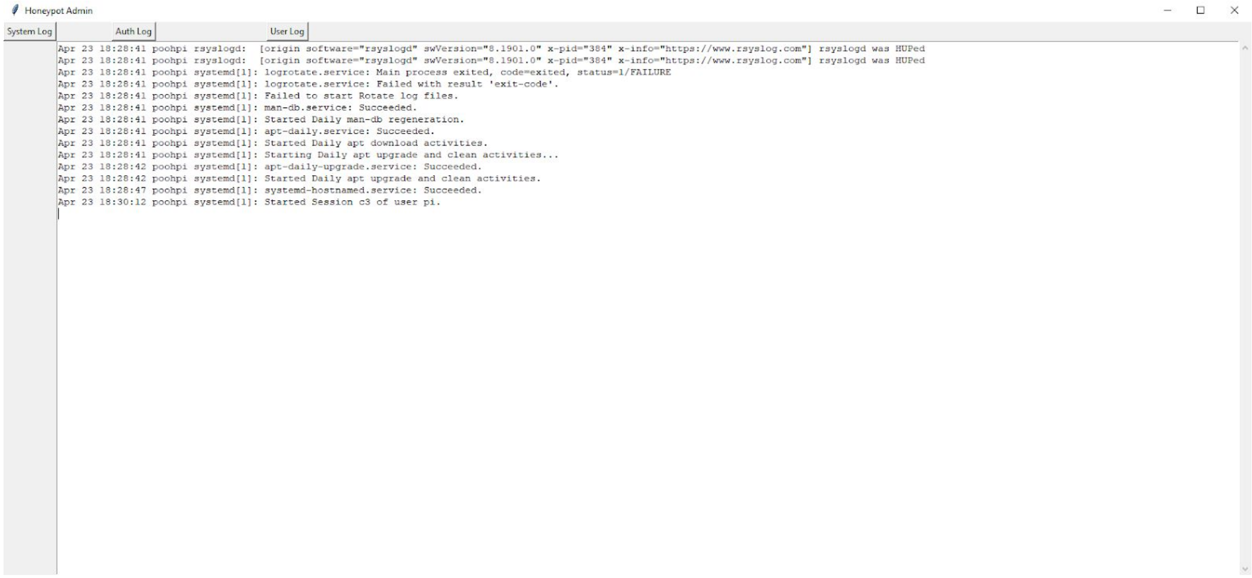
# UI Specification

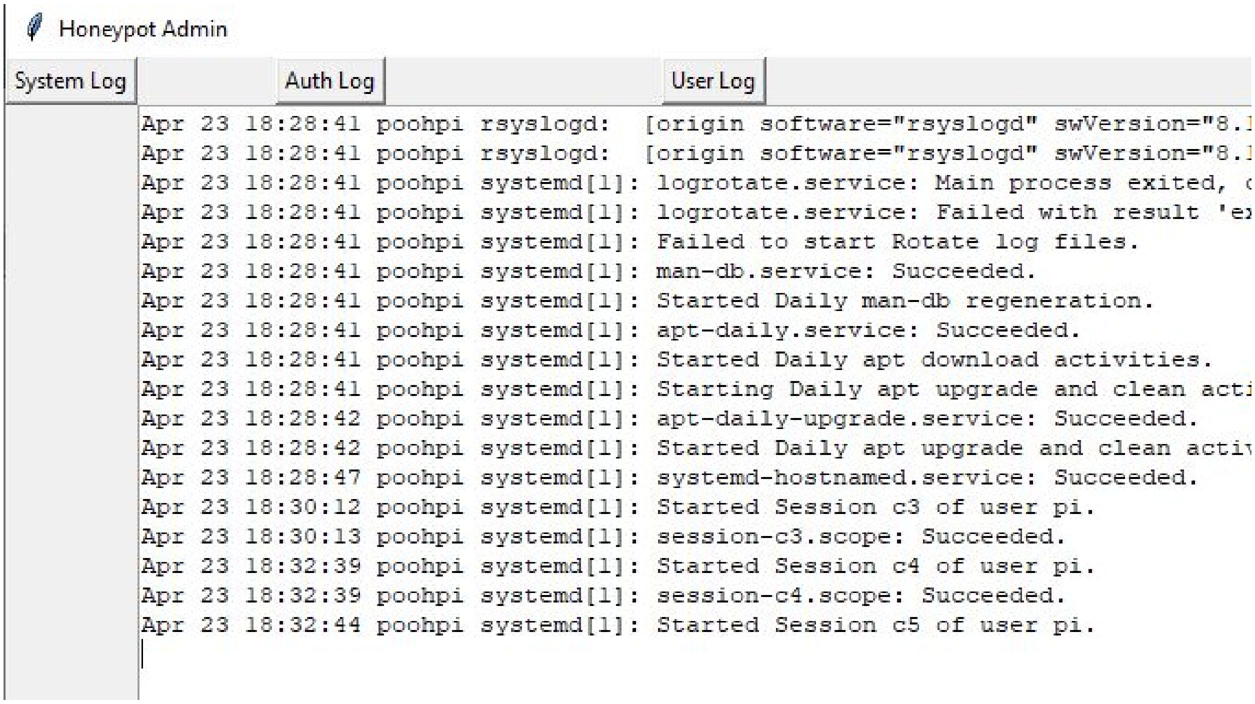
## Honeypot Admin Console

The Honeypot Admin console is used for observing a few different log files that are written on the server. There are 3 buttons to load a respective log file. The Console reads a log file from the server and writes a new log file on the admin machine. The log files are organized by date.



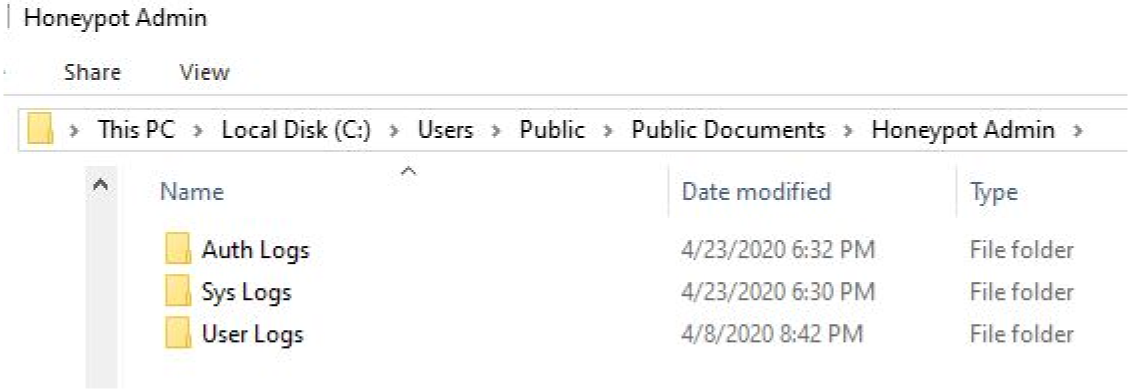
```
Apr 23 18:28:41 poohpi rsyslogd:  [origin software="rsyslogd" swVersion="8.1901.0" x-pid="384" x-info="https://www.rsyslog.com"] rsyslogd was HUPed
Apr 23 18:28:41 poohpi rsyslogd:  [origin software="rsyslogd" swVersion="8.1901.0" x-pid="384" x-info="https://www.rsyslog.com"] rsyslogd was HUPed
Apr 23 18:28:41 poohpi systemd[1]: logrotate.service: Main process exited, code=exited, status=1/FAILURE
Apr 23 18:28:41 poohpi systemd[1]: logrotate.service: Failed with result 'exit-code'.
Apr 23 18:28:41 poohpi systemd[1]: Failed to start Rotate log files.
Apr 23 18:28:41 poohpi systemd[1]: man-db.service: Succeeded.
Apr 23 18:28:41 poohpi systemd[1]: Started Daily man-db regeneration.
Apr 23 18:28:41 poohpi systemd[1]: apt-daily.service: Succeeded.
Apr 23 18:28:41 poohpi systemd[1]: Started Daily apt download activities.
Apr 23 18:28:41 poohpi systemd[1]: Starting Daily apt upgrade and clean activities...
Apr 23 18:28:42 poohpi systemd[1]: apt-daily-upgrade.service: Succeeded.
Apr 23 18:28:42 poohpi systemd[1]: Started Daily apt upgrade and clean activities.
Apr 23 18:28:47 poohpi systemd[1]: systemd-hostnamed.service: Succeeded.
Apr 23 18:30:12 poohpi systemd[1]: Started Session c3 of user pi.
```

## Closer look at Honeypot Admin Console

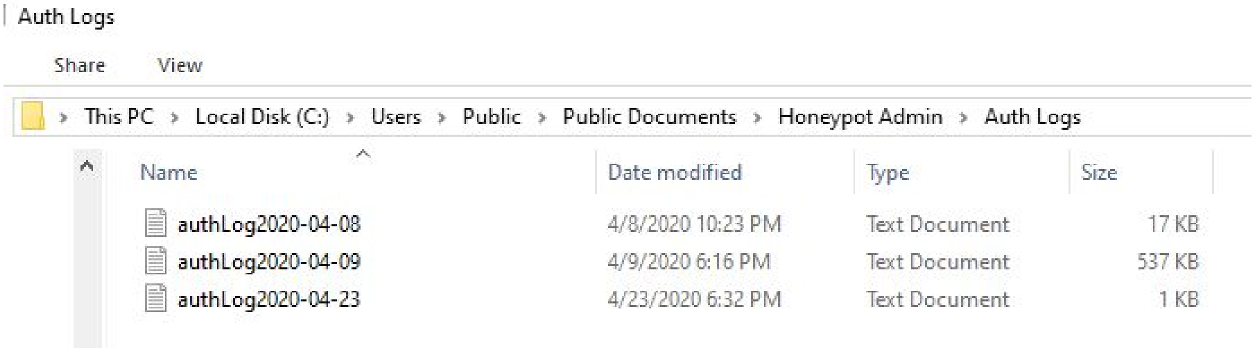


```
Apr 23 18:28:41 poohpi rsyslogd:  [origin software="rsyslogd" swVersion="8.
Apr 23 18:28:41 poohpi rsyslogd:  [origin software="rsyslogd" swVersion="8.
Apr 23 18:28:41 poohpi systemd[1]: logrotate.service: Main process exited,
Apr 23 18:28:41 poohpi systemd[1]: logrotate.service: Failed with result 'e
Apr 23 18:28:41 poohpi systemd[1]: Failed to start Rotate log files.
Apr 23 18:28:41 poohpi systemd[1]: man-db.service: Succeeded.
Apr 23 18:28:41 poohpi systemd[1]: Started Daily man-db regeneration.
Apr 23 18:28:41 poohpi systemd[1]: apt-daily.service: Succeeded.
Apr 23 18:28:41 poohpi systemd[1]: Started Daily apt download activities.
Apr 23 18:28:41 poohpi systemd[1]: Starting Daily apt upgrade and clean acti
Apr 23 18:28:42 poohpi systemd[1]: apt-daily-upgrade.service: Succeeded.
Apr 23 18:28:42 poohpi systemd[1]: Started Daily apt upgrade and clean activ
Apr 23 18:28:47 poohpi systemd[1]: systemd-hostnamed.service: Succeeded.
Apr 23 18:30:12 poohpi systemd[1]: Started Session c3 of user pi.
Apr 23 18:30:13 poohpi systemd[1]: session-c3.scope: Succeeded.
Apr 23 18:32:39 poohpi systemd[1]: Started Session c4 of user pi.
Apr 23 18:32:39 poohpi systemd[1]: session-c4.scope: Succeeded.
Apr 23 18:32:44 poohpi systemd[1]: Started Session c5 of user pi.
```

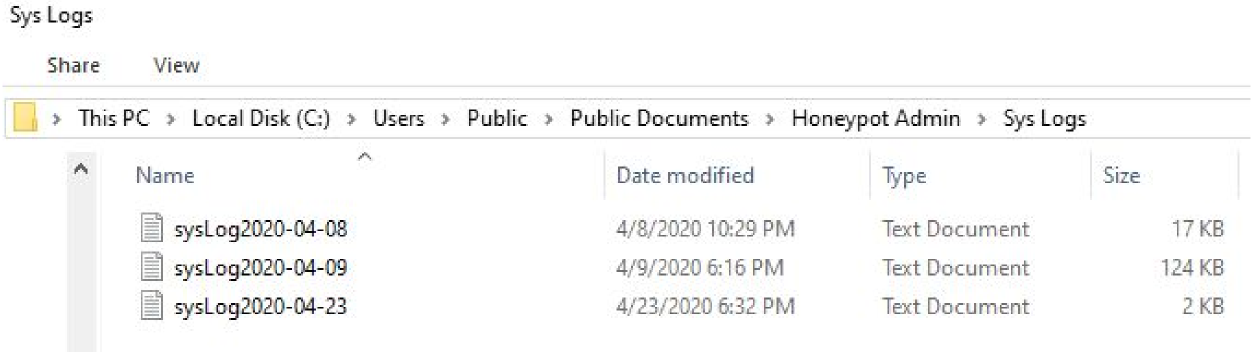
## Log Files


Honeypot Admin
Share
View
This PC > Local Disk (C:) > Users > Public > Public Documents > Honeypot Admin >

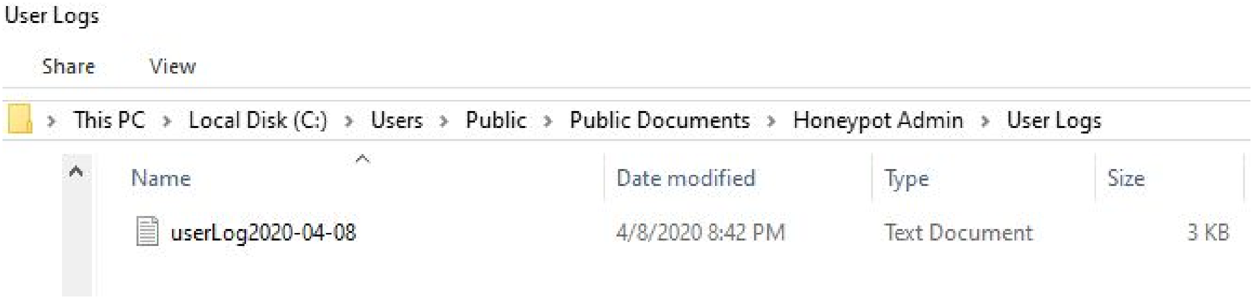
| Name | Date modified | Type |
|---|---|---|
| Auth Logs | 4/23/2020 6:32 PM | File folder |
| Sys Logs | 4/23/2020 6:30 PM | File folder |
| User Logs | 4/8/2020 8:42 PM | File folder |


Auth Logs
Share
View
This PC > Local Disk (C:) > Users > Public > Public Documents > Honeypot Admin > Auth Logs

| Name | Date modified | Type | Size |
|---|---|---|---|
| authLog2020-04-08 | 4/8/2020 10:23 PM | Text Document | 17 KB |
| authLog2020-04-09 | 4/9/2020 6:16 PM | Text Document | 537 KB |
| authLog2020-04-23 | 4/23/2020 6:32 PM | Text Document | 1 KB |


Sys Logs
Share
View
This PC > Local Disk (C:) > Users > Public > Public Documents > Honeypot Admin > Sys Logs

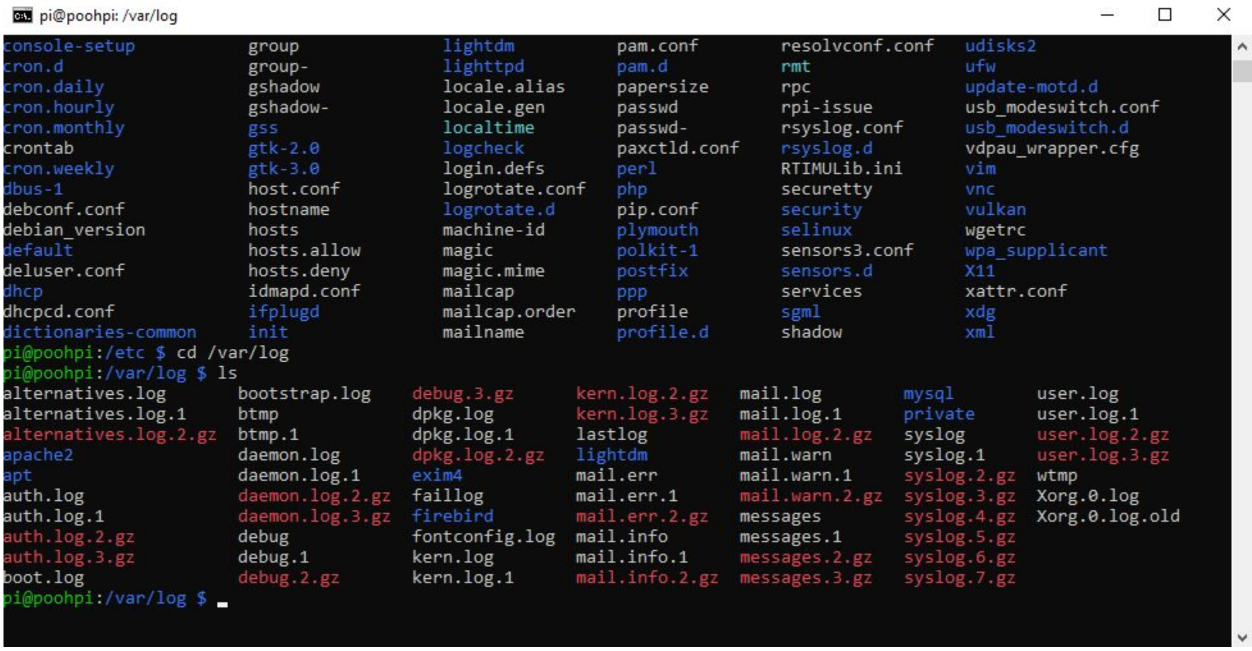
| Name | Date modified | Type | Size |
|---|---|---|---|
| sysLog2020-04-08 | 4/8/2020 10:29 PM | Text Document | 17 KB |
| sysLog2020-04-09 | 4/9/2020 6:16 PM | Text Document | 124 KB |
| sysLog2020-04-23 | 4/23/2020 6:32 PM | Text Document | 2 KB |


User Logs
Share
View
This PC > Local Disk (C:) > Users > Public > Public Documents > Honeypot Admin > User Logs

| Name | Date modified | Type | Size |
|---|---|---|---|
| userLog2020-04-08 | 4/8/2020 8:42 PM | Text Document | 3 KB |

**The Honeypot**

The Honeypot was hosted on a Raspberry Pi running a Linux based operating system (Raspbian). Ultimately, there would be little to no need to log into the server once all or most of the desired features are automated, but this is where a lot of the work and set up took place on this project. Navigate the directories using cd and ls. Use “Vim” to edit files by typing “vi [filename].” (see vim guide linked below for more commands) Install services like “mailutils” and “WordPress” using “apt-get.”
[“Basic Vim commands - For getting started”]:
https://coderwall.com/p/adv71w/basic-vim-commands-for-getting-started



```
console-setup           group              lightdm          pam.conf        resolvconf.conf   udisks2
cron.d                  group-             lighttpd         pam.d           rmt               ufw
cron.daily              gshadow            locale.alias     papersize       rpc               update-motd.d
cron.hourly             gshadow-           locale.gen       passwd          rpi-issue         usb_modeswitch.conf
cron.monthly            gss                localtime        passwd-         rsyslog.conf      usb_modeswitch.d
crontab                 gtk-2.0            logcheck         paxctld.conf    rsyslog.d         vdpau_wrapper.cfg
cron.weekly             gtk-3.0            login.defs       perl            RTIMULib.ini      vim
dbus-1                  host.conf          logrotate.conf   php             securetty         vnc
debconf.conf            hostname           logrotate.d      pip.conf        security          vulkan
debian_version          hosts              machine-id       plymouth        selinux           wgetrc
default                 hosts.allow        magic            polkit-1        sensors3.conf     wpa_supplicant
deluser.conf            hosts.deny         magic.mime       postfix         sensors.d         X11
dhcp                    idmapd.conf        mailcap          ppp             services          xattr.conf
dhcpcd.conf             ifplugd            mailcap.order    profile         sgml              xdg
dictionaries-common     init               mailname         profile.d       shadow            xml
pi@poohpi:/etc $ cd /var/log
pi@poohpi:/var/log $ ls
alternatives.log       bootstrap.log    debug.3.gz      kern.log.2.gz   mail.log         mysql        user.log
alternatives.log.1     btmp             dpkg.log        kern.log.3.gz   mail.log.1       private      user.log.1
alternatives.log.2.gz  btmp.1           dpkg.log.1      lastlog         mail.log.2.gz    syslog       user.log.2.gz
apache2                daemon.log       dpkg.log.2.gz   lightdm         mail.warn        syslog.1     user.log.3.gz
apt                    daemon.log.1     exim4           mail.err        mail.warn.1      syslog.2.gz  wtmp
auth.log               daemon.log.2.gz  faillog         mail.err.1      mail.warn.2.gz   syslog.3.gz  Xorg.0.log
auth.log.1             daemon.log.3.gz  firebird        mail.err.2.gz   messages         syslog.4.gz  Xorg.0.log.old
auth.log.2.gz          debug            fontconfig.log  mail.info       messages.1       syslog.5.gz
auth.log.3.gz          debug.1          kern.log        mail.info.1     messages.2.gz    syslog.6.gz
boot.log               debug.2.gz       kern.log.1      mail.info.2.gz  messages.3.gz    syslog.7.gz
pi@poohpi:/var/log $ _
```