MIT World Peace University

Digital Forensics and Investigation
Third Year B. Tech, Semester 5

System Log Analysis

Lab Assignment 4

Prepared By

Krishnaraj Thadesar
Cyber Security and Forensics
Batch A1, PA 20

September 25, 2023

Contents

1 Aim

To Analyse System Logs, and learn about difference scenarios that can be detected from them.

2 Objectives

1. To learn about the different types of logs that are generated by a system.
2. To learn different scenarios that can be detected from the logs.
3. To learn about the different tools that can be used to analyse the logs.

3 Theory

3.1 System Logs

System logs are records of events and activities that occur within a computer system. They are essential for monitoring and troubleshooting system behavior. Key points about system logs include:

- System logs capture information about system events, errors, and user activities.
- Types of system logs commonly include security logs, application logs, and system performance logs.
- Logs are crucial for diagnosing issues, auditing, and ensuring system security.

3.2 System Logs on Various Operating Systems

Different operating systems generate system logs in distinct ways. Here are some insights into system logs on various operating systems:

- On Linux, system logs are typically stored in the '/var/log' directory, with files like 'syslog' and 'auth.log'.
- Windows maintains event logs, categorized into Application, Security, and System logs, accessible through Event Viewer.
- macOS utilizes the 'Console' application to view system logs, including kernel logs and application-specific logs.

3.3 Tools to Analyse System Logs

Analyzing system logs efficiently requires specialized tools. Consider the following points:

- Log analyzers such as ELK Stack (Elasticsearch, Logstash, Kibana) provide a comprehensive platform for log management.

Figure 1: Elasticsearch

- Splunk is a popular commercial tool for log analysis, offering powerful search and visualization capabilities.

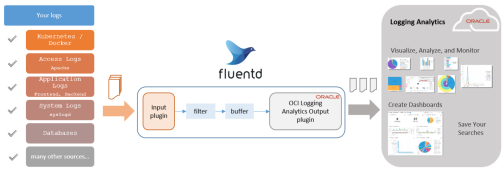

Figure 2: Fluentd

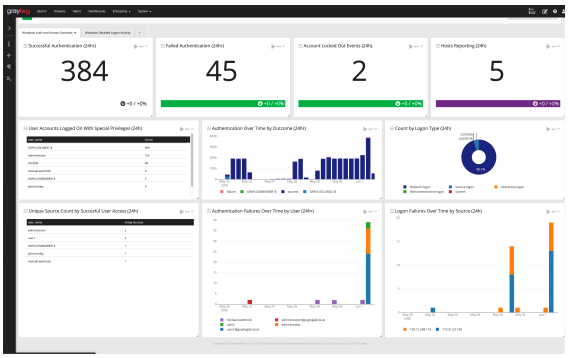

Figure 3: Gray log

- Open-source tools like Graylog and Fluentd are suitable for aggregating and analyzing logs in diverse environments.

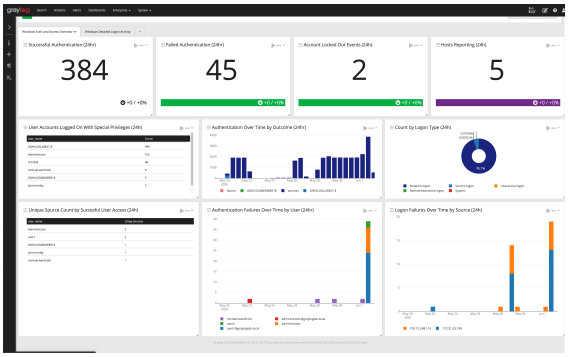

Figure 4: Gray log

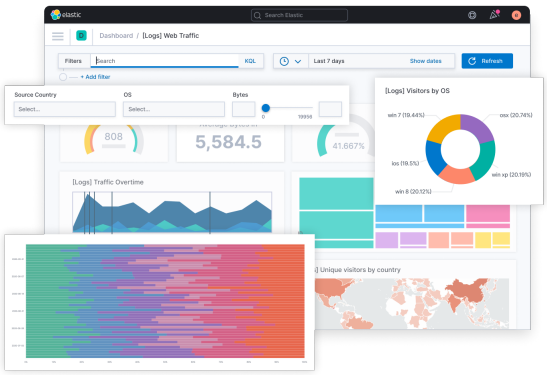

Figure 5: Kibana

3.4 Event Viewer in Windows

The Event Logger, also known as the Event Viewer, is a vital component of the Windows operating system for managing and analyzing system logs. Here are key points about the Event Logger and how it aids in log analysis:

- **Centralized Log Repositoryd** The Event Logger serves as a centralized repository for various logs generated by the Windows operating system. It categorizes logs into three main categories:
  - **Application Logsd** These logs contain information about applications, such as software crashes or errors.
  - **Security Logsd** Security logs record security-related events, including logins, logouts, and access control events.
  - **System Logsd** System logs capture events related to the Windows system itself, such as hardware and driver issues.
- **Event Classificationd** Events within the Event Logger are classified by event IDs, source, and severity levels. This classification helps in quickly identifying and prioritizing issues during log analysis.

- **Search and Filter Capabilitiesd** The Event Logger provides robust search and filter capabilities, allowing users to narrow down logs based on specific criteria. This is invaluable for pinpointing relevant events within extensive log data.
- **Custom Event Logsd** Administrators can create custom event logs, enabling the recording of specific application or system events for easier tracking and analysis.
- **Scheduled Tasksd** Windows allows users to set up scheduled tasks based on events in the Event Logger. This functionality enables automated responses to certain log entries, enhancing system management and security.
- **Integration with Third-Party Toolsd** The Event Logger can be integrated with third-party log analysis and monitoring tools for more advanced log management and correlation. This enhances the capabilities of log analysis beyond what the built-in Event Viewer provides.

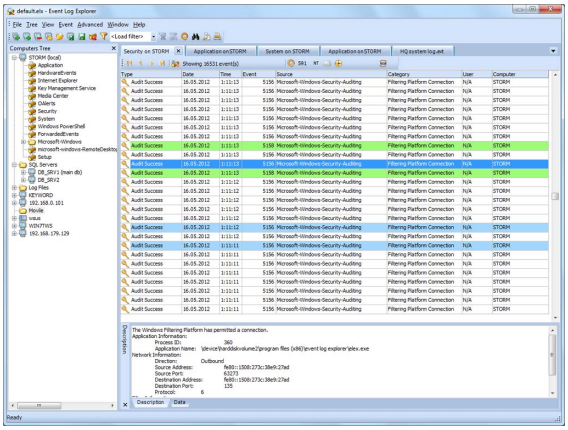

Figure 6: Event Viewer

3.5 Scenarios that can be detected from System Logs

System logs offer insights into various scenarios and events. Here are examples of scenarios that can be detected from system logs:

- Security breaches: Unauthorized access attempts, failed login attempts, and suspicious activities in security logs.
- Performance issues: System resource utilization, application crashes, and bottlenecks in application logs.
- Compliance violations: Tracking changes in system configurations and user activities for regulatory compliance.

4 Scenarios Performed and Results on Linux

Given Below are the Scenarios that were performed on the Linux System, and the results of the same. The text here is the output of the command

```
journalctl -f
```

4.1 Mounting Hard Disk Partitions

```
Sep 24 14:45:06 ntfs-3g[6854]: Version 2022.10.3 external FUSE 29
Sep 24 14:45:06 ntfs-3g[6854]: Mounted /dev/sda6 (Read-Write, label "Programs", NTFS 3.1)
Sep 24 14:45:06 ntfs-3g[6854]: Cmdline options: rw
Sep 24 14:45:06 ntfs-3g[6854]: Mount options: allow_other,nonempty,relatime,rw, fsname=/dev/sda6,blkdev,blksize=4096
Sep 24 14:45:06 ntfs-3g[6854]: Ownership and permissions disabled, configuration type 7
Sep 24 14:45:06 sudo[6844]: pam_unix(sudo:session): session closed for user root
Sep 24 14:45:06 dbus-daemon[487]: [system] Activating via systemd: service name='org.freedesktop.hostname1' unit='dbus-org.freedesktop.hostname1.service' requested by ':1.86' (uid=1000 pid=2564 comm="/usr/bin/gnome-shell")
```

4.2 Connecting and Disconnecting the Wireless Mouse

```

/usr/lib/gdm-x-session[2337]: (II) event7  - Logitech M585/M590: device removed
/usr/lib/gdm-x-session[2337]: (II) config/udev: removing device Logitech M585/M590
/usr/lib/gdm-x-session[2337]: (**) Option "fd" "38"
/usr/lib/gdm-x-session[2337]: (II) UnloadModule: "libinput"
/usr/lib/gdm-x-session[2337]: (II) systemd-logind: not releasing fd for 13:71, still in
/usr/lib/gdm-x-session[2337]: (II) config/udev: removing device Logitech M585/M590
/usr/lib/gdm-x-session[2337]: (**) Option "fd" "38"
/usr/lib/gdm-x-session[2337]: (II) UnloadModule: "libinput"
/usr/lib/gdm-x-session[2337]: (II) systemd-logind: releasing fd for 13:71
Sep 24 14:46:47 dbus-daemon[487]: [system] Activating via systemd: service name='org.freedesktop.Avahi' unit='dbus-org.freedesktop.Avahi.service' requested by ':1.153' (uid=969 pid=7234 comm="/usr/lib/colord-sane")
Sep 24 14:46:47 dbus-daemon[487]: [system] Activation via systemd failed for unit 'dbus-org.freedesktop.Avahi.service': Unit dbus-org.freedesktop.Avahi.service not found.
tracker-miner-f[3922]: Could not execute sparql: database is locked
kernel: usb 1-3: new full-speed USB device number 6 using xhci_hcd
kernel: usb 1-3: New USB device found, idVendor=046d, idProduct=c52b, bcdDevice =12.11
```

4.3 Connecting and Disconnecting the Wireless Keyboard

```
Sep 24 14:47:07 kernel: usb 1-1: new low-speed USB device number 7 using xhci_hcd
Sep 24 14:47:07 kernel: usb 1-1: New USB device found, idVendor=1a2c, idProduct=92 f6, bcdDevice= 1.16
Sep 24 14:47:07 kernel: usb 1-1: New USB device strings: Mfr=1, Product=2, SerialNumber=0
Sep 24 14:47:07 kernel: usb 1-1: Product: Redgear Shadow Blade Mechanical Keyboard
Sep 24 14:47:07 kernel: usb 1-1: Manufacturer: SEMICO
Sep 24 14:47:07 kernel: input: SEMICO   Redgear Shadow Blade Mechanical Keyboard as /devices/pci0000:00/0000:00:14.0/usb1/1-1/1-1:1.0/0003:1A2C:92F6.000C/input/input32
Sep 24 14:47:08 kernel: hid-generic 0003:1A2C:92F6.000C: input,hidraw2: USB HID v1 .10 Keyboard [SEMICO   Redgear Shadow Blade Mechanical Keyboard] on usb -0000:00:14.0-1/input0
Sep 24 14:47:08 kernel: input: SEMICO   Redgear Shadow Blade Mechanical Keyboard Consumer Control as /devices/pci0000:00/0000:00:14.0/usb1/1-1/1-1:1.1/0003:1A2C :92F6.000D/input/input33
```

```
Sep 24 14:47:08 kernel: input: SEMICO   Redgear Shadow Blade Mechanical Keyboard System Control as /devices/pci0000:00/0000:00:14.0/usb1/1-1/1-1:1.1/0003:1A2C:92F6.000D/input/input34
Sep 24 14:47:08 kernel: input: SEMICO   Redgear Shadow Blade Mechanical Keyboard as /devices/pci0000:00/0000:00:14.0/usb1/1-1/1-1:1.1/0003:1A2C:92F6.000D/input/input36
Sep 24 14:47:08 kernel: hid-generic 0003:1A2C:92F6.000D: input,hiddev97,hidraw3: USB HID v1.10 Keyboard [SEMICO   Redgear Shadow Blade Mechanical Keyboard] on usb-0000:00:14.0-1/input1
Sep 24 14:47:08 mtp-probe[7371]: checking bus 1, device 7: "/sys/devices/pci0000:00/0000:00:14.0/usb1/1-1"
Sep 24 14:47:08 mtp-probe[7371]: bus: 1, device: 7 was not an MTP device
Sep 24 14:47:08 /usr/lib/gdm-x-session[2337]: (II) config/udev: Adding input device SEMICO   Redgear Shadow Blade Mechanical Keyboard (/dev/input/event4)
Sep 24 14:47:08 /usr/lib/gdm-x-session[2337]: (**) SEMICO   Redgear Shadow Blade Mechanical Keyboard: Applying InputClass "libinput keyboard catchall"
Sep 24 14:47:08 /usr/lib/gdm-x-session[2337]: (II) Using input driver 'libinput' for 'SEMICO   Redgear Shadow Blade Mechanical Keyboard'
Sep 24 14:47:08 systemd-logind[494]: Watching system buttons on /dev/input/event4 (SEMICO   Redgear Shadow Blade Mechanical Keyboard)
```

4.4 Connecting and Disconnecting a Pendrive after Ejecting it Safely.

```

Sep 25 17:54:59 kernel: usb 1-3: new high-speed USB device number 12 using xhci_hcd
Sep 25 17:54:59 kernel: usb 1-3: New USB device found, idVendor=058f, idProduct=6387, bcdDevice= 1.00
Sep 25 17:54:59 kernel: usb 1-3: New USB device strings: Mfr=1, Product=2, SerialNumber=3
Sep 25 17:54:59 kernel: usb 1-3: Product: Mass Storage
Sep 25 17:54:59 kernel: usb 1-3: Manufacturer: Generic
Sep 25 17:54:59 kernel: usb 1-3: SerialNumber: 61EAF33F
Sep 25 17:54:59 kernel: usb-storage 1-3:1.0: USB Mass Storage device detected
Sep 25 17:54:59 kernel: scsi host2: usb-storage 1-3:1.0
Sep 25 17:54:59 mtp-probe[105648]: checking bus 1, device 12: "/sys/devices/pci0000:00/0000:00:14.0/usb1/1-3"
Sep 25 17:54:59 mtp-probe[105648]: bus: 1, device: 12 was not an MTP device
Sep 25 17:54:59 mtp-probe[105662]: checking bus 1, device 12: "/sys/devices/pci0000:00/0000:00:14.0/usb1/1-3"
Sep 25 17:54:59 mtp-probe[105662]: bus: 1, device: 12 was not an MTP device
Sep 25 17:54:59 dbus-daemon[487]: [system] Activating via systemd: service name='org.freedesktop.Avahi' unit='dbus-org.freedesktop.Avahi.service' requested by ':1.318' (uid=969 pid=105660 comm="/usr/lib/colord-sane")
Sep 25 17:54:59 dbus-daemon[487]: [system] Activation via systemd failed for unit 'dbus-org.freedesktop.Avahi.service': Unit dbus-org.freedesktop.Avahi.service not found.


# Eject

Sep 25 17:55:06 tracker-miner-f[3922]: tracker_indexing_tree_remove: assertion 'TRACKER_IS_INDEXING_TREE (tree)' failed
Sep 25 17:55:06 tracker-extract[4574]: g_file_new_for_uri: assertion 'uri != NULL' failed
Sep 25 17:55:06 tracker-extract[4574]: g_file_get_path: assertion 'G_IS_FILE (file)' failed
```

```
Sep 25 17:55:06 tracker-extract[4574]: GTask 0x55c3b9ec8760 (source object: 0 x55c3ba1399a0, source tag: (nil)) finalized without ever returning (using g_task_return_*()). This potentially indicates a bug in the program.
Sep 25 17:55:06 udisksd[1159]: Cleaning up mount point /run/media/krishnaraj/KRISH TONY (device 8:33 is not mounted)
Sep 25 17:55:06 udisksd[1159]: Unmounted /dev/sdc1 on behalf of uid 1000
Sep 25 17:55:06 systemd[1]: run-media-krishnaraj-KRISH\x20TONY.mount: Deactivated successfully.
Sep 25 17:55:06 gnome-shell[2564]: Failed to query filesystem: method Gio.File.query_filesystem_info_async: At least 4 arguments required, but only 3 passed
Sep 25 17:55:06 gnome-shell[2564]: Object .
Sep 25 17:55:06 gnome-shell[2564]: == Stack trace for context 0x55d57499c540 ==
Sep 25 17:55:06 gnome-shell[2564]: #0   55d57e14c538 i   /usr/share/gnome-shell/extensions/drive-menu@gnome-shell-extensions.gcampax.github.com/extension.js:89 (27fa701741f0 @ 70)
Sep 25 17:55:06 gnome-shell[2564]: #1   55d57e14c498 i   self-hosted:632 (ec406c1a650 @ 15)
Sep 25 17:55:07 kernel: sdc: detected capacity change from 61440000 to 0

# Disconnect
Sep 25 17:55:13 kernel: usb 1-3: USB disconnect, device number 12
Sep 25 17:55:13 dbus-daemon[487]: [system] Activating via systemd: service name='org.freedesktop.Avahi' unit='dbus-org.freedesktop.Avahi.service' requested by ':1.323' (uid=969 pid=105780 comm="/usr/lib/colord-sane")
Sep 25 17:55:13 dbus-daemon[487]: [system] Activation via systemd failed for unit 'dbus-org.freedesktop.Avahi.service': Unit dbus-org.freedesktop.Avahi.service not found.
```

4.5 Connecting and Disconnecting a Pendrive without Ejecting it Safely.

```
Sep 25 17:51:37 kernel: usb 1-3: new high-speed USB device number 9 using xhci_hcd
Sep 25 17:51:37 kernel: usb 1-3: New USB device found, idVendor=058f, idProduct=6387, bcdDevice= 1.00
Sep 25 17:51:37 kernel: usb 1-3: New USB device strings: Mfr=1, Product=2, SerialNumber=3
Sep 25 17:51:37 kernel: usb 1-3: Product: Mass Storage
Sep 25 17:51:37 kernel: usb 1-3: Manufacturer: Generic
Sep 25 17:51:37 kernel: usb 1-3: SerialNumber: 61EAF33F
Sep 25 17:51:37 kernel: usb-storage 1-3:1.0: USB Mass Storage device detected
Sep 25 17:51:37 kernel: scsi host2: usb-storage 1-3:1.0
Sep 25 17:51:37 mtp-probe[104808]: checking bus 1, device 9: "/sys/devices/pci0000:00/0000:00:14.0/usb1/1-3"
Sep 25 17:51:37 mtp-probe[104808]: bus: 1, device: 9 was not an MTP device
Sep 25 17:51:38 mtp-probe[104822]: checking bus 1, device 9: "/sys/devices/pci0000:00/0000:00:14.0/usb1/1-3"
Sep 25 17:51:38 mtp-probe[104822]: bus: 1, device: 9 was not an MTP device
Sep 25 17:51:38 dbus-daemon[487]: [system] Activating via systemd: service name='org.freedesktop.Avahi' unit='dbus-org.freedesktop.Avahi.service' requested by ':1.299' (uid=969 pid=104820 comm="/usr/lib/colord-sane")
Sep 25 17:51:38 dbus-daemon[487]: [system] Activation via systemd failed for unit 'dbus-org.freedesktop.Avahi.service': Unit dbus-org.freedesktop.Avahi.service not found.
Sep 25 17:51:38 kernel: scsi 2:0:0:0: Direct-Access     Generic  Flash Disk       8.07 PQ: 0 ANSI: 4
Sep 25 17:51:38 kernel: sd 2:0:0:0: Attached scsi generic sg2 type 0
Sep 25 17:51:38 kernel: sd 2:0:0:0: [sdc] 61440000 512-byte logical blocks: (31.5 GB/29.3 GiB)
Sep 25 17:51:38 kernel: sd 2:0:0:0: [sdc] Write Protect is off
```

```
Sep 25 17:51:38 kernel: sd 2:0:0:0: [sdc] Mode Sense: 23 00 00 00
Sep 25 17:51:38 kernel: sd 2:0:0:0: [sdc] Write cache: disabled, read cache:
    enabled, doesn't support DPO or FUA
Sep 25 17:51:38 kernel:  sdc: sdc1
Sep 25 17:51:38 kernel: sd 2:0:0:0: [sdc] Attached SCSI removable disk
Sep 25 17:51:39 dbus-daemon[487]: [system] Activating via systemd: service name='
    org.freedesktop.Avahi' unit='dbus-org.freedesktop.Avahi.service' requested by '
    :1.301' (uid=969 pid=104843 comm="/usr/lib/colord-sane")

# Remove without Eject

Sep 25 17:51:48 kernel: usb 1-3: USB disconnect, device number 9
Sep 25 17:51:48 udisksd[1159]: Cleaning up mount point /run/media/krishnaraj/KRISH
     TONY (device 8:33 no longer exists)
Sep 25 17:51:48 kernel: FAT-fs (sdc1): unable to read boot sector to mark fs as
    dirty
Sep 25 17:51:48 systemd[1]: run-media-krishnaraj-KRISH\x20TONY.mount: Deactivated
    successfully.
Sep 25 17:51:48 gnome-shell[2564]: Failed to query filesystem: method Gio.File.
    query_filesystem_info_async: At least 4 arguments required, but only 3 passed
Sep 25 17:51:48 dbus-daemon[487]: [system] Activating via systemd: service name='
    org.freedesktop.Avahi' unit='dbus-org.freedesktop.Avahi.service' requested by '
    :1.304' (uid=969 pid=104916 comm="/usr/lib/colord-sane")
Sep 25 17:51:48 dbus-daemon[487]: [system] Activation via systemd failed for unit
    'dbus-org.freedesktop.Avahi.service': Unit dbus-org.freedesktop.Avahi.service
    not found.
```

4.6 Switching on Bluetooth

```
Sep 25 17:43:57 bluetoothd[486]: Failed to set mode: Failed (0x03)
Sep 25 17:43:58 blueman.desktop[3056]: blueman-applet 17.43.58 WARNING
    PowerManager:203 on_adapter_property_changed: adapter powered on while in off
    state, turning bluetooth on
Sep 25 17:43:58 NetworkManager[548]: <info>  [1695644038.0038] manager: (04:C8
    :07:31:0F:FB): new Bluetooth device (/org/freedesktop/NetworkManager/Devices
    /12)
Sep 25 17:43:58 NetworkManager[548]: <info>  [1695644038.0041] device (04:C8
    :07:31:0F:FB): state change: unmanaged -> unavailable (reason 'managed', sys-
    iface-state: 'external')
Sep 25 17:43:58 NetworkManager[548]: <info>  [1695644038.0046] device (04:C8
    :07:31:0F:FB): state change: unavailable -> disconnected (reason 'none', sys-
    iface-state: 'managed')
Sep 25 17:44:01 systemd[1]: NetworkManager-dispatcher.service: Deactivated
    successfully.
Sep 25 17:44:02 systemd[1]: systemd-rfkill.service: Deactivated successfully.
Sep 25 17:44:11 systemd[1]: Reached target Bluetooth Support.
Sep 25 17:44:12 kernel: input: Samsung Level U2 (9304) (AVRCP) as /devices/virtual
    /input/input44
Sep 25 17:44:12 rtkit-daemon[1196]: Supervising 6 threads of 3 processes of 1
    users
```

4.7 Connecting to a Bluetooth Headset

```
Sep 25 17:44:12 kernel: Bluetooth: hci0: corrupted SCO packet
Sep 25 17:44:12 systemd-logind[494]: Watching system buttons on /dev/input/event17
     (Samsung Level U2 (9304) (AVRCP))
```

```
Sep 25 17:44:12 /usr/lib/gdm-x-session[2337]: (II) config/udev: Adding input device Samsung Level U2 (9304) (AVRCP) (/dev/input/event17)
Sep 25 17:44:12 /usr/lib/gdm-x-session[2337]: (**) Samsung Level U2 (9304) (AVRCP): Applying InputClass "libinput keyboard catchall"
Sep 25 17:44:12 /usr/lib/gdm-x-session[2337]: (II) Using input driver 'libinput' for 'Samsung Level U2 (9304) (AVRCP)'
Sep 25 17:44:12 /usr/lib/gdm-x-session[2337]: (II) systemd-logind: got fd for /dev/input/event17 13:81 fd 144 paused 0
Sep 25 17:44:12 /usr/lib/gdm-x-session[2337]: (**) Samsung Level U2 (9304) (AVRCP): always reports core events
Sep 25 17:44:12 /usr/lib/gdm-x-session[2337]: (**) Option "Device" "/dev/input/event17"
Sep 25 17:44:12 /usr/lib/gdm-x-session[2337]: (II) event17 - Samsung Level U2 (9304) (AVRCP): is tagged by udev as: Keyboard
Sep 25 17:44:12 /usr/lib/gdm-x-session[2337]: (II) event17 - Samsung Level U2 (9304) (AVRCP): device is a keyboard
Sep 25 17:44:12 /usr/lib/gdm-x-session[2337]: (II) event17 - Samsung Level U2 (9304) (AVRCP): device removed
Sep 25 17:44:12 /usr/lib/gdm-x-session[2337]: (**) Option "config_info" "udev:/sys/devices/virtual/input/input44/event17"
Sep 25 17:44:12 /usr/lib/gdm-x-session[2337]: (II) XINPUT: Adding extended input device "Samsung Level U2 (9304) (AVRCP)" (type: KEYBOARD, id 18)
Sep 25 17:44:12 /usr/lib/gdm-x-session[2337]: (II) event17 - Samsung Level U2 (9304) (AVRCP): is tagged by udev as: Keyboard
Sep 25 17:44:12 /usr/lib/gdm-x-session[2337]: (II) event17 - Samsung Level U2 (9304) (AVRCP): device is a keyboard
Sep 25 17:44:12 qbittorrent[9578]: qt.qpa.input.events: scroll event from unregistered device 12
Sep 25 17:44:12 pulseaudio[2716]: Battery Level: 20%
```

5 Platform

Operating System: Arch Linux x86-64
IDEs or Text Editors Used: Visual Studio Code
Compilers or Interpreters: None.

6 Conclusion

Thus, we have successfully analysed the system logs of a Linux System, and learnt about the different scenarios that can be detected from them.

References

[1] Where are Logs in Linux
Stackify

[2] Linux Logs Explained
plesk

[3] How To View And Analyze Logs With Windows Event Viewer
Better Stack