NTNU

DFRWS

DIGITAL FORENSIC RESEARCH CONFERENCE

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

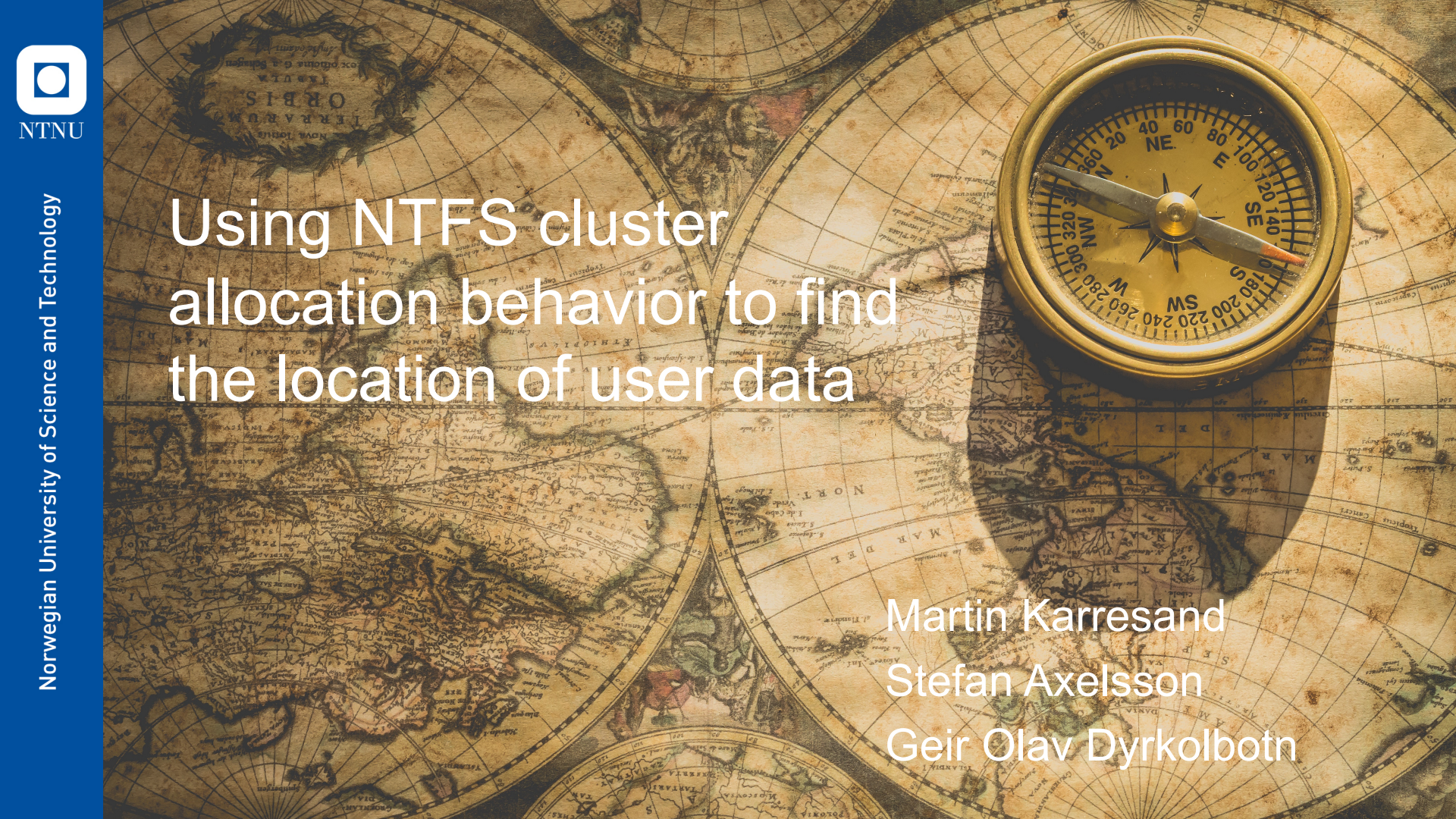
The Digital Forensic Research Conference

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


NTNU
Norwegian University of Science and Technology
Using NTFS cluster allocation behavior to find the location of user data
Martin Karresand
Stefan Axelsson
Geir Olav Dyrkolbotn

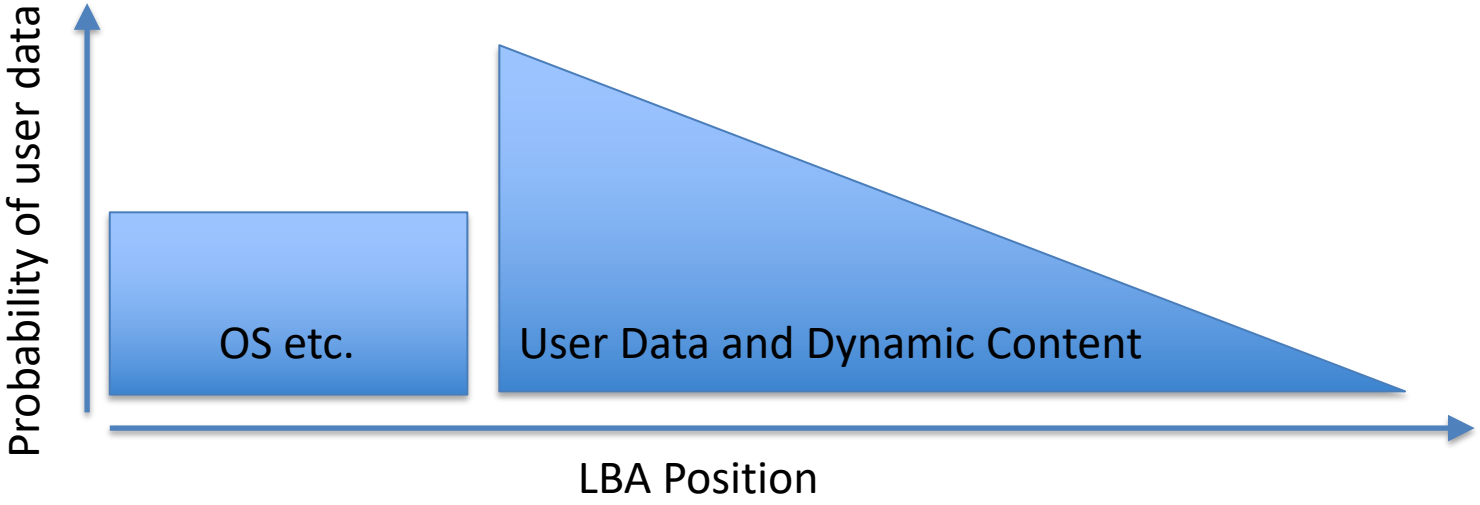
NTNU

Current Situation

NTNU

Our Vision

Hypothetic NTFS partition



NTNU

Experiment

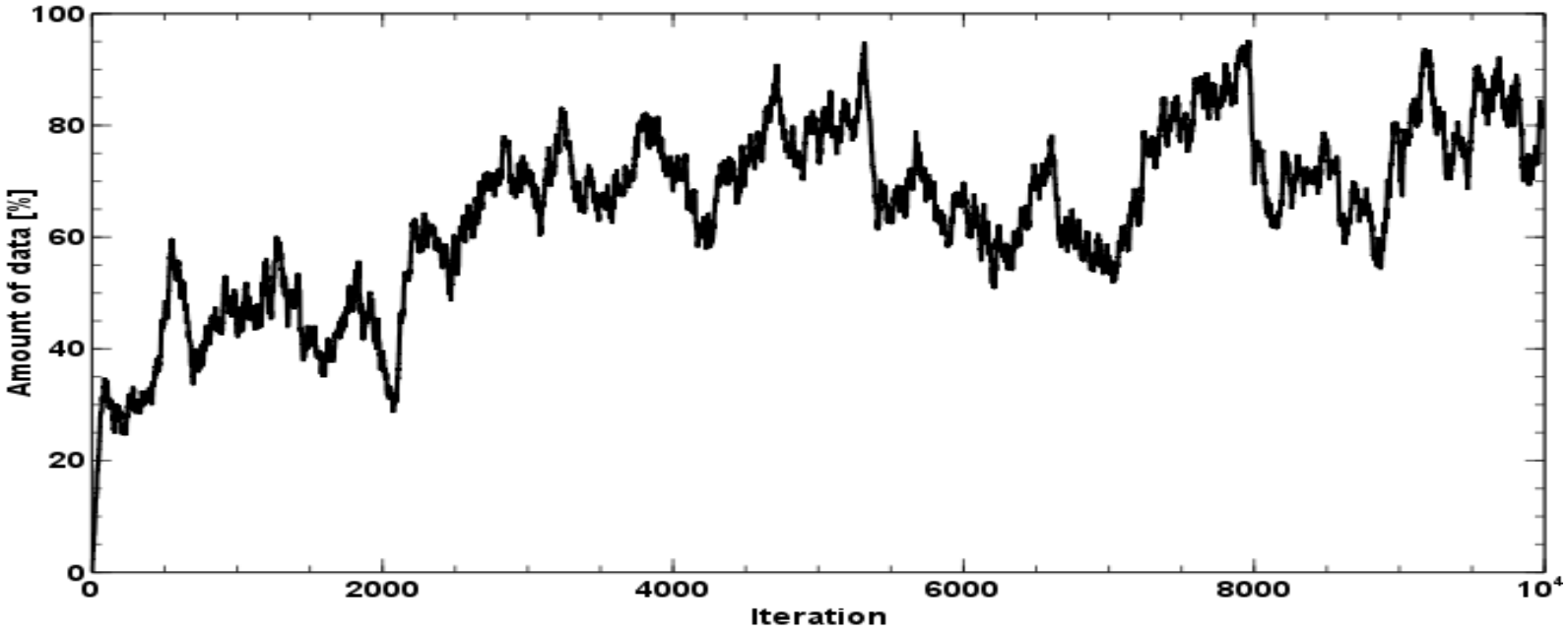
10000 file operations

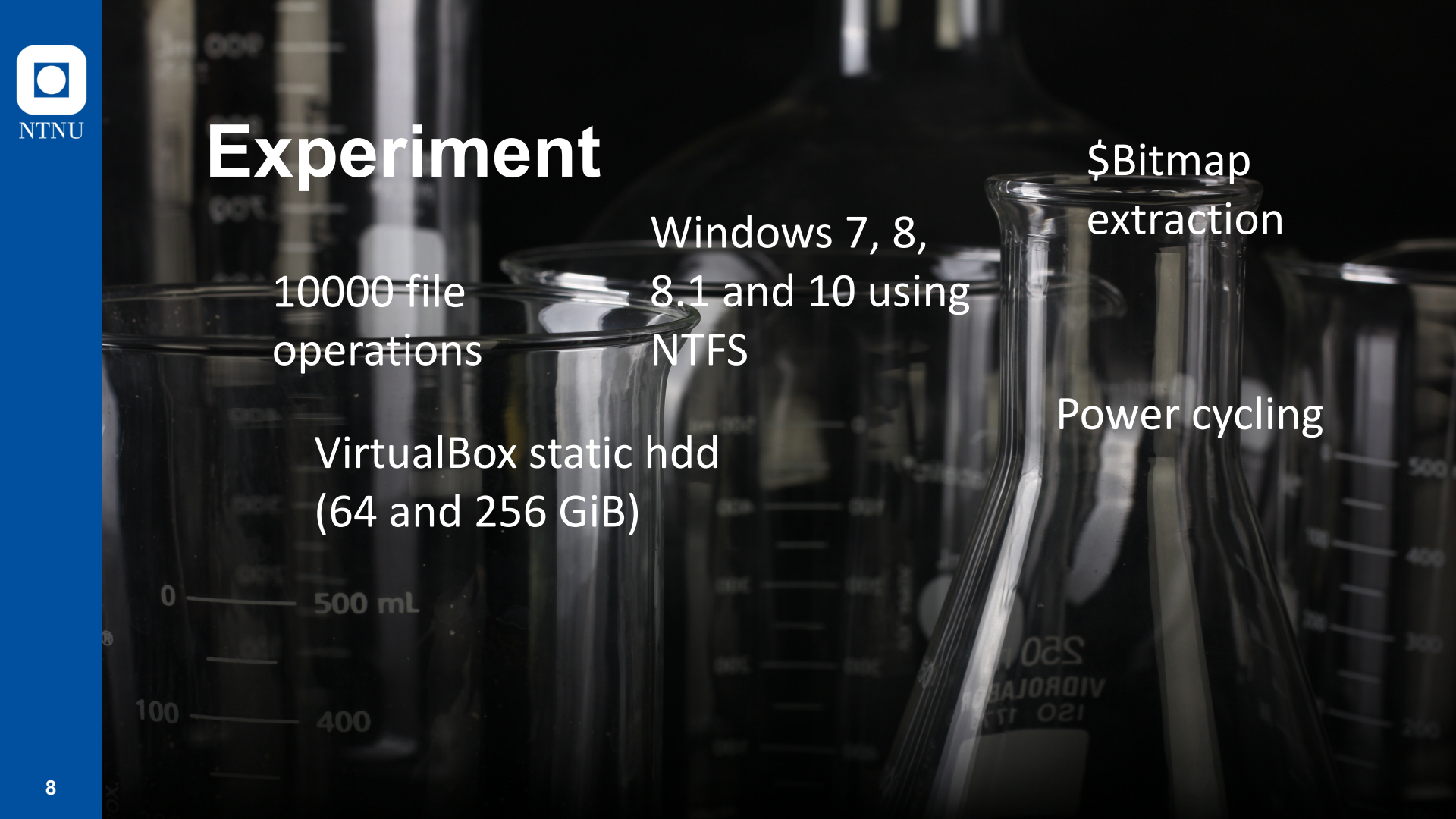
Windows 7, 8, 8.1 and 10 using NTFS

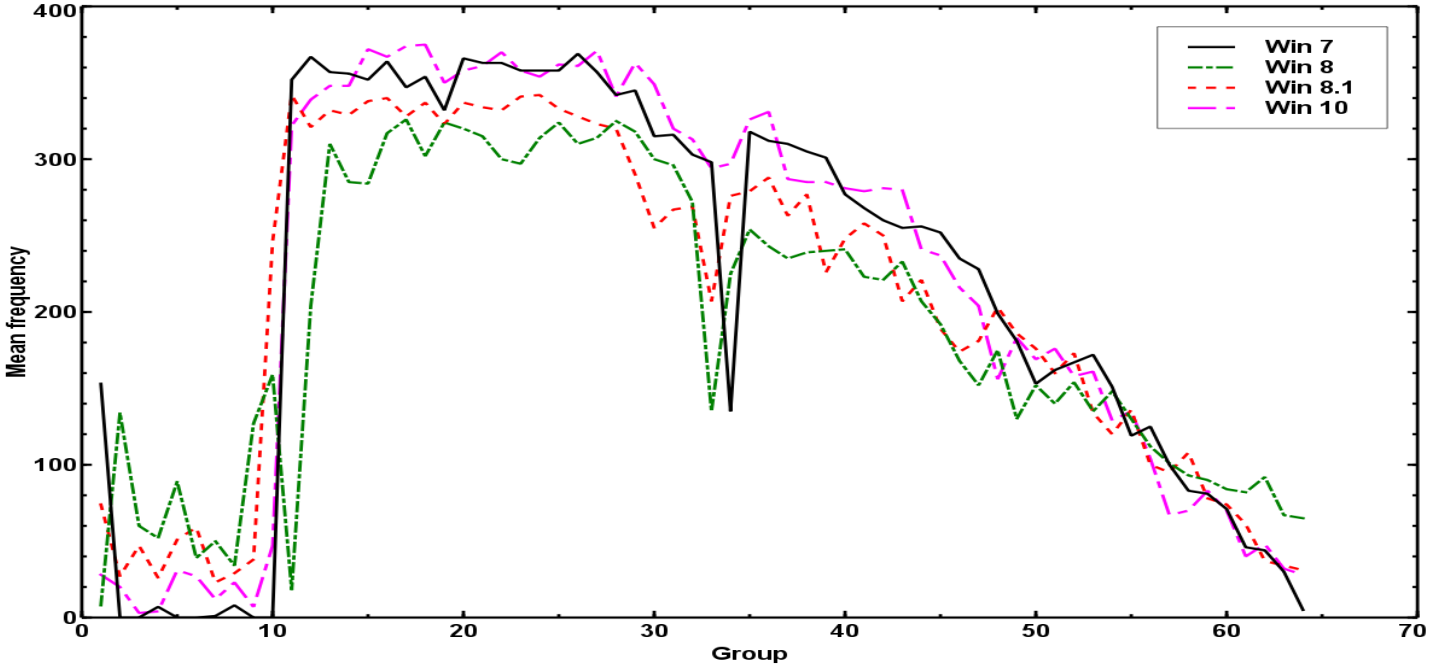
$Bitmap extraction

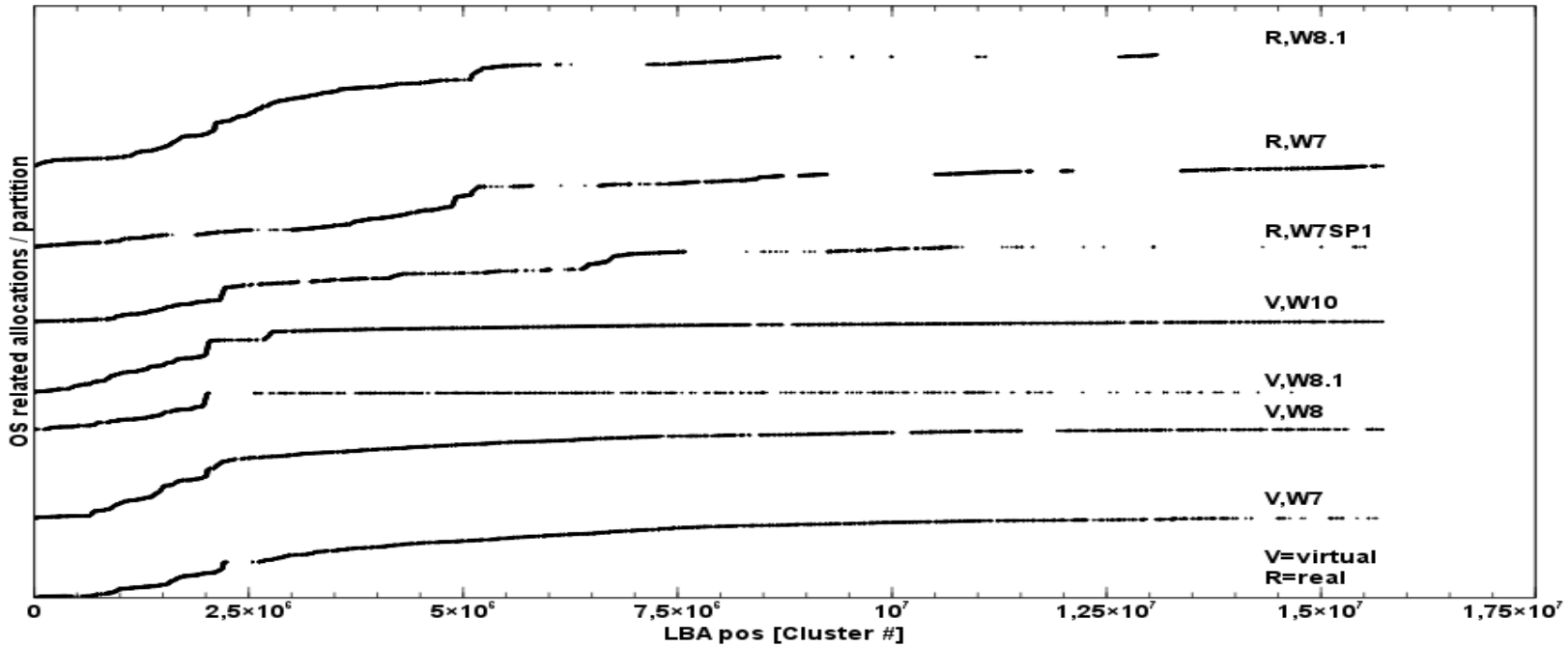
Power cycling

VirtualBox static hdd (64 and 256 GiB)


Amount of data [%]
Iteration
0
20
40
60
80
100
0
2000
4000
6000
8000
10^4


NTNU
Experiment
10000 file operations
Windows 7, 8, 8.1 and 10 using NTFS
VirtualBox static hdd (64 and 256 GiB)
$Bitmap extraction
Power cycling
0
500 mL
100
400


Win 7
Win 8
Win 8.1
Win 10
Mean frequency
Group
0
100
200
300
400
0
10
20
30
40
50
60
70


R,W8.1
R,W7
R,W7SP1
V,W10
V,W8.1
V,W8
V,W7
V=virtual
R=real
OS related allocations / partition
0
2,5×10^6
5×10^6
7,5×10^6
10^7
1,25×10^7
1,5×10^7
1,75×10^7
LBA pos [Cluster #]

NTNU

To infinity and beyond!

NTNU

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