at Tue Mar 1 14:50:52 2016  Invocation: foremost -v -t all -o outputMICT1 -i f\_z.data  Output directory: /usr/MICT1/outputMICT1  Configuration file: /usr/local/etc/foremost.conf  Processing: f\_z.data  |------------------------------------------------------------------  File: f\_z.data  Start: Tue Mar 1 14:50:52 2016  Length: 920 KB (942433 bytes)  Num Name (bs=512) Size File Offset Comment  0: 00000000.gif 3 KB 0 (500 x 223)  \*|  Finish: Tue Mar 1 14:50:52 2016  1 FILES EXTRACTED  gif:= 1  ------------------------------------------------------------------  Foremost finished at Tue Mar 1 14:50:52 2016  [root@centos-7-x64 MICT1]# |

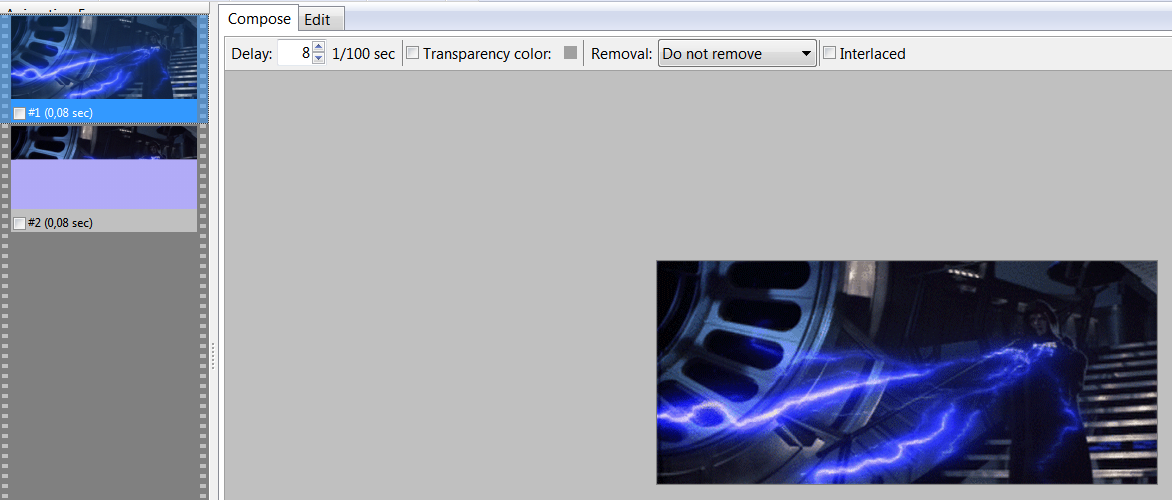
De file carving tool foremost genereerd een audit rapport, de audit.txt is hieronder gedocumenteerd.

|  |
| --- |
| Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus  Audit File  Foremost started at Tue Mar 1 14:50:52 2016  Invocation: foremost -v -t all -o outputMICT1 -i f\_z.data  Output directory: /usr/MICT1/outputMICT1  Configuration file: /usr/local/etc/foremost.conf  ------------------------------------------------------------------  File: f\_z.data  Start: Tue Mar 1 14:50:52 2016  Length: 920 KB (942433 bytes)    Num Name (bs=512) Size File Offset Comment  0: 00000000.gif 3 KB 0 (500 x 223)  Finish: Tue Mar 1 14:50:52 2016  1 FILES EXTRACTED    gif:= 1  ------------------------------------------------------------------  Foremost finished at Tue Mar 1 14:50:52 2016 |

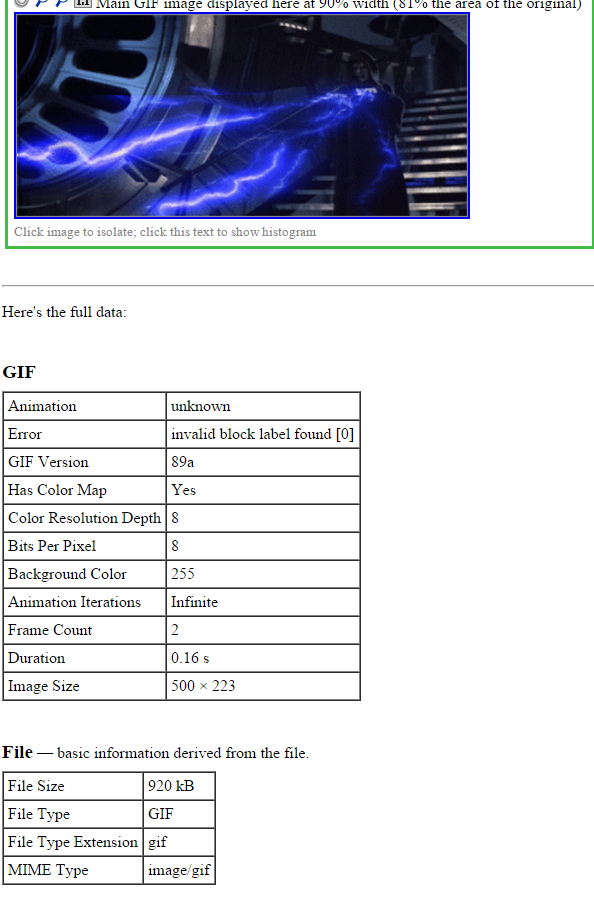
De output gegenereerd door foremost is een corrupted gif bestand van anderhalf frame. De gegenereerde gif is toegevoegd als bijlage. Uit nader onderzoek blijkt dat het gereconstrueerde gif hetzelfde is als f\_z.data te hernoemen naar f\_z.gif. Hieronder is een afbeelding (preview) van gegenereerde gif bestand.



Met de tool Gif Animator is geconcludeerd in de screenshot hieronder weergegeven dat de gereconstrueerde gif uit anderhalf afbeeldingen bestaat.



Ook deze gif is getest door de online webbased afbeelding auditer Jeffrey's Exif Viewer. De screenshot hieronder geeft een error code weer.



### Conclusie exercises week 3

Zowel de uit e\_r.data als de f\_z.data gereconstrueerde gifs zijn niet volledig of zonder fouten. Beide zoek methodes hebben hierin geen verschil kunnen maken in het volledig en foutloos reconstrueren van de gif bestanden. Handmatig zoeken aan de hand van de gif standaard specificaties heeft niets opgeleverd.

De gereconstrueerde gifs misten vele frames, wij vermoeden dat delen van de frames van de gifs wel in de bestanden, e\_r.data en f\_z.data staan. Echter vonden wij ze incompleet of corrupted en waren wij niet succesvol in het reconstrueren van foutloze frames.