Specification

Forensics and counter forensics on EXT filesystem

Specification

In my project I will focus on LINUX filesystem forensics and counter forensics, especially EXT4. Currently, there are multiple operating systems, using different filesystems across the world (figure 1), some of them are more reliable than others (figure 2) and data from them may be returned with higher recovery rate. As shown in figure 1 currently most used OS is Windows (NTFS or FAT), OS X (APFS or HFS) and LINUX (EXT or UFS). One of my main reasons, why I chose LINUX default filesystem over Windows's and Apple's is due to more open-source tools, information provided by standards and bigger community of supportive geeks.

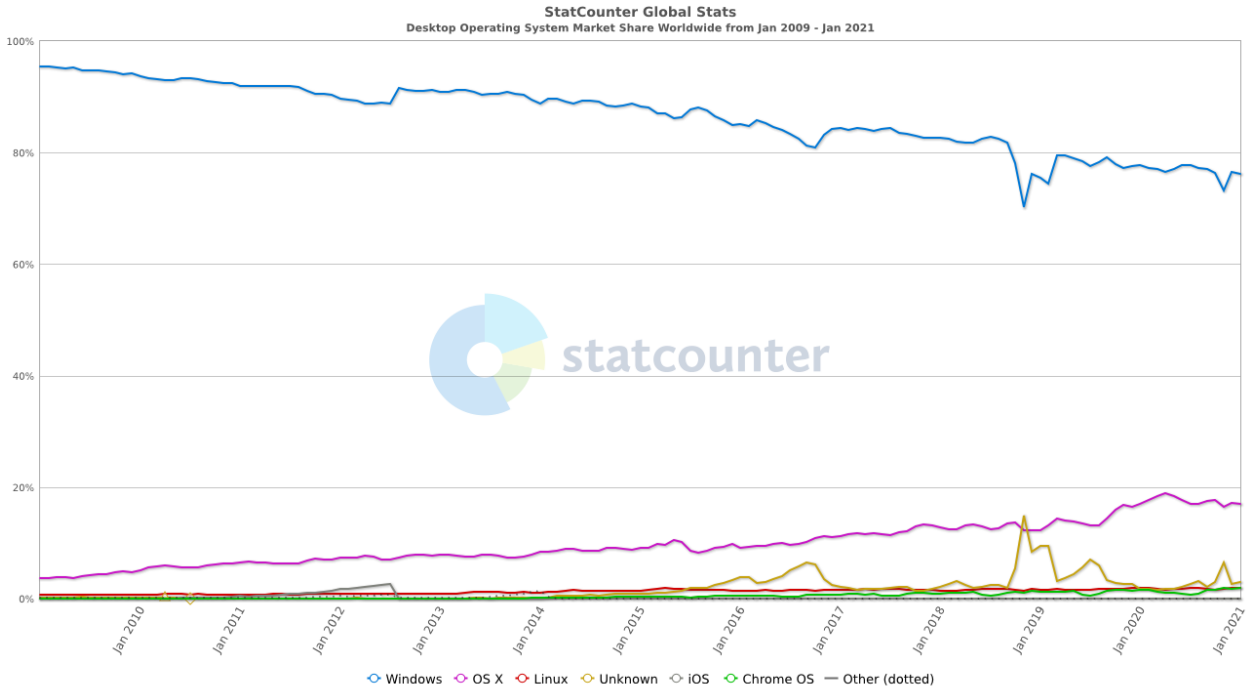
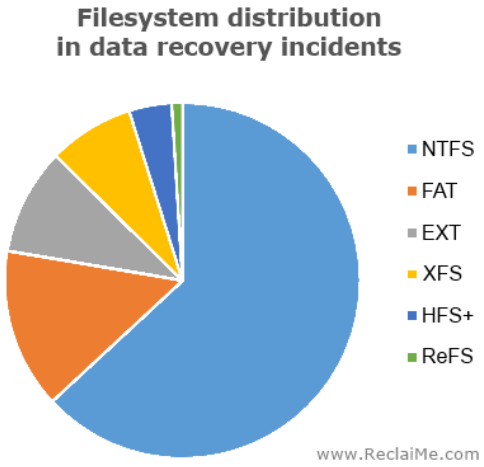


Figure 1 Most used OS from 2009 till 2021



NTFS	63%
FAT	14%
EXT	10%
XFS	8%
HFS+	4%
ReFS	1%

Figure 2 Most filesystems in data recovery incidents according to ReclaiMe

My main goals for this project are:

- Cover standards of EXT filesystem with main focus on EXT4.
- Compare EXT alternatives (NTFS, APFS, ZFS) – speed, reliability and different approaches used when these FSs are used in forensics.
- Compare LINUX (EXT, EXT2, EXT3 and EXT4) filesystems from forensics point of view.
- Explain from begging to end filesystem structure - try to program basic data recovery tool.
- Review counter forensics on EXT4. Write about EXT4 protection against anti forensics with techniques used and show examples how to practice this knowledge on real filesystem.

References

1) Operating System Market Share Worldwide. (2021). StatCounter Global Stats. https://gs.statcounter.com/os-market-share
2) Wikipedia contributors. (2020, December 18). *Ext4*. Wikipedia. https://en.wikipedia.org/wiki/Ext4
3) Wikipedia contributors. (2020b, December 28). *Ext3*. Wikipedia. https://en.wikipedia.org/wiki/Ext3
4) Thomas Göbel, T. G., & Harald Baier, H. B. (2018, March 1). *Anti-forensics in ext4: On secrecy and usability of timestamp-based data hiding*. ScienceDirect. https://www.sciencedirect.com/science/article/pii/S174228761830046X
5) Mohamad Ahtisham Wani, Ali Al Zahrani Wasim, & Ahmad Bhat. (2020, March 1). *File system anti-forensics types, techniques and tools*. ScienceDirect. https://www.sciencedirect.com/science/article/abs/pii/S1361372320300300?casa_token=nrziSXJlt-8AAAAA:pW38IlM7K_OBXLEOPutKboFZjHWqtdxHuU5E5x0gAcAehe9CrB63WfTcxg__aucvIhO9aYz8kc8