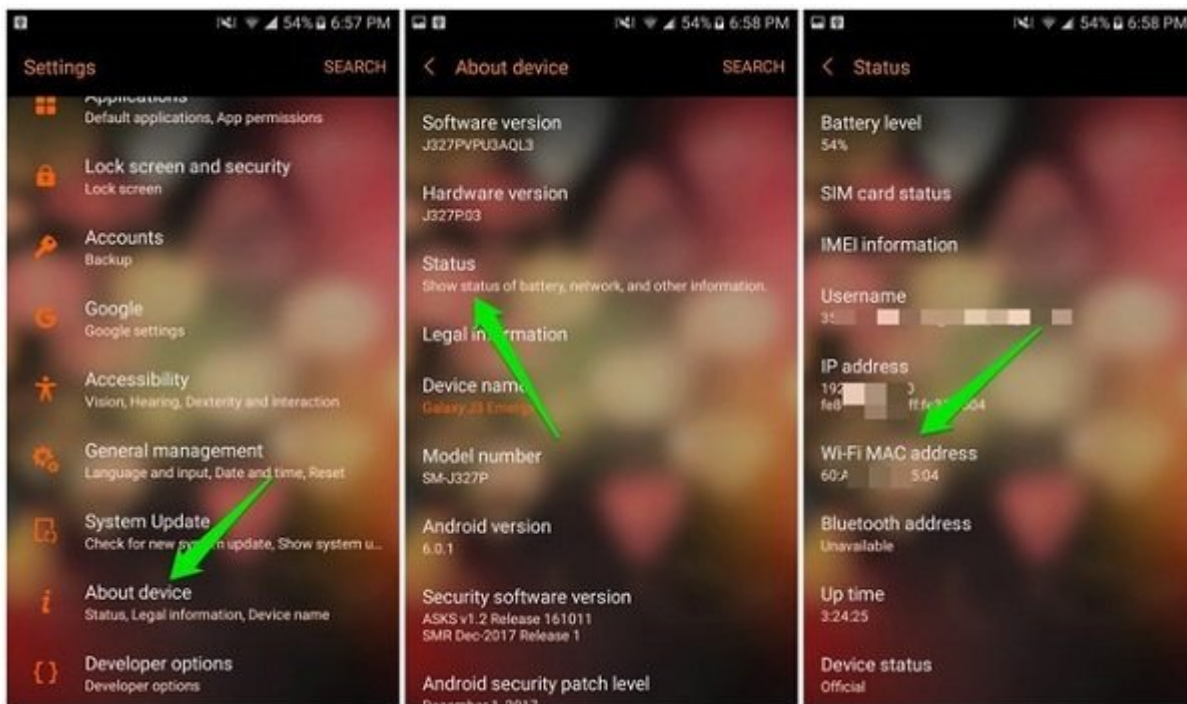




در عصری که همه ارتباطات و تعاملات بر بستر شبکه‌های ارتباطی شکل گرفته‌اند، بیشتر امور تجاری از طریق اینترنت و به ویژه دستگاه‌های همراه انجام می‌شوند. به همین دلیل کاربران همواره در جست‌وجوی پیدا کردن ترفندهای ویژه وای‌فای هستند تا بتوانند روی دستگاه‌های همراه سرعت ارتباطات را بیشتر و قطعی ارتباطات را کمتر کنند. در این مطلب می‌خواهیم به معرفی ترفندها و تکنیک‌ها بپردازیم که روی شبکه‌های وای‌فای تاثیرگذار هستند و از این ترفندها می‌توان روی گوشی‌های اندرویدی استفاده کرد.

### 1. پیدا کردن مک آدرس گوشی اندرویدی



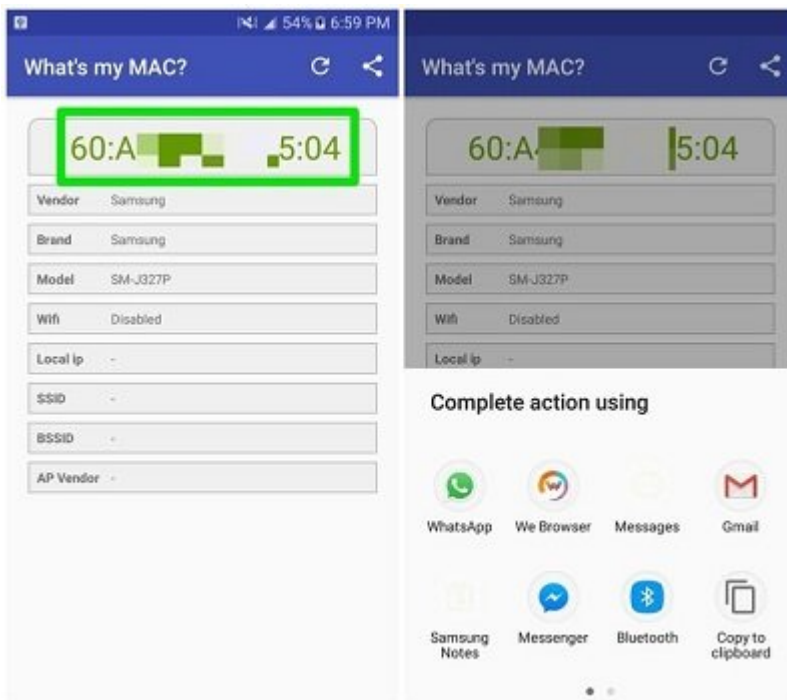
اگر مدیر شبکه‌ای هستید، به احتمال زیاد بیشتر وقت شما صرف مک‌آدرس‌ها می‌شود. مک‌آدرس برای شناسایی یک دستگاه در یک شبکه و مدیریت دستگاه‌ها استفاده می‌شود. درست است که مک‌آدرس شبیه به شناسه دستگاه (device ID) است، اما به‌طور خاص برای برقراری ارتباط در شبکه استفاده می‌شود. شما می‌توانید از مک‌آدرس برای محدود کردن دسترسی یک دستگاه خاص به شبکه، پیاده‌سازی خط‌مشی‌های شبکه و موارد مشابه استفاده کنید.

همان‌گونه که مشاهده می‌کنید مک‌آدرس‌ها نقش مهمی در دنیای شبکه بازی می‌کنند، بنابراین باید با روش‌های پیدا کردن مک‌آدرس گوشی‌های اندرویدی آشنا باشید. ساده‌ترین راه پیدا کردن مک‌آدرس یک گوشی اندروید مراجعه به بخش About دستگاه است. برای مشاهده مک‌آدرس به Settings بروید و گزینه About device را لمس کنید، سپس گزینه Status را لمس کنید تا مک‌آدرسی که زیر WiFi MAC address قرار گرفته است را مشاهده کنید.

## 2. با شماره‌گیری مک‌آدرس را پیدا کنید

اگر عاشق کدهای دستوری هستید، به احتمال زیاد این گزینه برای شما طراحی شده است. شبیه کدهای مخفی اندروید، برای پیدا کردن مک‌آدرس در گوشی اندرویدی یک کد دستوری در نظر گرفته شده است. برنامه شماره‌گیر تلفن را باز کنید و مقدار `##*#232338##*` را تایپ و شماره‌گیری کنید. پنجره‌ای ظاهر می‌شود که مک‌آدرس دستگاه را نشان می‌دهد. دقت کنید این تکنیک روی همه گوشی‌های اندرویدی قابل اجرا نیست. به‌طور مثال، این تکنیک روی گوشی‌های سامسونگ اجرا نمی‌شود.

## 3. از یک برنامه کاوش‌گر برای پیدا کردن مک‌آدرس استفاده کنید



اگر به‌طور مداوم باید مک‌آدرس گوشی اندرویدی را بررسی کنید، بهتر است به سراغ گزینه‌های حرفه‌ای‌تر بروید. برنامه‌های مختلفی برای این منظور طراحی شده‌اند که پیشنهاد ما `What's my MAC address` است. کافی است برنامه را نصب و اجرا کنید تا مک‌آدرس دستگاه را نشان دهد. این برنامه ضمن آن‌که مک‌آدرس دستگاه را نشان می‌دهد، SSID و BSSID (مک‌آدرس وای‌فای) که می‌تواند در برخی موارد مفید باشند را نشان می‌دهد.

## 4. بهبود قدرت سیگنال وای‌فای در اندروید

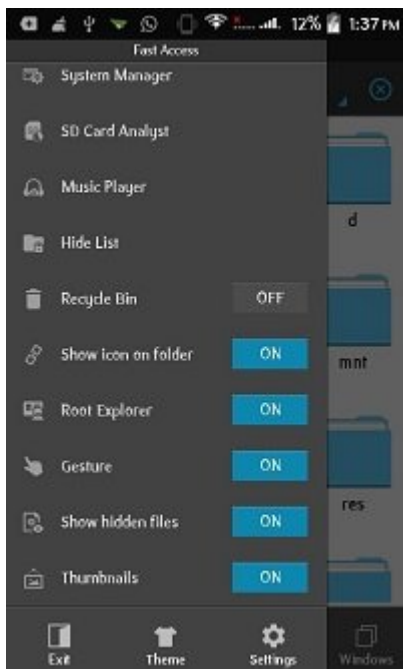


در گوشی‌های اندرویدی، وای‌فای اصلی‌ترین نقش اتصال به اینترنت را دارد، اما چگونه می‌توان سیگنال وای‌فای را تقویت کرد و از اینترنت پر سرعتی لذت برد؟ پاسخ در تجزیه و تحلیل وای‌فای مستتر است. شما باید سیگنال‌های وای‌فای را بررسی کنید و بهترین مکان را برای قرار دادن روتر انتخاب کنید. بیشتر برنامه‌های تحلیل‌گر سیگنال وای‌فای همچون Wifi Analyzer به خوبی از عهده انجام این کار بر می‌آیند. توانایی این نرم‌افزارها در اسکن و نمایش گرافیکی سیگنال‌های وای‌فای در قالب کانال‌هایی که استفاده می‌شوند در هنگام عیب‌یابی مشکلات و تداخل سیگنال‌های بی‌سیم در خانه یا محل کار مفید هستند. به‌طور مثال، ممکن است در محل کار فردی در ویندوز یک هات‌اسپات وای‌فای مجازی ایجاد کند، اما اطلاعاتی درباره کانال وای‌فای او نداشته باشید، در چنین مواقعی برنامه‌های تحلیل‌گر سیگنال‌ها به شما کمک می‌کنند. برنامه Wi-Fi Analyzer که برای گوشی‌های اندرویدی ارائه شده، نزدیک‌ترین اکسس‌پوینت‌هایی که پیرامون شما قرار دارند را اسکن می‌کند و نشان می‌دهد چه نقطه‌ای بهترین سیگنال و کمترین میزان ترافیک را دارد. این برنامه اندرویدی می‌تواند سیگنال وای‌فای گوشی اندرویدی را تقویت کند. برای آن‌که بهترین کانال برای وای‌فای را پیدا کنید، Wifi Analyzer را روی گوشی نصب و اجرا کنید و به گزینه نمایش گرافیکی سویچ کنید و بهترین مکان برای دریافت سیگنال‌های قدرتمند وای‌فای را پیدا کنید. برنامه فوق یک ابزار سنجش دقیق برای پیدا کردن قدرتمندترین سیگنال در اختیارتان قرار می‌دهد.

## 5. مشاهده و بازیابی گذرواژه‌های وای‌فای ذخیره شده در گوشی اندرویدی



کاربران در محیط خانه، محل کار یا زمانی که به خانه دوستی مراجعه می‌کنند به شبکه‌های وای‌فای مختلفی متصل می‌شوند که گاهی اوقات گذرواژه اتصال به وای‌فای را فراموش می‌کنند. اندروید قابلیت در اختیار کاربران قرار داده تا گذرواژه‌ها ذخیره شده در گوشی اندرویدی را بازیابی کند. در گوشی‌های اندرویدی گذرواژه وای‌فای در پوشه روت دستگاه ذخیره می‌شود. برای مشاهده این پوشه به دسترسی سطح ریشه نیاز دارید. در این پوشه هر آن چیزی که مرتبط با امنیت است، همچون الگوهای امنیتی WEP، WPA، WPA-2 و... را مشاهده می‌کنید. برای مشاهده گذرواژه‌های ذخیره روی گوشی اندرویدی، گوشی باید روت شده باشد. در گوشی اندرویدی روت شده، برنامه ES File Explorer را باز کنید و سپس گزینه Check Root Explorer را روشن کنید.



پوشه Device را باز کنید



و به مسیر `data/misc/wifi` بروید.



در این پوشه فایل‌های مختلفی پیدا می‌کنید. فایل `wpa_supplicant.conf` را درون ES File Text Editor باز کنید.

```
wpa_supplicant.conf

ctrl_interface=/data/misc/wpa_supplicant
update_config=1
device_name=A500s
manufacturer=XOLO
model_name=A500s
model_number=A500s
serial_number=0123456789ABCDEF
device_type=10-0050F204-5
os_version=01020300
config_methods=physical_display
virtual_push_button keypad

network=(
  ssid="GIONEE S5.5"
  psk="123456789"
  key_mgmt=WPA-PSK
  sim_slot="-1"
  imsi="none"
  pcsc="none"
  priority=3
)

network=(
  ssid="EliteWiFi"
  psk="ABCDEF00000003"
  key_mgmt=WPA-PSK
)
```

گذرواژه‌های ذخیره شده تحت عنوان Saved Wifi Password قابل مشاهده هستند. ssid=xxx نام شبکه وای‌فای و psk=xxxx گذرواژه وای‌فای است

```
wpa_supplicant.conf

ctrl_interface=/data/misc/wpa_supplicant
update_config=1
device_name=A500s
manufacturer=XOLO
model_name=A500s
model_number=A500s
serial_number=0123456789ABCDEF
device_type=10-0050F204-5
os_version=01020300
config_methods=physical_display
virtual_push_button keypad

network=(
  ssid="GIONEE S5.5"
  psk="123456789"
  key_mgmt=WPA-PSK
  sim_slot="-1"
  imsi="none"
  pcsc="none"
  priority=3
)

network=(
  ssid="EliteWiFi"
  psk="ABCDEF00000003"
  key_mgmt=WPA-PSK
)
```

## 6. بررسی و مسدود کردن دسترسی سایر دستگاه‌ها به شبکه وای‌فای

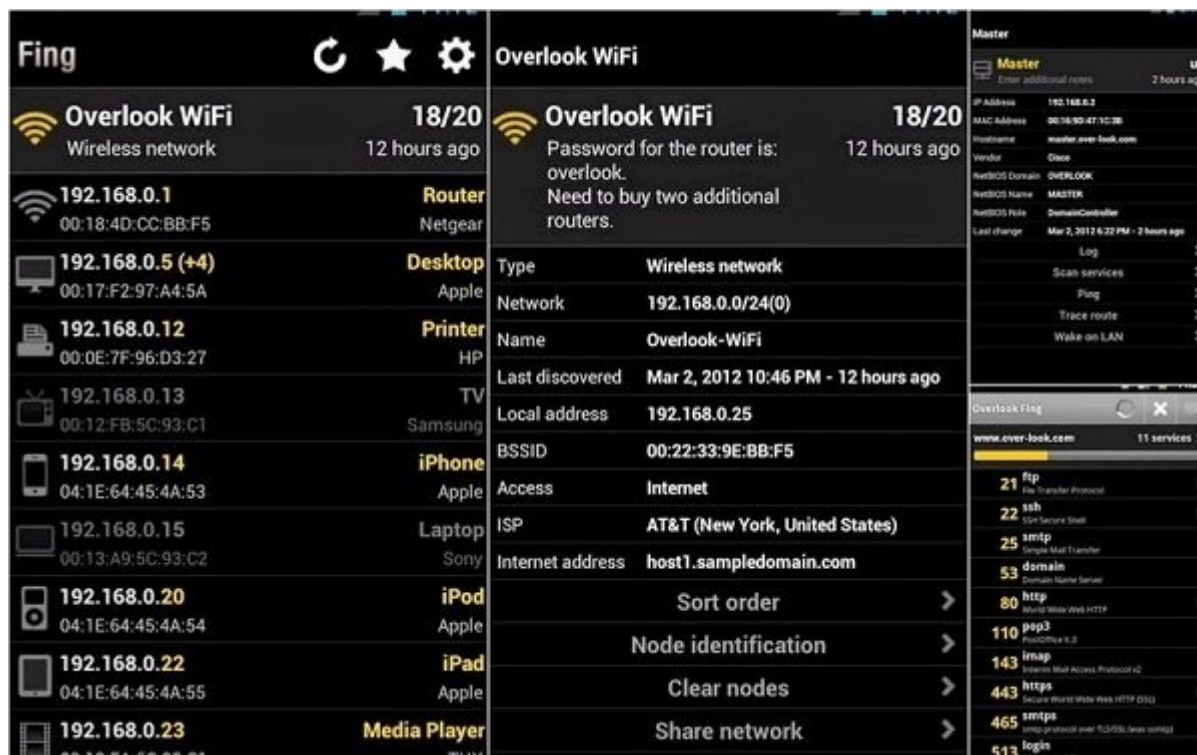
اگر احساس می‌کنید پهنای باند توسط سایر دستگاه‌ها بدون دلیل مصرف می‌شود، باید ارتباط دستگاه‌ها با وای‌فای را قطع کنید. برای بررسی این موضوع ابتدا باید دستگاه‌هایی که به شبکه وای‌فای متصل شده‌اند را پیدا کنید. Wifi Inspect یک برنامه اندرویدی خوب است که اجازه انجام چنین کاری را می‌دهد. این برنامه می‌تواند اطلاعاتی همچون شبکه وای‌فای که به آن متصل هستید را نشان دهد و کارهایی همچون پویش درگاه‌ها، پویش ping، upnp، و کارهایی از این دست را انجام دهد.



پس از شناسایی دستگاه‌های متصل به وای‌فای برای مسدود کردن آن‌ها باید از ابزار Block WiFi - Wifi Inspector استفاده کنید. این برنامه اجازه می‌دهد در چند ثانیه و با سرعتی بالا دسترسی تمامی دستگاه‌های متصل به وای‌فای را غیر فعال کنید.

## 7. پیدا کردن تعداد دستگاه‌هایی که به وای‌فای متصل شده‌اند

در بیشتر موارد به درستی نمی‌دانید چه تعداد دستگاه به شبکه وای‌فای متصل هستند. برای آگاهی از این موضوع دو راهکار پیش روی شما قرار دارد، به پنل مدیریتی روتر وارد شوید و تعداد دستگاه‌های متصل به اینترنت را مشاهده کنید یا برنامه‌هایی که برای این منظور طراحی شده‌اند را روی دستگاهی که از آن استفاده می‌کنید نصب کنید.



Fing یکی از معتبرترین برنامه‌های اندرویدی است که اجازه می‌دهد تعداد دستگاه‌های متصل به وای‌فای را همراه با مک‌آدرس آن‌ها مشاهده کنید، با استفاده از آدرس آی‌پی یا مک‌آدرس به جست‌وجوی کاربری بپردازید، به جست‌وجوی

سرویس‌ها (FTP، SSH) پردازید، محاوره‌ای در ارتباط با DNS انجام دهید، پینگ کنید و کارهای مرتبط با شبکه است را انجام دهید.

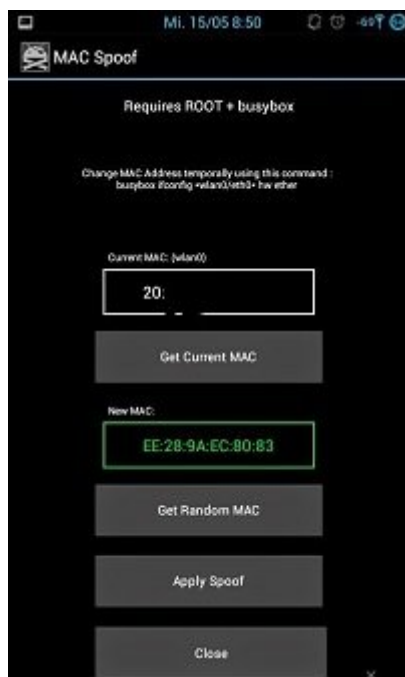
## 8. محافظت از شبکه وای‌فای در برابر حملات هکری، MITM و استخراج اطلاعات



با اقداماتی نظیر محدود کردن دستگاه‌های متصل به شبکه می‌توان تا حدودی با حملات سایبری مقابله کرد، اما در مورد حملات مرد میانی، استراق سمع، قطع دسترسی به شبکه وای‌فای و انواع دیگری از حملات هکری چه کاری باید انجام داد؟ برای محافظت از گوشی‌های اندرویدی در برابر این مدل حملات باید از نرم‌افزارهای خاصی استفاده کرد. برنامه‌هایی اندرویدی و ویندوزی همچون FaceNiff، Cain & Abel، ettercap، DroidSheep با استفاده از تکنیک‌های خاصی به شما اجازه می‌دهند مشکلات امنیتی شبکه‌های وای‌فای را پیدا کنید و به مقابله با دسترسی‌های غیرمجاز به شبکه وای‌فای یا شنود اطلاعات پردازید. به‌طور مثال، WiFi Protector یک برنامه امنیتی اندرویدی است که برای مقابله با حملات جعل ARP و محافظت از شبکه‌های وای‌فای طراحی شده است. این برنامه به‌طور مستمر شبکه و پارامترهای مربوط به شبکه را بررسی می‌کند. زمانی که رفتار غیر عادی را شناسایی کرد، هشدار نشان می‌دهد که نوع هشدارها قابل پیکربندی است. به‌طور مثال، برنامه WifiKill زمانی که گوشی روت شده باشد، قابلیت‌های خوبی در اختیار کاربران قرار می‌دهد، در حالت استاندارد نیز مکانیسم امنیتی خوبی را ارائه می‌کند که عدم نیاز به پیکربندی، هماهنگ‌سازی عملکرد برنامه متناسب با نیازهای کاری، عدم شناسایی نرم‌افزار توسط هکرها، عملکردی در سکوت کامل بدون تولید صداهای آزاردهنده، اعلان‌های قابل تنظیم، پخش آهنگ در زمان حمله، فعال کردن حالت ارتعاش در زمان شناسایی یک الگوی حمله، توانایی کار کردن در شبکه‌های محلی پیچیده (شبهه به WLAN و WDS)، پیاده‌سازی تمهیدات امنیتی خودکار، به‌کارگیری حداقلی منابع و کمترین مصرف باتری از ویژگی‌های این نرم‌افزار است.

## 9. تغییر مک آدرس گوشی اندرویدی





هر کاربری در اینترنت یک آدرس آی پی و مک آدرس خاص خود را دارد، اما در برخی موارد باید مک آدرس گوشی اندرویدی به دلیل مقابله با حملات هکری یا زمانی که مک آدرس برای عدم دسترسی به وای فای مسدود شده تغییر پیدا کند. برای تغییر مک آدرس گوشی، ابتدا باید گوشی را روت کنید و سپس برنامه [Mac Spoof](#) را روی گوشی نصب کنید. این برنامه بدون پیچیدگی خاصی اجازه می دهد مک آدرس گوشی را تغییر دهید (مک آدرس را به روش دیگری نیز می توان تغییر داد. در این روش به نرم افزارهای [BusyBox](#) و [Terminal App](#) نیاز دارید. در روش فوق باید گوشی در حالت روت شده قرار داشته باشد. پس از دانلود و نصب نرم افزارها، برنامه terminal app که یک ترمینال شبیه ساز در اختیارتان قرار می دهد را باز کنید و دستور `subusybox iplink show eth0` را درون آن بنویسید. این فرمان آدرس مک فعلی را نشان می دهد. اکنون فرمان `busybox ifconfig eth0 hw ether 00:11:22:33:44:55` را بنویسید. دقت کنید به جای `00:11:22:33:44:55` باید مک آدرس مدنظر خود را بنویسید. برای اطمینان از این موضوع که مک آدرس به درستی تغییر پیدا کرده فرمان `busybox iplink show eth0` را بنویسید و نتیجه را مشاهده کنید.

## 10. چگونه وضعیت تماسها، پیامها، دادهها و میزان وای فای مصرف شده در اندروید را مشاهده کنیم؟

اگر تمایل دارید از طریق یک نرم افزار کاربردی روی پیامهای کوتاه دریافت شده، دادهها و میزان مصرف وای فای نظارت دقیقی داشته باشید نرم افزار [Track It Call,SMS,Data Monitor](#) برای شما طراحی شده است. نرم افزار فوق به شکل روزانه، هفتگی، ماهانه یا زمان بندی های سفارشی در ارتباط با تماسها، پیامهای کوتاه، مقدار ترافیکی که از اینترنت موبایلی یا وای فای مصرف شده گزارشی در اختیارتان قرار می دهد. اطلاعات فوق به شکل نموداری و تصویری نشان داده می شود تا کاربر بتواند به درستی گزارشها را تحلیل کند.

## 11. تبدیل گوشی اندرویدی به یک وبکم نظارت تصویری

گوشی اندرویدی می تواند با تبدیل شدن به یک وبکم تحت شبکه، کاربر را بی نیاز از خرید وبکم کند. کاربران می توانند از دوربین گوشی اندرویدی به عنوان یک دوربین نظارت تصویری نیز استفاده کنند. برای انجام این کار به نرم افزار [IP Webcam](#) نیاز دارید. شما می توانید با نصب این برنامه روی گوشی اندرویدی، آن را توسط هر دستگاه اندرویدی یا کامپیوتر کنترل کنید و استریم های زنده ویدیویی را درون شبکه وای فای منتشر کنید. زمانی که نرم افزار فوق را روی گوشی اندرویدی نصب کنید، گزینه های جالبی در اختیارتان قرار می گیرد که اجازه می دهد دوربین را روی هر پلتفرمی توسط VLC Player یا مرورگر وب مشاهده کنید. برنامه فوق اجازه می دهد استریم ویدیویی درون شبکه وای فای با صدا یا بدون صدا و بدون استفاده از اینترنت انتقال پیدا کند. تنها کاری که باید انجام دهید، نصب برنامه روی گوشی، روشن کردن وای فای گوشی و انتخاب گزینه Start Server نرم افزار است. با انجام این کار دوربین گوشی روشن می شود و پایین صفحه یک شماره آی پی همراه با پورت ظاهر می شود. اگر آدرس آی پی و شماره

پورت را درون مرورگر خود وارد کنید، دسترسی به پنل مدیریتی ظاهر شده و استریم ویدویی روی صفحه نمایش کامپیوتر نشان داده می شود. در تنظیمات این پنل مدیریتی می توانید گزینه صدا را فعال یا غیر فعال کنید و در زمان نمایش تصویر از دوربین عقبی گوشی به دوربین پشتی سوئیچ کنید. گزینه های جالب دیگری نیز وجود دارد که به مرور زمان با آن ها آشنا می شوید.

## 12. پیدا کردن شبکه های بی سیمی که SSID آن ها نمایان نیست

روترهای امروزی با قابلیت های امنیتی قدرتمندی شبیه به الگوهای رمزنگاری، فیلتر کردن مک آدرس ها، غیر فعال کردن DHCP و استفاده از آدرس آی پی ایستا و پنهان کردن SSID به بازار عرضه می شوند. هر مکانیزم امنیتی بی سیم به شما کمک می کند تا سطح دسترسی کاربران غیرمجاز به شبکه را کم کنید. پنهان کردن نام شبکه بی سیم در برخی موارد برای کارمندان یک سازمان مشکلاتی را به وجود می آورد. inSSIDer نرم افزار رایگان و متن بازی است که برای پوشش وای فای استفاده می شود. این برنامه بدون هیچ گونه پیکربندی گیج کننده ای قابل استفاده است. زمانی که نرم افزار را دانلود و نصب کنید، [inSSIDer](#) به طور خودکار شروع به پوشش اکسس پوینت های در دسترس می کند. پس از آن که ارزیابی مربوطه کامل شد، فهرستی از SSID ها، کانال ها، RSSI، مک آدرس ها، حداکثر نرخ انتقال، نوع شبکه و اطلاعاتی مرتبط با شبکه را ارائه می کند. البته کاربردهای نرم افزار به موارد یاد شده محدود نمی شود و می توانید برای بهینه سازی و مدیریت یک شبکه وای فای از آن استفاده کنید.

## 13. یک دیوار آتش ایده آل برای کم کردن مصرف داده ها

[DroidWall](#) یک دیوار آتش قدرتمند برای دستگاه های اندرویدی است که اجازه می دهد روی برنامه هایی که قرار است از طریق وای فای یا شبکه های سلولی به اینترنت دسترسی داشته باشند محدودیت هایی را اعمال کنید. این برنامه همچون دیوارهای آتش دسکتاپی به برنامه های خاصی اجازه می دهد به اینترنت متصل شوند یا محدودیت هایی برای برنامه ها اعمال شود. لازم به توضیح است که این برنامه به دسترسی روت نیاز دارد.

## 14. مشاهده سرعت فعلی شبکه در نوار وضعیت اندروید

اگر روی گوشی اندرویدی به طور مرتب فایل هایی را دانلود می کنید، اما درباره سرعت دانلود اطلاع دقیقی ندارید باید از نرم افزار [Internet Speed Lite Meter](#) استفاده کنید. زمانی که برنامه فوق روی گوشی اندرویدی نصب شد، مقداری در نوار وضعیت بالای صفحه ظاهر می شود که سرعت فعلی اینترنت را نشان می دهد. از ویژگی های شاخص این نرم افزار می توان به ارائه اطلاعات بلادرنگ از سرعت شبکه، جدا کردن گزارش آماری شبکه وای فای و سلولی و نظارت بر داده های ترافیکی در 30 روز گذشته اشاره کرد.

## 15. انتقال بی سیم فایل ها از اندروید به کامپیوتر شخصی

نرم افزارهای مختلفی همچون Zappia، ShareIT، SendAnywhere و... برای انتقال بی سیم فایل ها از اندروید به کامپیوتر شخصی ارائه شده اند. نرم افزار [AirDroid](#) گزینه رایگان ایده آل دیگری است که اجازه می دهد به فایل های روی گوشی یا تبلت اندرویدی توسط ویندوز، لینوکس و مک دسترسی پیدا کنید و آن ها را مدیریت کنید. از ویژگی های شاخص این نرم افزار می توان به انتقال فایل ها میان پلتفرم های مختلف، دسترسی و کنترل از راه دور (بدون نیاز به روت)، مدیریت تماس ها و پیام های کوتاه، نمایش قرینه ای اعلان ها و پاسخ گویی به تماس ها از طریق کامپیوتر شخصی اشاره کرد

منبع:

[gtricks](#)

prophethacker

تاریخ انتشار:

01 دی 1398

---

نشانی منبع:

<https://www.shabakeh-mag.com/mobile-tricks/android-tricks/16398/15-%D8%AA%DA%A9%D9%86%DB%8C%DA%A9-%D9%88-%D8%AA%D8%B1%D9%81%D9%86%D8%AF-%D8%AC%D8%A7%D9%84%D8%A8-%D9%88%D8%A7%DB%8C%E2%80%8C%D9%81%D8%A7%DB%8C-%D8%A8%D8%B1%D8%A7%DB%8C-%DA%AF%D9%88%D8%B4%DB%8C%E2%80%8C%D9%87%D8%A7%DB%8C-%D8%A7%D9%86%D8%AF%D8%B1%D9%88%DB%8C%D8%AF%DB%8C>