Firmware Scavenger Hunt

- **amcrest.bin**
  - What is the root user's password? (Hint: Use `john` or `hashcat` to crack it. The password is 5 characters, all lowercase.)
  - What is the default host IP address (`DefaultHostIp`) listed in the `config.lua` file found in this firmware?
- **ks_ac1200.img**
  - There are several strange user accounts listed in this firmware image (see `passwd/shadow` files). One of those strange user accounts is allowed to run any command as root using sudo, without supplying a password. Yikes! Which user is this, and where is that sudo rule found?
  - There is a file called "`login.json`" somewhere in this firmware image which defines an admin username and password hash. What is admin's password? (Again, `john` or `hashcat` can crack it fast. It's 5 characters, all lower-case).
- **surfboard.bin**
  - There is a file called "`rfs.cfg`" somewhere in this firmware image. What is the value of the `RFS_HOSTMNTDIR` variable in that configuration file?
  - It looks like the firmware authors used an piece of old, once-popular HTML editing software to build all the .HTM files for the web server. What software did they use? (Hint: The `<meta name=generator … >` tag will show this).
- **wavlink_D4G.bin**
  - A file in this firmware called "`RT2860_default_vlan`" defines WiFi AP configuration information. What are the primary and secondary DNS server IP addresses listed in this file?
  - There is a shell (`.sh`) script in the web "`cgi-bin/`" folder which looks like it's designed to export the system settings as a single file. It encrypts that file before sending it though, using AES 256 CBC. What password is used to encrypt that data?

Answers

- **amcrest.bin**
  - vizxv
  - 192.168.1.108
- **ks_ac1200.img**
  - test, /etc/sudoers.d/test
  - admin
- **surfboard.bin**
  - /cygdrive/c/nfsshare
  - Microsoft Frontpage 4.0
- **wavlink_D4G.bin**
  - primary 8.8.8.8, secondary 114.114.114.114
  - 803f5d