MICT1 Groep 3

WEEKOPDRACHTEN WEEK 4

AUTEURS

Tristan **J**anssen

Chris **K**uipers

Juul **S**teins

Mick **U**bags

Zuyd Hogeschool

Faculteit ICT

OPLEIDING

HBO-ICT

MODULE

MICT1

Opdracht

Onderzoek het bestand “data”. Dit bestand bevat een dump van 162 clusters met een grootte van 4k. De dump komt van een onbekend bestandssysteem.

Probeer bestanden uit de RAM- en/of Disk-slack van het image te herstellen.

Resultaat

Het bestand “data” bevatte meerdere afbeeldingen; JPEG file, PNG file en een GIF file:

JPEG

PNG

Hoewel er een PNG file gevonden is, is deze te klein om weer te geven. De afmeting van de afbeelding is 1 bij 1 pixel.

GIF

Tot slot is er een zwaar corrupt GIF bestand gevonden, echter is het niet gelukt deze te herstellen.

Methode

Het bestand “data” is geanalyseerd door middel van de *Synalyze It!*, een Hex Editor voor Mac OS X.

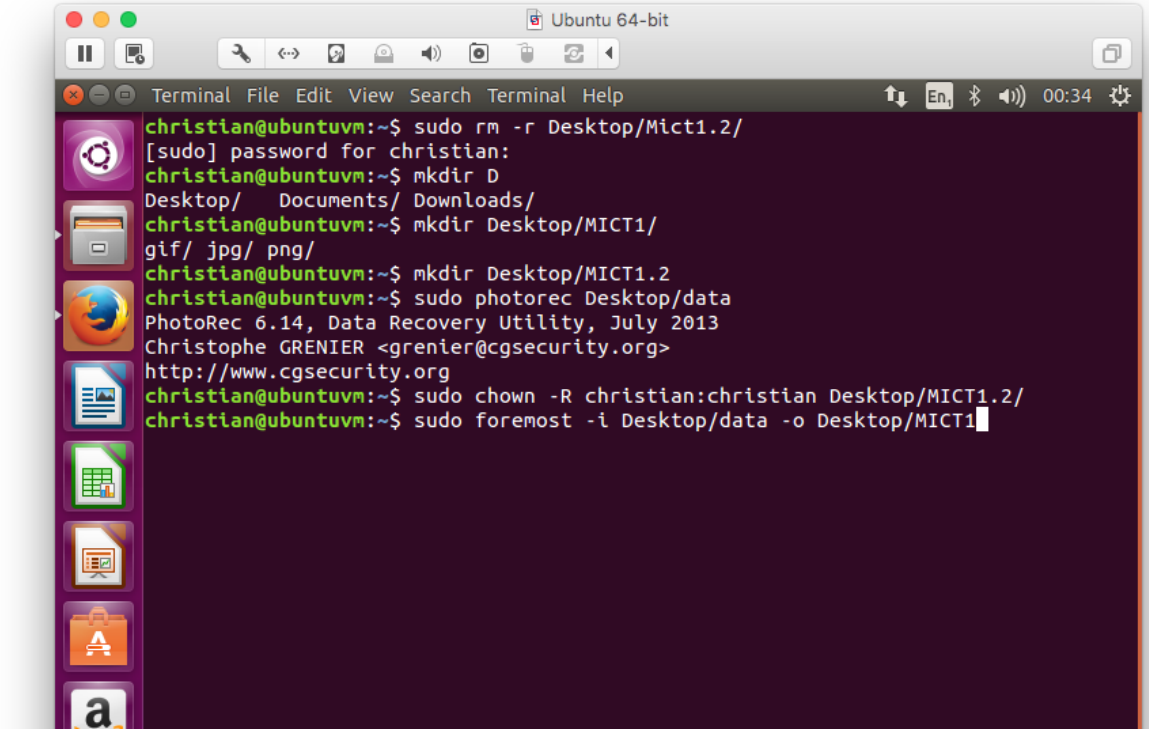
Het bestand in eerste instantie snel geanalyseerd door er met een Hex Editor doorheen te lopen. Vervolgens is er gebruik gemaakt van de File Carver foremost in een Ubuntu virtuele machine.

Bevindingen

Aan de hand van de beschreven methode zijn onderstaande resultaten gevonden.

Door gebruik te maken van een snelle, handmatige analyse met behulp van een Hex Editor werden er JFIF tekst strings gevonden. Deze data wijst op een of meerdere JPEG (achtige) afbeeldingen. Dankzij deze indicatie wisten we dat we in de juiste richting aan het kijken waren.

Vervolgens is in een Ubuntu VM de File Carver foremost gebruikt. Foremost analyseert de data bit voor bit, op zoek naar headers, footers of andere aanduidingen op bekende bestandsformaten. Dit leverde de gewenste resultaten.



JPEG afbeeldingen

Foremost herstelde twee JPEG afbeeldingen, deze foto's zijn, op hun resolutie na, gelijk aan elkaar. Het lijkt er dan ook op dat de kleine versie de thumbnail is van de grote afbeelding. De herstelde foto is hierbeneden weergegeven.

Na het bestuderen van de metadata van de afbeeldingen valt er te concluderen dat de bestanden zijn bewerkt en/of geopend met Adobe Creative Cloud Photoshop.

Ook is er een PNG afbeelding uit de dump gehaald. Deze PNG is op dit moment echter niet van significante waarde gezien de resolutie 1 bij 1 pixel bedraagt. Daarbij is er geen relevante gegevens in de metadata gevonden.

Tot slot bevatte het originele bestand een GIF afbeelding. Deze afbeelding was in dermate beschadigde staat dat herstelpogingen zijn mislukt. Helaas kon er geen relevante informatie uit de metadata van dat bestand worden gehaald. Als er wordt gekeken naar de locatie van de GIF, aan het einde van een JPEG cluster, is het zeer waarschijnlijk dat de GIF een stukje Diskslack betreft.

Bronnen

Bron	URL
Zuyd Repository op GitHub	https://github.com/ZuydUniversity/MICT1
Online Hex Editor	https://hexed.it
Foremost Man Page	http://linux.die.net/man/1/foremost
World Wide Web Consortium JPEG Specification	https://www.w3.org/Graphics/JPEG/jfif3.pdf
Wikipedia JPEG File Format	https://en.wikipedia.org/wiki/JPEG_File_Interchange_Format
World Wide Web Consortium GIF89a Specification	https://www.w3.org/Graphics/GIF/spec-gif89a.txt