Identifying the Types of Logs Available on Windows and Linux for Forensic Investigation and use of Tools for it.

***Abstract*—This paper explores the various types of logs available in Windows and Linux operating systems for forensic investigations. In addition, the study examines the role of third-party tools in reading, analyzing, and interpreting these logs.**

I. Introduction

Logs are records of system, network, or application activities. In cybersecurity, they play a crucial role in detecting and responding to incidents, conducting forensic analysis, ensuring compliance, and monitoring system health.

In digital forensics, logs serve as key evidence during investigations. They help forensic analysts in the following ways:

- **Identifying suspicious activities**: Logs can reveal unauthorized access attempts, malware execution, and abnormal system behaviors.
- **Tracing user actions**: By examining logs, investigators can trace user activities, such as file transfers, login/logout times, and system modifications.
- **Reconstructing events**: Logs allow forensic experts to piece together the timeline of an attack or security breach, helping them understand what happened and how it occurred.
- **Detecting data breaches**: Logs provide insight into potential data breaches by showing patterns of data access or exfiltration, enabling analysts to detect unauthorized data movements.

II. Importance of Logs in Forensic Investigations

Logs assist forensic investigators in several ways:

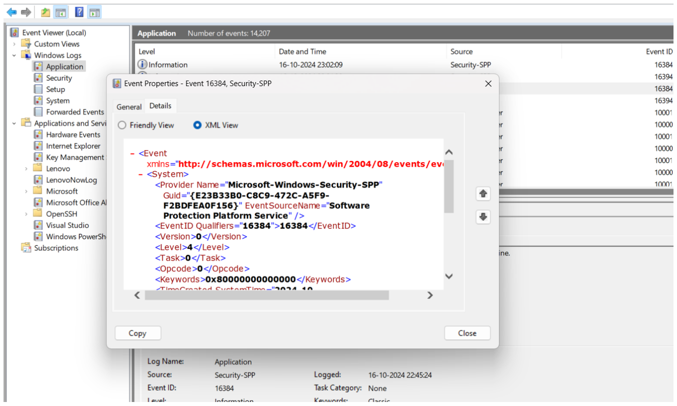
- **Reconstruct Events**: Logs provide timelines of activities that help trace past actions on the system.
- **Identify Security Breaches**: Security logs reveal unauthorized access attempts or malware activities.
- **Trace User Activities**: Logs track login attempts, file access, system changes, and other user actions.
- **Collect Evidence**: Logs serve as evidence in digital forensics, proving the occurrence of certain activities.

III. Types of Logs in Windows

Windows logs are primarily accessed via the Event Viewer (`eventvwr.msc`). Below are the key logs:

A. System Logs

- **Purpose**: Logs system events such as startup, shutdown, hardware issues, and driver problems.
- **Location**: `C:/Windows/System32/winevt/Logs/`
- **Example**: Detecting hardware failures or system reboots.



Application Number of events: 14,207

```
Level          Date and Time         Source         Event ID
Information    16-10-2024 23:02:09   Security-SPP   16384
```

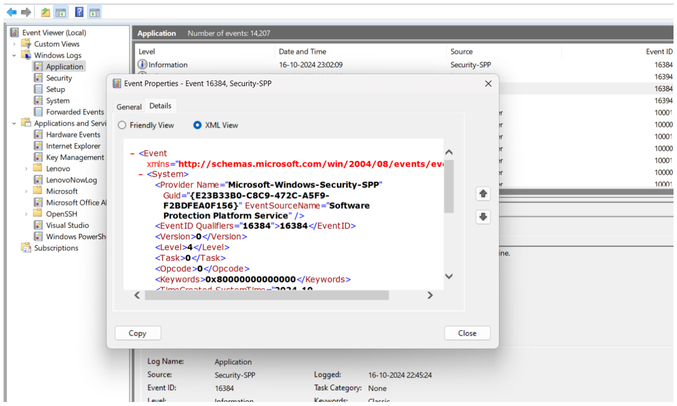
```
- <Event
   xmlns="http://schemas.microsoft.com/win/2004/08/events/ev
 - <System>
     <Provider Name="Microsoft-Windows-Security-SPP"
       Guid="{E23B33B0-C8C9-472C-A5F9-
       F2BDFEA0F156}" EventSourceName="Software
       Protection Platform Service" />
     <EventID Qualifiers="16384">16384</EventID>
     <Version>0</Version>
     <Level>4</Level>
     <Task>0</Task>
     <Opcode>0</Opcode>
     <Keywords>0x80000000000000</Keywords>
```

Log Name: Application
Source: Security-SPP Logged: 16-10-2024 22:45:24
Event ID: 16384 Task Category: None

Fig. 1. This is an example of system log.

B. Application Logs

- **Purpose**: Logs application-specific events like errors, crashes, and installation issues.
- **Example**: Tracking issues with installed software like Microsoft Office.



Application Number of events: 14,207

```
Level          Date and Time         Source         Event ID
Information    16-10-2024 23:02:09   Security-SPP   16384
```

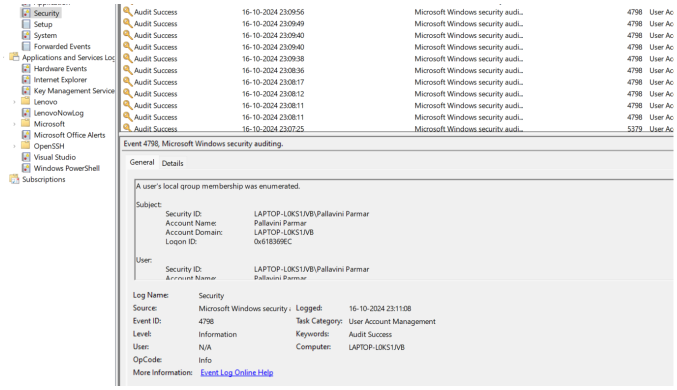
```
- <Event
   xmlns="http://schemas.microsoft.com/win/2004/08/events/ev
 - <System>
     <Provider Name="Microsoft-Windows-Security-SPP"
       Guid="{E23B33B0-C8C9-472C-A5F9-
       F2BDFEA0F156}" EventSourceName="Software
       Protection Platform Service" />
     <EventID Qualifiers="16384">16384</EventID>
     <Version>0</Version>
     <Level>4</Level>
     <Task>0</Task>
     <Opcode>0</Opcode>
     <Keywords>0x80000000000000</Keywords>
```

Log Name: Application
Source: Security-SPP Logged: 16-10-2024 22:45:24
Event ID: 16384 Task Category: None

Fig. 2. This is an application log.

C. Security Logs

- **Purpose**: Logs events related to security, such as login attempts, permission changes, and access controls.
- **Event IDs to Note**:
  - 4624: Successful logon.
  - 4625: Failed logon.
  - 4688: Process creation.
- **Example**: Investigating unauthorized access or failed login attempts.



```
Audit Success   16-10-2024 23:09:56   Microsoft Windows security audi...   4798   User Ac
Audit Success   16-10-2024 23:09:49   Microsoft Windows security audi...   4798   User Ac
Audit Success   16-10-2024 23:09:40   Microsoft Windows security audi...   4798   User Ac
Audit Success   16-10-2024 23:09:40   Microsoft Windows security audi...   4798   User Ac
Audit Success   16-10-2024 23:09:38   Microsoft Windows security audi...   4798   User Ac
Audit Success   16-10-2024 23:08:36   Microsoft Windows security audi...   4798   User Ac
Audit Success   16-10-2024 23:08:17   Microsoft Windows security audi...   4798   User Ac
Audit Success   16-10-2024 23:08:12   Microsoft Windows security audi...   4798   User Ac
Audit Success   16-10-2024 23:08:11   Microsoft Windows security audi...   4798   User Ac
Audit Success   16-10-2024 23:08:11   Microsoft Windows security audi...   4798   User Ac
Audit Success   16-10-2024 23:07:25   Microsoft Windows security audi...   5379   User Ac
```

Event 4798, Microsoft Windows security auditing.

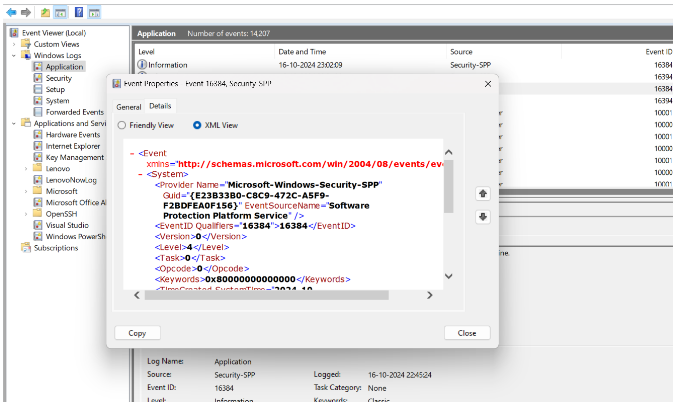
```
A user's local group membership was enumerated.

Subject:
        Security ID:        LAPTOP-L0KS1JVB\Pallavini Parmar
        Account Name:       Pallavini Parmar
        Account Domain:     LAPTOP-L0KS1JVB
        Logon ID:           0x618369EC

User:
        Security ID:        LAPTOP-L0KS1JVB\Pallavini Parmar
        Account Name:       Pallavini Parmar
```

```
Log Name:          Security
Source:            Microsoft Windows security a   Logged:          16-10-2024 23:11:08
Event ID:          4798                           Task Category:   User Account Management
Level:             Information                    Keywords:        Audit Success
User:              N/A                            Computer:        LAPTOP-L0KS1JVB
OpCode:            Info
More Information:  Event Log Online Help
```

Fig. 3. This is security log

D. Forwarded Event Logs

- **Purpose**: Events collected from other machines and forwarded to a central location.
- **Example**: Collecting logs from multiple systems in a network environment.



Application Number of events: 14,207

```
Level          Date and Time         Source         Event ID
Information    16-10-2024 23:02:09   Security-SPP   16384
                                                    16394
                                                    16384
                                                    16394
                                                    10001
                                                    10000
                                                    10001
                                                    10000
                                                    10001
                                                    10000
                                                    10001
```

Event Properties - Event 16384, Security-SPP

```
- <Event
   xmlns="http://schemas.microsoft.com/win/2004/08/events/ev
 - <System>
     <Provider Name="Microsoft-Windows-Security-SPP"
       Guid="{E23B33B0-C8C9-472C-A5F9-
       F2BDFEA0F156}" EventSourceName="Software
       Protection Platform Service" />
     <EventID Qualifiers="16384">16384</EventID>
     <Version>0</Version>
     <Level>4</Level>
     <Task>0</Task>
     <Opcode>0</Opcode>
     <Keywords>0x80000000000000</Keywords>
```

```
Log Name:   Application
Source:     Security-SPP     Logged:          16-10-2024 22:45:24
Event ID:   16384            Task Category:   None
```

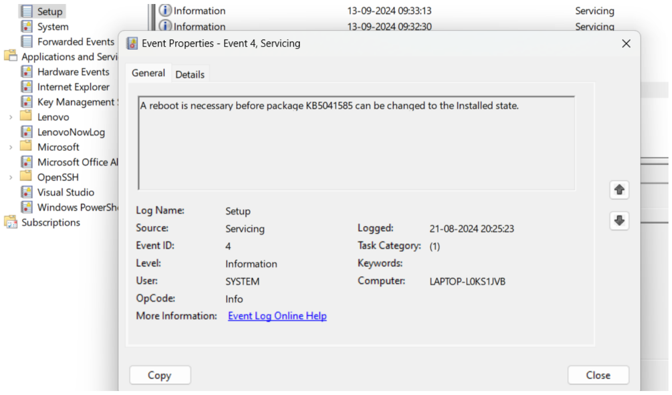
Fig. 4. forwarding event logs.

E. Setup Logs

- **Purpose**: Logs events during system installation or configuration changes.
- **Example**: Identifying configuration changes during system setup.

IV. KEY TYPES OF LOGS IN LINUX

Linux logs are usually stored in `/var/log/`. Below are some important types of logs:



```
Information   13-09-2024 09:33:13   Servicing
Information   13-09-2024 09:32:30   Servicing
```

Event Properties - Event 4, Servicing

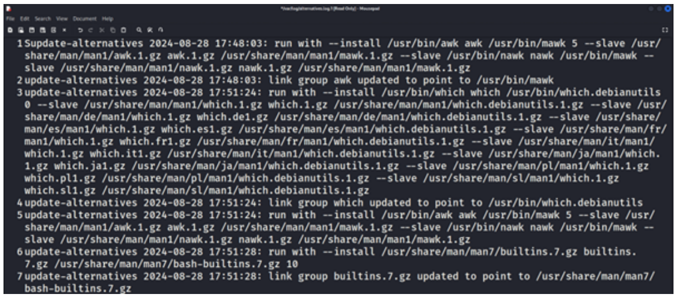
A reboot is necessary before package KB5041585 can be changed to the Installed state.

```
Log Name:          Setup
Source:            Servicing       Logged:          21-08-2024 20:25:23
Event ID:          4               Task Category:   (1)
Level:             Information     Keywords:
User:              SYSTEM          Computer:        LAPTOP-L0KS1JVB
OpCode:            Info
More Information:  Event Log Online Help
```

Fig. 5. This is the imge of setup log

A. Syslog (`/var/log/syslog` or `/var/log/messages`)

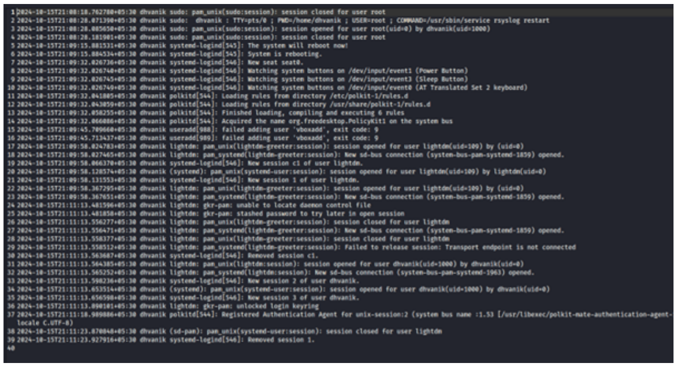
- **Purpose**: General-purpose log for system-wide messages.
- **Example**: Recording system startup/shutdown or hardware issues.



```
update-alternatives 2024-08-28 17:48:03: run with --install /usr/bin/awk awk /usr/bin/mawk 5 --slave /usr/
 share/man/man1/awk.1.gz awk.1.gz /usr/share/man/man1/mawk.1.gz --slave /usr/bin/nawk nawk /usr/bin/mawk --
 slave /usr/share/man/man1/nawk.1.gz nawk.1.gz /usr/share/man/man1/mawk.1.gz
update-alternatives 2024-08-28 17:48:03: link group awk updated to point to /usr/bin/mawk
update-alternatives 2024-08-28 17:51:24: run with --install /usr/bin/which which /usr/bin/which.debianutils
 0 --slave /usr/share/man/man1/which.1.gz which.1.gz /usr/share/man/man1/which.debianutils.1.gz --slave /usr/
 share/man/de/man1/which.1.gz which.de1.gz /usr/share/man/de/man1/which.debianutils.1.gz --slave /usr/share/
 man/es/man1/which.1.gz which.es1.gz /usr/share/man/es/man1/which.debianutils.1.gz --slave /usr/share/man/fr/
 man1/which.1.gz which.fr1.gz /usr/share/man/fr/man1/which.debianutils.1.gz --slave /usr/share/man/it/man1/
 which.1.gz which.it1.gz /usr/share/man/it/man1/which.debianutils.1.gz --slave /usr/share/man/ja/man1/which.
 1.gz which.ja1.gz /usr/share/man/ja/man1/which.debianutils.1.gz --slave /usr/share/man/pl/man1/which.1.gz
 which.pl1.gz /usr/share/man/pl/man1/which.debianutils.1.gz --slave /usr/share/man/sl/man1/which.1.gz
 which.sl1.gz /usr/share/man/sl/man1/which.debianutils.1.gz
update-alternatives 2024-08-28 17:51:24: link group which updated to point to /usr/bin/which.debianutils
update-alternatives 2024-08-28 17:51:24: run with --install /usr/bin/awk awk /usr/bin/mawk 5 --slave /usr/
 share/man/man1/awk.1.gz awk.1.gz /usr/share/man/man1/mawk.1.gz --slave /usr/bin/nawk nawk /usr/bin/mawk --
 slave /usr/share/man/man1/nawk.1.gz nawk.1.gz /usr/share/man/man1/mawk.1.gz
update-alternatives 2024-08-28 17:51:28: run with --install /usr/share/man/man7/builtins.7.gz builtins.
 7.gz /usr/share/man/man7/bash-builtins.7.gz 10
update-alternatives 2024-08-28 17:51:28: link group builtins.7.gz updated to point to /usr/share/man/man7/
 bash-builtins.7.gz
```

B. Auth Log (`/var/log/auth.log` or `/var/log/secure`)

- **Purpose**: Logs all authentication-related events such as login attempts and sudo usage.
- **Example**: Detecting unauthorized access or brute-force attacks.

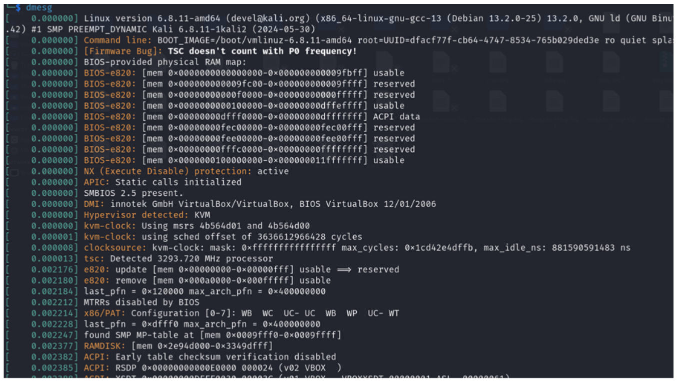


```
2024-10-15T21:08:18.762780+05:30 dhvanik sudo: pam_unix(sudo:session): session closed for user root
2024-10-15T21:08:28.071390+05:30 dhvanik sudo:  dhvanik : TTY=pts/0 ; PWD=/home/dhvanik ; USER=root ; COMMAND=/usr/sbin/service rsyslog restart
2024-10-15T21:08:28.085650+05:30 dhvanik sudo: pam_unix(sudo:session): session opened for user root(uid=0) by dhvanik(uid=1000)
2024-10-15T21:08:28.181901+05:30 dhvanik sudo: pam_unix(sudo:session): session closed for user root
2024-10-15T21:09:15.881531+05:30 dhvanik systemd-logind[545]: The system will reboot now!
2024-10-15T21:09:15.884534+05:30 dhvanik systemd-logind[545]: System is rebooting.
2024-10-15T21:09:32.026736+05:30 dhvanik systemd-logind[546]: New seat seat0.
2024-10-15T21:09:32.026740+05:30 dhvanik systemd-logind[546]: Watching system buttons on /dev/input/event1 (Power Button)
2024-10-15T21:09:32.026745+05:30 dhvanik systemd-logind[546]: Watching system buttons on /dev/input/event3 (Sleep Button)
2024-10-15T21:09:32.026749+05:30 dhvanik systemd-logind[546]: Watching system buttons on /dev/input/event0 (AT Translated Set 2 keyboard)
2024-10-15T21:09:32.041805+05:30 dhvanik polkitd[544]: Loading rules from directory /etc/polkit-1/rules.d
2024-10-15T21:09:32.043059+05:30 dhvanik polkitd[544]: Loading rules from directory /usr/share/polkit-1/rules.d
2024-10-15T21:09:32.058255+05:30 dhvanik polkitd[544]: Finished loading, compiling and executing 6 rules
2024-10-15T21:09:32.066086+05:30 dhvanik polkitd[544]: Acquired the name org.freedesktop.PolicyKit1 on the system bus
2024-10-15T21:09:45.709660+05:30 dhvanik useradd[988]: failed adding user 'vboxadd', exit code: 9
2024-10-15T21:09:45.713437+05:30 dhvanik useradd[989]: failed adding user 'vboxadd', exit code: 9
2024-10-15T21:09:58.024783+05:30 dhvanik lightdm: pam_unix(lightdm-greeter:session): session opened for user lightdm(uid=109) by (uid=0)
2024-10-15T21:09:58.027465+05:30 dhvanik lightdm: pam_systemd(lightdm-greeter:session): New sd-bus connection (system-bus-pam-systemd-1859) opened.
2024-10-15T21:09:58.066370+05:30 dhvanik systemd-logind[546]: New session c1 of user lightdm.
2024-10-15T21:09:58.128574+05:30 dhvanik (systemd): pam_unix(systemd-user:session): session opened for user lightdm(uid=109) by lightdm(uid=0)
2024-10-15T21:09:58.131553+05:30 dhvanik systemd-logind[546]: New session 1 of user lightdm.
2024-10-15T21:09:58.367295+05:30 dhvanik lightdm: pam_unix(lightdm-greeter:session): session opened for user lightdm(uid=109) by (uid=0)
2024-10-15T21:09:58.367651+05:30 dhvanik lightdm: pam_systemd(lightdm-greeter:session): New sd-bus connection (system-bus-pam-systemd-1859) opened.
2024-10-15T21:11:13.481596+05:30 dhvanik lightdm: gkr-pam: unable to locate daemon control file
2024-10-15T21:11:13.481858+05:30 dhvanik lightdm: gkr-pam: stashed password to try later in open session
2024-10-15T21:11:13.556277+05:30 dhvanik lightdm: pam_unix(lightdm-greeter:session): session closed for user lightdm
2024-10-15T21:11:13.556471+05:30 dhvanik lightdm: pam_systemd(lightdm-greeter:session): New sd-bus connection (system-bus-pam-systemd-1859) opened.
2024-10-15T21:11:13.558377+05:30 dhvanik lightdm: pam_unix(lightdm-greeter:session): session closed for user lightdm
2024-10-15T21:11:13.558512+05:30 dhvanik lightdm: pam_systemd(lightdm-greeter:session): Failed to release session: Transport endpoint is not connected
2024-10-15T21:11:13.563687+05:30 dhvanik systemd-logind[546]: Removed session c1.
2024-10-15T21:11:13.564385+05:30 dhvanik lightdm: pam_unix(lightdm:session): session opened for user dhvanik(uid=1000) by dhvanik(uid=0)
2024-10-15T21:11:13.565252+05:30 dhvanik lightdm: pam_systemd(lightdm:session): New sd-bus connection (system-bus-pam-systemd-1963) opened.
2024-10-15T21:11:13.598236+05:30 dhvanik systemd-logind[546]: New session 2 of user dhvanik.
2024-10-15T21:11:13.653514+05:30 dhvanik (systemd): pam_unix(systemd-user:session): session opened for user dhvanik(uid=1000) by dhvanik(uid=0)
2024-10-15T21:11:13.656598+05:30 dhvanik systemd-logind[546]: New session 3 of user dhvanik.
2024-10-15T21:11:13.890101+05:30 dhvanik lightdm: gkr-pam: unlocked login keyring
2024-10-15T21:11:18.989886+05:30 dhvanik polkitd[544]: Registered Authentication Agent for unix-session:2 (system bus name :1.53 [/usr/libexec/polkit-mate-authentication-agent-
 locale C.UTF-8)
2024-10-15T21:11:23.870848+05:30 dhvanik (sd-pam): pam_unix(systemd-user:session): session closed for user lightdm
2024-10-15T21:11:23.927916+05:30 dhvanik systemd-logind[546]: Removed session 1.
```

Fig. 6. authlogs.

C. *Dmesg (`dmesg` or `/var/log/dmesg`)*

- **Purpose**: Logs kernel-level messages, especially hardware-related events during boot.
- **Example**: Tracking kernel warnings and hardware changes.

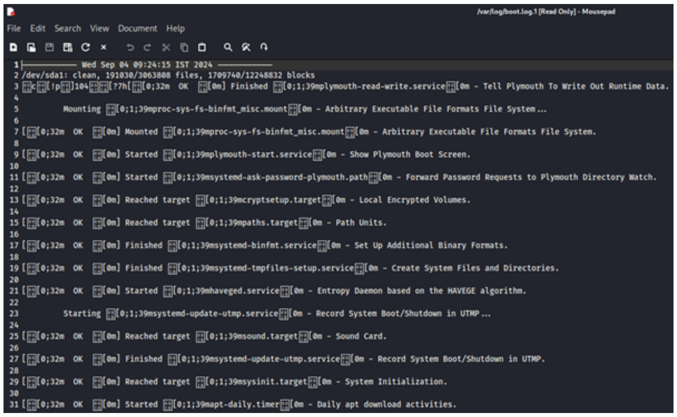


```
└─$ dmesg
[    0.000000] Linux version 6.8.11-amd64 (devel@kali.org) (x86_64-linux-gnu-gcc-13 (Debian 13.2.0-25) 13.2.0, GNU ld (GNU Binu
.42) #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30)
[    0.000000] Command line: BOOT_IMAGE=/boot/vmlinuz-6.8.11-amd64 root=UUID=dfacf77f-cb64-4747-8534-765b029ded3e ro quiet spla
[    0.000000] [Firmware Bug]: TSC doesn't count with P0 frequency!
[    0.000000] BIOS-provided physical RAM map:
[    0.000000] BIOS-e820: [mem 0×0000000000000000-0×000000000009fbff] usable
[    0.000000] BIOS-e820: [mem 0×000000000009fc00-0×000000000009ffff] reserved
[    0.000000] BIOS-e820: [mem 0×00000000000f0000-0×00000000000fffff] reserved
[    0.000000] BIOS-e820: [mem 0×0000000000100000-0×00000000dffeffff] usable
[    0.000000] BIOS-e820: [mem 0×00000000dfff0000-0×00000000dfffffff] ACPI data
[    0.000000] BIOS-e820: [mem 0×00000000fec00000-0×00000000fec00fff] reserved
[    0.000000] BIOS-e820: [mem 0×00000000fee00000-0×00000000fee00fff] reserved
[    0.000000] BIOS-e820: [mem 0×00000000fffc0000-0×00000000ffffffff] reserved
[    0.000000] BIOS-e820: [mem 0×0000000100000000-0×000000011fffffff] usable
[    0.000000] NX (Execute Disable) protection: active
[    0.000000] APIC: Static calls initialized
[    0.000000] SMBIOS 2.5 present.
[    0.000000] DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
[    0.000000] Hypervisor detected: KVM
[    0.000000] kvm-clock: Using msrs 4b564d01 and 4b564d00
[    0.000001] kvm-clock: using sched offset of 3636612966428 cycles
[    0.000008] clocksource: kvm-clock: mask: 0×ffffffffffffffff max_cycles: 0×1cd42e4dffb, max_idle_ns: 881590591483 ns
[    0.000013] tsc: Detected 3293.720 MHz processor
[    0.002176] e820: update [mem 0×00000000-0×00000fff] usable ⟹ reserved
[    0.002180] e820: remove [mem 0×000a0000-0×000fffff] usable
[    0.002184] last_pfn = 0×120000 max_arch_pfn = 0×400000000
[    0.002212] MTRRs disabled by BIOS
[    0.002214] x86/PAT: Configuration [0-7]: WB  WC  UC- UC  WB  WP  UC- WT
[    0.002228] last_pfn = 0×dfff0 max_arch_pfn = 0×400000000
[    0.002247] found SMP MP-table at [mem 0×0009fff0-0×0009ffff]
[    0.002377] RAMDISK: [mem 0×2e94d000-0×3349dfff]
[    0.002382] ACPI: Early table checksum verification disabled
[    0.002385] ACPI: RSDP 0×00000000000E0000 000024 (v02 VBOX  )
[    0.002388] ACPI: XSDT 0×00000000DFFF0030 00003C (v01 VBOX   VBOXXSDT 00000001 ASL  00000061)
```

Fig. 7. dmasssage.

D. *Boot Log (`/var/log/boot.log`)*

- **Purpose**: Logs events during the system's boot process.
- **Example**: Detecting boot failures or anomalies during system startup.



/var/log/boot.log.1 [Read Only] - Mousepad
File Edit Search View Document Help

```
------------ Wed Sep 04 09:24:15 IST 2024 ------------
/dev/sda1: clean, 191030/3063808 files, 1709740/12248832 blocks
□c□[!p□]104□□[?7h[□[0;32m  OK  □[0m] Finished □[0;1;39mplymouth-read-write.service□[0m - Tell Plymouth To Write Out Runtime Data.

         Mounting □[0;1;39mproc-sys-fs-binfmt_misc.mount□[0m - Arbitrary Executable File Formats File System...

[□[0;32m  OK  □[0m] Mounted □[0;1;39mproc-sys-fs-binfmt_misc.mount□[0m - Arbitrary Executable File Formats File System.

[□[0;32m  OK  □[0m] Started □[0;1;39mplymouth-start.service□[0m - Show Plymouth Boot Screen.

[□[0;32m  OK  □[0m] Started □[0;1;39msystemd-ask-password-plymouth.path□[0m - Forward Password Requests to Plymouth Directory Watch.

[□[0;32m  OK  □[0m] Reached target □[0;1;39mcryptsetup.target□[0m - Local Encrypted Volumes.

[□[0;32m  OK  □[0m] Reached target □[0;1;39mpaths.target□[0m - Path Units.

[□[0;32m  OK  □[0m] Finished □[0;1;39msystemd-binfmt.service□[0m - Set Up Additional Binary Formats.

[□[0;32m  OK  □[0m] Finished □[0;1;39msystemd-tmpfiles-setup.service□[0m - Create System Files and Directories.

[□[0;32m  OK  □[0m] Started □[0;1;39mhaveged.service□[0m - Entropy Daemon based on the HAVEGE algorithm.

         Starting □[0;1;39msystemd-update-utmp.service□[0m - Record System Boot/Shutdown in UTMP...

[□[0;32m  OK  □[0m] Reached target □[0;1;39msound.target□[0m - Sound Card.

[□[0;32m  OK  □[0m] Finished □[0;1;39msystemd-update-utmp.service□[0m - Record System Boot/Shutdown in UTMP.

[□[0;32m  OK  □[0m] Reached target □[0;1;39msysinit.target□[0m - System Initialization.

[□[0;32m  OK  □[0m] Started □[0;1;39mapt-daily.timer□[0m - Daily apt download activities.
```

Fig. 8. bootlogs.

E. *Faillog (`/var/log/faillog`)*

- **Purpose**: Tracks failed login attempts.
- **Example**: Detecting brute-force attacks by analyzing multiple failed login attempts.

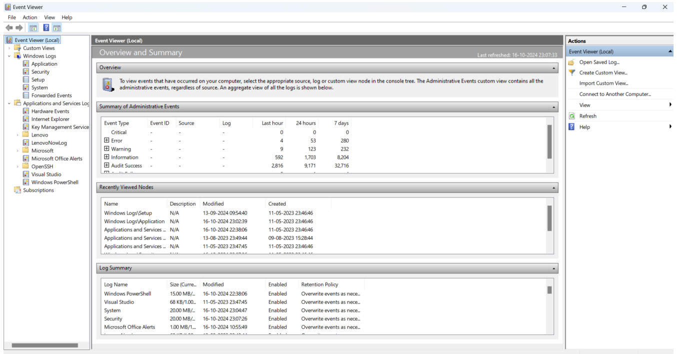
F. *Lastlog (`/var/log/lastlog`)*

- **Purpose**: Contains information on the last login of all users.
- **Example**: Reviewing the time and origin of the last user login.

V. Windows Tools

A. *Event Log Explorer*

- **Purpose**: Event Log Explorer is used to analyze and manage Windows event logs. It helps system administrators view, monitor, and analyze events on local or remote Windows machines.
- **How it works**: It connects to the Windows Event Log Service and pulls event logs from various sources, like Application, Security, and System logs.
- **Features**:
  - Search, filter, and group event logs.
  - Bookmarking important events.
  - Exporting event logs to formats such as HTML, PDF, and Excel.
  - Multiple viewing options, including side-by-side comparisons.
- **Pros**:
  - Easy to use for non-technical users.
  - Efficient for managing large volumes of logs.
  - Supports both real-time and historical log analysis.
- **Cons**:
  - Limited advanced search capabilities compared to other tools.
  - Only supports Windows platforms.



To view events that have occurred on your computer, select the appropriate source, log or custom view node in the console tree. The Administrative Events custom view contains all the administrative events, regardless of source. An aggregate view of all the logs is shown below.

Event Type	Event ID	Source	Log	Last hour	24 hours	7 days
Critical	-	-	-	0	0	0
⊞ Error	-	-	-	4	53	280
⊞ Warning	-	-	-	9	123	232
⊞ Information	-	-	-	592	1,703	8,204
⊞ Audit Success	-	-	-	2,816	9,171	32,716

Name	Description	Modified	Created
Windows Logs\Setup	N/A	13-09-2024 09:54:40	11-05-2023 23:46:46
Windows Logs\Application	N/A	16-10-2024 23:02:39	11-05-2023 23:46:46
Applications and Services ...	N/A	16-10-2024 22:38:06	11-05-2023 23:46:46
Applications and Services ...	N/A	13-08-2023 23:49:44	09-08-2023 15:28:44
Applications and Services ...	N/A	11-05-2023 23:47:45	11-05-2023 23:46:46

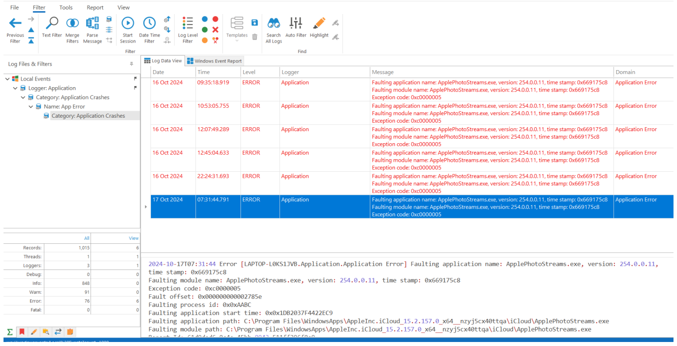
Log Name	Size (Curre...	Modified	Enabled	Retention Policy
Windows PowerShell	15.00 MB/...	16-10-2024 22:38:06	Enabled	Overwrite events as nece...
Visual Studio	68 KB/1.00...	11-05-2023 23:47:45	Enabled	Overwrite events as nece...
System	20.00 MB/...	16-10-2024 23:04:47	Enabled	Overwrite events as nece...
Security	20.00 MB/...	16-10-2024 23:07:26	Enabled	Overwrite events as nece...
Microsoft Office Alerts	1.00 MB/1....	16-10-2024 10:55:49	Enabled	Overwrite events as nece...

Fig. 9. This is event view tool.

B. *LogViewPlus*

- **Purpose**: LogViewPlus is designed to help users analyze log files generated by various systems, not limited to Windows event logs.
- **How it works**: It allows users to read logs in real-time, merge multiple logs, and perform advanced search queries across large datasets.
- **Features**:
  - Real-time log monitoring.
  - Merging multiple log files into a unified view.
  - Filtering, searching, and highlighting important events.
  - Supports tailing and auto-refresh of logs.
- **Pros**:

  - Multi-platform support, including Windows and Java applications.
  - Powerful search and filtering options.
  - Intuitive interface with clear visualization of logs.
- **Cons**:
  - Free version has limited features.
  - Complex setup for users unfamiliar with logging tools.



Local Events
Logger: Application
Category: Application Crashes
Name: App Error
Category: Application Crashes

Date	Time	Level	Logger	Message	Domain
16 Oct 2024	09:35:18.919	ERROR	Application	Faulting application name: ApplePhotoStreams.exe, version: 254.0.0.11, time stamp: 0x669175c8 Faulting module name: ApplePhotoStreams.exe, version: 254.0.0.11, time stamp: 0x669175c8 Exception code: 0xc0000005	Application Error
16 Oct 2024	10:53:05.755	ERROR	Application	Faulting application name: ApplePhotoStreams.exe, version: 254.0.0.11, time stamp: 0x669175c8 Faulting module name: ApplePhotoStreams.exe, version: 254.0.0.11, time stamp: 0x669175c8 Exception code: 0xc0000005	Application Error
16 Oct 2024	12:07:49.289	ERROR	Application	Faulting application name: ApplePhotoStreams.exe, version: 254.0.0.11, time stamp: 0x669175c8 Faulting module name: ApplePhotoStreams.exe, version: 254.0.0.11, time stamp: 0x669175c8 Exception code: 0xc0000005	Application Error
16 Oct 2024	12:45:04.633	ERROR	Application	Faulting application name: ApplePhotoStreams.exe, version: 254.0.0.11, time stamp: 0x669175c8 Faulting module name: ApplePhotoStreams.exe, version: 254.0.0.11, time stamp: 0x669175c8 Exception code: 0xc0000005	Application Error
16 Oct 2024	22:24:31.693	ERROR	Application	Faulting application name: ApplePhotoStreams.exe, version: 254.0.0.11, time stamp: 0x669175c8 Faulting module name: ApplePhotoStreams.exe, version: 254.0.0.11, time stamp: 0x669175c8 Exception code: 0xc0000005	Application Error
17 Oct 2024	07:31:44.791	ERROR	Application	Faulting application name: ApplePhotoStreams.exe, version: 254.0.0.11, time stamp: 0x669175c8 Faulting module name: ApplePhotoStreams.exe, version: 254.0.0.11, time stamp: 0x669175c8 Exception code: 0xc0000005	Application Error

	All	View
Records:	1,015	6
Threads:	1	1
Loggers:	3	1
Debug:	0	0
Info:	848	0
Warn:	91	0
Error:	76	6
Fatal:	0	0

```
2024-10-17T07:31:44 Error [LAPTOP-L0KS1JVB.Application.Application Error] Faulting application name: ApplePhotoStreams.exe, version: 254.0.0.11,
time stamp: 0x669175c8
Faulting module name: ApplePhotoStreams.exe, version: 254.0.0.11, time stamp: 0x669175c8
Exception code: 0xc0000005
Fault offset: 0x000000000002785e
Faulting process id: 0x0xAABC
Faulting application start time: 0x0x1DB2037F4422EC9
Faulting application path: C:\Program Files\WindowsApps\AppleInc.iCloud_15.2.157.0_x64__nzyj5cx40ttqa\iCloud\ApplePhotoStreams.exe
Faulting module path: C:\Program Files\WindowsApps\AppleInc.iCloud_15.2.157.0_x64__nzyj5cx40ttqa\iCloud\ApplePhotoStreams.exe
```

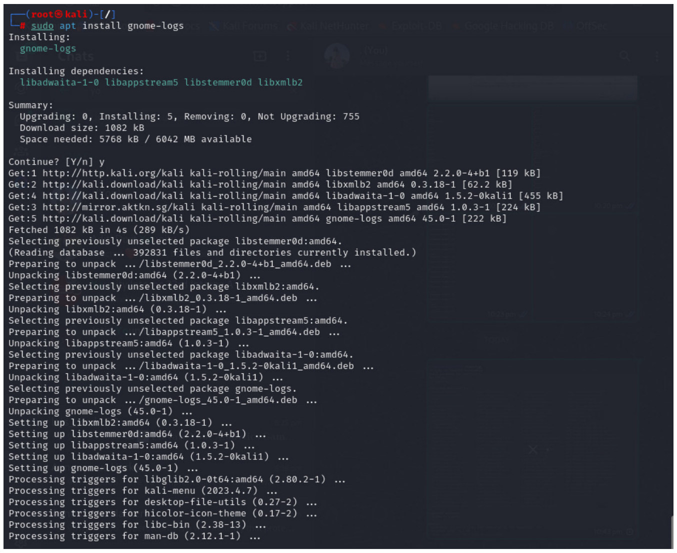
Fig. 10. This is event view tool.

VI. KALI TOOLS

1.Gnome Logs

left=0pt

- **Overview**: Gnome Logs is an intuitive log viewer designed for the GNOME desktop environment, providing users with an easy way to access and manage system logs.
- **Installation**: To install Gnome Logs, run the command: `sudo apt install gnome-logs`.
- **Usage**: Gnome Logs offers a categorized view of logs, including:
  - **System Logs**: Provides details about the overall system performance and status.
  - **User Logs**: Displays user-specific activities and events.
  - **Kernel Logs**: Shows kernel-level messages and events for in-depth troubleshooting.
- **Features**:
  - User-friendly and clean interface for easy navigation.
  - Categorizes logs for quick access and efficient troubleshooting.
  - Allows filtering and searching for specific log entries.
  - Integrates seamlessly with the GNOME desktop environment.
- **Pros**:
  - Lightweight and easy to install.
  - Well-integrated with GNOME desktop.
  - Suitable for users who prefer a simple and minimalistic log viewer.
- **Cons**:
  - Limited functionality compared to more advanced log management tools.
  - Primarily designed for GNOME environments, so may not work well outside GNOME.



```
┌──(root㉿kali)-[/]
└─# sudo apt install gnome-logs
Installing:
  gnome-logs

Installing dependencies:
  libadwaita-1-0 libappstream5 libstemmer0d libxmlb2

Summary:
  Upgrading: 0, Installing: 5, Removing: 0, Not Upgrading: 755
  Download size: 1082 kB
  Space needed: 5768 kB / 6042 MB available

Continue? [Y/n] y
Get:1 http://http.kali.org/kali kali-rolling/main amd64 libstemmer0d amd64 2.2.0-4+b1 [119 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 libxmlb2 amd64 0.3.18-1 [62.2 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 libadwaita-1-0 amd64 1.5.2-0kali1 [455 kB]
Get:3 http://mirror.aktkn.sg/kali kali-rolling/main amd64 libappstream5 amd64 1.0.3-1 [224 kB]
Get:5 http://kali.download/kali kali-rolling/main amd64 gnome-logs amd64 45.0-1 [222 kB]
Fetched 1082 kB in 4s (289 kB/s)
Selecting previously unselected package libstemmer0d:amd64.
(Reading database ... 392831 files and directories currently installed.)
Preparing to unpack .../libstemmer0d_2.2.0-4+b1_amd64.deb ...
Unpacking libstemmer0d:amd64 (2.2.0-4+b1) ...
Selecting previously unselected package libxmlb2:amd64.
Preparing to unpack .../libxmlb2_0.3.18-1_amd64.deb ...
Unpacking libxmlb2:amd64 (0.3.18-1) ...
Selecting previously unselected package libappstream5:amd64.
Preparing to unpack .../libappstream5_1.0.3-1_amd64.deb ...
Unpacking libappstream5:amd64 (1.0.3-1) ...
Selecting previously unselected package libadwaita-1-0:amd64.
Preparing to unpack .../libadwaita-1-0_1.5.2-0kali1_amd64.deb ...
Unpacking libadwaita-1-0:amd64 (1.5.2-0kali1) ...
Selecting previously unselected package gnome-logs.
Preparing to unpack .../gnome-logs_45.0-1_amd64.deb ...
Unpacking gnome-logs (45.0-1) ...
Setting up libxmlb2:amd64 (0.3.18-1) ...
Setting up libstemmer0d:amd64 (2.2.0-4+b1) ...
Setting up libappstream5:amd64 (1.0.3-1) ...
Setting up libadwaita-1-0:amd64 (1.5.2-0kali1) ...
Setting up gnome-logs (45.0-1) ...
Processing triggers for libglib2.0-0t64:amd64 (2.80.2-1) ...
Processing triggers for kali-menu (2023.4.7) ...
Processing triggers for desktop-file-utils (0.27-2) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for libc-bin (2.38-13) ...
Processing triggers for man-db (2.12.1-1) ...
```

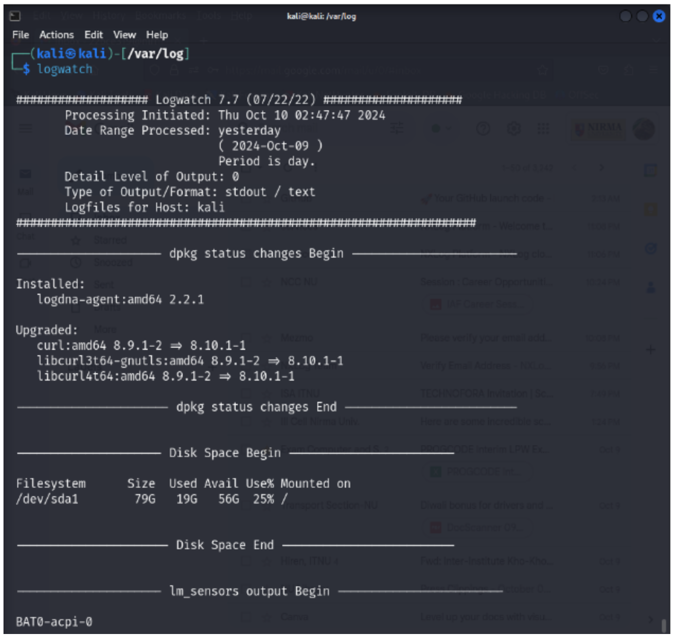
Fig. 11. This is kali linux gnom tool.

2. Logwatch

left=0pt

- **Overview**: Logwatch is a log analysis tool that generates detailed summaries and reports from various system logs, helping administrators monitor system activity and detect potential issues.
- **Installation**: To install Logwatch, run the command: `sudo apt install logwatch`.
- **Usage**:
  - Execute `sudo logwatch` to generate log summaries directly in the terminal.
  - Supports sending log summaries via email for remote monitoring and alerts.
- **Features**:
  - Generates customizable reports for system logs.
  - Offers scheduling options to automate log analysis and report generation.
  - Provides log summaries in various formats, including terminal output and email.
  - Can filter and summarize logs based on specific services and time ranges.
- **Pros**:
  - Easy to set up and use for automated log monitoring.
  - Flexible and customizable reporting options.
  - Helps quickly identify and summarize critical events in logs.
- **Cons**:
  - Limited to predefined log parsing rules, which may not cover all log types.

- Requires configuration for advanced customization and email setup.



kali@kali: /var/log

```
┌──(kali㉿kali)-[/var/log]
└─$ logwatch

################### Logwatch 7.7 (07/22/22) ####################
       Processing Initiated: Thu Oct 10 02:47:47 2024
       Date Range Processed: yesterday
                             ( 2024-Oct-09 )
                             Period is day.
       Detail Level of Output: 0
       Type of Output/Format: stdout / text
       Logfiles for Host: kali
##################################################################

 --------------------- dpkg status changes Begin ------------------------

Installed:
   logdna-agent:amd64 2.2.1

Upgraded:
   curl:amd64 8.9.1-2 => 8.10.1-1
   libcurl3t64-gnutls:amd64 8.9.1-2 => 8.10.1-1
   libcurl4t64:amd64 8.9.1-2 => 8.10.1-1

 ---------------------- dpkg status changes End -------------------------


 --------------------- Disk Space Begin ------------------------

Filesystem      Size  Used Avail Use% Mounted on
/dev/sda1        79G   19G   56G  25% /


 ---------------------- Disk Space End -------------------------


 --------------------- lm_sensors output Begin ------------------------

BAT0-acpi-0
```

Fig. 12. this is a logwatch kali linux tool

VII. macOS System Logs

macOS provides various logs that record system events, errors, hardware diagnostics, and other crucial information valuable for digital forensic analysis. These logs can be accessed through different paths or commands. Below are some essential macOS logs:

A. General System Log

This log records general system events, errors, warnings, and notifications.

- **Path:** `/var/log/system.log`

B. Kernel Log

The Kernel Log contains messages from the macOS kernel, including hardware diagnostics and driver issues.

- **Path:** Accessed via the Console app or using the `dmesg` command in Terminal.
- **Command:** `dmesg`

C. Install Log

This log tracks macOS installation events, including software updates, application installs, and system changes.

- **Path:** `/var/log/install.log`

D. Power Management Log

The Power Management Log records events related to sleep, wake, shutdown, and restart activities.

- **Path:** `/var/log/powermanagement.log`

E. Wi-Fi Log

This log contains information about the system's wireless activity, such as connection attempts and network issues.

- **Path:** `/var/log/wifi.log`

3.GoAccess

Overview: GoAccess is an open-source log analyzer primarily designed for analyzing web logs, such as Apache or Nginx logs, in real-time. It provides an efficient way to visualize and interpret web traffic data, making it valuable for web administrators and digital forensic experts.

Installation: To install GoAccess on Kali Linux, use the following command:

```
sudo apt install goaccess
```

Usage: After installation, you can run GoAccess to analyze a log file with the command:

```
goaccess /path/to/logfile -c
```

This command will launch the interactive terminal interface for real-time analysis. To generate an HTML report, use:

```
goaccess /path/to/logfile -o /path/to/report.html
```

Features:

- **Real-time Log Analysis:** Provides instant feedback on web traffic data, including visitor details, status codes, and bandwidth usage.
- **Interactive Interface:** GoAccess offers an interactive terminal interface that allows users to navigate through various statistics easily.
- **HTML Dashboard:** Ability to output data in HTML format for a web-based view, making it suitable for remote monitoring and reporting.
- **Detailed Visitor Data:** Offers insights into HTTP status codes, bandwidth, referrers, and visitor data.

Advantages:

- **Efficiency:** Extremely fast and efficient, capable of processing large web log files quickly.
- **Real-time Reports:** Provides real-time data and insightful reports that help monitor and analyze web traffic effectively.
- **Resource Optimization:** Consumes minimal system resources, even when processing large log files.

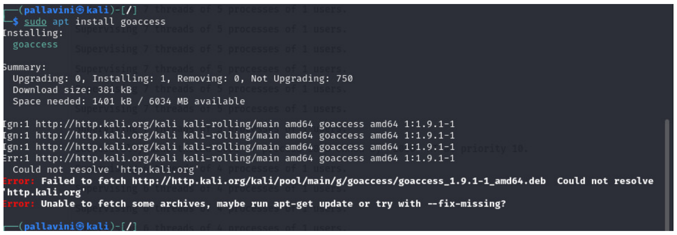
Disadvantages:

- **Focus on Web Logs:** Primarily designed for web server logs, limiting its functionality for general system log analysis.
- **Limited Log Format Support:** Supports specific web log formats, which may not be suitable for analyzing other types of logs without modification.

Application in Digital Forensics:

- GoAccess is useful in web-related forensic investigations, as it can quickly analyze large volumes of web server logs to identify suspicious behavior, such as unauthorized access attempts or unusual traffic patterns.

- The tool's real-time analysis feature is advantageous for monitoring ongoing incidents and collecting data for forensic reports.
- By generating HTML-based dashboards, GoAccess allows forensic analysts to present and visualize data interactively, aiding in detailed and clear reporting.



```
┌──(pallavini㉿kali)-[/]
└─$ sudo apt install goaccess
Installing:
  goaccess

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 750
  Download size: 381 kB
  Space needed: 1401 kB / 6034 MB available

Ign:1 http://http.kali.org/kali kali-rolling/main amd64 goaccess amd64 1:1.9.1-1
Ign:1 http://http.kali.org/kali kali-rolling/main amd64 goaccess amd64 1:1.9.1-1
Ign:1 http://http.kali.org/kali kali-rolling/main amd64 goaccess amd64 1:1.9.1-1
Err:1 http://http.kali.org/kali kali-rolling/main amd64 goaccess amd64 1:1.9.1-1
  Could not resolve 'http.kali.org'
Error: Failed to fetch http://http.kali.org/kali/pool/main/g/goaccess/goaccess_1.9.1-1_amd64.deb  Could not resolve
'http.kali.org'
Error: Unable to fetch some archives, maybe run apt-get update or try with --fix-missing?

┌──(pallavini㉿kali)-[/]
```

Fig. 13. this is a logwatch kali linux tool