# Forensic investigations of rare operating systems

What do you think of when you hear „rare operating system“?

# whereis 'Herbert Bärschneider'

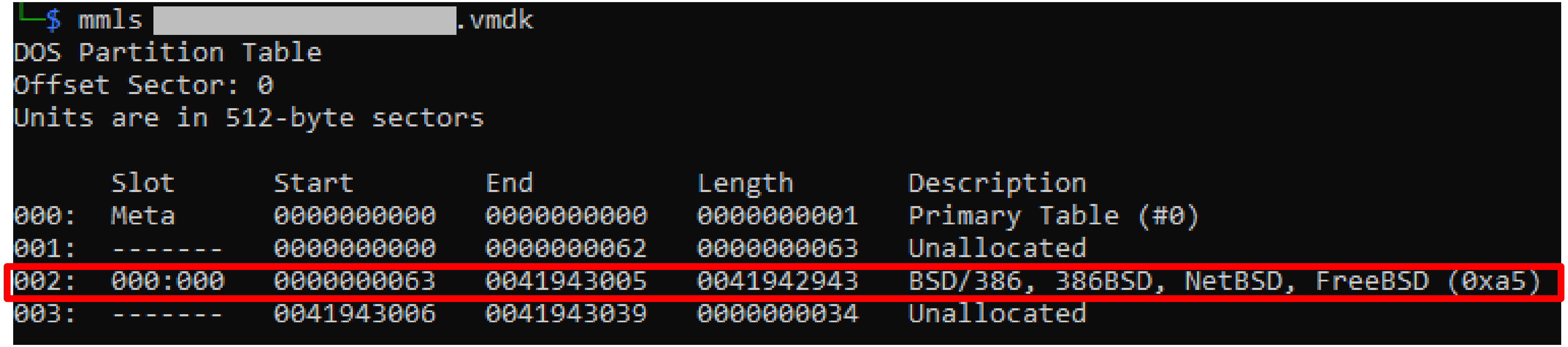
- Almost 3,5 years of investigating cyber attacks against Small and Medium-sized Businesses (SMBs)
- Did some System Administration before
- Did some University Studies in parallel

# Todays goals

- Know a possible method for preparing (forensic) investigations of rare operating systems
- Create interest in looking at rare operating system
- Be able to perform a small imperfect forensic investigation of a rare operating system based on prior experience with Windows Forensics and Linux Forensics

# Example „Citrix NetScaler“ 1/4

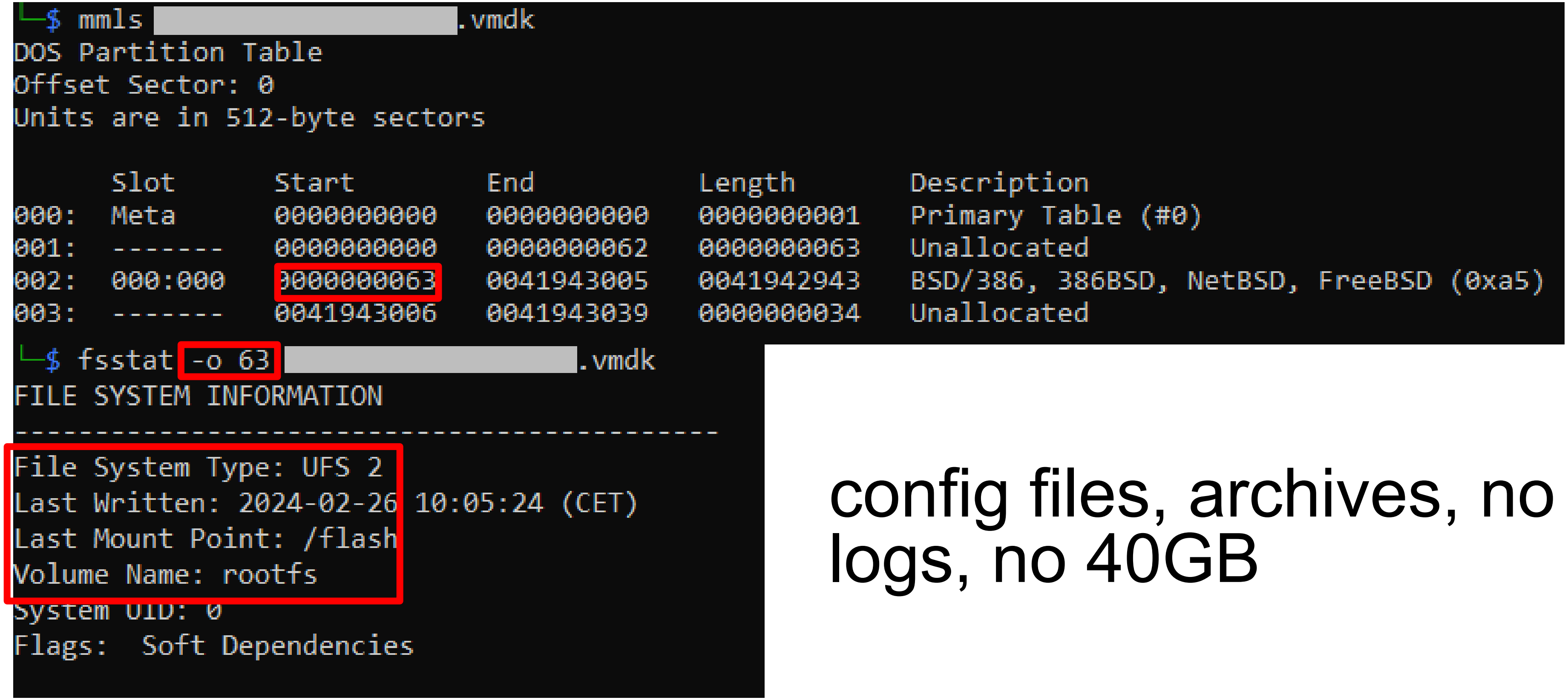
- VMWare virtual disk from a Citrix NetScaler system



```
└─$ mmls [redacted].vmdk
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
001:  -------   0000000000   0000000062   0000000063   Unallocated
002:  000:000   0000000063   0041943005   0041942943   BSD/386, 386BSD, NetBSD, FreeBSD (0xa5)
003:  -------   0041943006   0041943039   0000000034   Unallocated
```

# Example „Citrix NetScaler“ 2/4

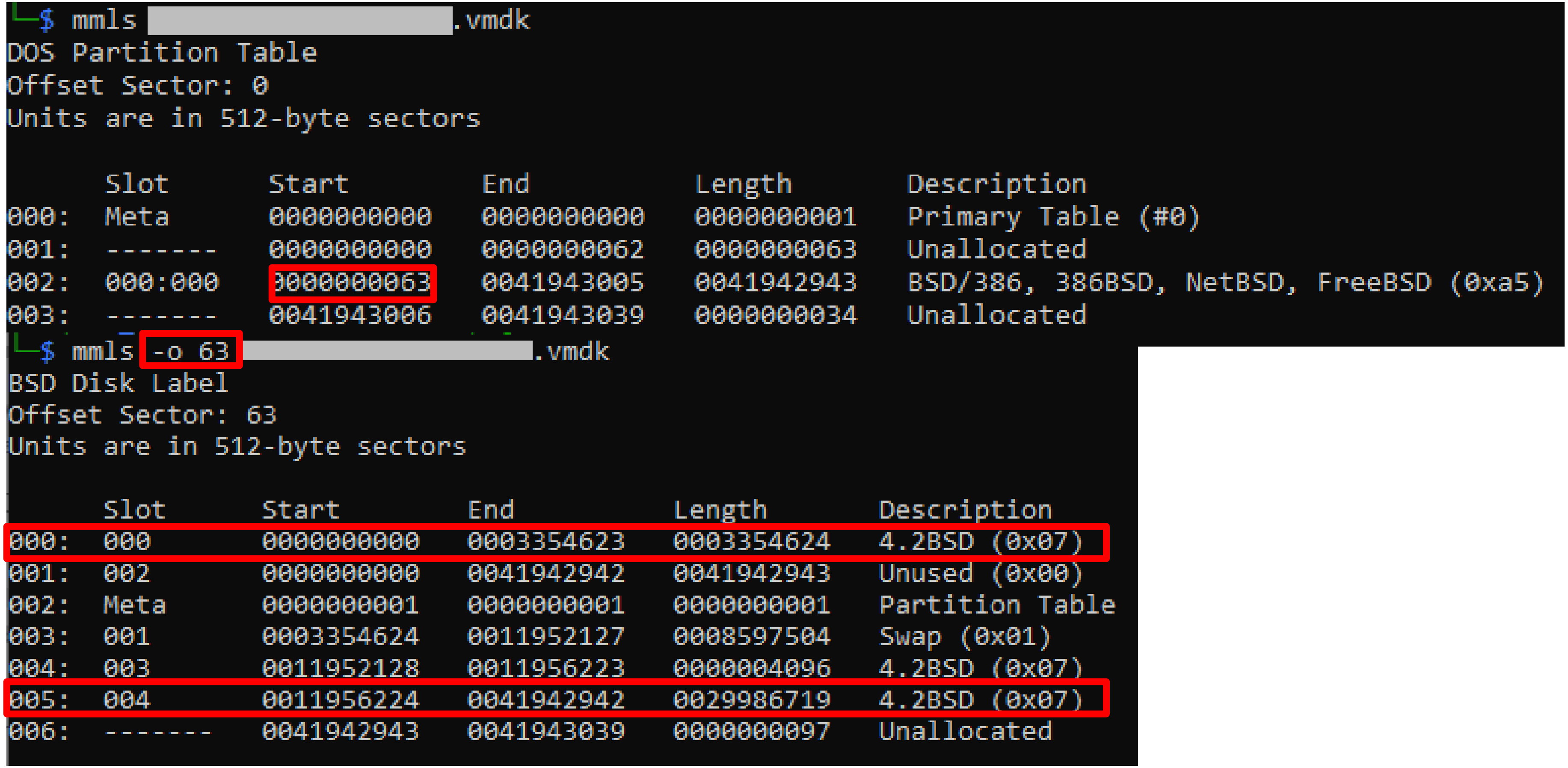


```
└─$ mmls [redacted].vmdk
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
001:  -------   0000000000   0000000062   0000000063   Unallocated
002:  000:000   0000000063   0041943005   0041942943   BSD/386, 386BSD, NetBSD, FreeBSD (0xa5)
003:  -------   0041943006   0041943039   0000000034   Unallocated
└─$ fsstat -o 63 [redacted].vmdk
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: UFS 2
Last Written: 2024-02-26 10:05:24 (CET)
Last Mount Point: /flash
Volume Name: rootfs
System UID: 0
Flags:  Soft Dependencies
```

config files, archives, no logs, no 40GB

# Example „Citrix NetScaler“ 3/4



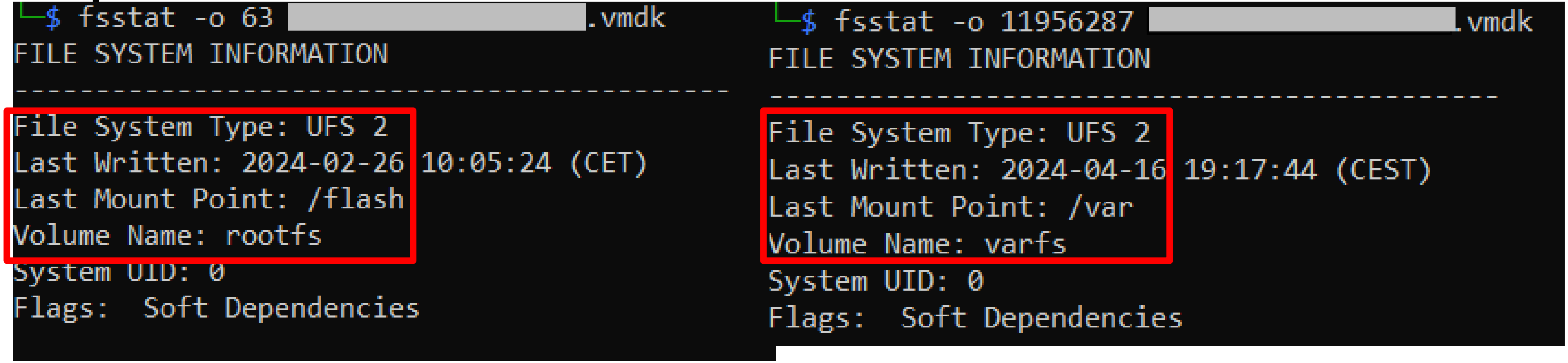
```
└─$ mmls [redacted].vmdk
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
001:  -------   0000000000   0000000062   0000000063   Unallocated
002:  000:000   0000000063   0041943005   0041942943   BSD/386, 386BSD, NetBSD, FreeBSD (0xa5)
003:  -------   0041943006   0041943039   0000000034   Unallocated
└─$ mmls -o 63 [redacted].vmdk
BSD Disk Label
Offset Sector: 63
Units are in 512-byte sectors

      Slot      Start        End          Length       Description
000:  000       0000000000   0003354623   0003354624   4.2BSD (0x07)
001:  002       0000000000   0041942942   0041942943   Unused (0x00)
002:  Meta      0000000001   0000000001   0000000001   Partition Table
003:  001       0003354624   0011952127   0008597504   Swap (0x01)
004:  003       0011952128   0011956223   0000004096   4.2BSD (0x07)
005:  004       0011956224   0041942942   0029986719   4.2BSD (0x07)
006:  -------   0041942943   0041943039   0000000097   Unallocated
```

# Example „Citrix NetScaler“ 4/4

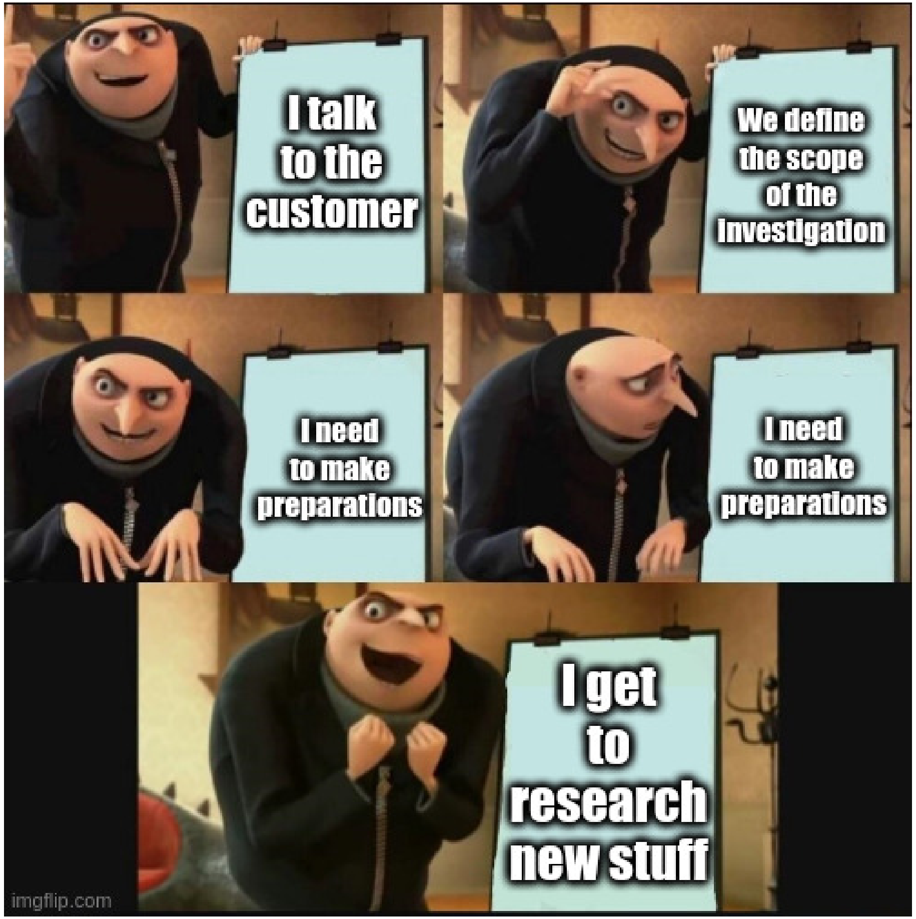
- Nested disk labels reveal another relevant partition



```
└─$ fsstat -o 63 [redacted].vmdk
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: UFS 2
Last Written: 2024-02-26 10:05:24 (CET)
Last Mount Point: /flash
Volume Name: rootfs
System UID: 0
Flags:  Soft Dependencies
```

```
└─$ fsstat -o 11956287 [redacted].vmdk
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: UFS 2
Last Written: 2024-04-16 19:17:44 (CEST)
Last Mount Point: /var
Volume Name: varfs
System UID: 0
Flags:  Soft Dependencies
```

# Preparing an Investigation 1/4


I talk to the customer
We define the scope of the investigation
I need to make preparations
I need to make preparations
I get to research new stuff
imgflip.com

# Preparing an Investigation 2/4

Dear Santa,

Here is my wish list:

public content about forensic investigations

authoritative documentation of the OS

installation media or premade image

Love,

# Preparing an Investigation 3/4

- Check presence of typical elements from other Unix-like operating systems
- Explore live system
  - Content of user home directory
  - Configuration of services / daemons
  - Configuration of jobs / scheduled tasks
  - Standard log location and content

# Preparing an Investigation 4/4

- Condense the information into a form that you can reference during your actual investigation
  - Knowledge base article
  - Investigation procedure
  - Baseline of expectable data

# Our friends along the way 1/2

POSIX standard
reused Open-Source Software
imgflip.com

# Our friends along the way 2/2

- Texteditor & Hexeditor
- TheSleuthKit
- Unix-like Artifact Collector (ht

# Try it yourself

- Try preparing an investigation against an operating system from the BSD family
  - compare your results against „Forensic investigation artifacts on BSD“ (https://github.com/Herbert-Karl/masterthesis)

# Options for contribution

- More blog posts about your investigations (data sources you used and how you used them)
- Extend coverage of Unix-like Artifact Collector for
  - ZOS
  - illumos-based operating systems
  - Haiku

# Question time!

Bsides Munich 2025, Herbert Bärschneider