# MICT1 – Exercise Week 4

# What we found

Door gebruik te maken van verschillende tools is een Star Wars gerelateerde .jpg gevonden (631KB) (Figure 1, Figure 4). Daarnaast is ook een .gif (37 bytes) en een .png (67 bytes) gevonden van 1 x 1 pixel groot (Figure 2 Figure 3). Vermoedelijk mist data/ is data overschreven waardoor beide files niet volledig zijn.

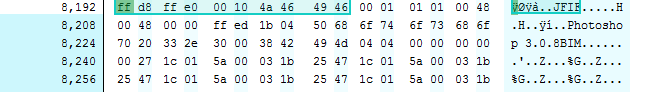


Figure : Star Wars jpg, decimale offset 8192

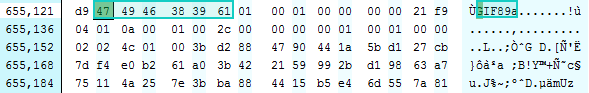


Figure : gif, decimale offset 655,121

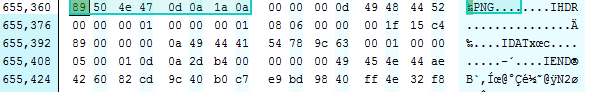


Figure 3: png, decimale offset 655,360

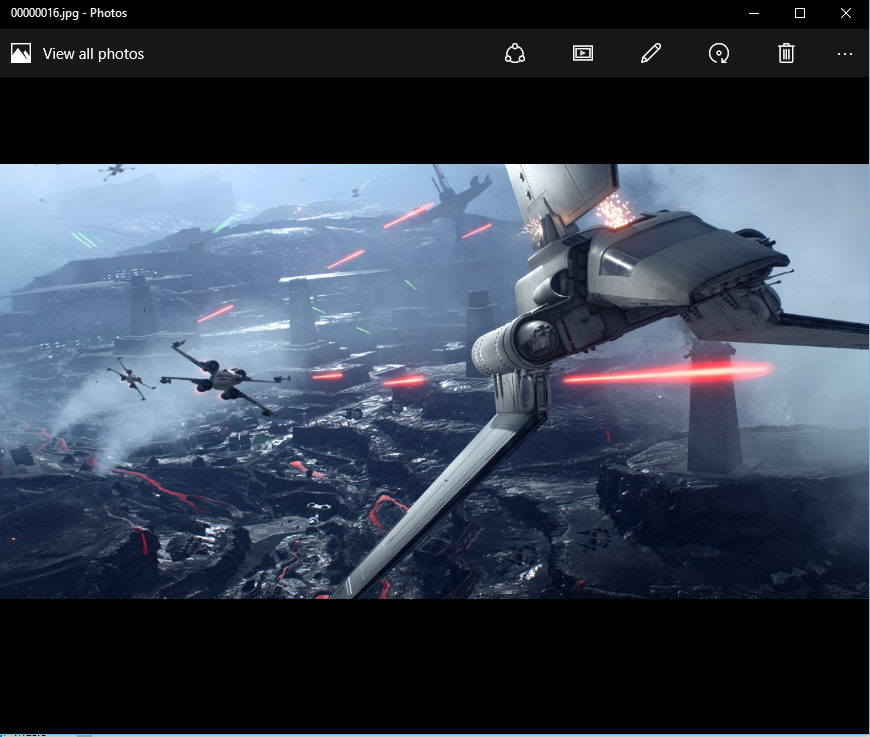


Figure : Star Wars, two T-65 X-Wing Starfighters hunting a Lambda-class T-4a shuttle above Sullust.

Naast de bovenstaande files zijn er ook andere files gevonden (Figure 5). Deze files zijn dermate verknoeit dat deze bestanden niet te openen zijn en vermoedelijk alleen een header bevatten. Dit gaat om de bestanden die hierboven **niet** zijn benoemd (jpg,png,gif).

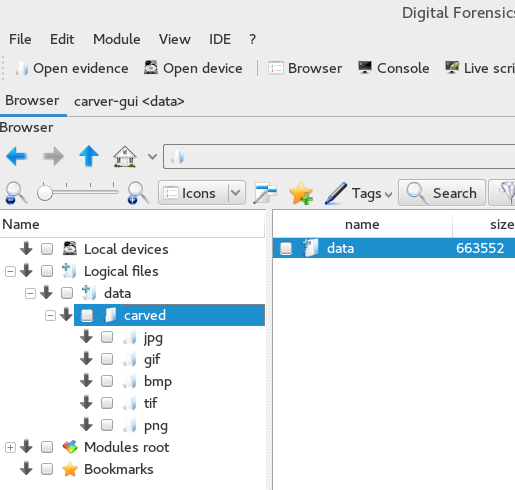


Figure : Resterende bestanden

|  |  |  |  |
| --- | --- | --- | --- |
| Number | Name | Size |  |
| 0: | 00000016.jpg | 631 KB |  |
| 1: | 00001279.gif | 37 B |  |
| 2: | 00000105.bmp | 595 KB |  |
| 3: | 00000351.bmp | 472 KB |  |
| 4: | 00001048.bmp | 123 KB |  |
| 5: | 00001247.bmp | 24 KB |  |
| 6: | 00000007.exe | 644 KB |  |
| 7: | 00000175.exe | 560 KB |  |
| 8: | 00000307.exe | 494 KB |  |
| 9: | 00000394.exe | 450 KB |  |
| 10: | 00000402.exe | 446 KB |  |
| 11: | 00000591.exe | 352 KB |  |
| 12: | 00000609.exe | 343 KB |  |
| 13: | 00000777.exe | 259 KB |  |
| 14: | 00000788.exe | 253 KB |  |
| 15: | 00000796.exe | 249 KB |  |
| 16: | 00000884.exe | 205 KB |  |
| 17: | 00001076.exe | 109 KB |  |
| 18: | 00001086.exe | 104 KB |  |
| 19: | 00001109.exe | 93 KB |  |
| 20: | 00001234.exe | 30 KB |  |
| 21: | 00001280.png | 67 B |  |

Figure : Foremost data output filelist

# Where we found it

Table : Audit.txt uit foremost.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Number | Name | Size | File Offset (dec) | Comment |
| 0: | 00000016.jpg | 631 KB | 8192 |  |
| 1: | 00001279.gif | 37 B | 655121 | (1 x 1) |
| 2: | 00000105.bmp | 595 KB | 54217 | (Header dump) |
| 3: | 00000351.bmp | 472 KB | 179852 | (Header dump) |
| 4: | 00001048.bmp | 123 KB | 536900 | (Header dump) |
| 5: | 00001247.bmp | 24 KB | 638592 | (Header dump) |
| 6: | 00000007.exe | 644 KB | 3917 | (Header dump) |
| 7: | 00000175.exe | 560 KB | 89863 | (Header dump) |
| 8: | 00000307.exe | 494 KB | 157443 | (Header dump) |
| 9: | 00000394.exe | 450 KB | 201952 | (Header dump) |
| 10: | 00000402.exe | 446 KB | 206175 | (Header dump) |
| 11: | 00000591.exe | 352 KB | 303096 | (Header dump) |
| 12: | 00000609.exe | 343 KB | 312166 | (Header dump) |
| 13: | 00000777.exe | 259 KB | 398154 | (Header dump) |
| 14: | 00000788.exe | 253 KB | 403884 | (Header dump) |
| 15: | 00000796.exe | 249 KB | 407825 | (Header dump) |
| 16: | 00000884.exe | 205 KB | 452912 | (Header dump) |
| 17: | 00001076.exe | 109 KB | 551007 | (Header dump) |
| 18: | 00001086.exe | 104 KB | 556543 | (Header dump) |
| 19: | 00001109.exe | 93 KB | 567808 | (Header dump) |
| 20: | 00001234.exe | 30 KB | 631937 | (Header dump) |
| 21: | 00001280.png | 67 B | 655360 | (1 x 1) |

Table 2: Data gevonden met DFF.

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Filetype | Start offset (hex) | End offset (hex) |
| 0x2be8c-0x4452c | BMP | 0x2be8c | 0x4452c |
| 0x2be8c-0x4452c\_562949953421321 | BMP | 0x2be8c | 0x4452c |
| 0x9be80-0xb4520 | BMP | 0x9be80 | 0xb4520 |
| 0x9be80-0xb4520\_562949953421323 | BMP | 0x9be80 | 0xb4520 |
| 0x83144-0x9b7e4 | BMP | 0x83144 | 0x9b7e4 |
| 0x83144-0x9b7e4\_562949953421322 | BMP | 0x83144 | 0x9b7e4 |
| 0xd3c9-0x25a69 | BMP | 0xd3c9 | 0x25a69 |
| 0xd3c9-0x25a69\_562949953421320 | BMP | 0xd3c9 | 0x25a69 |
| 0x9ff11-0x9ff36 | GIF | 0x9ff11 | 0x9ff36 |
| 0x9ff11-0x9ff36\_562949953421318 | GIF | 0x9ff11 | 0x9ff36 |
| 0x3c5a-0x4da4 | JPG | 0x3c5a | 0x4da4 |
| 0x3c5a-0x4da4\_562949953421316 | JPG | 0x3c5a | 0x4da4 |
| 0x2000-0x3a9c | JPG | 0x2000 | 0x3a9c |
| 0x2000-0x3a9c\_562949953421314 | JPG | 0x2000 | 0x3a9c |
| 0x2952-0x3a9c | JPG | 0x2952 | 0x3a9c |
| 0x2952-0x3a9c\_562949953421315 | JPG | 0x2952 | 0x3a9c |
| 0xa0000-0x13b2d00 | PNG | 0xa0000 | 0x13b2d00 |
| 0xa0000-0x13b2d00\_562949953421327 | PNG | 0xa0000 | 0x13b2d00 |
| 0x3b24-0xbebfd24 | TIF | 0x3b24 | 0xbebfd24 |
| 0x3b24-0xbebfd24\_562949953421325 | TIF | 0x3b24 | 0xbebfd24 |

# How we found it

Voor deze opdracht zijn twee soorten tools gebruikt. Twee forensische tools en verschillende hex viewers.

Het “data” bestand is geanalyseerd met gebruik van open-source forensische programma’s aanwezig op Kali Linux 2016.1. De programma’s die zijn gebruikt is het Digital Forensic Framework (DFF) en Foremost. Daarnaast is gebruik gemaakt van hex editor Neo, gHex en Notepad++.

Als eerste is gebruik gemaakt van foremost. Met foremost is het mogelijk om bestanden te herstellen door middel van zoeken naar headers, footers en datastructuren. In Table 2 staat de uitleg van het gebruikte commando dat het “data” bestand onderzoekt.

Table : uitleg foremost commando

|  |  |
| --- | --- |
| [foremost] [-av] [all] [/media/sf\_mict1/data] | |
| [foremost] | Initialiseert het foremost programma. |
| [-av] | Dit zijn parameters. -v zorgt dat tijdens het analyseren van het bestand de output wordt weergeven op het scherm. -a zorgt dat geen error detectie plaats vindt aangaande met corrupte bestanden. |
| [all] | Run all pre-defined extraction methods. Zoekt door het bewijs naar headers van alle soorten bestanden. Een lijst van bestanden waarop foremost zoekt is te vinden in de foremost handleiding (Namikus, 2006). |
| [/media/sf\_mict1/data] | Locatie van bestand dat dient te worden geanalyseerd. |

Daarna is het “data” bestand geanalyseerd met DFF. Hieronder zijn de stappen gedocumenteerd die hebben geleid tot het vinden van de gevonden bestanden.

1. DFF openen. (Figure 6)
2. “Open evidence”.
3. “Select evidence type”. (Figure 7)
4. “Raw format” Aanvinken.
5. Klik op de groene plus om
6. Zoek het verdachte “data” bestand. (Figure 8)
7. Klik “OK” en het bewijs is toegevoegd.
8. Het bewijs is nu te vinden onder “Logical files”. (Figure 10)
9. Rechtermuisklik op het verdachte “data” bestand.
10. “Open with >” (Figure 11)
    1. “Search >”
    2. “cavergui”
11. In carver-gui<data> stab, vink aan: (Figure 12)
    1. pgp:txt
    2. images
12. Klik op “Start”.
13. Teurg in het “Browser” tab is de carved data weergeven. (Figure 13)

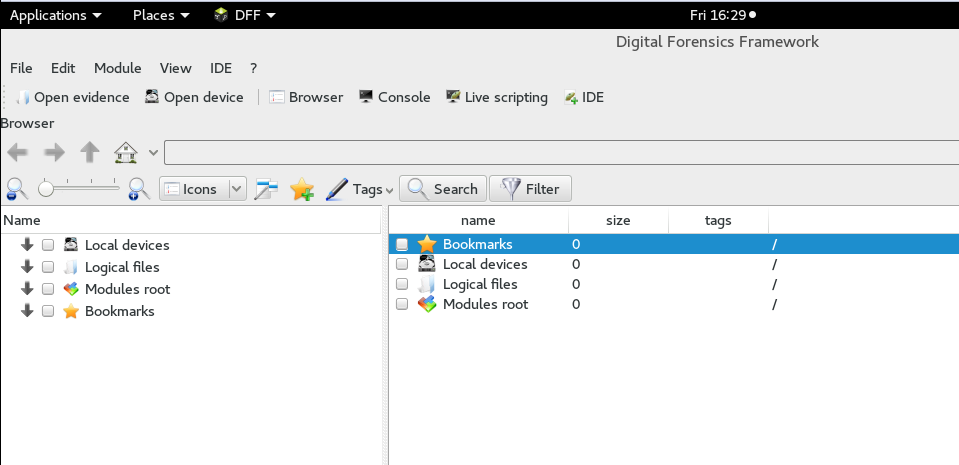


Figure : DFF

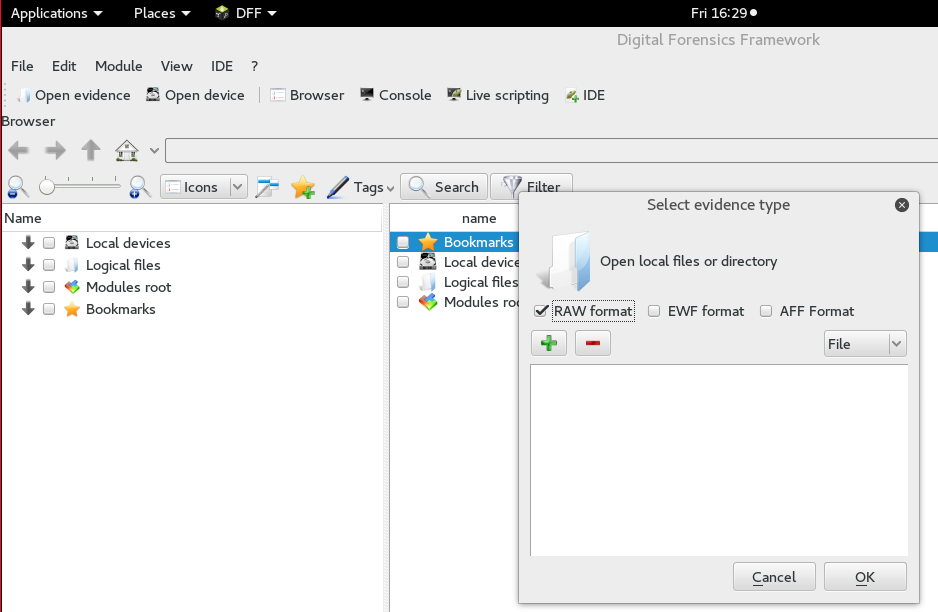


Figure : Open evidence type

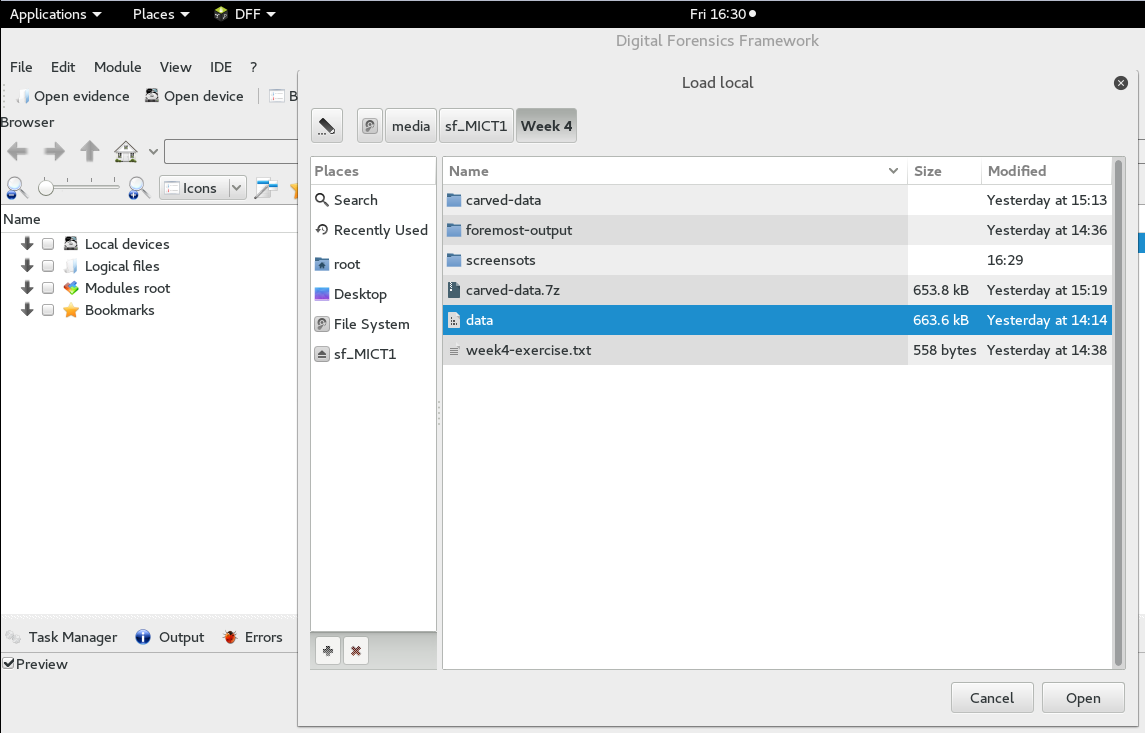


Figure : Select data file

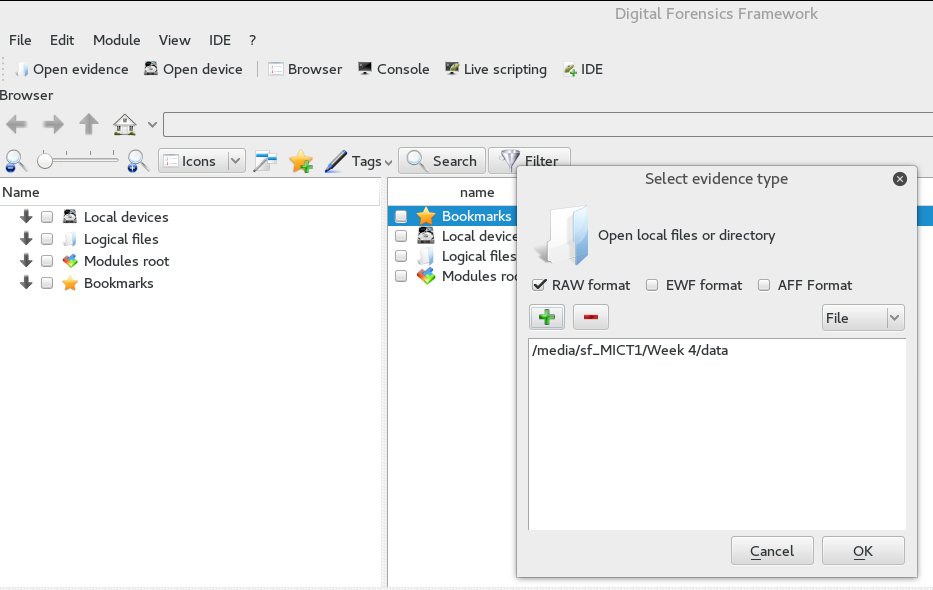


Figure : Select evidence type

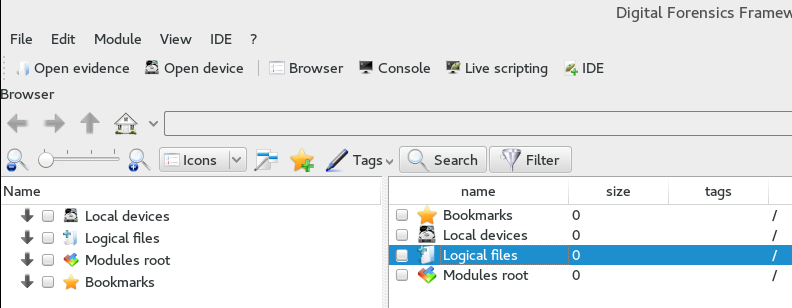


Figure : evidence toegevoegd onder local files

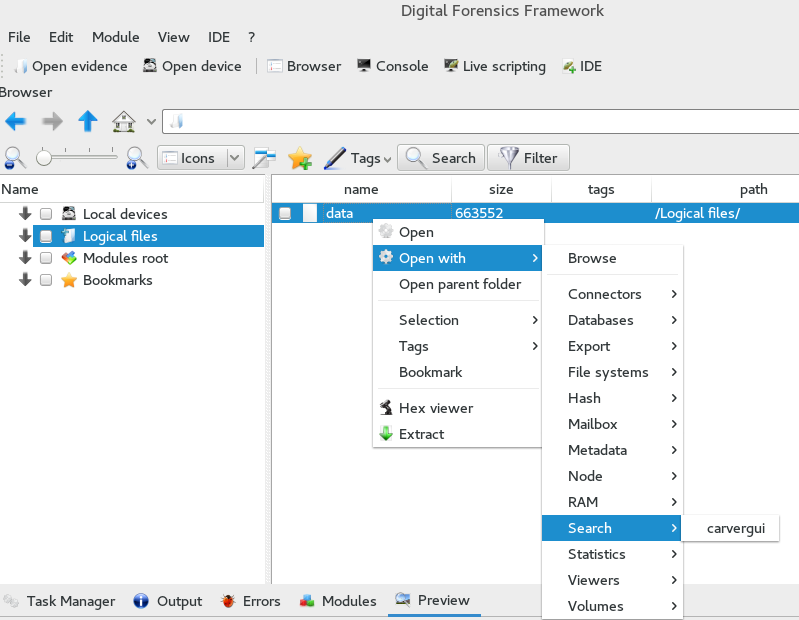


Figure : open Carvergui

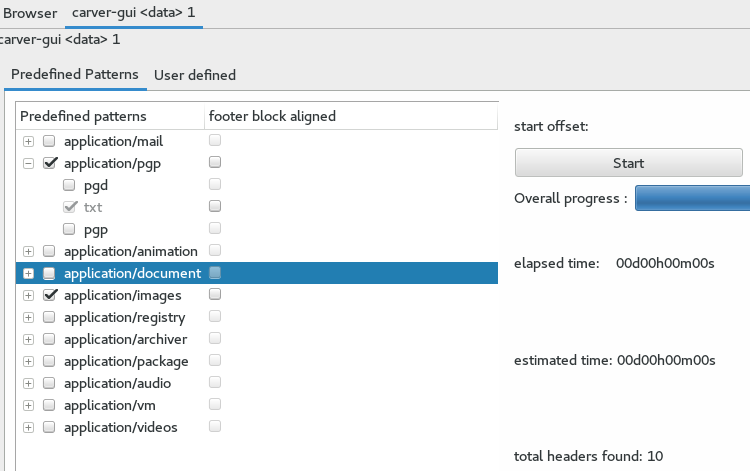


Figure : Select file types

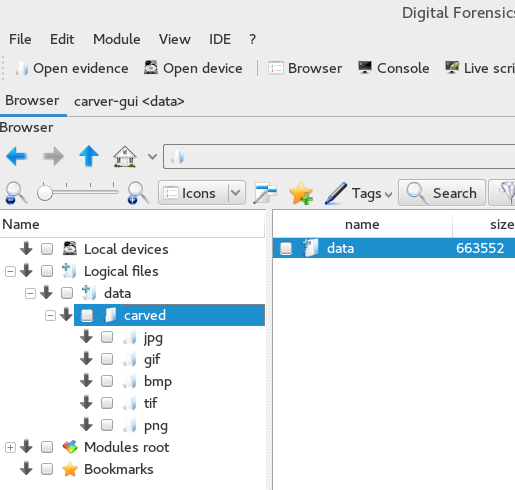


Figure : output carved data