MVS 21

MAGNET VIRTUAL SUMMIT

MAGNET FORENSICS®

Countering the USB Kill Switch

From Anti-Anti-Forensics, to Surprise, Surprise!

$ whoami

- **Ali Hadi**, Professor @Champlain College
- Research Fellow @Leahy Center for Digital Investigations
- Co-Founder and Research Director @Cyber5W
- 21+ Technical Certificates
- Interested in: DFIR, Adversary Emulation, and Offensive Security
- Have a question? @binaryz0ne

Outline

- Case Background
  - What is USB Kill Switch
  - Related Stories/Projects
  - How USB Kill Switch (USK) Works
  - How to Counter USK
- Case Studies
  - Linux USB Forensics
  - System Shutdown
  - Shutdown + Secure Delete
  - Surprise, Surprise: You Can Run, But We'll Find You!!!
- Findings
- References

Case Background

MVS 21
MAGNET VIRTUAL SUMMIT

Not USBKILL…

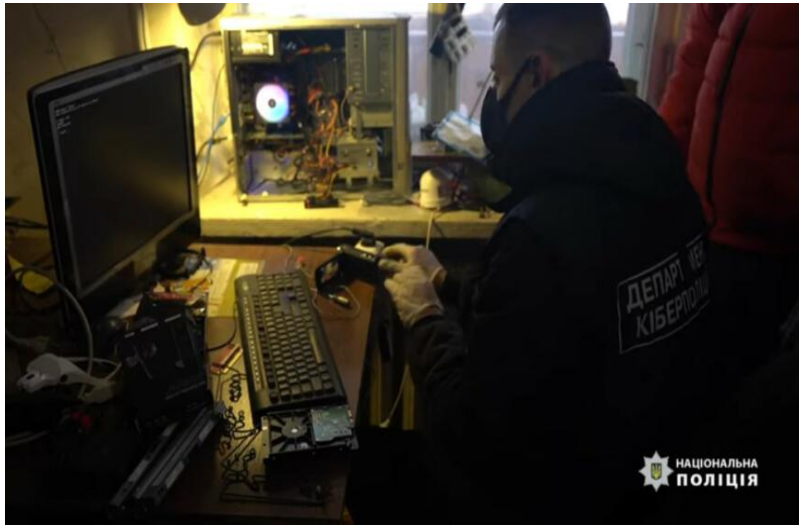
[1]

“The USBKill is a device that stress tests hardware. When plugged in power is taken from a USB-Port, multiplied, and discharged into the data-lines, typically disabling an unprotected device”[1] .

usbkill → The USB Kill Switch (UKS)

A software which can be used for anti-forensics

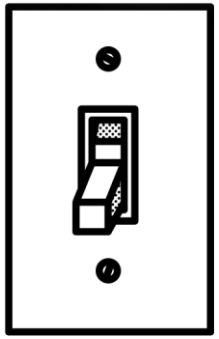
“USBKill is anti-forensic software distributed via GitHub, written in Python for the BSD, Linux, and OS X operating systems. It is designed to serve as a kill switch if the computer on which it is installed should fall under the control of individuals or entities against the desires of the owner. It is free software, available under the GNU General Public License [2]”.



Related Stories...

- The Rise & Fall of Silk Road, https://www.wired.com/2015/05/silk-road-2/
- The FBI staged a lovers' fight to catch the kingpin of the web's biggest illegal drug marketplace, https://www.businessinsider.com/ross-ulbricht-will-be-sentenced-soon--heres-how-he-was-arrested-2015-5?r=US&IR=T
- Police can demand fingerprints but not passcodes to unlock phones, rules judge, https://nakedsecurity.sophos.com/2014/11/03/police-can-demand-fingerprints-but-not-passcodes-to-unlock-phones-rules-judge/

How to Counter UKS?



[4]

- The key is understanding:
  - how it works (UKS behavior)
  - files associated with it (e.g. configuration files)

- By default, config is located by default under /etc named usbkill.ini

UKS Behaviour

The default behavior of the UKS is to shutdown the system.

However, the software is customizable, which means you can define what is to be done or executed before shut down [2, 3, 4].

[5]

UKS Whitelisting ...

It keeps a whitelist of devices that are to connect to the USB ports of the computer.

If a device connects to the computer that is out of the whitelist, it will take actions to protect the device, such as device locking, hard drive encryption, or data wiping [2].

UKS for USB Leakage Prevention

Can also be used to protect your computer by preventing the invisible malware or spyware and preventing unauthorized (or hidden) file copying [1].

[*]

Related Projects

1. **BusKill:** set a udev rule that will be triggered, if the USB drive is removed. The rules can be set to lock, shutdown, or self-destruct of the Laptop [5].

2. **Silk Guardian:** is an anti-forensic Linux Kernel Module (LKM) kill-switch that waits for a change on your usb ports then deletes precious files and turns off your computer [6].

usbkill.ini Configuration

Scrolling through the **usbkill.ini** configuration file

Our focus:

- remove_file_cmd
- files_to_remove
- folders_to_remove
- Custom settings

~ : bash — Konsole

File Edit View Bookmarks Settings Help

```
user1@klinux:~$ cat /etc/usbkill.ini
#
#
# Hephaestos <hephaestos@riseup.net> - 8764 EF6F D5C1 7838 8D10 E061 CF84 9CE5 42D0 B12B
# <https://github.com/hephaest0s/usbkill>
#
# This program is free software: you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation, either version 3 of the License, or
# (at your option) any later version.
#
# This program is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public License
# along with this program. If not, see <http://www.gnu.org/licenses/>.

[config]
```

Case Studies

MVS 21
MAGNET VIRTUAL SUMMIT

Case Studie(s)

1. Linux USB Forensics
2. Shutdown System
3. Shutdown + Secure Delete + Custom config
4. Surprise, Surprise: You Can Run, But We'll Find You!!!

Note(s):

- UKS log file is excluded from investigation
- System used was Kubuntu 20.04

[7]

Linux USB Forensics

Investigating USBs on Linux Systems

MVS 21

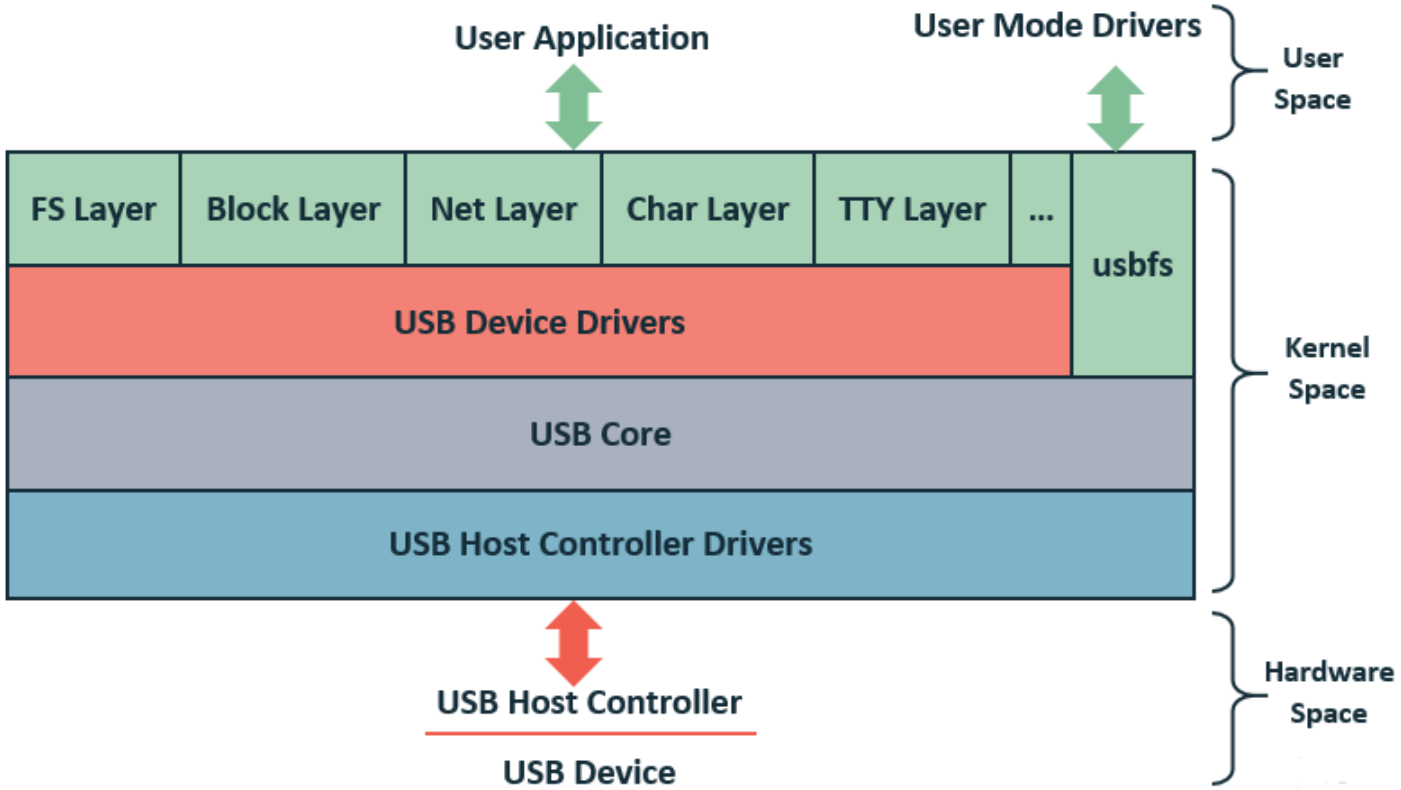
MAGNET VIRTUAL SUMMIT

How Linux Identifies a USB Device

The USB host controller is responsible for detecting a valid USB device in both hardware and kernel spaces of the Linux system regardless of a USB device driver existence:

- Associated host controller driver translates the low-level information of the physical layer into higher level info specific for the USB protocol
- Information is moved to the generic USB core layer in the kernel space
- Detected device is viewed in the user space according to the available drivers, interfaces, and applications (*different and dependent on the Linux distro*)
- To learn more, check "Linux Device Drivers for your Girl Friend" ☺

USB Subsystem in Linux



USB Artifacts of Interest

Main information to look for:

- Serial Numbers
- Manufacturers
- Vendor ID (VID)
- Product ID (PID)
- Date and Time of Connection/Removal

USB Artifacts on Linux vs. Windows

Artifact	Linux	Windows
Date & time of connection	/proc and log files: ● syslog (Debian based) ● messages (Redhat based) ● debug.log ● dmesg ● kern.log ● Journals	Setupapi.dev.log, USBSTOR (Windows Registry)
Vendor ID (VID)		USB (SYSTEM)
Vendor Name		USBSTOR (SYSTEM)
Product ID (PID)		USB (SYSTEM)
Product Name		USBSTOR (SYSTEM)
Manufacturer		MountedDevices
Serial Number		USBSTOR (SYSTEM)
Date & time of disconnection		USBSTOR (SYSTEM)
Others		MountedDevices (SYSTEM), MountPoints2 (NTUSER.DAT), FriendlyName (SOFTWARE), etc

USB Subsystem in Linux

/proc/bus/usb/devices

Multiple lines of output, where each letter represents parts of the USB device specification:

T: Topology

B: Bandwidth

D: Device descriptor information

P: Product ID information

S = String descriptors

C = Configuration descriptor information

I = Interface descriptor information

E = Endpoint descriptor information

USB Subsystem in Linux

- Every valid USB device has one or more configuration, the config is like a profile and Linux only supports one config for each device.
- Each configuration of a device has one or more interfaces. The interface defines the functionality that device provides. For every independent functionality, there is an associated interface.
- For example, a multi-function device (MFD) USB printer that has features of printing, scanning, and faxing, most likely have at least three interfaces, one for each functionality.
- There may be a USB device driver for each interface or one driver for all interfaces.

USB Subsystem in Linux

- Each interface is associated with one or more endpoints. The endpoint serves like a pipe, that transmits information to/from the device the interface, based on the provided functionality.

- Based on the type of the transmitted information, the endpoint type may be:
  - Control: transfer control information, e.g., query information about the device.
  - Interrupt: fast transfer of small data, generally, up to 8 bytes. Examples are serial ports and HIDs.
  - Bulk: slow transfer of relatively big data, e.g., transfer of data for mass storage devices.
  - Isochronous: transfer of big data, such as audio and video.

USB Subsystem in Linux

All endpoints' types can be an in or out direction, determining the direction of the data transfer.

The in indicates the data transfer from the USB device to the machine, while out indicates data transfer from the host machine to the USB device.

However, the control endpoint is bi-directional.

USB Subsystem in Linux

```
E:  Ad=xx(s) Atr=xx(ssss) MxPS=dddd Ivl=dddss
|   |                  |              |                    |__Interval (max) between transfers
|   |                  |              |__EndpointMaxPacketSize
|   |                  |__Attributes(EndpointType)
|   |__EndpointAddress(I=In,O=Out)
|__Endpoint tag
```

```
E:  Ad=81(I) Atr=02(Bulk) MxPS= 512 Ivl=0ms
E:  Ad=02(O) Atr=02(Bulk) MxPS= 512 Ivl=31875us
```

- The Endpoints in the screenshot indicates in and out directions respectively. There addresses (in hex) are 0x81 the first and the second 0x02.
- The MxPs, defines the size of data that can be transferred in a single go.

USB Subsystem in Linux

T refers to the USB device position within the USB tree, represented by <usb bus number, usb tree level, usb port>

D refers to the device descriptor, including its version, class/category, and the number of available configurations for this device.

According to the number of configurations there would be **C** lines, however, in most cases, one line.

USB Subsystem in Linux

C:* #Ifs=dd Cfg#=dd Atr=xx MPwr=dddmA

| | | | | |__MaxPower in mA

| | | | |__Attributes

| | | |__ConfigurationNumber

| | |__NumberOfInterfaces (determines how many “I” lines there will be)

| |__ "*" indicates the active configuration (others are " ")

|__Config info tag

```
C:  #Ifs= 1 Cfg#= 1 Atr=80 MxPwr=200mA
```

C refers to the configuration descriptor and includes number of interfaces under this configuration, the configuration index, device attributes, and maximum power for this configuration.

USB Subsystem in Linux

```
I:* If#=dd Alt=dd #EPs=dd Cls=xx(sssss) Sub=xx Prot=xx Driver=ssss
| | |        |         |         |                     |         |          |__Driver name or "(none)"
| | |        |         |         |                     |         |
| | |        |         |         |                     |         |__InterfaceProtocol
| | |        |         |         |                 |__InterfaceSubClass
| | |        |         |         |__InterfaceClass
| | |        |         |__NumberOfEndpoints (determine number of “E” lines)
| | |        |__AlternateSettingNumber
| | |__InterfaceNumber
| |__ "*" indicates the active altsetting (others are " ")
|__Interface info tag
```

USB Subsystem in Linux

- The “Driver=…” entry indicates the interface to driver mapping
- If the value is “(none)”, this indicates that there is no associated driver.

```
P:  Vendor=0930 ProdID=6544 Rev=01.00
S:  Manufacturer=TOSHIBA
S:  Product=TransMemory
S:  SerialNumber=147227C8183FCE11994C0B48
C:  #Ifs= 1 Cfg#= 1 Atr=80 MxPwr=200mA
I:  If#=0x0 Alt= 0 #EPs= 2 Cls=08(stor.) Sub=06 Prot=50 Driver=usb-storage
```

USB Subsystem in Linux

P: Vendor=xxxx ProdID=xxxx Rev=xx.xx

| | | |__Product revision number

| | |__Product ID code

| |__Vendor ID code

|__Device tag #2

```
P:  Vendor=0930 ProdID=6544 Rev=01.00
```

USB Subsystem in Linux

S: Manufacturer=ssss

| |__The device manufacturer name, read from the device.

|

S: Product=ssss

| |__The device product description, read from the device.

|

S: SerialNumber=ssss

| |__The device serial Number, read from the device.

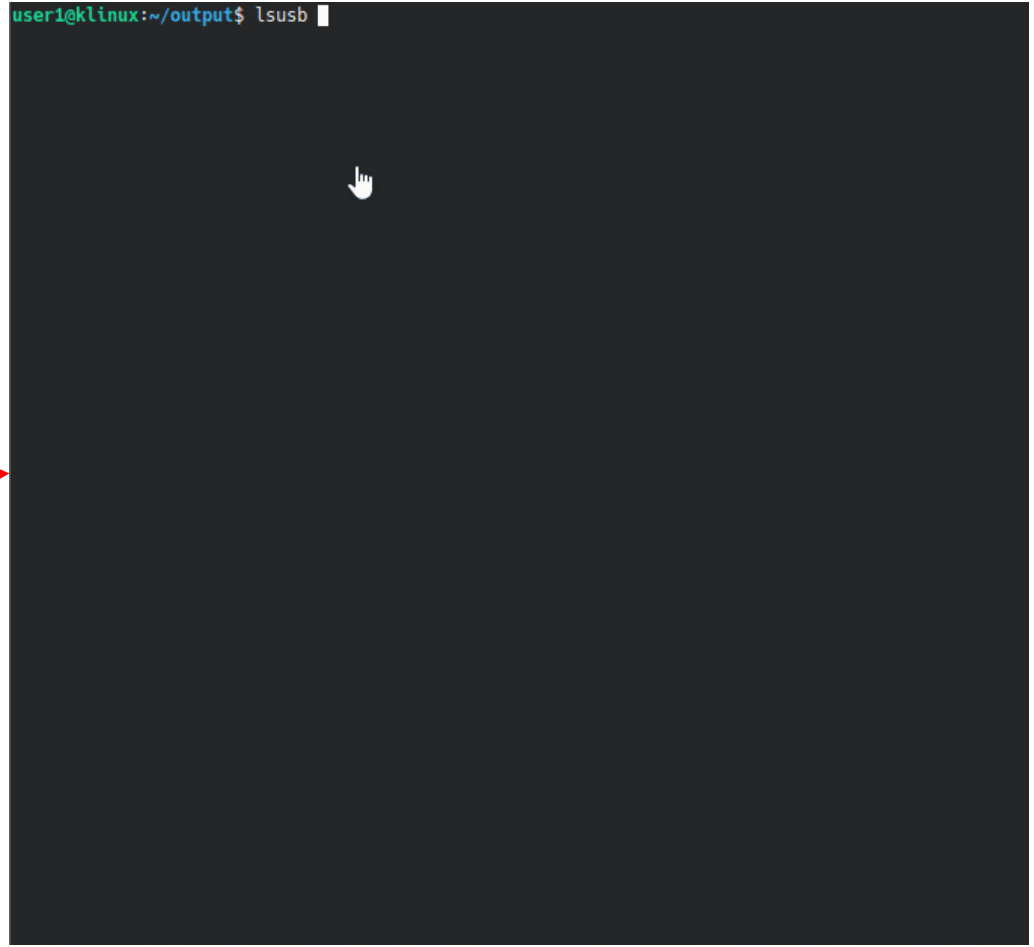
|

|__String info tag

```
S:  Manufacturer=TOSHIBA
S:  Product=TransMemory
S:  SerialNumber=147227C8183FCE11994C0B48
```

USB Device Artifacts on Linux

lsusb



After the word “ID”, the numbers pair represents the Vendor ID and Product ID. These numbers can be checked online.

DeviceHunt

Check the Vendor ID and Product ID (aka Device ID)

https://devicehunt.com/

Type	Vendor ID	Device ID
USB	0930	6544

Device Details

TransMemory-Mini / Kingston DataTraveler 2.0 Stick

Type	Information
ID	6544

Vendor Details

Toshiba Corp.

Type	Information
ID	0930

Type	Vendor ID	Vendor Name	Device ID	Device Name
USB	0930	Toshiba Corp.	6544	TransMemory-Mini / Kingston DataTraveler 2.0 Stick

Search for Vendor ID

/var/log/syslog

```
user1@klinux:~/output$
```

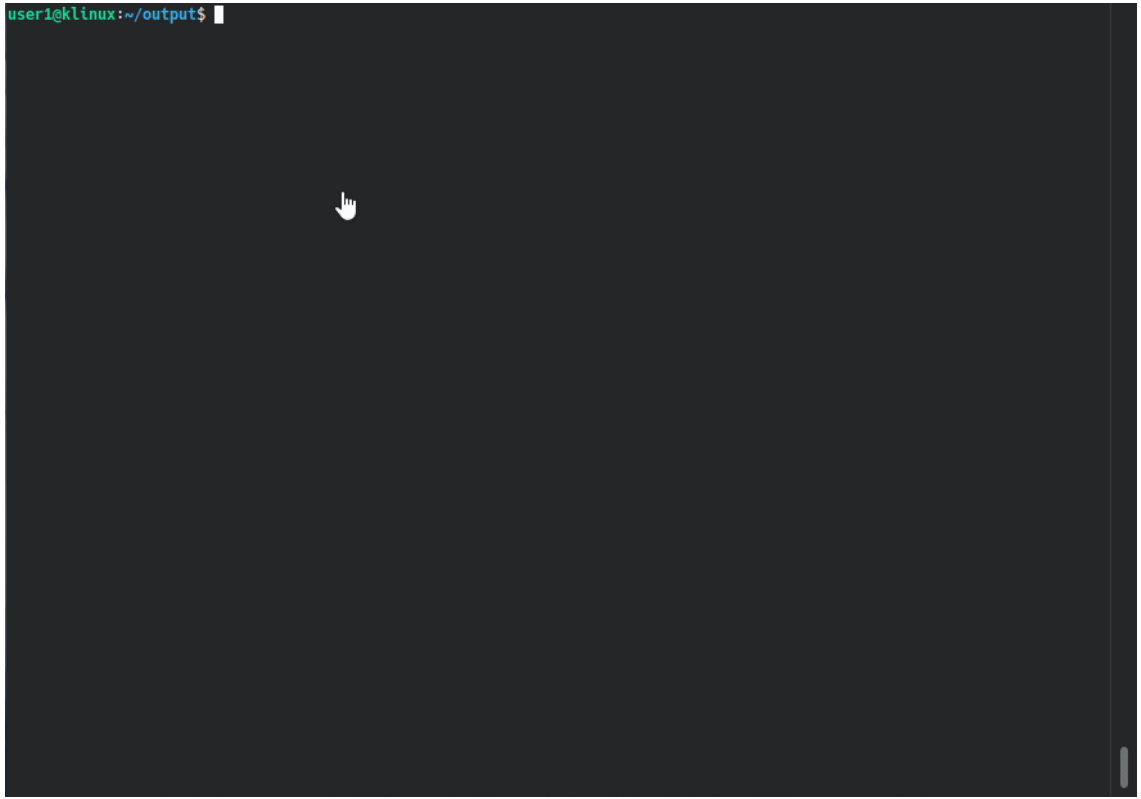
USB Device Artifacts on Linux

usb-devices shellscript

```
user1@klinux:~/output$
```

USB Device Artifacts on Linux

/sys/bus/usb/devices/



USB Device Artifacts on Linux

cat /sys/kernel/debug/usb/devices

Kernel 2.6.31+

```
T:  Bus=01 Lev=01 Prnt=01 Port=00 Cnt=01 Dev#=  2 Spd=480  MxCh= 0
D:  Ver= 2.00 Cls=00(>ifc ) Sub=00 Prot=00 MxPS=64 #Cfgs=  1
P:  Vendor=0930 ProdID=6544 Rev= 1.00
S:  Manufacturer=TOSHIBA
S:  Product=TransMemory
S:  SerialNumber=147227C8183FCE11994C0B48
C:* #Ifs= 1 Cfg#= 1 Atr=80 MxPwr=200mA
I:* If#= 0 Alt= 0 #EPs= 2 Cls=08(stor.) Sub=06 Prot=50 Driver=usb-storage
E:  Ad=81(I) Atr=02(Bulk) MxPS= 512 Ivl=0ms
E:  Ad=02(O) Atr=02(Bulk) MxPS= 512 Ivl=31875us
```

Usbrip

sudo -H python3 -m pip install --upgrade usbrip

```
user1@klinux:~$
user1@klinux:~$ usbrip events history

          _      {{4}}    {v2.2.2-1}
 _ _ ___| |_ ___[ ]___
| | |_ -| . |  _[ ] . |
|___|___|___|_| [ ]  _|
               x[ ]_|   https://github.com/snovvcrash/usbrip


[*] Started at 2021-04-16 19:55:02
[19:55:02] [INFO] Trying to run journalctl...
[19:55:02] [INFO] Successfully runned journalctl
[19:55:02] [INFO] Reading journalctl output
100%|                                        | 8295/8295 [00:00<00:00, 396044.89line/s]
[?] How would you like your event history list to be generated?

    1. Terminal stdout
    2. JSON-file

[>] Please enter the number of your choice (default 1): 1
```

[12,13]

```
-----------------------------------------------
Connected:      2021-04-15 21:45:09
Host:           klinux
VID:            0930
PID:            6544
Product:        TransMemory
Manufacturer:   TOSHIBA
Serial Number:  147227C8183FCE11994C0B48
Bus-Port:       1-1
Disconnected:   ∅
-----------------------------------------------
```

```
-----------------------------------------------
Connected:      2021-04-16 13:26:59
Host:           klinux
VID:            0930
PID:            6544
Product:        TransMemory
Manufacturer:   TOSHIBA
Serial Number:  147227C8183FCE11994C0B48
Bus-Port:       1-1
Disconnected:   2021-04-16 19:57:07
-----------------------------------------------
```

System Shutdown

aka poweroff

MVS 21
MAGNET VIRTUAL SUMMIT

Case #1: Shutdown System

Understand how normal shutdowns happen and what goes with it, then compare with how an unexpected shutdown event

During a normal shutdown, the system will:

1. Stop the file system journal
2. Stop processes and services
3. Unmount the file system
4. Log that the system is shutting down/rebooting regardless whether it was due to Power key being pressed by the user, a failure in hardware, temperature, or even shutting down in order

Most of those events will not happen during an abnormal shutdown event!!

Case #1: Shutdown System

Normal shutdown

```
Apr 20 22:22:41 klinux systemd[1]: Stopping User Manager for UID 120...
Apr 20 22:22:41 klinux systemd[1046]: Stopped target Main User Target.
Apr 20 22:22:41 klinux systemd[1046]: Stopping D-Bus User Message Bus...
Apr 20 22:22:41 klinux systemd[1046]: dbus.service: Succeeded.
Apr 20 22:22:41 klinux systemd[1046]: Stopped D-Bus User Message Bus.
Apr 20 22:22:41 klinux systemd[1046]: Stopped target Basic System.
Apr 20 22:22:41 klinux systemd[1046]: Stopped target Paths.
Apr 20 22:22:41 klinux systemd[1046]: Stopped target Sockets.
Apr 20 22:22:41 klinux systemd[1046]: Stopped target Timers.
Apr 20 22:22:41 klinux systemd[1046]: dbus.socket: Succeeded.
Apr 20 22:22:41 klinux systemd[1046]: Closed D-Bus User Message Bus Socket.
Apr 20 22:22:41 klinux systemd[1046]: dirmngr.socket: Succeeded.
Apr 20 22:22:41 klinux systemd[1046]: Closed GnuPG network certificate management daemon.
Apr 20 22:22:41 klinux systemd[1046]: gpg-agent-browser.socket: Succeeded.
Apr 20 22:22:41 klinux systemd[1046]: Closed GnuPG cryptographic agent and passphrase cache (access for web browsers).
Apr 20 22:22:41 klinux systemd[1046]: gpg-agent-extra.socket: Succeeded.
Apr 20 22:22:41 klinux systemd[1046]: Closed GnuPG cryptographic agent and passphrase cache (restricted).
Apr 20 22:22:41 klinux systemd[1046]: gpg-agent-ssh.socket: Succeeded.
Apr 20 22:22:41 klinux systemd[1046]: Closed GnuPG cryptographic agent (ssh-agent emulation).
Apr 20 22:22:41 klinux systemd[1046]: gpg-agent.socket: Succeeded.
Apr 20 22:22:41 klinux systemd[1046]: Closed GnuPG cryptographic agent and passphrase cache.
Apr 20 22:22:41 klinux systemd[1046]: pk-debconf-helper.socket: Succeeded.
Apr 20 22:22:41 klinux systemd[1046]: Closed debconf communication socket.
Apr 20 22:22:41 klinux systemd[1046]: pulseaudio.socket: Succeeded.
Apr 20 22:22:41 klinux systemd[1046]: Closed Sound System.
Apr 20 22:22:41 klinux systemd[1046]: snapd.session-agent.socket: Succeeded.
Apr 20 22:22:41 klinux systemd[1046]: Closed REST API socket for snapd user session agent.
Apr 20 22:22:41 klinux systemd[1046]: Reached target Shutdown.
Apr 20 22:22:41 klinux systemd[1046]: systemd-exit.service: Succeeded.
Apr 20 22:22:41 klinux systemd[1046]: Finished Exit the Session.
Apr 20 22:22:41 klinux systemd[1046]: Reached target Exit the Session.
Apr 20 22:22:41 klinux systemd[1]: user@120.service: Succeeded.
Apr 20 22:22:41 klinux systemd[1]: Stopped User Manager for UID 120.
Apr 20 22:22:41 klinux systemd[1]: Stopping User Runtime Directory /run/user/120...
Apr 20 22:22:41 klinux systemd[1176]: run-user-120.mount: Succeeded.
Apr 20 22:22:41 klinux systemd[1]: run-user-120.mount: Succeeded.
Apr 20 22:22:41 klinux systemd[1]: user-runtime-dir@120.service: Succeeded.
Apr 20 22:22:41 klinux systemd[1]: Stopped User Runtime Directory /run/user/120.
Apr 20 22:22:41 klinux systemd[1]: Removed slice User Slice of UID 120.
```

Case #1: Shutdown System

Normal reboot

```
Apr 20 22:25:01 klinux systemd[1]: Stopping User Manager for UID 120...
Apr 20 22:25:01 klinux systemd[1050]: Stopped target Main User Target.
Apr 20 22:25:01 klinux systemd[1050]: Stopping D-Bus User Message Bus...
Apr 20 22:25:01 klinux systemd[1050]: dbus.service: Succeeded.
Apr 20 22:25:01 klinux systemd[1050]: Stopped D-Bus User Message Bus.
Apr 20 22:25:01 klinux systemd[1050]: Stopped target Basic System.
Apr 20 22:25:01 klinux systemd[1050]: Stopped target Paths.
Apr 20 22:25:01 klinux systemd[1050]: Stopped target Sockets.
Apr 20 22:25:01 klinux systemd[1050]: Stopped target Timers.
Apr 20 22:25:01 klinux systemd[1050]: dbus.socket: Succeeded.
Apr 20 22:25:01 klinux systemd[1050]: Closed D-Bus User Message Bus Socket.
Apr 20 22:25:01 klinux systemd[1050]: dirmngr.socket: Succeeded.
Apr 20 22:25:01 klinux systemd[1050]: Closed GnuPG network certificate management daemon.
Apr 20 22:25:01 klinux systemd[1050]: gpg-agent-browser.socket: Succeeded.
Apr 20 22:25:01 klinux systemd[1050]: Closed GnuPG cryptographic agent and passphrase cache (access for web browsers).
Apr 20 22:25:01 klinux systemd[1050]: gpg-agent-extra.socket: Succeeded.
Apr 20 22:25:01 klinux systemd[1050]: Closed GnuPG cryptographic agent and passphrase cache (restricted).
Apr 20 22:25:01 klinux systemd[1050]: gpg-agent-ssh.socket: Succeeded.
Apr 20 22:25:01 klinux systemd[1050]: Closed GnuPG cryptographic agent (ssh-agent emulation).
Apr 20 22:25:01 klinux systemd[1050]: gpg-agent.socket: Succeeded.
Apr 20 22:25:01 klinux systemd[1050]: Closed GnuPG cryptographic agent and passphrase cache.
Apr 20 22:25:01 klinux systemd[1050]: pk-debconf-helper.socket: Succeeded.
Apr 20 22:25:01 klinux systemd[1050]: Closed debconf communication socket.
Apr 20 22:25:01 klinux systemd[1050]: pulseaudio.socket: Succeeded.
Apr 20 22:25:01 klinux systemd[1050]: Closed Sound System.
Apr 20 22:25:01 klinux systemd[1050]: snapd.session-agent.socket: Succeeded.
Apr 20 22:25:01 klinux systemd[1050]: Closed REST API socket for snapd user session agent.
Apr 20 22:25:01 klinux systemd[1050]: Reached target Shutdown.
Apr 20 22:25:01 klinux systemd[1050]: systemd-exit.service: Succeeded.
Apr 20 22:25:01 klinux systemd[1050]: Finished Exit the Session.
Apr 20 22:25:01 klinux systemd[1050]: Reached target Exit the Session.
Apr 20 22:25:01 klinux systemd[1]: user@120.service: Succeeded.
Apr 20 22:25:01 klinux systemd[1]: Stopped User Manager for UID 120.
Apr 20 22:25:01 klinux systemd[1]: Stopping User Runtime Directory /run/user/120...
Apr 20 22:25:01 klinux systemd[1131]: run-user-120.mount: Succeeded.
Apr 20 22:25:01 klinux systemd[1]: run-user-120.mount: Succeeded.
Apr 20 22:25:01 klinux systemd[1]: user-runtime-dir@120.service: Succeeded.
Apr 20 22:25:01 klinux systemd[1]: Stopped User Runtime Directory /run/user/120.
Apr 20 22:25:01 klinux systemd[1]: Removed slice User Slice of UID 120.
```

Case #1: Shutdown System

boot.log file

After starting the system, we shall see a clean check of the file system and the date it was powered back on!

```
------------ Tue Apr 20 22:24:16 EEST 2021 ------------
/dev/sda5: clean, 237205/1605632 files, 2181010/6421760 blocks
[  OK  ] Finished Create Volatile Files and Directories.
         Starting Network Name Resolution...
         Starting Network Time Synchronization...
         Starting Update UTMP about System Boot/Shutdown...
[  OK  ] Finished Update UTMP about System Boot/Shutdown.
[  OK  ] Finished Load AppArmor profiles.
[  OK  ] Started Entropy daemon using the HAVEGE algorithm.
         Starting Load AppArmor profiles managed internally by snapd...
[  OK  ] Finished Load AppArmor profiles managed internally by snapd.
[  OK  ] Started Network Time Synchronization.
[  OK  ] Reached target System Initialization.
[  OK  ] Started ACPI Events Check.
[  OK  ] Started CUPS Scheduler.
[  OK  ] Started Daily Cleanup of Temporary Directories.
[  OK  ] Reached target Paths.
[  OK  ] Reached target System Time Set.
[  OK  ] Reached target System Time Synchronized.
[  OK  ] Started Trigger anacron every hour.
[  OK  ] Started Daily apt download activities.
[  OK  ] Started Daily apt upgrade and clean activities.
[  OK  ] Started Periodic ext4 Online Metadata Check for All Filesystems.
[  OK  ] Started Discard unused blocks once a week.
[  OK  ] Started Refresh fwupd metadata regularly.
[  OK  ] Started Daily rotation of log files.
[  OK  ] Started Daily man-db regeneration.
[  OK  ] Started Message of the Day.
```

Seats!

- “A seat consists of all hardware devices assigned to a specific workplace.”
- The system will log “New seat seat0” which indicates that the login manager started successfully on the system
- When the system service starts, it will create the default seat which is seat0
- If a successful shutdown/reboot happened, then there will be an entry indicating that and will see a seat being created after that once the system powers up again
- We can use **journalctl** for this:

$ journalctl -D /var/log/journal/ SEAT_ID=seat0

New Seats: Shutdown vs Rebooting System

Shutdown

```
Apr 18 11:21:35 klinux systemd-logind[654]: System is powering down.
Apr 20 20:02:26 klinux systemd-logind[655]: New seat seat0.
Apr 20 20:02:26 klinux systemd-logind[655]: Watching system buttons on /dev/input/event0 (Power Button)
Apr 20 20:02:26 klinux systemd-logind[655]: Watching system buttons on /dev/input/event1 (AT Translated Set 2 keyboard)
Apr 20 20:02:27 klinux sddm-helper: pam_unix(sddm-greeter:session): session opened for user sddm by (uid=0)
Apr 20 20:02:27 klinux systemd-logind[655]: New session 1 of user sddm.
Apr 20 20:02:27 klinux systemd: pam_unix(systemd-user:session): session opened for user sddm by (uid=0)
Apr 20 20:02:53 klinux dbus-daemon[618]: [system] Failed to activate service 'org.bluez': timed out (service_start_timeout=25000ms)
Apr 20 20:02:57 klinux sddm-helper: pam_kwallet5(sddm:auth): (null): pam_sm_authenticate
Apr 20 20:02:57 klinux sddm-helper: pam_kwallet5(sddm:setcred): pam_kwallet5: pam_sm_setcred
Apr 20 20:02:57 klinux sddm-helper: pam_unix(sddm:session): session opened for user user1 by (uid=0)
Apr 20 20:02:57 klinux systemd-logind[655]: New session 3 of user user1.
```

Rebooting

```
Apr 20 22:11:18 klinux systemd-logind[658]: System is rebooting.
Apr 20 22:11:39 klinux systemd-logind[659]: New seat seat0.
Apr 20 22:11:39 klinux systemd-logind[659]: Watching system buttons on /dev/input/event0 (Power Button)
Apr 20 22:11:39 klinux systemd-logind[659]: Watching system buttons on /dev/input/event1 (AT Translated Set 2 keyboard)
Apr 20 22:11:40 klinux sddm-helper: pam_unix(sddm-greeter:session): session opened for user sddm by (uid=0)
Apr 20 22:11:40 klinux systemd-logind[659]: New session 1 of user sddm.
Apr 20 22:11:40 klinux systemd: pam_unix(systemd-user:session): session opened for user sddm by (uid=0)
Apr 20 22:11:49 klinux sddm-helper: pam_kwallet5(sddm:auth): (null): pam_sm_authenticate
Apr 20 22:11:49 klinux sddm-helper: pam_kwallet5(sddm:setcred): pam_kwallet5: pam_sm_setcred
Apr 20 22:11:49 klinux sddm-helper: pam_unix(sddm:session): session opened for user user1 by (uid=0)
Apr 20 22:11:49 klinux systemd-logind[659]: New session 3 of user user1.
Apr 20 22:11:49 klinux systemd: pam_unix(systemd-user:session): session opened for user user1 by (uid=0)
```

Booting with No Previous Shutdown!

We can see the system is booting, but there was no shutdown routine before, only a USB being recognized by the system

```
Apr 21 11:08:59 klinux kernel: [45006.395526] usb 4-1: USB disconnect, device number 2
Apr 21 11:09:28 klinux kernel: [45035.404053] usb 4-1: new SuperSpeed Gen 1 USB device number 3 using xhci_hcd
Apr 21 11:09:28 klinux kernel: [45035.429617] usb 4-1: New USB device found, idVendor=13fe, idProduct=6300, bcdDevice= 1.00
Apr 21 11:09:28 klinux kernel: [45035.429620] usb 4-1: New USB device strings: Mfr=1, Product=2, SerialNumber=3
Apr 21 11:09:28 klinux kernel: [45035.429622] usb 4-1: Product: USB DISK 3.0
Apr 21 11:09:28 klinux kernel: [45035.429624] usb 4-1: Manufacturer:
Apr 21 11:09:28 klinux kernel: [45035.429625] usb 4-1: SerialNumber: 072096C56611C059
Apr 21 11:09:28 klinux kernel: [45035.438850] usb-storage 4-1:1.0: USB Mass Storage device detected
Apr 21 11:09:28 klinux kernel: [45035.440661] scsi host33: usb-storage 4-1:1.0
Apr 21 11:09:28 klinux mtp-probe: checking bus 4, device 3: "/sys/devices/pci0000:00/0000:00:15.0/0000:03:00.0/usb4/4-1"
Apr 21 11:09:28 klinux mtp-probe: bus: 4, device: 3 was not an MTP device
Apr 21 11:09:28 klinux mtp-probe: checking bus 4, device 3: "/sys/devices/pci0000:00/0000:00:15.0/0000:03:00.0/usb4/4-1"
Apr 21 11:09:28 klinux mtp-probe: bus: 4, device: 3 was not an MTP device
Apr 21 11:09:54 klinux kernel: [    0.000000] Linux version 5.4.0-72-generic (buildd@lcy01-amd64-019) (gcc version 9.3.0 (Ubuntu 9.3.0-17ubuntu1~20.04)) #80-Ubuntu SMP Mon Apr 12 17:35:00 UTC 2021 (Ubuntu 5.4.0-72.80-generic 5.4.101)
Apr 21 11:09:54 klinux kernel: [    0.000000] Command line: BOOT_IMAGE=/boot/vmlinuz-5.4.0-72-generic root=UUID=13017bf2-5ce8-485d-954b-f17a94095d0f ro quiet splash
Apr 21 11:09:54 klinux kernel: [    0.000000] KERNEL supported cpus:
Apr 21 11:09:54 klinux kernel: [    0.000000]   Intel GenuineIntel
Apr 21 11:09:54 klinux kernel: [    0.000000]   AMD AuthenticAMD
Apr 21 11:09:54 klinux kernel: [    0.000000]   Hygon HygonGenuine
Apr 21 11:09:54 klinux kernel: [    0.000000]   Centaur CentaurHauls
Apr 21 11:09:54 klinux kernel: [    0.000000]   zhaoxin   Shanghai
```

No Shutdown!

Kernel Booting

Shutdown + Secure Delete (srm)

Subtitle

MVS 21
MAGNET VIRTUAL SUMMIT

Case #2: Shutdown + Secure Delete

- Shutdown is the default activity that UKS does, so we'll check the rest
- srm command syntax used

```
# use srm to remove files.
# Check srm --help for available options
##remove_file_cmd = srm -l
remove_file_cmd = srm -l -r -z
```

- Folders to be removed

```
# What folders should be removed upon a kill?
# Provide absolute paths to the files (paths that start with '/' or '~').
# Content in folders will be removed recursively
# Use " not ' to define the strings, e.g.:
# folders_to_remove = ["~/Desktop/sensitive/", "~/Desktop/dpr_journal_entries/"]
folders_to_remove = ["/home/user1/Documents/","/home/user1/secret/"]
```

Case #2: Shutdown + Secure Delete

```
SRM(1)                                General Commands Manual                                SRM(1)

NAME
       srm - secure remove (secure_deletion toolkit)

SYNOPSIS
       srm [-d] [-f] [-l] [-l] [-r] [-v] [-z] files

DESCRIPTION
       srm is designed to delete data on mediums in a secure manner which can not be recovered by thieves, law enforcement
       or other threats.  The wipe algorythm is based on the paper "Secure Deletion of Data from Magnetic and  Solid-State
       Memory"  presented  at  the  6th Usenix Security Symposium by Peter Gutmann, one of the leading civilian cryptogra-
       phers.

       The secure data deletion process of srm goes like this:

       *      1 pass with 0xff

       *      5 random passes. /dev/urandom is used for a secure RNG if available.

       *      27 passes with special values defined by Peter Gutmann.

       *      5 random passes. /dev/urandom is used for a secure RNG if available.

       *      Rename the file to a random value

       *      Truncate the file
 Manual page srm(1) line 1 (press h for help or q to quit)
```

Case #2: Shutdown + Secure Delete

usbkill running as seen in file system timeline activity (fls+mactime)

1219	.a..	r/rrwxr-xr-x	1000	1000	1057974	/home/user1/Downloads/usbkill/usbkill.sh
24240	.a..	r/rrw-r--r--	0	0	1181100	/usr/lib/python3.8/__pycache__/platform.cpython-38.pyc
45718	.a..	r/rrw-r--r--	0	0	1188712	/usr/lib/python3.8/__pycache__/configparser.cpython-38.pyc
56978	.a..	r/rrw-r--r--	0	0	1188713	/usr/lib/python3.8/__pycache__/datetime.cpython-38.pyc
174	.a..	r/rrw-r--r--	0	0	286166	/home/user1/Downloads/usbkill/usbkill/__pycache__/__init__.cpython-38.pyc
174	.a..	r/rrw-r--r--	0	0	286166	/var/cache/apt/archives/python3-apt_2.0.0ubuntu0.20.04.2_amd64.deb (deleted-realloc)
10384	.a..	r/rrw-r--r--	0	0	286167	/home/user1/Downloads/usbkill/usbkill/__pycache__/usbkill.cpython-38.pyc
10384	.a..	r/rrw-r--r--	0	0	286167	/home/user1/Downloads/usbkill/usbkill/__pycache__/usbkill.cpython-38.pyc.139703412226608 (deleted-realloc)
5071	.a..	r/rrw-rw-r--	0	0	786644	/etc/usbkill.ini

Another output (log2timeline)

Last Access Time	FILE	OS Last Access Time	OS:/home/tsurugi/Desktop/mvs2021/root/home/user1/Downloads/usbkill/usbkill/__pycache__/usbkill.cpython-38.pyc Type: file
Last Access Time	FILE	OS Last Access Time	OS:/home/tsurugi/Desktop/mvs2021/root/home/user1/Downloads/usbkill/usbkill.sh Type: file
Last Access Time	FILE	OS Last Access Time	OS:/home/tsurugi/Desktop/mvs2021/root/home/user1/Downloads/usbkill/usbkill/__pycache__/__init__.cpython-38.pyc Type: file
Last Access Time	FILE	OS Last Access Time	OS:/home/tsurugi/Desktop/mvs2021/root/usr/lib/python3.8/__pycache__/platform.cpython-38.pyc Type: file
Last Access Time	FILE	OS Last Access Time	OS:/home/tsurugi/Desktop/mvs2021/root/usr/lib/python3.8/__pycache__/configparser.cpython-38.pyc Type: file
Content Modification Time	FILE	OS Content Modification Time	OS:/home/tsurugi/Desktop/mvs2021/root/var/log/auth.log Type: file
Metadata Modification Time	FILE	OS Metadata Modification Time	OS:/home/tsurugi/Desktop/mvs2021/root/var/log/auth.log Type: file
Last Access Time	FILE	OS Last Access Time	OS:/home/tsurugi/Desktop/mvs2021/root/etc/usbkill.ini Type: file
Last Access Time	FILE	OS Last Access Time	OS:/home/tsurugi/Desktop/mvs2021/root/usr/lib/python3.8/__pycache__/datetime.cpython-38.pyc Type: file
Content Modification Time	LOG	systemd-journal	klinux [sudo pid: 1501] pam_unix(sudo:auth): Couldn't open /etc/securetty: No such file or directory
Content Modification Time	LOG	systemd-journal	klinux [sudo pid: 1501] user1 : TTY=pts/1 ; PWD=/home/user1 ; USER=root ; COMMAND=/home/user1/Downloads/usbkill/usbkill.sh
Content Modification Time	LOG	systemd-journal	klinux [sudo pid: 1501] pam_unix(sudo:session): session opened for user root by (uid=0)
Content Modification Time	FILE	OS Content Modification Time	OS:/home/tsurugi/Desktop/mvs2021/root/var/log/journal/c6f62e7af663460b86b40138ad3947e4/user-1000.journal Type: file
Metadata Modification Time	FILE	OS Metadata Modification Time	OS:/home/tsurugi/Desktop/mvs2021/root/var/log/journal/c6f62e7af663460b86b40138ad3947e4/user-1000.journal Type: file

All results have been filtered for brevity

USB is Plugged into the System

Content Modification Time	LOG	systemd-journal	klinux [kernel] usb 4-1: new SuperSpeed Gen 1 USB device number 2 using xhci_hcd
Content Modification Time	LOG	systemd-journal	klinux [kernel] usb 4-1: New USB device found idVendor=13fe idProduct=6300 bcdDevice= 1.00
Content Modification Time	LOG	systemd-journal	klinux [kernel] usb 4-1: New USB device strings: Mfr=1 Product=2 SerialNumber=3
Content Modification Time	LOG	systemd-journal	klinux [kernel] usb 4-1: Product: USB DISK 3.0
Content Modification Time	LOG	systemd-journal	klinux [kernel] usb 4-1: Manufacturer:
Content Modification Time	LOG	systemd-journal	klinux [kernel] usb 4-1: SerialNumber: 072096C56611C059
Content Modification Time	LOG	systemd-journal	klinux [mtp-probe pid: 1571] checking bus 4 device 2: "/sys/devices/pci0000:00/0000:00:15.0/0000:03:00.0/usb4/4-1"
Content Modification Time	LOG	systemd-journal	klinux [mtp-probe pid: 1571] bus: 4 device: 2 was not an MTP device
Content Modification Time	LOG	systemd-journal	klinux [kernel] usb-storage 4-1:1.0: USB Mass Storage device detected
Content Modification Time	LOG	systemd-journal	klinux [kernel] scsi host33: usb-storage 4-1:1.0
Content Modification Time	LOG	systemd-journal	klinux [kernel] usbcore: registered new interface driver usb-storage
Content Modification Time	LOG	systemd-journal	klinux [kernel] usbcore: registered new interface driver uas
Content Modification Time	LOG	systemd-journal	klinux [mtp-probe pid: 1581] checking bus 4 device 2: "/sys/devices/pci0000:00/0000:00:15.0/0000:03:00.0/usb4/4-1"
Content Modification Time	LOG	systemd-journal	klinux [mtp-probe pid: 1581] bus: 4 device: 2 was not an MTP device
Content Modification Time	LOG	Log File	[NetworkManager pid: 623] <info> [1619396544.8881] NetworkManager (version 1.22.10) is starting... (for the first time)
Content Modification Time	LOG	Log File	[NetworkManager pid: 623] <info> [1619396544.8885] Read config: /etc/NetworkManager/NetworkManager.conf (lib: 10-c

srm in action

files getting wiped

0	m.c.	-/rrw-r--r--	1000	1000	1057937	/$OrphanFiles/OrphanFile-1057937 (deleted)
0	m.c.	r/rrw-rw-r--	1000	1000	1057969	/home/user1/Documents/top3.jpeg (deleted)
0	m.c.	r/rrw-rw-r--	1000	1000	1057970	/home/user1/Documents/tkctzdfijbc.xng (deleted)
0	m.c.	r/rrw-rw-r--	1000	1000	1057970	/home/user1/Documents/top-secret1.png (deleted)
0	m.c.	r/rrw-rw-r--	1000	1000	1057971	/home/user1/Documents/nani.gmzz (deleted)
0	m.c.	-/rrw-rw-r--	1000	1000	1057972	/$OrphanFiles/OrphanFile-1057972 (deleted)
0	m.c.	r/rrw-rw-r--	1000	1000	1057973	/home/user1/Documents/top4.jpeg (deleted)
0	m.c.	r/rrw-rw-r--	1000	1000	1057977	/home/user1/Documents/top5.jpeg (deleted)
22656	.a..	r/rrwxr-xr-x	0	0	1187241	/usr/bin/srm
0	mac.	d/drwxrwxr-x	1000	1000	1332123	/home/user1/secrets (deleted)
0	m.c.	-/rrw-rw-r--	1000	1000	1332124	/$OrphanFiles/OrphanFile-1332124 (deleted)
0	m.c.	-/rrw-rw-r--	1000	1000	1332125	/$OrphanFiles/OrphanFile-1332125 (deleted)
0	m.c.	-/rrw-rw-r--	1000	1000	1332126	/$OrphanFiles/OrphanFile-1332126 (deleted)
0	m.c.	-/rrw-r--r--	1000	1000	1332127	/$OrphanFiles/OrphanFile-1332127 (deleted)
0	m.c.	-/rrw-rw-r--	1000	1000	1332128	/$OrphanFiles/OrphanFile-1332128 (deleted)
0	m.c.	-/rrw-rw-r--	1000	1000	1332129	/$OrphanFiles/OrphanFile-1332129 (deleted)
0	m.c.	-/rrw-rw-r--	1000	1000	1332130	/$OrphanFiles/OrphanFile-1332130 (deleted)
8388608	m.c.	r/rrw-r-----	0	101	1450339	/var/log/journal/c6f62e7af663460b86b40138ad3947e4/system.journal
2448	m.c.	r/rrw-r--r--	0	0	555917	/var/log/usbkill/usbkill.log
292392	m.c.	r/rrw-r-----	104	4	556615	/var/log/syslog
177715	m.c.	r/rrw-r-----	104	4	556616	/var/log/kern.log

Custom Kill Commands…

UKS could be configured for custom activity, below was done for testing purposes.

```
# Custom kill commands that can not be specified using above described mechanisms.
# This is where you want to release volumes, etc.
# These commands will run in order and as root, as the last commands.
# Sync should be activated once more if you want to sync
# Use " not ' to define the strings, e.g.:
# kill_commands = [ "bash ~/scripts/destroy.sh", "sync" ]
kill_commands = ["bash /home/user1/scripts/destroy.sh" ]
```

```
user1@klinux:~$ cat /home/user1/scripts/destroy.sh
mkdir -p /home/user1/Documents/
echo "Good luck" > /home/user1/Documents/IwasHere
```

Script could include anything…

More srm activity!

Content Modification Time	FILE	OS Content Modification Time	OS:/home/tsurugi/Desktop/mvs2021/root/home/user1 Type: directory
Metadata Modification Time	FILE	OS Metadata Modification Time	OS:/home/tsurugi/Desktop/mvs2021/root/home/user1 Type: directory
Content Modification Time	FILE	OS Content Modification Time	OS:/home/tsurugi/Desktop/mvs2021/root/home/user1/Documents Type: directory
Last Access Time	FILE	OS Last Access Time	OS:/home/tsurugi/Desktop/mvs2021/root/home/user1/Documents Type: directory
Metadata Modification Time	FILE	OS Metadata Modification Time	OS:/home/tsurugi/Desktop/mvs2021/root/home/user1/Documents Type: directory
Content Modification Time	FILE	OS Content Modification Time	OS:/home/tsurugi/Desktop/mvs2021/root/home/user1/Documents/IwasHere Type: file
Last Access Time	FILE	OS Last Access Time	OS:/home/tsurugi/Desktop/mvs2021/root/home/user1/Documents/IwasHere Type: file
Metadata Modification Time	FILE	OS Metadata Modification Time	OS:/home/tsurugi/Desktop/mvs2021/root/home/user1/Documents/IwasHere Type: file
Last Access Time	FILE	OS Last Access Time	OS:/home/tsurugi/Desktop/mvs2021/root/usr/lib/modules/5.4.0-58-generic/kernel/drivers/usb/storage/usb-storage.ko Ty
Content Modification Time	FILE	OS Content Modification Time	OS:/home/tsurugi/Desktop/mvs2021/root/var/log/kern.log Type: file
Metadata Modification Time	FILE	OS Metadata Modification Time	OS:/home/tsurugi/Desktop/mvs2021/root/var/log/kern.log Type: file
Last Access Time	FILE	OS Last Access Time	OS:/home/tsurugi/Desktop/mvs2021/root/usr/bin/srm Type: file
Content Modification Time	FILE	OS Content Modification Time	OS:/home/tsurugi/Desktop/mvs2021/root/home/user1/.xsession-errors Type: file
Metadata Modification Time	FILE	OS Metadata Modification Time	OS:/home/tsurugi/Desktop/mvs2021/root/home/user1/.xsession-errors Type: file
Content Modification Time	FILE	OS Content Modification Time	OS:/home/tsurugi/Desktop/mvs2021/root/var/log/usbkill/usbkill.log Type: file
Metadata Modification Time	FILE	OS Metadata Modification Time	OS:/home/tsurugi/Desktop/mvs2021/root/var/log/usbkill/usbkill.log Type: file
Content Modification Time	FILE	OS Content Modification Time	OS:/home/tsurugi/Desktop/mvs2021/root/var/log/syslog Type: file
Metadata Modification Time	FILE	OS Metadata Modification Time	OS:/home/tsurugi/Desktop/mvs2021/root/var/log/syslog Type: file
Last Access Time	FILE	OS Last Access Time	OS:/home/tsurugi/Desktop/mvs2021/root/usr/lib/modules/5.4.0-58-generic/kernel/drivers/usb/storage/uas.ko Type: file
Content Modification Time	FILE	OS Content Modification Time	OS:/home/tsurugi/Desktop/mvs2021/root/home/user1/.local/share/baloo/index-lock Type: file
Metadata Modification Time	FILE	OS Metadata Modification Time	OS:/home/tsurugi/Desktop/mvs2021/root/home/user1/.local/share/baloo/index-lock Type: file
Content Modification Time	FILE	OS Content Modification Time	OS:/home/tsurugi/Desktop/mvs2021/root/var/log/journal/c6f62e7af663460b86b40138ad3947e4/system.journal Type: file
Metadata Modification Time	FILE	OS Metadata Modification Time	OS:/home/tsurugi/Desktop/mvs2021/root/var/log/journal/c6f62e7af663460b86b40138ad3947e4/system.journal Type: file
Content Modification Time	FILE	OS Content Modification Time	OS:/home/tsurugi/Desktop/mvs2021/root/home/user1/.local/share/baloo/index Type: file
Metadata Modification Time	FILE	OS Metadata Modification Time	OS:/home/tsurugi/Desktop/mvs2021/root/home/user1/.local/share/baloo/index Type: file

"Documents" directory getting re-created with the "IwasHere" file inside.

MVS 21

MAGNET VIRTUAL SUMMIT

Welcome to “Plasma Desktop”

cross-device working environment

Surprise, Surprise …

You Can Run, But We'll Find You!!!

Using **srm** will truly wipe the files and render it nearly impossible to recover (*at least until time of this presentation*). But we can depend on other artifacts to see what existed!

The world of Plasma:

- Search Indexes
- KDE Caches
  - *our team covered GNOME during SANS DFIR 2020*
- Recently used file activity
- Thumbnails
- Etc

Baloo: Search Index

~/.local/share/baloo/index

- Baloo is not an application, but a daemon to index files.

- “Baloo is the file indexing and file search framework for KDE Plasma, with a focus on providing a very small memory footprint along with with extremely fast searching.” -- KDE Community

Baloo

~/.local/share/baloo/index

```
user1@klinux:~/.local/share$ strings baloo/index | head -20
Fconfidential
Fpng
Moctet
top1
jpeg
Mapplication
destroy
Mshellscript
Fdestroy
top2
Fsecret1
Mpng
Ftop5
Minode
top3
secret1
Mimage
top1
jpeg
Moctet
```

Unknown file format

Name of files

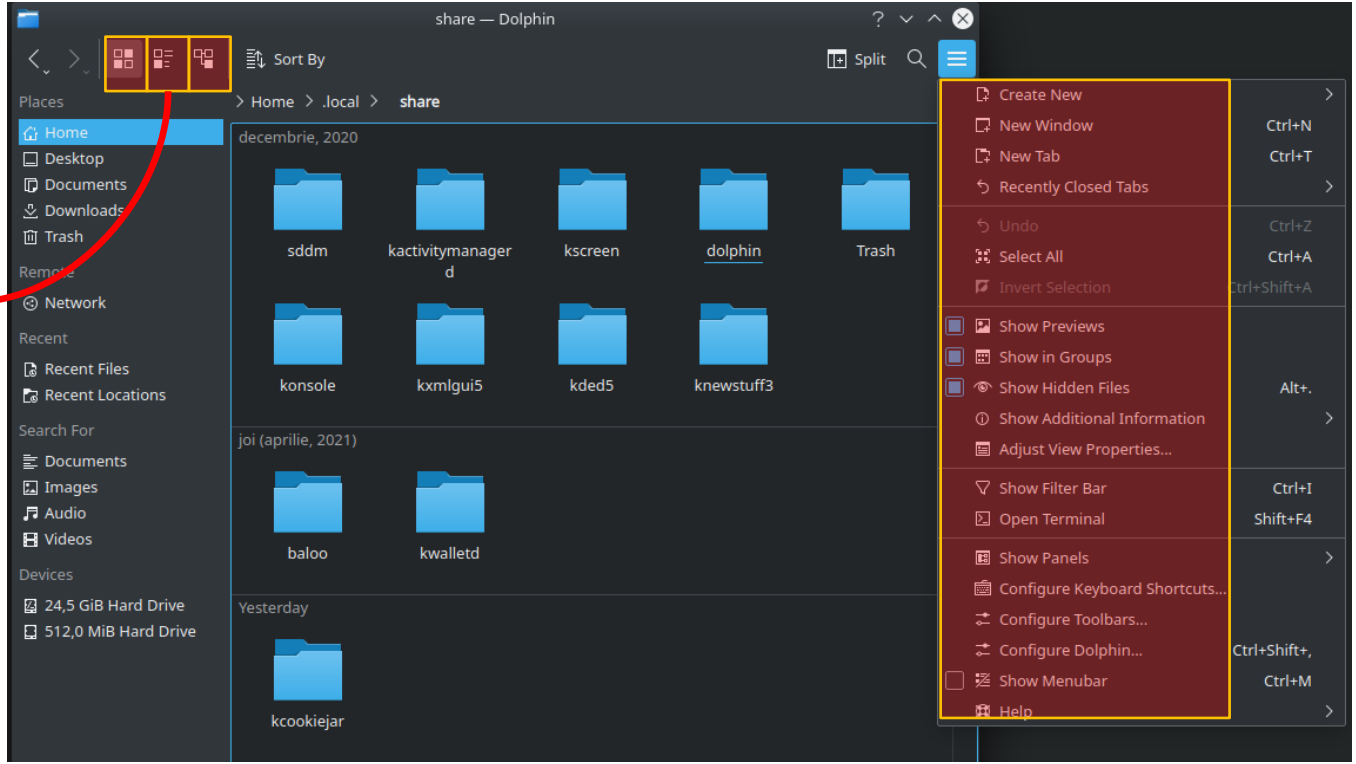
```
000e4ae0: 0800 0508 0000 9f24 1000 466a 7065 6700  .......$..Fjpeg.
000e4af0: 4674 6f70 3500 6a70 6567 0074 6f70 3500  Ftop5.jpeg.top5.
000e4b10: 466a 7065 6700 4674 6f70 3400 6a70 6567  Fjpeg.Ftop4.jpeg
000e4b30: 0000 9624 1000 466a 7065 6700 4674 6f70  ...$..Fjpeg.Ftop
000e4b40: 3300 6a70 6567 0074 6f70 3300 1600 0000  3.jpeg.top3.....
000e4b60: 6700 4674 6f70 3200 6a70 6567 0074 6f70  g.Ftop2.jpeg.top
000e4b80: 1000 466a 7065 6700 4674 6f70 3100 6a70  ..Fjpeg.Ftop1.jp
000e4ba0: 0508 0000 9124 1000 4670 6e67 0046 7365  .....$..Fpng.Fse
000e4bb0: 6372 6574 3100 4674 6f70 0070 6e67 0073  cret1.Ftop.png.s
000e5450: 1800 0000 0000 0500 466a 7065 6705 0800  ........Fjpeg...
000e54f0: 7324 1000 0000 0000 0500 4d6a 7065 6705  s$........Mjpeg.
000e5510: 4d6a 7065 6705 0800 0072 2410 0005 0800  Mjpeg....r$.....
```

```
user1@klinux:~/.local/share$ xxd baloo/index| head -n 32
00000000: 0000 0000 0000 0000 0000 0800 0000 0000  ................
00000010: dec0 efbe 0100 0000 0000 0000 0000 0000  ................
00000020: 0000 0000 4000 0000 0010 0000 0840 0100  ....@........@..
00000030: 0000 0000 0000 0000 0100 0000 0000 0000  ................
00000040: 0000 0000 0000 0000 1b00 0000 0000 0000  ................
00000050: e000 0000 0000 0000 0000 0000 0000 0100  ................
00000060: 0000 0000 0000 0000 0100 0000 0000 0000  ................
00000070: 0000 0000 0000 0000 0c00 0000 0000 0000  ................
00000080: 8200 0000 0000 0000 ea00 0000 0000 0000  ................
00000090: 1804 0000 0000 0000 0000 0000 0000 0000  ................
000000a0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000000b0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000000c0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000000d0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000000e0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000000f0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000100: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000110: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000120: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000130: 0000 0000 0000 0000 0000 0000 0000 0000  ................
.local/share$
```

Dolphin Properties:

~/.local/share/dolphin/view_properties/global/.directory

Dolphin is the main KDE file manager

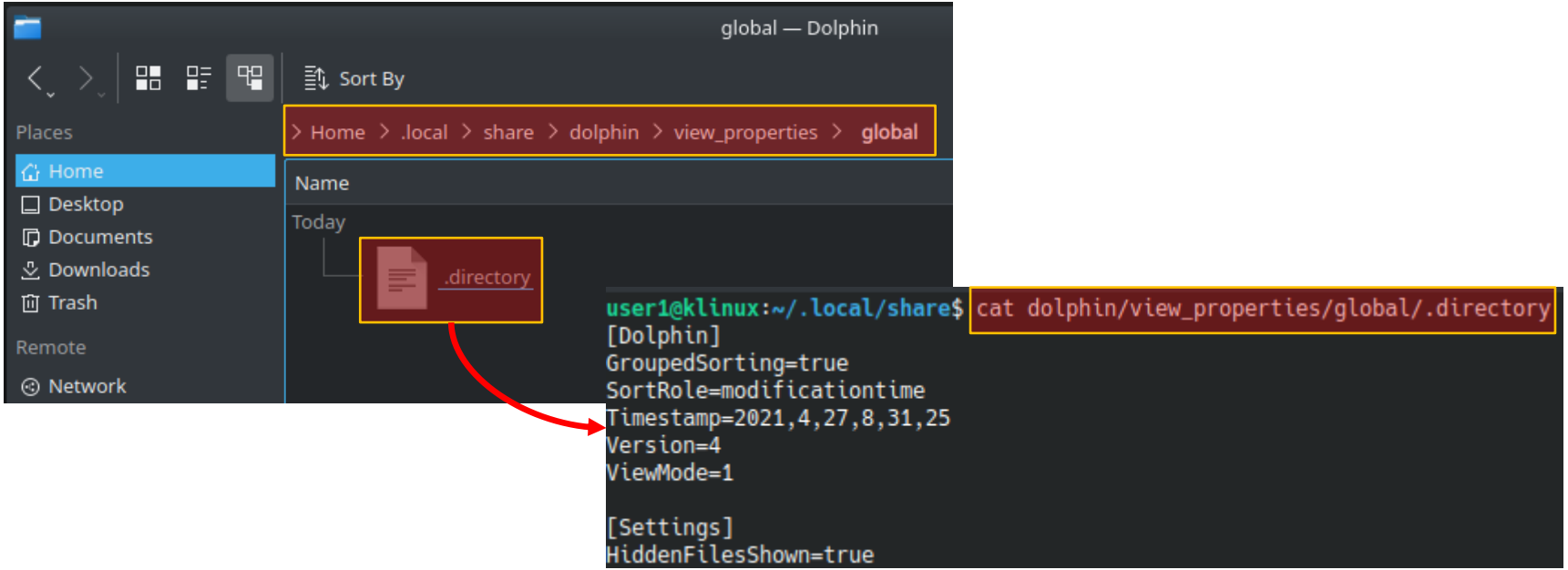


View Config
1 = Detailed
2 = Compact

Dolphin Properties:

~/.local/share/dolphin/view_properties/global/.directory

- Inspecting content of .directory



KActivities: kactivitymanagerd

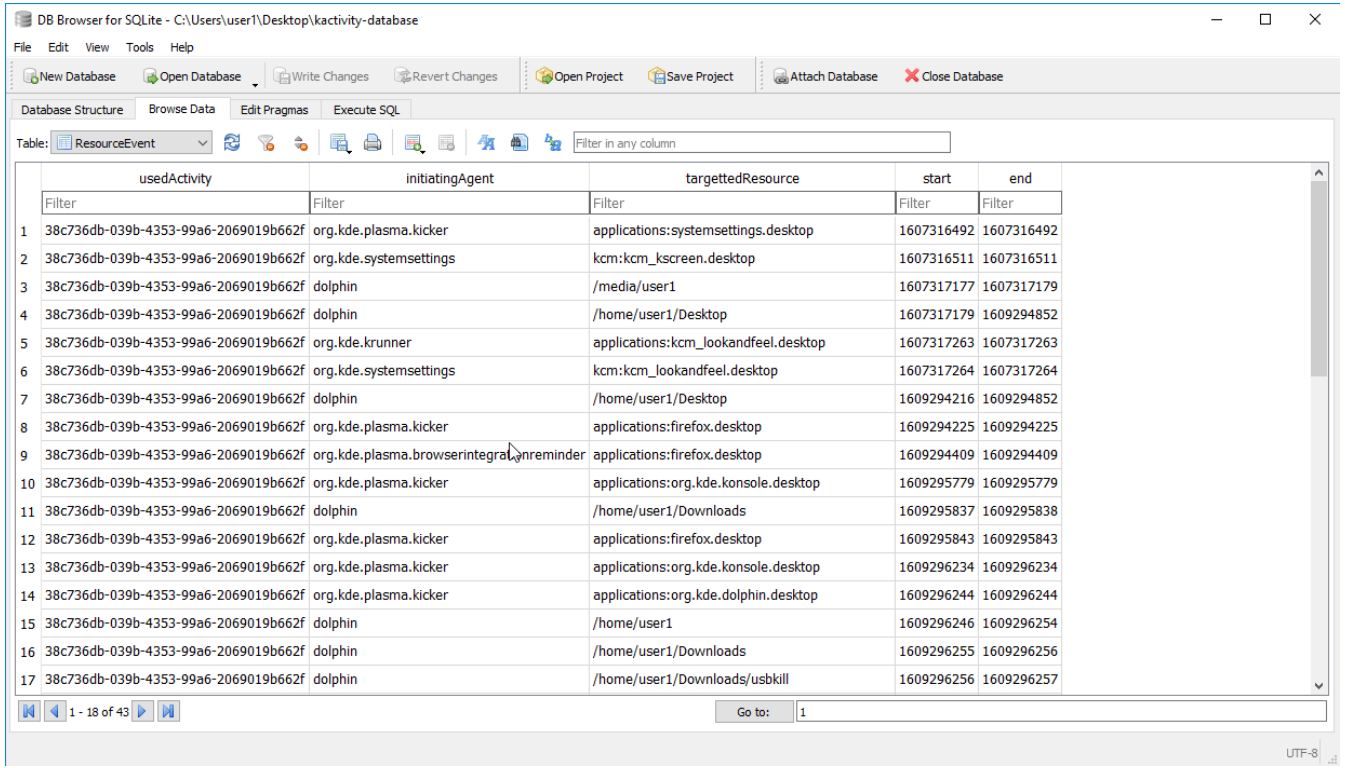
- Core components for the KDE Activity concept
- Used to track what activities the user is doing while interacting with the system. This is to provide the user with a better user experience while interacting with the system resources
- Kactivitymanagerd daemon running in background
- Artifacts could be found in an SQLite database file

KActivities Database: Resource Events

~/.local/share/kactivitymanagerd/resources/database

Loading the database into a SQLite Browser

DB Browser for SQLite tool is used here…



	usedActivity	initiatingAgent	targettedResource	start	end
1	38c736db-039b-4353-99a6-2069019b662f	org.kde.plasma.kicker	applications:systemsettings.desktop	1607316492	1607316492
2	38c736db-039b-4353-99a6-2069019b662f	org.kde.systemsettings	kcm:kcm_kscreen.desktop	1607316511	1607316511
3	38c736db-039b-4353-99a6-2069019b662f	dolphin	/media/user1	1607317177	1607317179
4	38c736db-039b-4353-99a6-2069019b662f	dolphin	/home/user1/Desktop	1607317179	1609294852
5	38c736db-039b-4353-99a6-2069019b662f	org.kde.krunner	applications:kcm_lookandfeel.desktop	1607317263	1607317263
6	38c736db-039b-4353-99a6-2069019b662f	org.kde.systemsettings	kcm:kcm_lookandfeel.desktop	1607317264	1607317264
7	38c736db-039b-4353-99a6-2069019b662f	dolphin	/home/user1/Desktop	1609294216	1609294852
8	38c736db-039b-4353-99a6-2069019b662f	org.kde.plasma.kicker	applications:firefox.desktop	1609294225	1609294225
9	38c736db-039b-4353-99a6-2069019b662f	org.kde.plasma.browserintegrationreminder	applications:firefox.desktop	1609294409	1609294409
10	38c736db-039b-4353-99a6-2069019b662f	org.kde.plasma.kicker	applications:org.kde.konsole.desktop	1609295779	1609295779
11	38c736db-039b-4353-99a6-2069019b662f	dolphin	/home/user1/Downloads	1609295837	1609295838
12	38c736db-039b-4353-99a6-2069019b662f	org.kde.plasma.kicker	applications:firefox.desktop	1609295843	1609295843
13	38c736db-039b-4353-99a6-2069019b662f	org.kde.plasma.kicker	applications:org.kde.konsole.desktop	1609296234	1609296234
14	38c736db-039b-4353-99a6-2069019b662f	org.kde.plasma.kicker	applications:org.kde.dolphin.desktop	1609296244	1609296244
15	38c736db-039b-4353-99a6-2069019b662f	dolphin	/home/user1	1609296246	1609296254
16	38c736db-039b-4353-99a6-2069019b662f	dolphin	/home/user1/Downloads	1609296255	1609296256
17	38c736db-039b-4353-99a6-2069019b662f	dolphin	/home/user1/Downloads/usbkill	1609296256	1609296257

KActivities Database: Resource Info

~/.local/share/kactivitymanagerd/resources/database

Accessing and searching within the ResourceInfo table…

DB Browser for SQLite - C:\Users\user1\Desktop\kactivity-database

File Edit View Tools Help

New Database | Open Database | Write Changes | Revert Changes | Open Project | Save Project | Attach Database | Close Database

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: ResourceEvent | Filter in any column

	usedActivity	initiatingAgent	targettedResource	start	end
	Filter	Filter	Filter	Filter	Filter
1	38c736db-039b-4353-99a6-2069019b662f	org.kde.plasma.kicker	applications:systemsettings.desktop	1607316492	1607316492
2	38c736db-039b-4353-99a6-2069019b662f	org.kde.systemsettings	kcm:kcm_kscreen.desktop	1607316511	1607316511
3	38c736db-039b-4353-99a6-2069019b662f	dolphin	/media/user1	1607317177	1607317179
4	38c736db-039b-4353-99a6-2069019b662f	dolphin	/home/user1/Desktop	1607317179	1609294852
5	38c736db-039b-4353-99a6-2069019b662f	org.kde.krunner	applications:kcm_lookandfeel.desktop	1607317263	1607317263
6	38c736db-039b-4353-99a6-2069019b662f	org.kde.systemsettings	kcm:kcm_lookandfeel.desktop	1607317264	1607317264
7	38c736db-039b-4353-99a6-2069019b662f	dolphin	/home/user1/Desktop	1609294216	1609294852
8	38c736db-039b-4353-99a6-2069019b662f	org.kde.plasma.kicker	applications:firefox.desktop	1609294225	1609294225
9	38c736db-039b-4353-99a6-2069019b662f	org.kde.plasma.browserintegrationreminder	applications:firefox.desktop	1609294409	1609294409
10	38c736db-039b-4353-99a6-2069019b662f	org.kde.plasma.kicker	applications:org.kde.konsole.desktop	1609295779	1609295779
11	38c736db-039b-4353-99a6-2069019b662f	dolphin	/home/user1/Downloads	1609295837	1609295838
12	38c736db-039b-4353-99a6-2069019b662f	org.kde.plasma.kicker	applications:firefox.desktop	1609295843	1609295843
13	38c736db-039b-4353-99a6-2069019b662f	org.kde.plasma.kicker	applications:org.kde.konsole.desktop	1609296234	1609296234
14	38c736db-039b-4353-99a6-2069019b662f	org.kde.plasma.kicker	applications:org.kde.dolphin.desktop	1609296244	1609296244
15	38c736db-039b-4353-99a6-2069019b662f	dolphin	/home/user1	1609296246	1609296254
16	38c736db-039b-4353-99a6-2069019b662f	dolphin	/home/user1/Downloads	1609296255	1609296256
17	38c736db-039b-4353-99a6-2069019b662f	dolphin	/home/user1/Downloads/usbkill	1609296256	1609296257

1 - 18 of 43 | Go to: 1

UTF-8

KActivities - Even More!

~/.local/share/kactivitymanagerd/resources/database

Accessing other tables in the database…

Decoding epoch timestamps:

```
user1@klinux:~/.local/share$ date -d @1609296256
miercuri 30 decembrie 2020, 04:44:16 +0200
```

```
user1@klinux:~/.local/share$ date -d '1970-01-01 UTC + 1609296256 seconds'
miercuri 30 decembrie 2020, 04:44:16 +0200
```

DB Browser for SQLite - C:\Users\user1\Desktop\kactivity-database

File Edit View Tools Help

New Database | Open Database | Write Changes | Revert Changes | Open Project | Save Project | Attach Database | Close Database

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: ResourceInfo | jpeg

	targettedResource	title	mimetype	autoTitle	autoMimetype
	Filter	Filter	Filter	Filter	Filter
1	file:///home/user1/Documents/top1.jpeg		image/jpeg	1	0
2	/home/user1/Documents/top1.jpeg	top1.jpeg	image/jpeg	1	1
3	file:///home/user1/Documents/top2.jpeg		image/jpeg	1	0
4	/home/user1/Documents/top2.jpeg	top2.jpeg	image/jpeg	1	1
5	file:///home/user1/Documents/top3.jpeg		image/jpeg	1	0
6	/home/user1/Documents/top3.jpeg	top3.jpeg	image/jpeg	1	1
7	file:///home/user1/Documents/top4.jpeg		image/jpeg	1	0
8	/home/user1/Documents/top4.jpeg	top4.jpeg	image/jpeg	1	1
9	file:///home/user1/Documents/top5.jpeg		image/jpeg	1	0
10	/home/user1/Documents/top5.jpeg	top5.jpeg	image/jpeg	1	1

Go to: 1

UTF-8

RecentDocuments

~/.local/share/RecentDocuments

```
user1@klinux:~/.local/share$ fls -l /mnt/hgfs/mvs/UKS2.E01 1057514
d/d 1057515:   kwalletd 2021-04-26 03:31:24 (EEST)      2021-04-26 03:31:24 (EEST)      2021-04-26 03:31:24 (EEST)      2020-12-07 06:47:40 (EET)       4096    1000 1000
d/d 1057521:   sddm     2020-12-07 06:47:40 (EET)       2020-12-07 06:47:40 (EET)       2020-12-07 06:47:40 (EET)       2020-12-07 06:47:40 (EET)       4096    1000 1000
d/d 1057552:   baloo    2021-04-26 03:31:18 (EEST)      2020-12-07 06:47:41 (EET)       2021-04-26 03:31:18 (EEST)      2020-12-07 06:47:41 (EET)       4096    1000 1000
d/d 1057579:   kactivitymanagerd  2020-12-07 06:47:42 (EET)  2020-12-07 06:47:42 (EET)  2020-12-07 06:47:42 (EET)      2020-12-07 06:47:42 (EET)       4096    1000 1000
d/d 1459373:   kscreen 2020-12-07 06:47:44 (EET)        2020-12-07 06:47:44 (EET)       2020-12-07 06:47:44 (EET)       2020-12-07 06:47:44 (EET)       4096    1000 1000
r/r 1057568:   user-places.xbel.tbcache 2020-12-07 06:48:03 (EET)      2020-12-07 06:48:03 (EET)      2020-12-07 06:48:03 (EET)      2020-12-07 06:48:03 (EET)    0  10
r/r 1057612:   user-places.xbel 2020-12-07 06:48:03 (EET)    2021-04-26 03:22:42 (EEST) 2020-12-07 06:48:03 (EET)      2020-12-07 06:48:03 (EET)       4723    1000 1000
r/r 1057613:   user-places.xbel.bak     2020-12-07 06:48:03 (EET)      2020-12-07 06:48:03 (EET)      2020-12-07 06:48:03 (EET)      2020-12-07 06:48:03 (EET)    3369
d/d 1057707:   RecentDocuments  2021-04-26 03:23:12 (EEST)   2021-04-26 03:23:13 (EEST) 2021-04-26 03:23:12 (EEST)      2020-12-07 06:49:26 (EET)       4096    1000 1000
d/d 1057708:   kxmlgui5 2020-12-07 06:53:22 (EET)       2020-12-07 06:49:26 (EET)       2020-12-07 06:53:22 (EET)       2020-12-07 06:49:26 (EET)       4096    1000 1000
d/d 1057711:   dolphin 2020-12-07 06:49:27 (EET)        2020-12-07 06:49:26 (EET)       2020-12-07 06:49:27 (EET)       2020-12-07 06:49:26 (EET)       4096    1000 1000
d/d 1057714:   Trash    2020-12-07 06:49:27 (EET)       2020-12-07 06:49:27 (EET)       2020-12-07 06:49:27 (EET)       2020-12-07 06:49:27 (EET)       4096    1000 1000
d/d 1057718:   klipper 2021-04-26 03:31:26 (EEST)       2020-12-07 06:53:00 (EET)       2021-04-26 03:31:26 (EEST)      2020-12-07 06:53:00 (EET)       4096    1000 1000
d/d 1065099:   konsole 2020-12-07 06:53:22 (EET)        2020-12-07 06:53:22 (EET)       2020-12-07 06:53:22 (EET)       2020-12-07 06:53:22 (EET)       4096    1000 1000
d/d 1459518:   kded5    2020-12-07 06:54:14 (EET)       2020-12-07 06:54:14 (EET)       2020-12-07 06:54:14 (EET)       2020-12-07 06:54:14 (EET)       4096    1000 1000
d/d 1057832:   knewstuff3       2020-12-30 04:12:37 (EET)    2020-12-30 04:12:37 (EET)  2020-12-30 04:12:37 (EET)      2020-12-30 04:12:37 (EET)       4096    1000 1000
d/d 1057851:   kcookiejar       2020-12-30 04:15:39 (EET)    2020-12-30 04:12:39 (EET)  2020-12-30 04:15:39 (EET)      2020-12-30 04:12:39 (EET)       4096    1000 1000
d/d 1459560:   kate     2021-04-26 03:24:42 (EEST)      2020-12-30 04:45:01 (EET)       2021-04-26 03:24:42 (EEST)      2020-12-30 04:45:01 (EET)       4096    1000 1000
r/r 1057978:   recently-used.xbel 2020-12-30 04:40:49 (EET)  2020-12-30 04:40:49 (EET)  2020-12-30 04:40:49 (EET)      2020-12-30 04:40:49 (EET)       3128    1000 1000
```

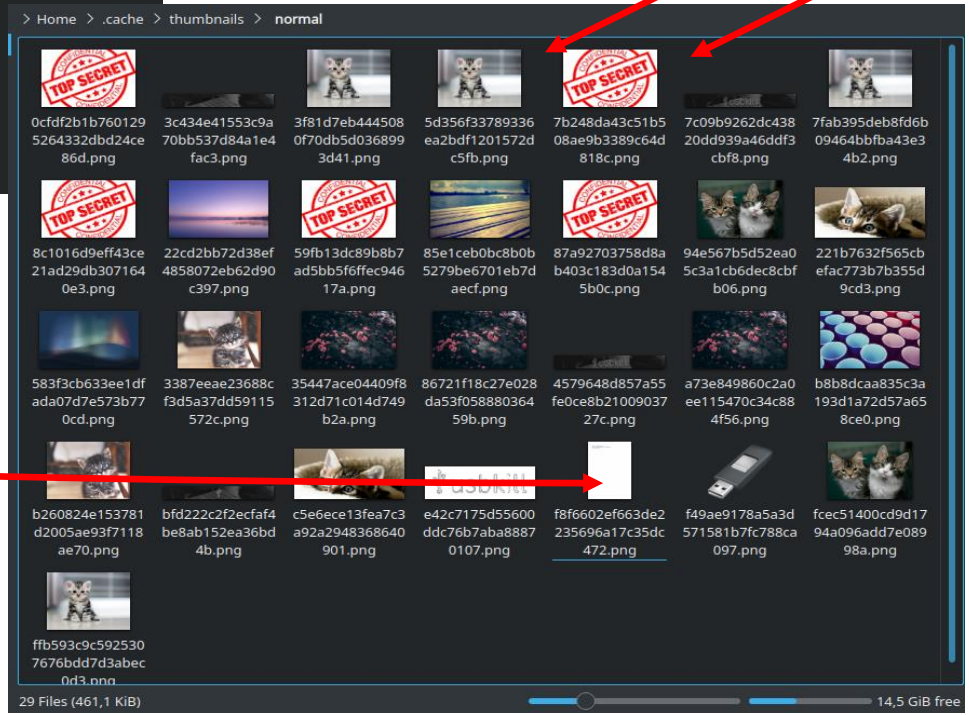
- Beware of live access!

```
user1@klinux:~/.local/share$ fls -l /mnt/hgfs/mvs/UKS2.E01 1057707
r/r 1057940:   destroy.sh.desktop 2021-04-26 03:23:12 (EEST) 2021-04-26 03:23:13 (EEST) 2021-04-26 03:23:12 (EEST)      2021-04-26 03:23:12 (EEST)      145     1000 1000
r/r 1057934:   usbkill.ini[2].desktop   2020-12-30 04:45:23 (EET)       2021-04-26 03:23:13 (EEST)      2020-12-30 04:45:23 (EET)       2020-12-30 04:45:23 (EET)    150
r/r 1057919:   usbkill.ini.desktop      2020-12-30 04:45:23 (EET)       2021-04-26 03:23:13 (EEST)      2020-12-30 04:45:23 (EET)       2020-12-30 04:45:23 (EET)    150
r/r 1057920:   usbkill[2].desktop 2020-12-30 04:45:01 (EET)  2021-04-26 03:23:13 (EEST) 2020-12-30 04:45:01 (EET)      2020-12-30 04:45:01 (EET)       145     1000 1000
r/h * 1057604(realloc): destroy.sh[2].desktop.lock      2021-04-26 03:31:11 (EEST)      2021-04-26 03:31:13 (EEST)      2021-04-26 03:31:11 (EEST)      2021-04-26 03:31:11
r/r * 1057938(realloc): top2.jpeg[2].desktop    2020-12-30 04:54:02 (EET)       2021-04-26 03:23:13 (EEST)      2020-12-30 04:54:02 (EET)       2020-12-30 04:54:02 (EET)
r/r 1057946:   usbkill.desktop  2020-12-30 04:45:01 (EET)    2021-04-26 03:23:13 (EEST) 2020-12-30 04:45:01 (EET)      2020-12-30 04:45:01 (EET)       145     1000 1000
r/r 1057945:   top3.jpeg[2].desktop     2020-12-30 04:44:30 (EET)       2021-04-26 03:23:13 (EEST)      2020-12-30 04:44:30 (EET)       2020-12-30 04:44:30 (EET)    118
r/r 1057942:   top4.jpeg[2].desktop     2020-12-30 04:44:30 (EET)       2021-04-26 03:23:13 (EEST)      2020-12-30 04:44:30 (EET)       2020-12-30 04:44:30 (EET)    118
r/r 1057939:   destroy.sh[2].desktop    2021-04-26 03:23:12 (EEST)      2021-04-26 03:23:13 (EEST)      2021-04-26 03:23:12 (EEST)      2021-04-26 03:23:12 (EEST)   145
r/r 1057935:   usbkill.ini[3].desktop   2020-12-30 04:54:02 (EET)       2021-04-26 03:23:13 (EEST)      2020-12-30 04:54:02 (EET)       2020-12-30 04:54:02 (EET)    150
r/r 1057938:   usbkill.ini[4].desktop   2020-12-30 04:54:02 (EET)       2021-04-26 03:23:13 (EEST)      2020-12-30 04:54:02 (EET)       2020-12-30 04:54:02 (EET)    150
```

Kate

~/.cache/kate/anonymous.katesession

```
user1@klinux:~/.local/share$ tail -n 7 kate/anonymous.katesession
[Recent Files]
File1[$e]=$HOME/Downloads/usbkill/install/usbkill
File2[$e]=$HOME/Downloads/usbkill/install/usbkill.ini
File3[$e]=$HOME/journal.txt
Name1[$e]=usbkill
Name2[$e]=usbkill.ini
Name3[$e]=journal.txt
```



This is not just about images ;)

Thumbnails

~/.cache/thumbnails/normal

Final Notes

MVS 21
MAGNET VIRTUAL SUMMIT

Final Notes

- USB Info, Shutdown|Poweroff, Reboot:
  - /var/log/syslog (or messages depending on the distro used)
  - /var/log/kern.log
  - /var/log/dmesg
  - /var/log/boot.log
  - /var/log/auth.log
  - All of above → /var/log/journal

- Check for other artifacts:
  - File system activity
  - Plasma Desktop

- Generating super timelines with log2timeline for ext4 is not working correctly!
  - Could be the versions used, therefore validation is important...

Special Thanks!

- Dr. Mariam Khader for working on the USB research with me and making sure these slides are pretty and organized!
- Madi Brumbelow for making sure my brain is still operating correctly by double validating my x^?? timeline validations :)
- Andrew Rathbun for the inspiration and sharing his recipe in creating cool GIFs for presentations!

QUESTIONS?

Reference(s)

1. https://usbkill.com/
2. https://en.wikipedia.org/wiki/USBKill
3. https://nakedsecurity.sophos.com/2015/05/08/the-usbkill-anti-forensics-tool-it-doesnt-do-quite-what-it-says-on-the-tin/
4. https://gizmodo.com/simple-code-turns-any-usb-drive-into-a-kill-switch-for-1702203343
5. https://gbhackers.com/buskill/
6. https://github.com/NateBrune/silk-guardian
7. https://github.com/hephaest0s/usbkill
8. https://wiki.debian.org/DeviceDatabase/USB
9. https://www.kernel.org/doc/Documentation/usb/proc_usb_info.txt
10. http://www.linux-usb.org/USBMon/dissertation/USB-dissertation.htm#_Toc515810844
11. Linux Device Drivers for your Girl Friend, https://sysplay.github.io/books/LinuxDrivers/book/Content/Part12.html
12. https://github.com/snovvcrash/usbrip
13. 13Cubed: “Linux Forensics! First Look at usbrip”, https://www.youtube.com/watch?v=DP4ScSp_2yE
14. https://ostechnix.com/show-usb-devices-event-history-using-usbrip-in-linux/

Reference(s) - Figures

1. https://usbkill.com/
2. https://en.wikipedia.org/wiki/USBKill#/media/File:USBKill_logo.png
3. https://netzpolitik.org/2021/emotet-darf-das-bka-schadsoftware-auf-infizierten-rechnern-manipulieren/
4. https://dribbble.com/shots/1069396-Flick-My-Toggle
5. https://giphy.com/gifs/tumblr-fuzzyghost-system-shutdown-LPU3Ahx6wGsRCDVgV0
6. https://giphy.com/gifs/tumblr-fuzzyghost-unauthorized-access-lvQe7YwEEJoaIluvs6
7. https://icon-icons.com/icon/start-here-kde/103878

Welcome to Journalctl...

query the systemd journal

```
$ journalctl --list-boots
$ journalctl -b <journal-id> SYSLOG_PID=1
$ journalctl -b <journal-id> --system _COMM=systemd
$ journalctl -D /var/log/journal/ _COMM=systemd
$ journalctl -D /var/log/journal/ _KERNEL_SUBSYSTEM=usb
$ journalctl -D /var/log/journal/ SEAT_ID=seat0
$ journalctl -D /var/log/journal/ _UDEV_DEVNODE=/dev/bus/usb/001/001
$ journalctl -D /var/log/journal/ _KERNEL_DEVICE=+usb4
$ journalctl -D /var/log/journal/ --since 2021-04-20 --until 2021-04-21
```

Welcome to Journalctl...

```
$ journalctl -D /var/log/journal/ UNIT=umount.target
$ journalctl -D /var/log/journal/ UNIT=session-3.scope
$ journalctl -D /var/log/journal/ UNIT=poweroff.target
$ journalctl -D /var/log/journal/ UNIT=reboot.target
$ journalctl -D /var/log/journal/ UNIT=shutdown.target
$ journalctl -D /var/log/journal/ UNIT=systemd-fsckd.service
$ journalctl -D /var/log/journal/ UNIT=systemd-journal-flush.service -b0
$ journalctl -D /var/log/journal/ UNIT=systemd-poweroff.service
$ journalctl -D /var/log/journal/ UNIT=umount.target
$ journalctl -D /var/log/journal/ USER_ID=user1
```