WLAN – "Hack"

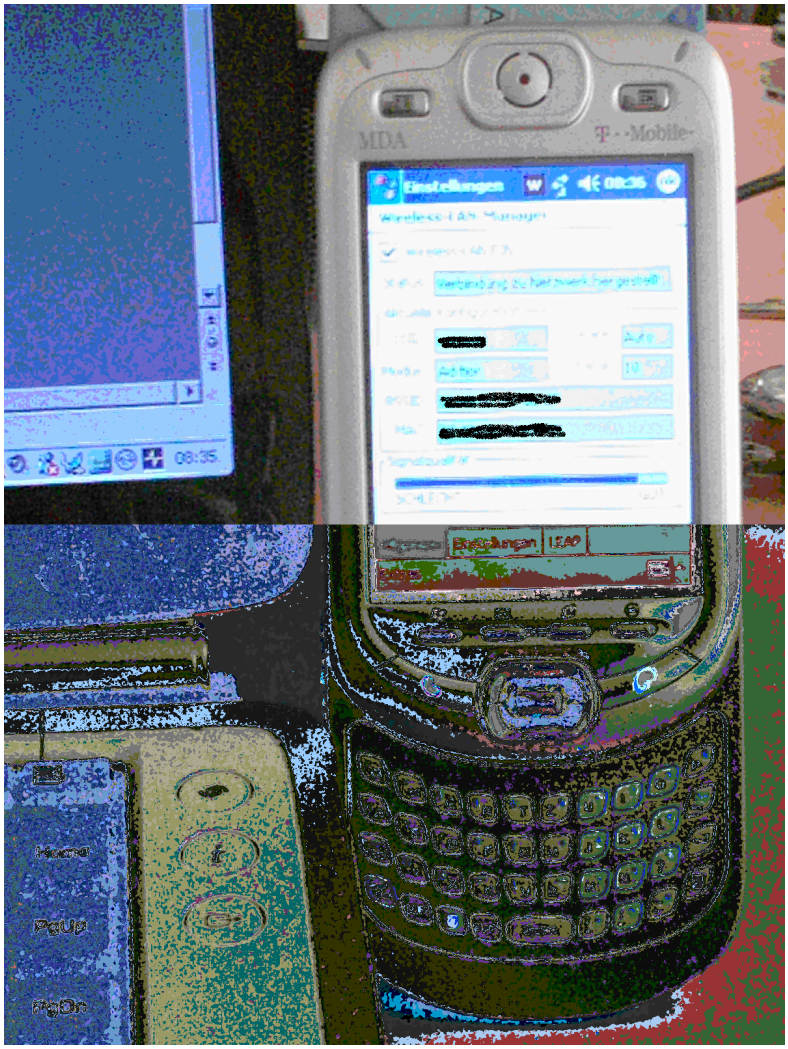
Disclaimer:

Diese Anleitung soll Sie nicht dazu verleiten, kriminelle Tätigkeiten durchzuführen. Sie machen sich unter Umständen strafbar. Informieren Sie sich vorher im BDSG und TDSG und anderen relevanten Gesetzen über mögliche Verbote. Ich übernehme KEINE Verantwortung für einen Missbrauch. Die nachfolgende Beschreibung habe ich MIT Genehmigung des WLAN-Netzwerk-Eigentümers durchgeführt.

Beginnen wir:

Letzte Woche war ich mit meiner Freundin im Urlaub (Ferien auf dem Bauernhof). Da ich mich auch mal erholen wollte, entschied ich mich, nur zwei Notebooks, einen mobilen Drucker und mein neustes Spielzeug, den MDA III mitzunehmen.

Bei der Ankunft habe ich aus Spaß mal meinen MDA III auf WLAN-Betrieb gestellt und durch die Gegend geschleppt … und …. Das Ergebnis: Zwei WLANs.



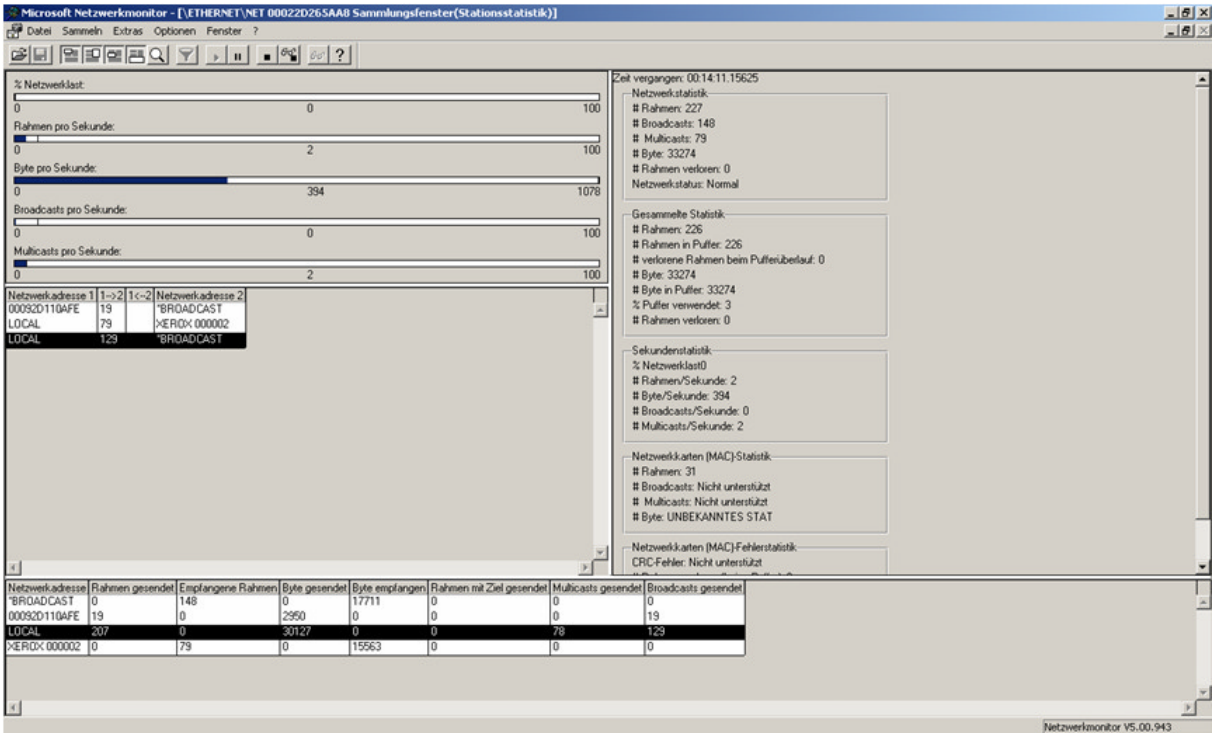
Das Bild zeigt den MDA III und mein Toshiba Notebook mit einer WLAN Verbindung. Das Problem war jetzt, das ich nicht so einfach eine WLAN Verbindung hergestellt bekommen habe, weil das Netzwerk dann wohl doch rudimentär geschützt war.

Eigentlich hatte ich mir ja vorgenommen, so einmal täglich das Internetcafe im Nachbarort aufzusuchen, aber da ich sah, das der Sohn unserer Vermieter jetzt WLAN hatte, fragte ich ihn, ob ich das WLAN nutzen kann (wir sind schon seit fast 8 Jahren einmal im Jahr dort zu Besuch). Scherzhaft sagte er, wenn ich wüsste, wie ich eine Verbindung herstellen kann, könnte ich seine Internet-Verbindung nutzen. Daraus machte ich dann eine Aufgabe und verzichtete auf die Bekanntgabe der Verbindungsdaten *gg* und stellte mich der Herausforderung, ein Netzwerk zu knacken (hatte ich bisher nur in Schulungsumgebungen gemacht).

Also den MDA III und das Toshiba Notebook für die Verwendung von WLAN konfiguriert.

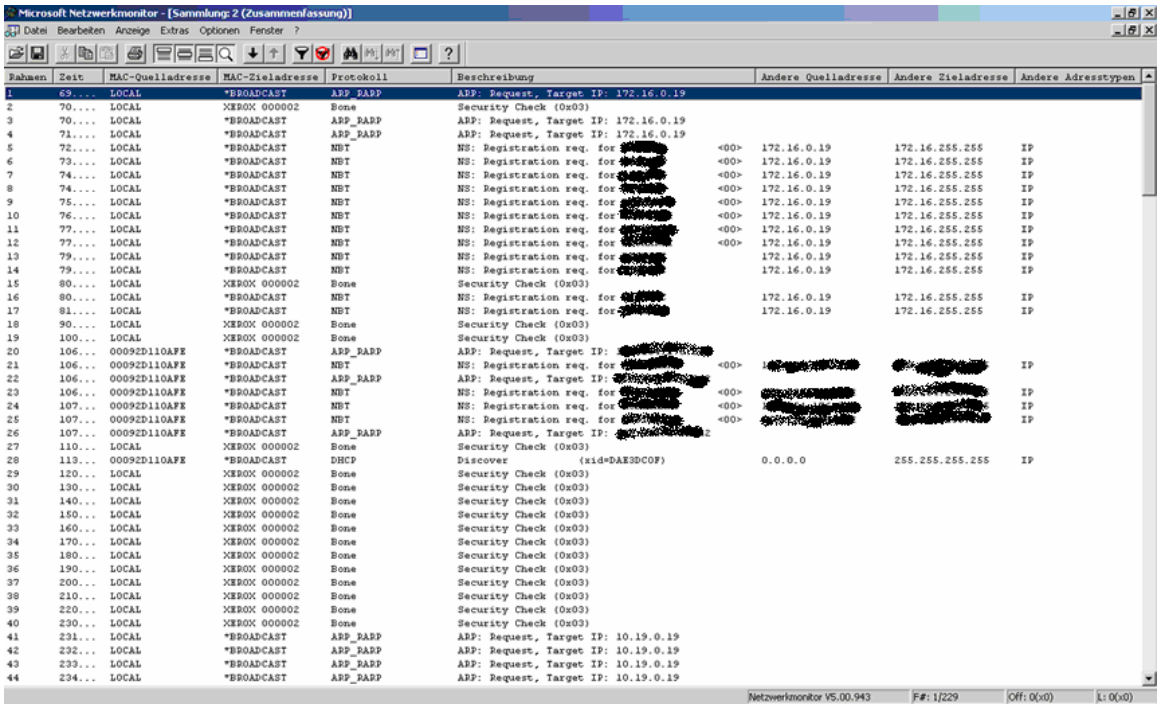
WEP wurde nicht verwendet, nur ein MAC-Filter. Die SSIDs wurden auch angezeigt, lt. XP Konfig und MDA III Konfig wurde kein WEP verwendet (was man ja auch leicht hätte knacken können, denn alle Tools hatte ich wie immer auf meinem Notebook dabei).

Also was tun? MAC-Adressen spoofen? Als erstes habe ich mal den Netzwerkmonitor angeschmissen und geschaut, was so alles passiert. Welcher Netzwerkmonitor – natürlich der von Windows (besser SMS 2003 – ist ja alles lizensiert):



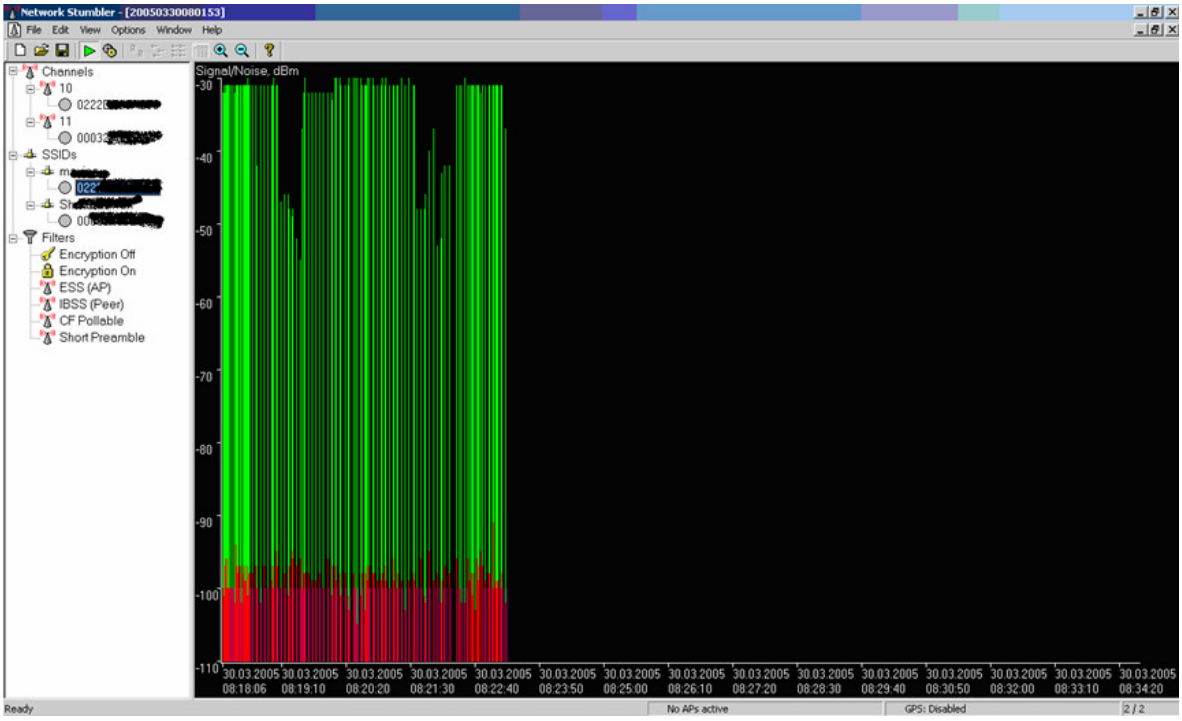
Prima, da war doch schon mal etwas Verkehr im Netz ✍

Die Details waren auch sehr aufschlussreich.



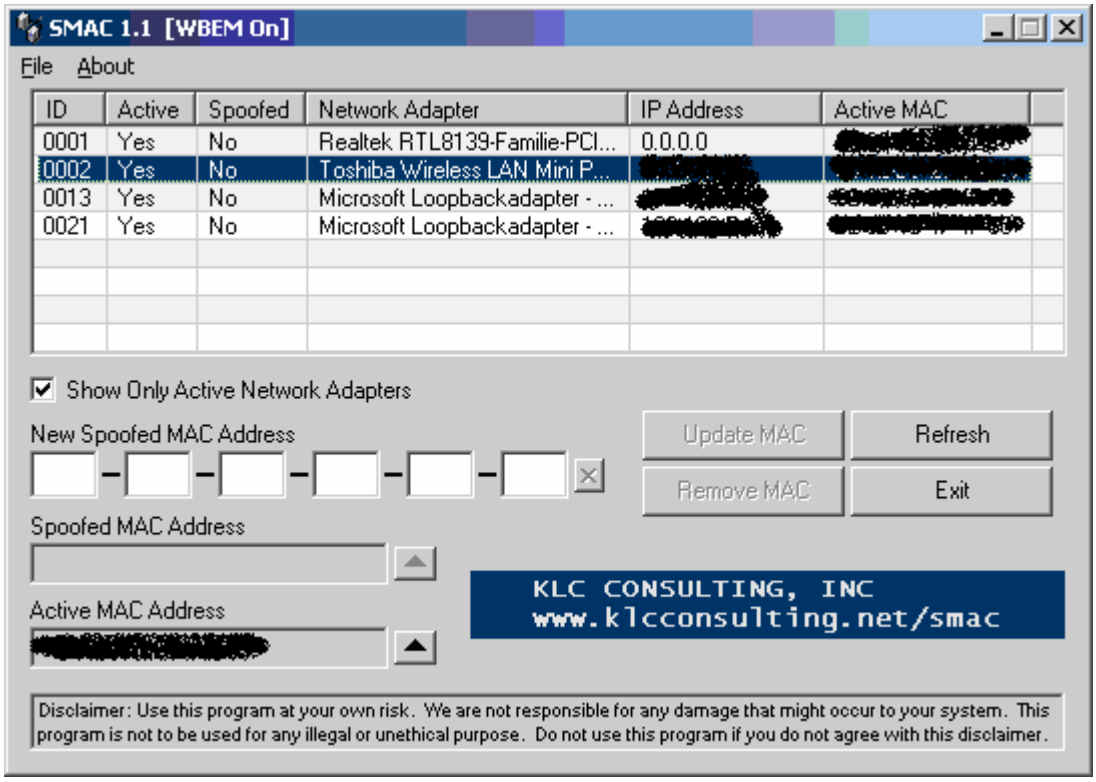
Nach ein paar Versuchen mit den beiden WLANs habe ich eine SSID als nicht interessant befunden (keine Internet Verbindung möglich) und widmete mich der anderen SSID, wo MAC-Adressen Filterung aktiv war.

Ich musste jetzt nur noch ne MAC-Adresse ermitteln. Da meine WLAN-Karte vom Toshi Notebook zum Glück den ORiNOCO-Chipsatz hatte, konnte ich den NetStumpler anwenden. Einfach das Tool starten, nen paar Sekunden warten und dann werden Dir die SSIDs und MAC-Adressen angezeigt.



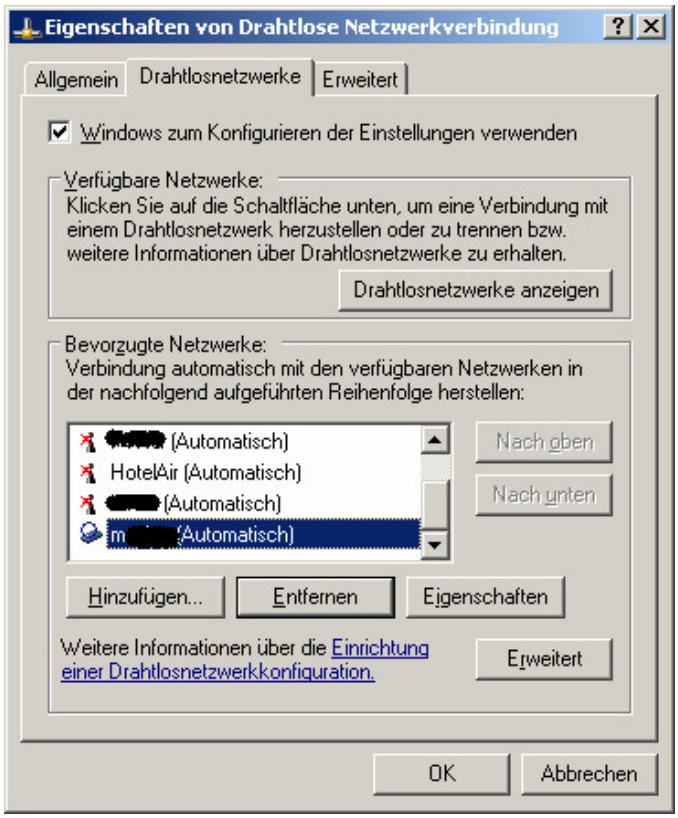
Dann habe ich mir eine MAC-Adresse aus dem Scan rausgesucht und dann musste ich nur noch ein Tool haben, mit welchem ich die MAC-Adresse meiner WLAN-Karte

"spoofen" kann. Dazu habe ich SMAC verwendet (ihr kennt die Werbung: Das smackt mir ✍).

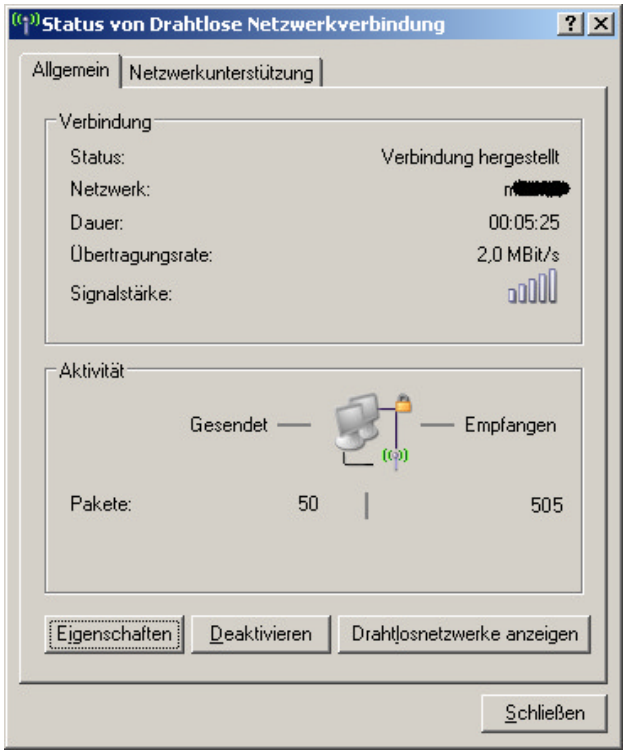


Einfach die ermittelte MAC-eintragen, updaten und dann geht es ab. Es gibt zwar noch andere Möglichkeiten, MACs zu fälschen, aber das ist doch für einen Windows User wie mich, ganz praktisch.

Auf meinem Windows XP Notebook werden alle Netzwerke angezeigt. HotelAir ist übrigens nicht das Netz, was ich erreichen wollte, sondern ein Hotspot aus einem Hotel wo ich vor ein paar Wochen war (Windows XP behält ja die Hotspots in seiner Liste *gg*).



Die Verbindung der WLAN Karten hatte ich mal auf DHCP gestellt und schon hatte ich eine IP – Danke lieber WLAN-Router. Ja, und das war es dann schon. Die Verbindung konnte hergestellt werden und ich konnte surfen (leider nicht immer, da das Netz nicht immer verfügbar war).



Der Sohn der Vermieter war sichtlich beeindruckt (und ich war auch ganz stolz auf mich, wie einfach so was ist). Ich musste ihm Schritt für Schritt erklären, was ich gemacht habe und daraus ist dieses "Tagebuch" entstanden.

Worauf ich verzichtet habe ist jetzt natürlich die Hauswand unseres Vermieters mit den notwendigen Zugangsdaten zu versehen, damit Wardriver schnell an die Zugangsdaten kommen.

Disclaimer:

Sollten Sie das ganze hier nachvollziehen wollen, stellen Sie sicher, dass Sie NICHT gegen geltende Gesetze verstossen und die Genehmigung des Netzwerkbetreibers haben. Sie machen sich sonst strafbar.