Using NTFS cluster allocation behavior to find the location of user data

By
Martin Karresand, Stefan Axelsson, and Geir Olav Dyrkolbotn

From the proceedings of
The Digital Forensic Research Conference
DFRWS 2019 USA
Portland, OR (July 15th - 19th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

https://dfrws.org
Using NTFS cluster allocation behavior to find the location of user data

Martin Karresand
Stefan Axelsson
Geir Olav Dyrkolboth
Current Situation
Our Vision
Hypothetic NTFS partition

- **OS etc.**
- **User Data and Dynamic Content**
Experiment

VirtualBox static hdd
(64 and 256 GiB)

Windows 7, 8, 8.1 and 10 using NTFS

10000 file operations

$Bitmap extraction

Power cycling
Experiment

10000 file operations

VirtualBox static hdd (64 and 256 GiB)

Windows 7, 8, 8.1 and 10 using NTFS

$Bitmap extraction

Power cycling
To infinity and beyond!
Questions?

martin@filecarving.net
or
martin.karresand@ntnu.no

Supported by the Research Council of Norway programme IKTPLUSS, under the R&D project Ars Forensica grant agreement 248094/O70