Tamper assessment: No seals. Metal strip on case seemingly designed as IO/aesthetics. Metal strip scratches upon disassembling the case. Critical IC’s located beneath non-removable cooling plate. Two exposed storage devices. Exposed Hard Drive (personal information encrypted).

|  |  |
| --- | --- |
| Port | Probable intent |
| UTP | Internet services, remote maintenance |
| HDMI | Connection to screen |
| Coax | External Antenna |
| USB | Firmware updates |
| 3.5 mm | Stereo |
|  |  |
|  |  |

Port list (External):  
ANT: High quality audio.  
3.5mm: Audio output  
HDMI: Video output  
LAN: Internet (google play)  
S/PDIF: Audio  
USB: local maintenance.  
  
Internals: Removeable hard drive, contents seemingly encrypted.   
 Disconnectable fan.  
 Internal antennae connected by wires  
 Important IC’s beneath non-removable cooling plate

|  |  |  |
| --- | --- | --- |
| Type | Label | Description |
| Wireless | BCM43602KLMG | WLAN, no Datasheet |
| Signal process. | GH15B 513J10 | Voltage Regulator |
| Signal process. | 15171A | Rise Time Converter, no Datasheet, obsolete |
| Signal process. | SGM8908 | Stereo Line driver |
| Power Supply | AP65450 | Buck Converter |
| Wireless | BCM20706 | Bluetooth |
| Mutable storage | 4512A2GTL | EEPROM |
| Storage | ? | Unknown Kingston (memory manufacturer) IC |
| Processor | ? | Label unreadable due to thermal paste, unremovable |

Summary: very few critical IC’s are accessible without risking damage to the board overall. Perhaps some data can be extracted from the 4512A2GTL or Kingston chip. No debug ports beyond the USB connector (which is authenticated).   
  
  
  
  
  
Mosquito killer:  
  
Case easy to open, no seals

Ports: none (powered by outlet)

|  |  |  |
| --- | --- | --- |
| Type | Label | Description |
| Wireless | ? | WLAN, probably microcontroller |
| Storage | 25SF081 | On-chip SSD, SPI controlled. |