Forensic Memory Analysis: Files mapped in memory

Ruud van Baar
Wouter Alink
Alex van Ballegooij
Netherlands Forensic Institute

August 12, 2008
DFRWS 2008 Baltimore

Justitie

Introduction

- Why analyse memory dumps?
- Files mapped in memory
- Implementation
- Results
- Demonstration

Why analyse memory?

- Interesting data [Walters 2007]
  - Processes
  - Network information
  - Passwords
  - Cryptography keys
  - …
- Can provide information about recent activities on a system
- Mapped files…

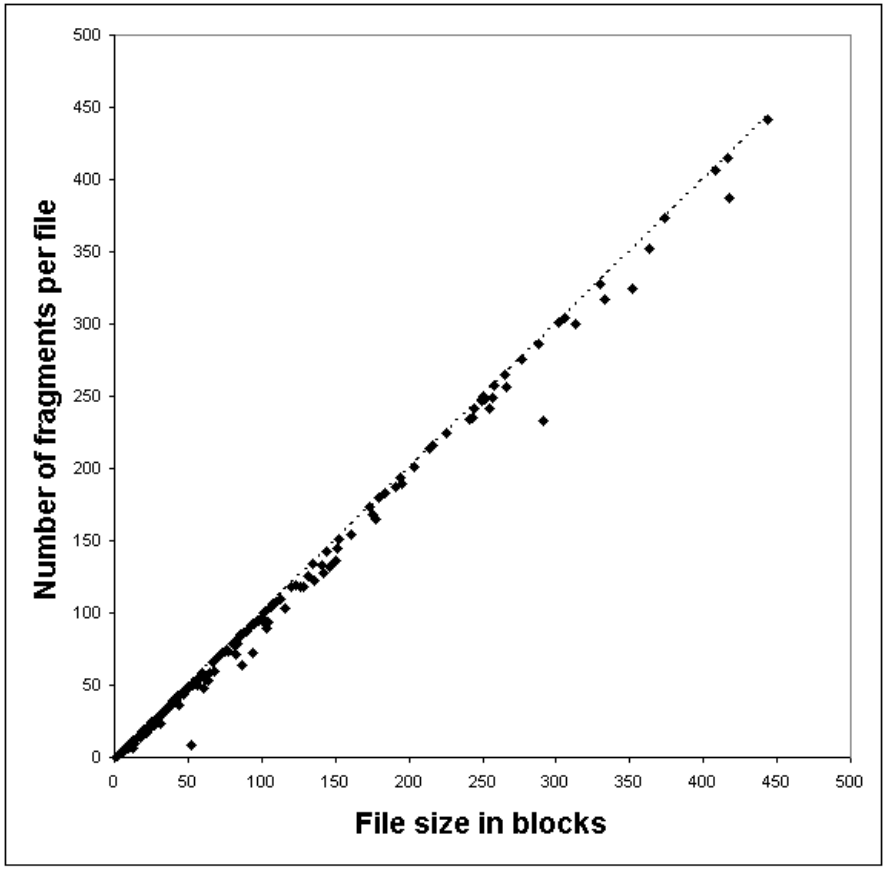
Files mapped in memory

- Link files to a user or process
- Point out recently used data
- Identify data in a memory dump to reduce search space for other information, e.g. passwords

Fragmentation

Problem:

High degree of fragmentation of files in memory

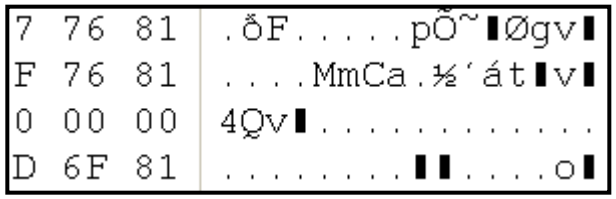


Approach

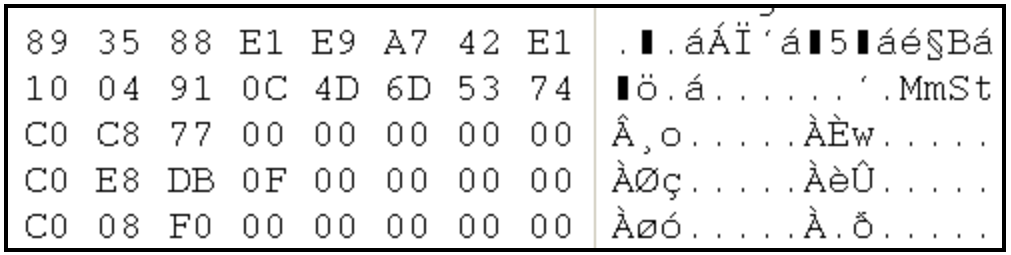
- Recognize pool structures used by the Windows Memory manager
  - Process structures [Schuster 2006]
  - File structures [Dolan-Gavitt 2007]
  - Link these structures if possible
- Carve for unidentified structures

Different methods of identification

- Find process structures
- Identify private and shared files
- Carve for specific file-mapping structures
  - Control areas (MmCa)
  - Page tables (MmSt)



```
7 76 81   .õF.....pÕ˜▮Øgv▮
F 76 81   ....MmCa.½´át▮v▮
0 00 00   4Qv▮............
D 6F 81   ........▮▮....o▮
```



```
89 35 88 E1 E9 A7 42 E1   .▮.áÁÏ´á▮5▮áé§Bá
10 04 91 0C 4D 6D 53 74   ▮ö.á.....´.MmSt
C0 C8 77 00 00 00 00 00   Â¸o.....ÀÈw.....
C0 E8 DB 0F 00 00 00 00   ÀØç.....ÀèÛ.....
C0 08 F0 00 00 00 00 00   Àøó.....À.õ.....
```

File information

- Original path in file system
- Not always available; Backup:
  - Use known mapping to eliminate fragmentation
  - Header/footer information

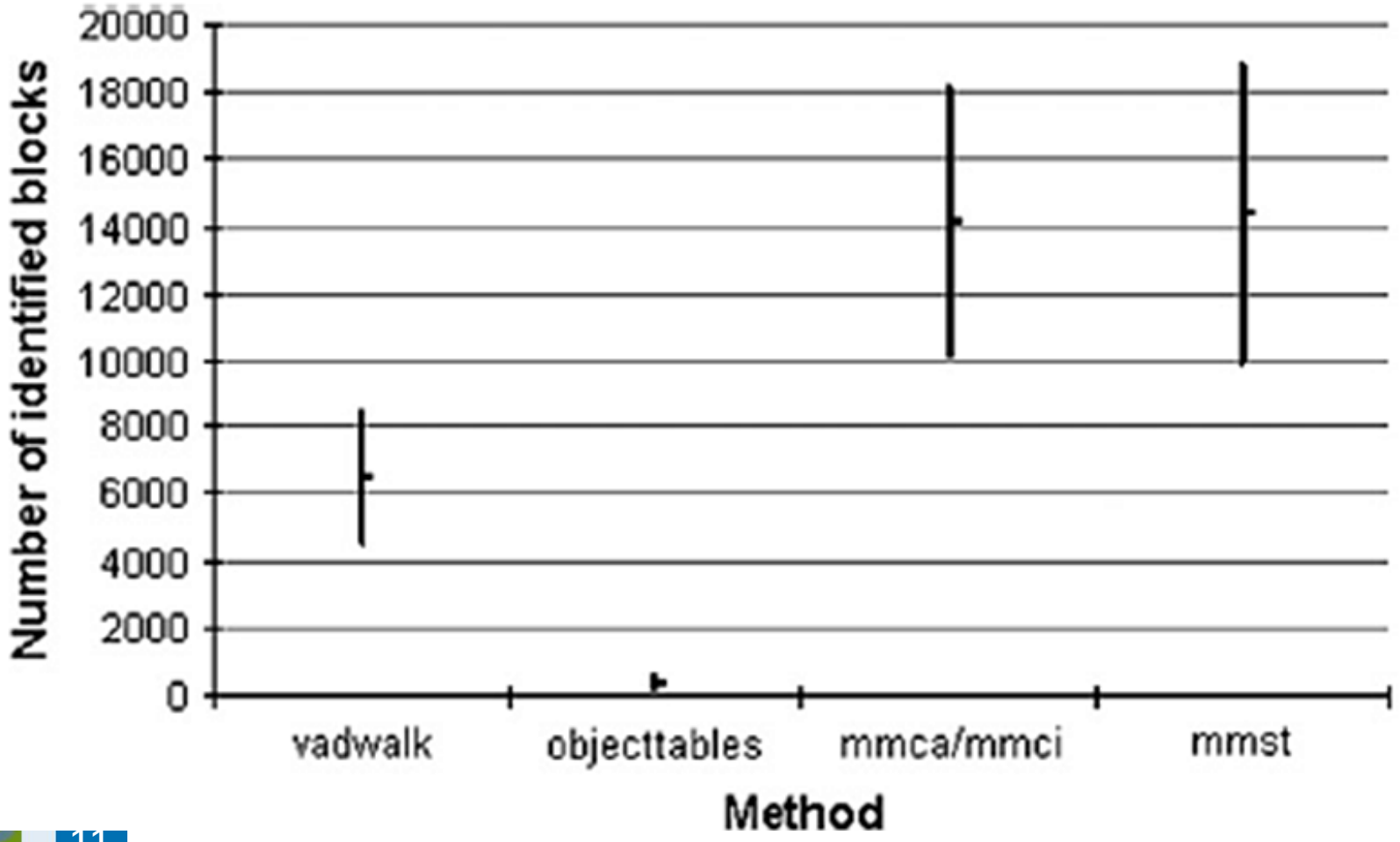
Implementation

- Proof of concept
- Currently only Windows XP SP2
- File size not always known
- Needs more testing
  - Different configurations (PAE, 64 bit)
  - Larger memory dumps

Results by extension

DFRWS 2005 -1		DFRWS 2005 -2		Windows XP	
.dll	202	.dll	211	.dll	298
.pnf	82	.exe	28	.gif	86
.exe	29	.mmf	11	.ttf	52
.mmf	11	.ttf	8	.ini	31
.png	11	.log	5	.jpg	30

Results by method



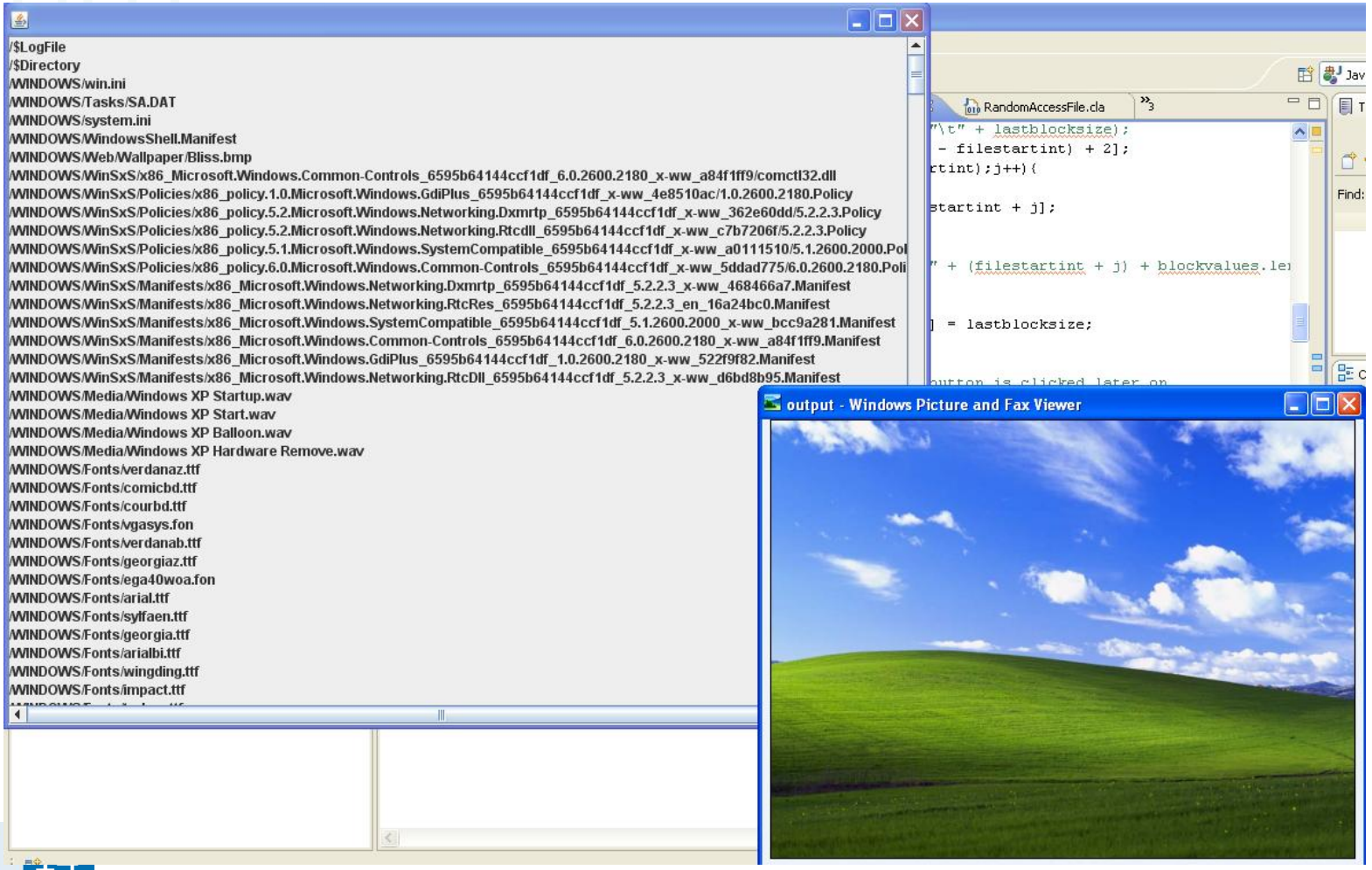
Conclusion

- Possible to identify 25% of pages as part of mapped files
- 40% of these pages can be linked to the relating process or processes
- Less informative methods result in more pages identified

Demonstration

- Test memory dump of a VMWare system running Windows XP SP2 with 256MB of RAM.
- VirtualBLOB [XIRAF 2006]

Demonstration



Contact

Ruud van Baar ruud@holmes.nl
Wouter Alink
Alex van Ballegooij
Netherlands Forensic Institute