File Carving using Foremost

By Alice Lee

Table of Contents

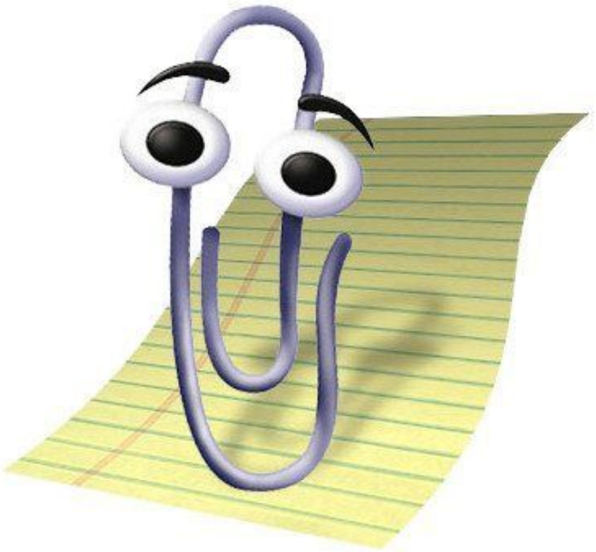
1. What is File Carving?
2. Common Techniques
3. File Carving vs Data Carving
4. Foremost
5. Demo
6. Summary

What is File Carving?

- Process to recover deleted or fragmented files
- Recovery technique
  - Contents and structures > file system structures
- Commonly used in digital forensics
  - Best for cybercrimes
    - *Collecting and restoring evidence*
    - *Recovering corrupt or missing files*

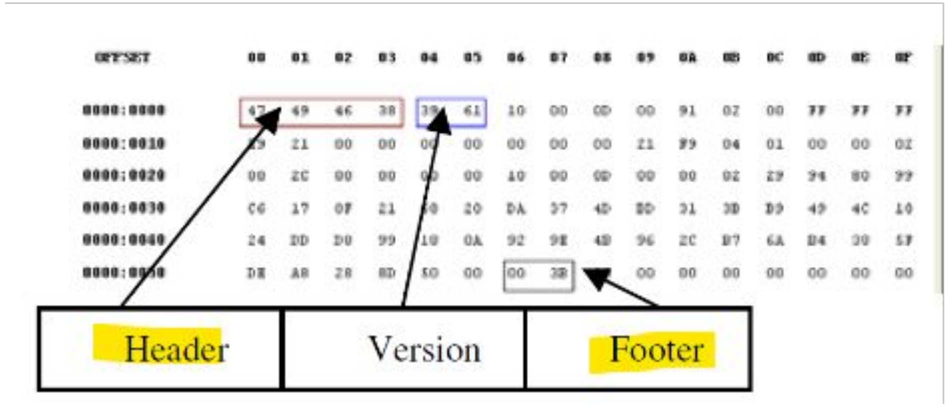
Common Techniques

- Header-Based Carving
- File Structure Based Carving
- Content Based Carving



Header-Based Carving

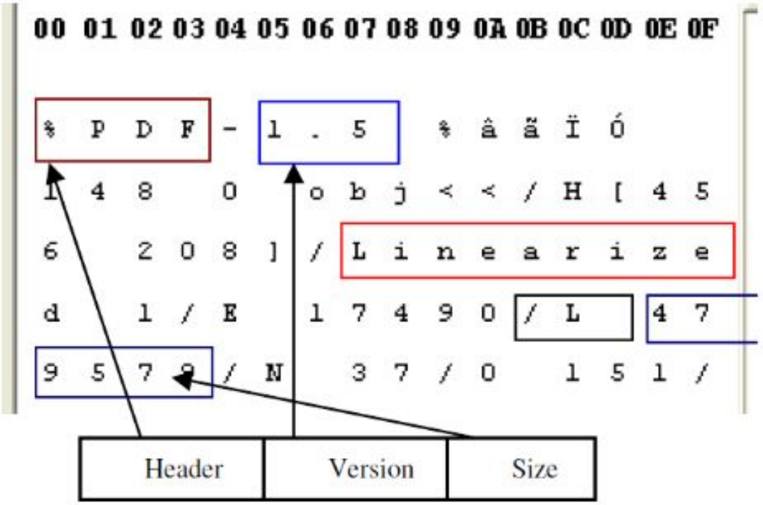
- Header
  - First few bytes of data
- Footer
  - Last few bytes of data



```
OFFSET      00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

0000:0000   47 49 46 38 39 61 10 00 0D 00 91 02 00 FF FF FF
0000:0010   F9 21 00 00 00 00 00 00 00 21 F9 04 01 00 00 02
0000:0020   00 2C 00 00 00 00 10 00 0D 00 00 02 2F 94 8F 99
0000:0030   C6 17 0F 21 50 20 DA 37 4D BD 31 3B D9 49 4C 10
0000:0040   24 DD D0 99 10 0A 92 9E 4B 96 2C B7 6A D4 30 5F
0000:0050   DE A8 28 8D 50 00 00 3B       00 00 00 00 00 00 00
```

- Header-footer based carving
- Header-maximum size carving
  - *If there is no footer, then a maximum file size is used*



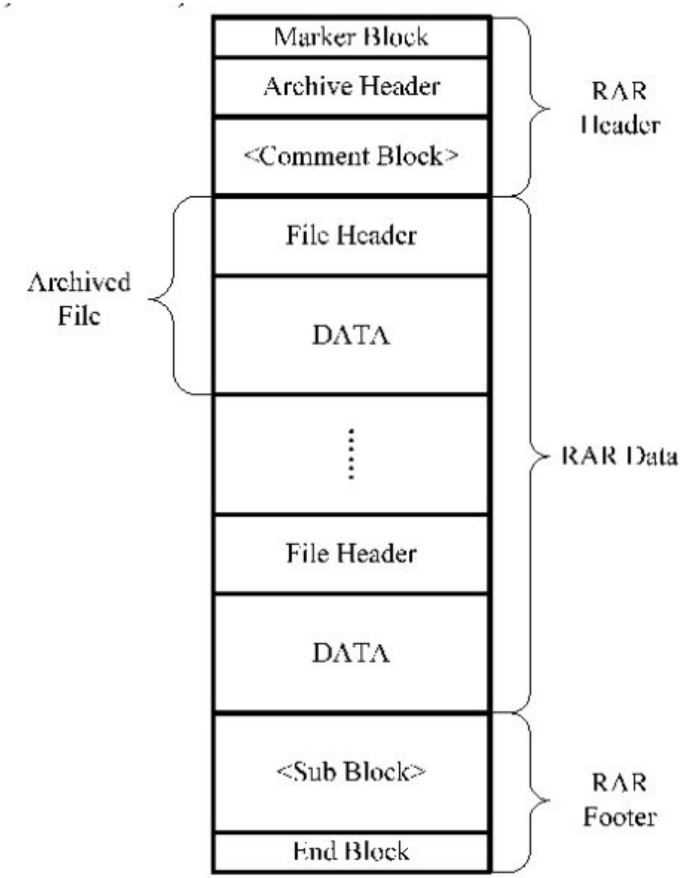
```
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

%  P  D  F  -  1  .  5     %  â  ã  Ï  Ó
1  4  8     0     o  b  j  <  <  /  H  [  4  5
6     2  0  8  ]  /  L  i  n  e  a  r  i  z  e
d     1  /  E     1  7  4  9  0  /  L     4  7
9  5  7  9  /  N     3  7  /  0     1  5  1  /
```

HTTPS://WWW.INSTITUTOPOINCARE.COM.BR/SITE/INDEX.PHP?OPTION=COM_CONTENT&VIEW=ARTICLE&ID=30:DATACARVING&CATID=8&ITEMID=126

File Structure Based Carving

- Internal layout of a file must be known
- Basic Elements
  - Header
  - Footer
  - Identifier strings
  - Size information



HTTPS://WWW.SEMANTICSCHOLAR.ORG/PAPER/AN-AUTOMATIC-CARVING-METHOD-FOR-RAR-FILE-BASED-ON-WEI-ZHENG/4C614E87D3CF4C09EB698B8D5E0346134B143FCF

Content Based Carving

- Identification of files
- Headers, footers, or known file signatures are optional
- Characteristics
  - Character count
  - Text/Language Recognition
  - Information Entropy

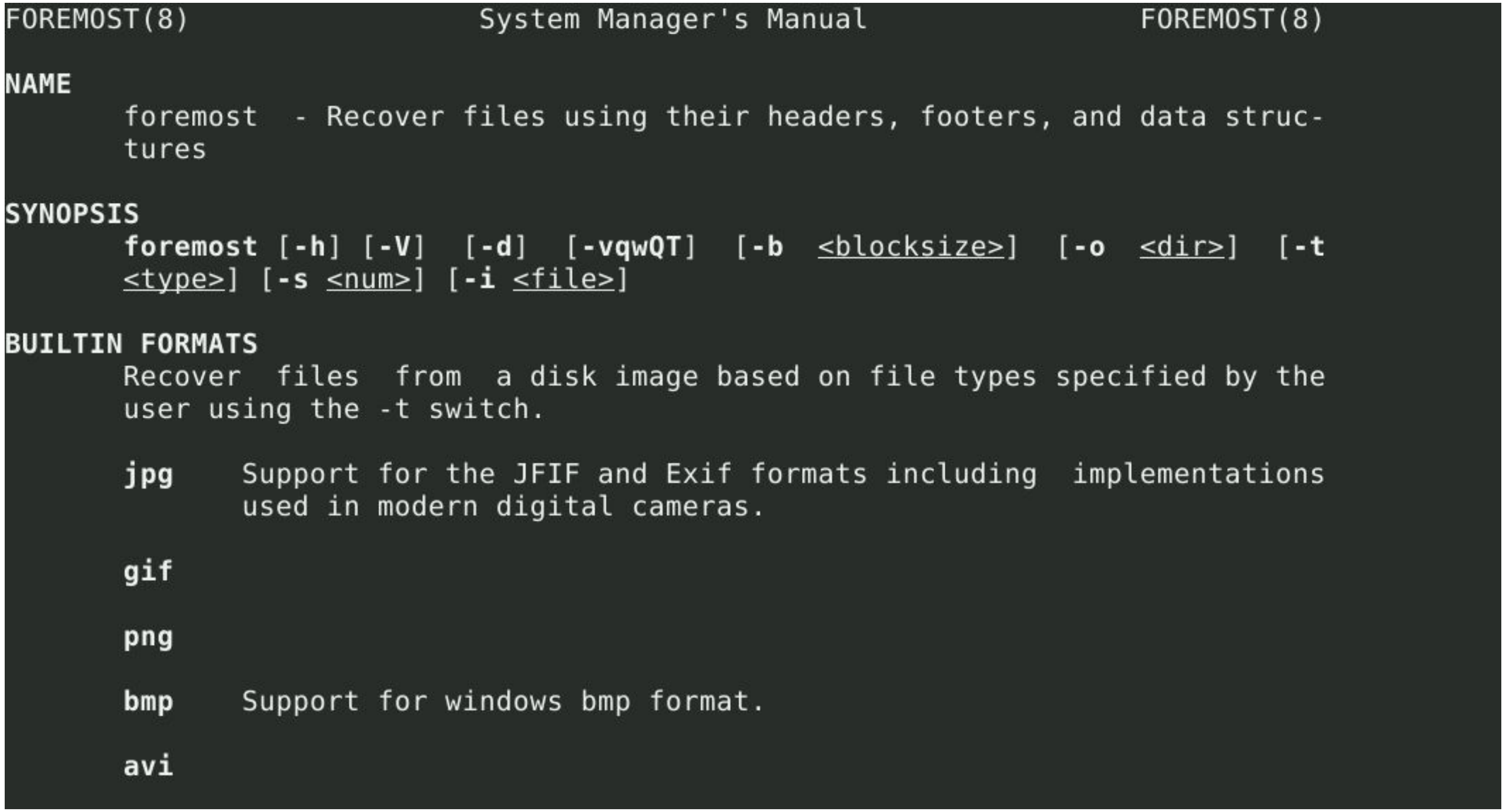
File Carving vs Data Carving

- File Carving
  - Specific in identifying and extracting known file types
- Data Carving
  - Broader approach for recreating deleted raw data

Foremost

- A Kali Linux tool used to recover files on their headers, footers, and internal data structures of a bit-stream image file of a drive or directly on a drive
- Designed for:
  - Digital forensics
  - Security auditing
  - Penetration testing
- Demonstration: using Foremost on a bit-stream image of a USB

Demo



```
FOREMOST(8)                System Manager's Manual               FOREMOST(8)

NAME
       foremost  - Recover files using their headers, footers, and data struc-
       tures

SYNOPSIS
       foremost [-h] [-V]  [-d]  [-vqwQT]  [-b  <blocksize>]  [-o  <dir>]  [-t
       <type>] [-s <num>] [-i <file>]

BUILTIN FORMATS
       Recover  files  from  a disk image based on file types specified by the
       user using the -t switch.

       jpg    Support for the JFIF and Exif formats including  implementations
              used in modern digital cameras.

       gif

       png

       bmp    Support for windows bmp format.

       avi
```

Summary

- File Carving
- Common Techniques
  - Header-Based File Carving
  - File Structure Based File Carving
  - Content Based Carving
- File Carving vs Data Carving
- Foremost
  - Demo

Thank you!

Any questions?