Bots im Kontext von Spam

Need Captcha Entry Team by urigarin 22.09.08

Posted in Data Entry, Data Processing

Hello, I need captcha Entry team for various captchas site. I can pay $.75-1/1k. If you can do more than huge captchas per day. please bid if you are interested system is much faster all time. … (Budget: $30-250, Jobs: Data Entry, Data Processing)

eco AK Sicherheit
Februar 2009

Christian J. Dietrich
dietrich [at] internet-sicherheit . de

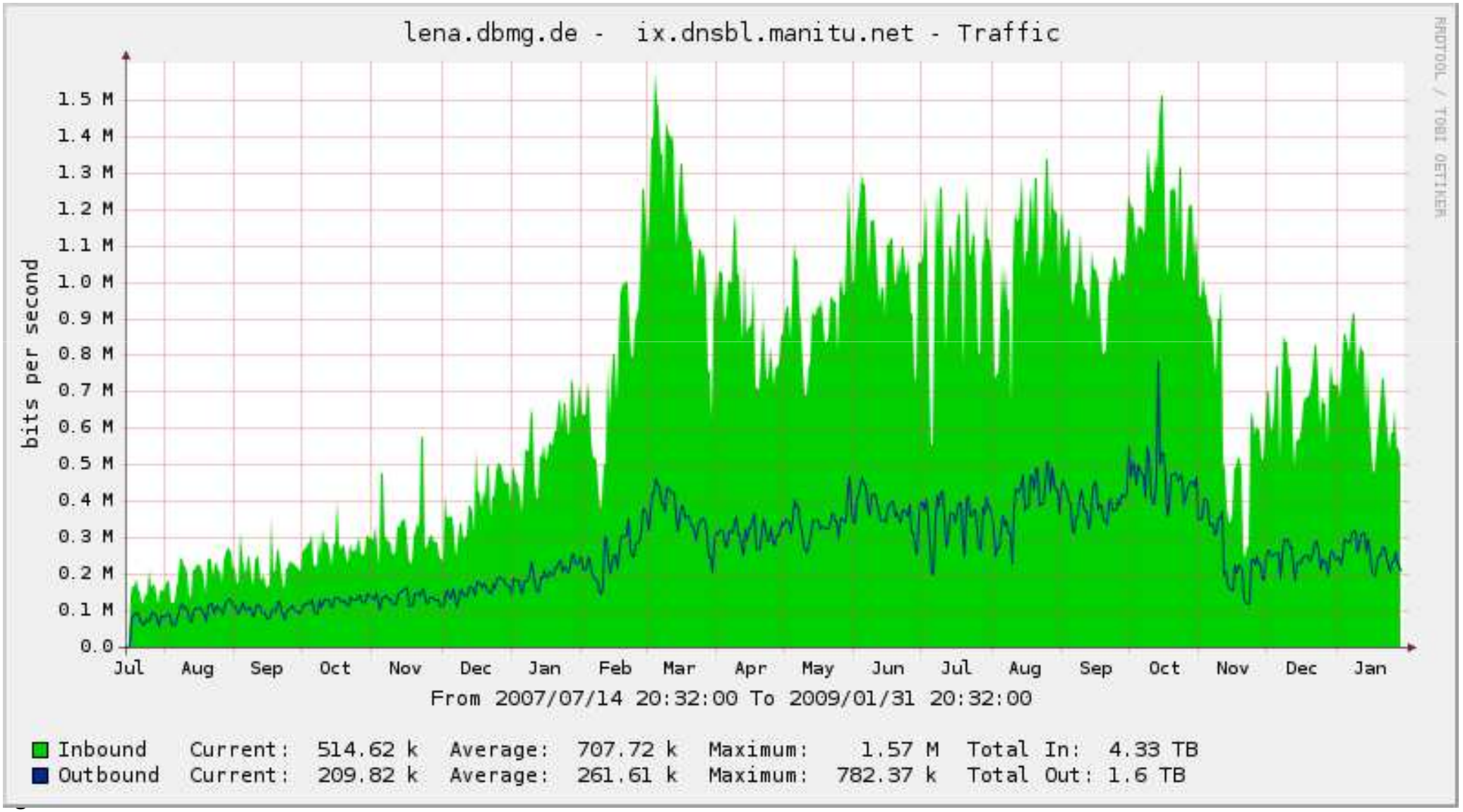
Institut für Internet-Sicherheit
https://www.internet-sicherheit.de
FH Gelsenkirchen

if(is) internet-sicherheit.

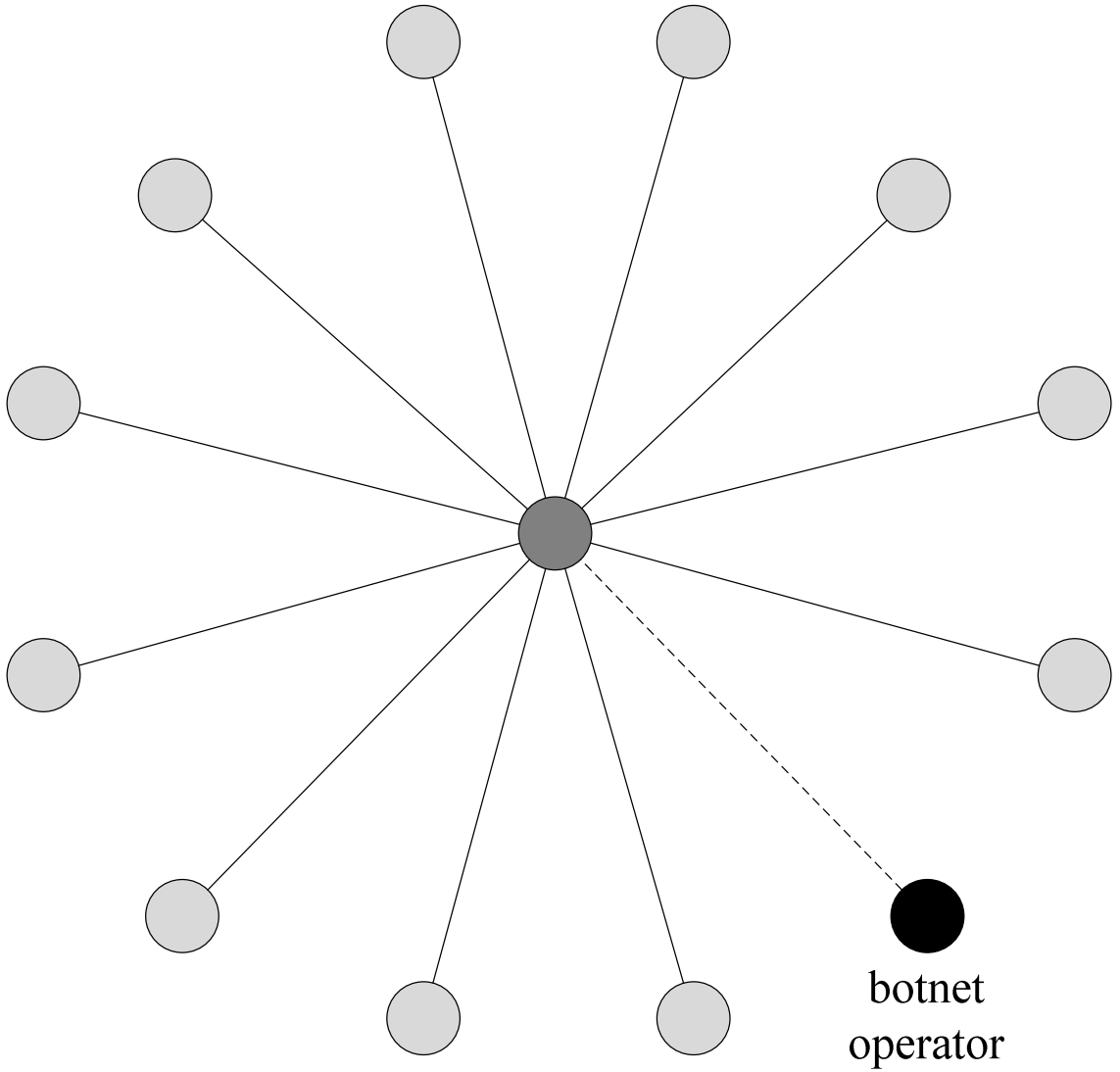
Inhalt

- Einleitung
- **Aktuelle Spam-Entwicklung im Detail**
- Die Tools der Spammer
  „Make money fast – the spammer‘s way“
- Botnet Security Mechanisms
- Fazit

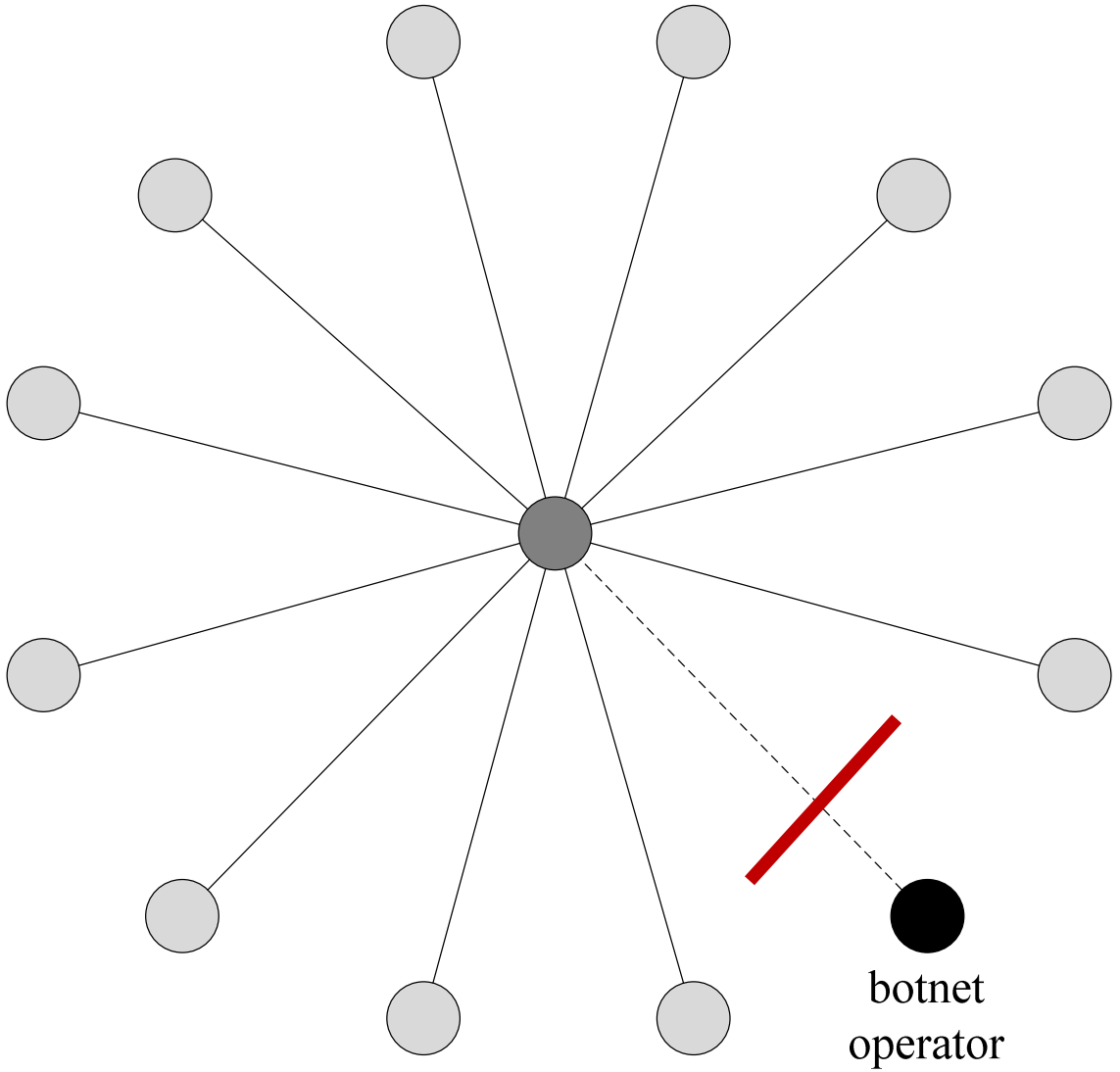
Spam? Wo ist das Problem?



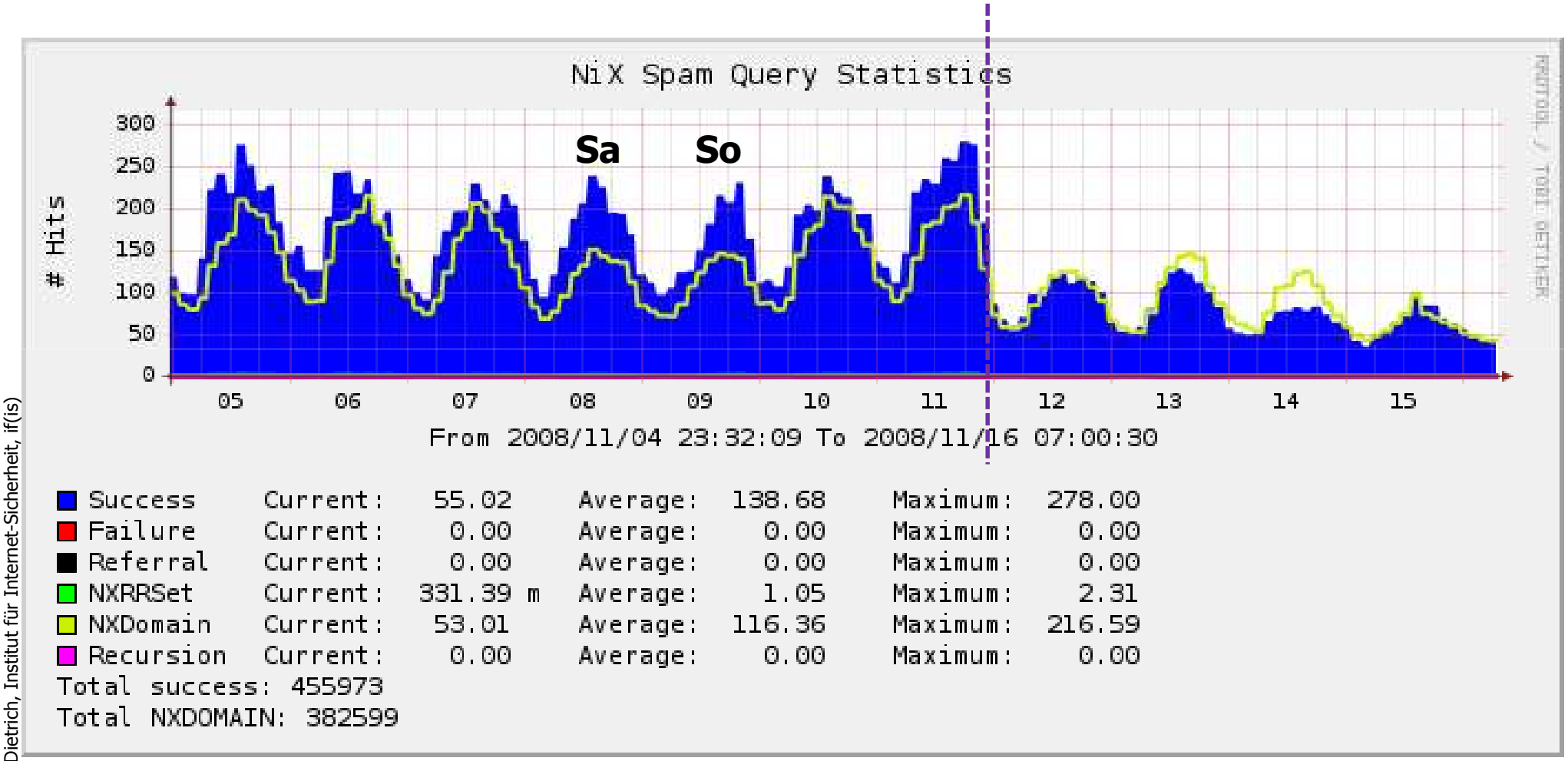
Botnet-Infrastruktur



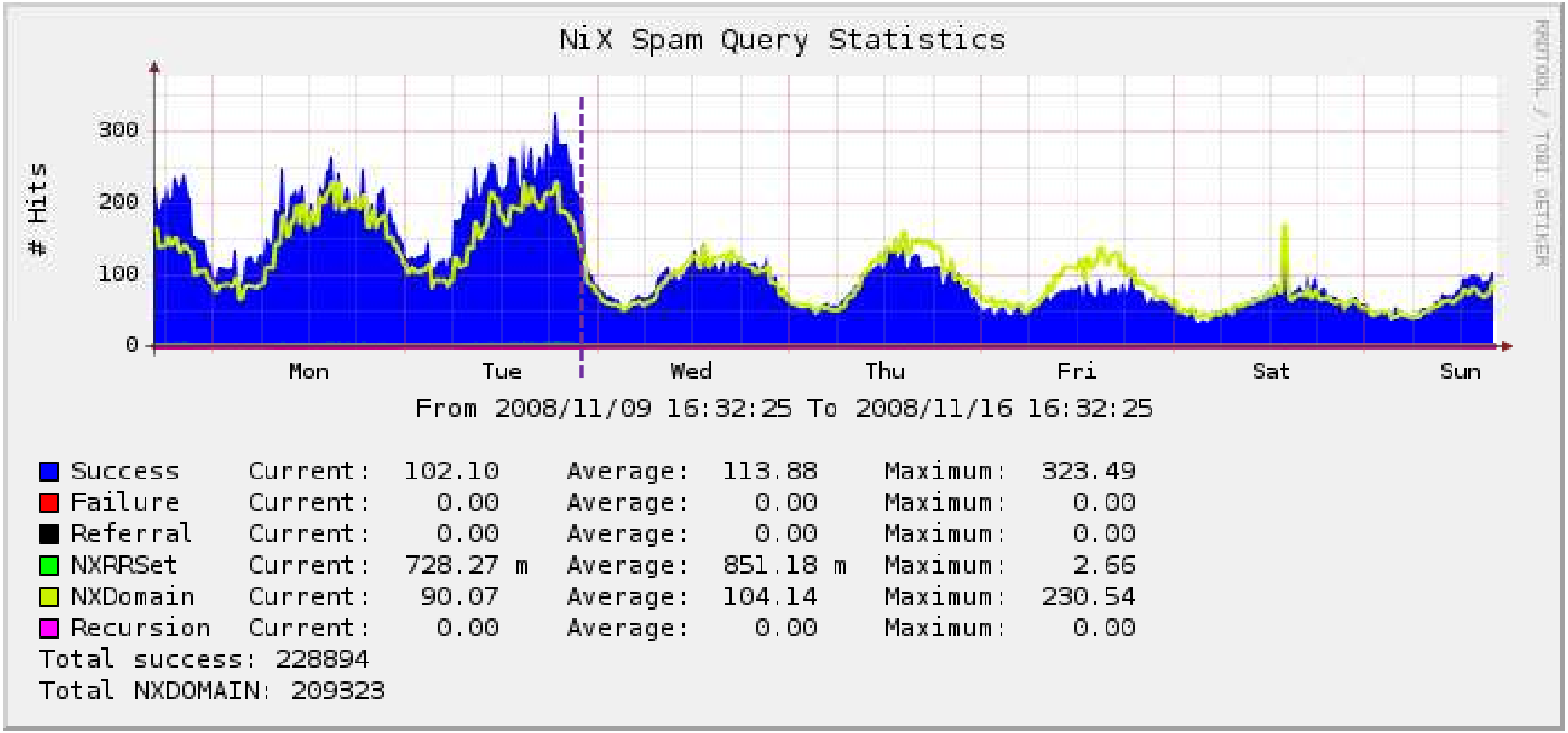
Botnet C&C abgeschnitten



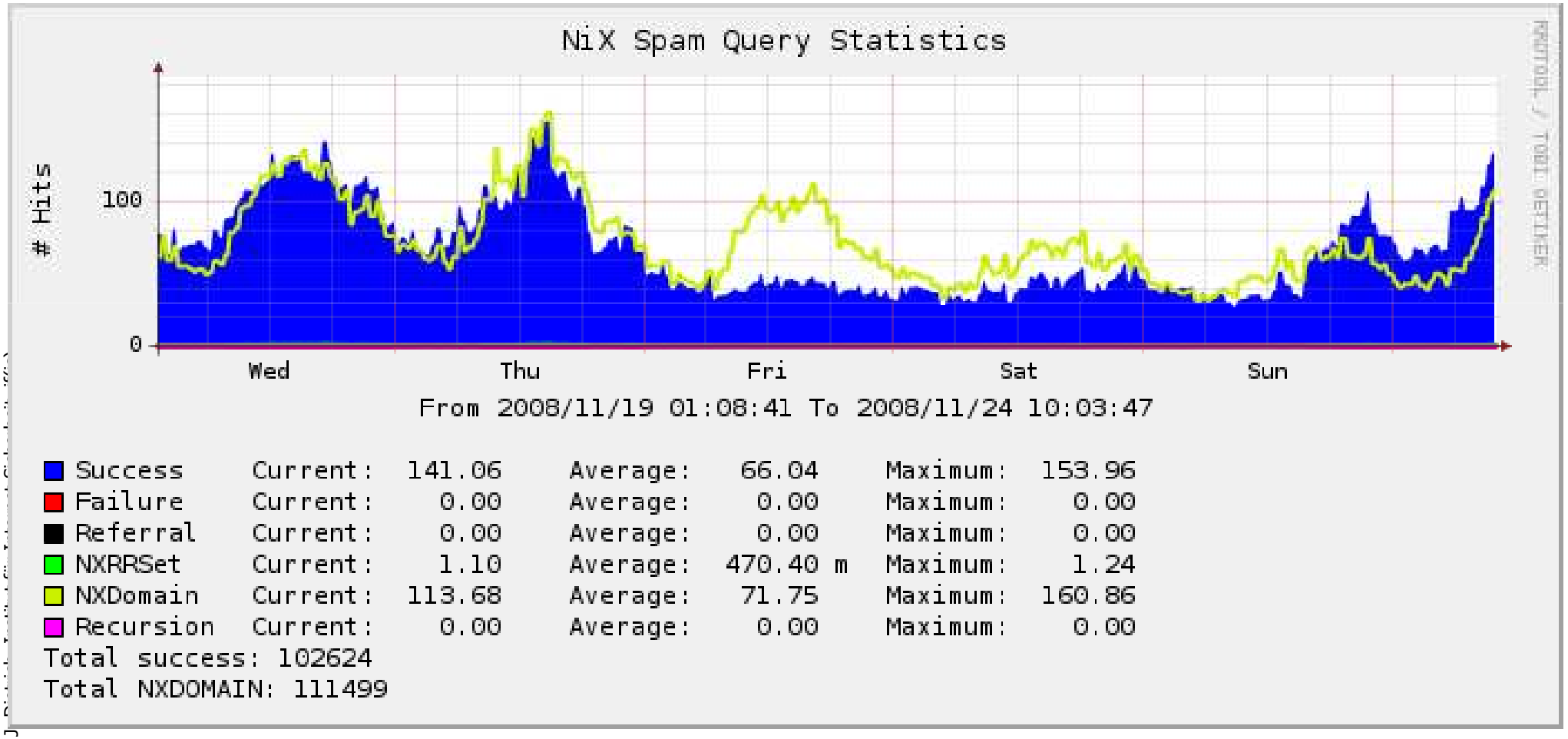
McColo (US ISP) taken offline 11/11/2008



McColo (US ISP) taken offline 11/11/2008

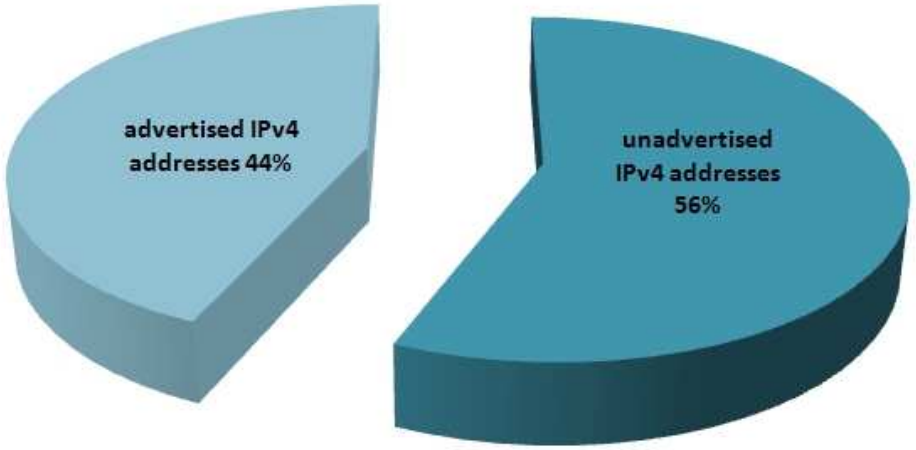


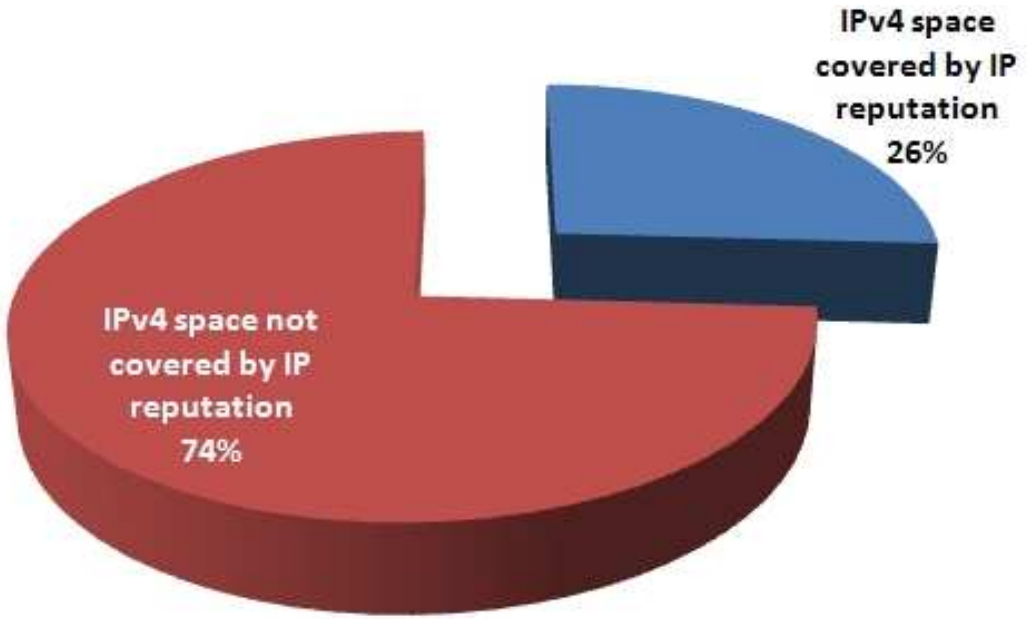
DDoS on InternetX (Schlund NS) 21/11/2008



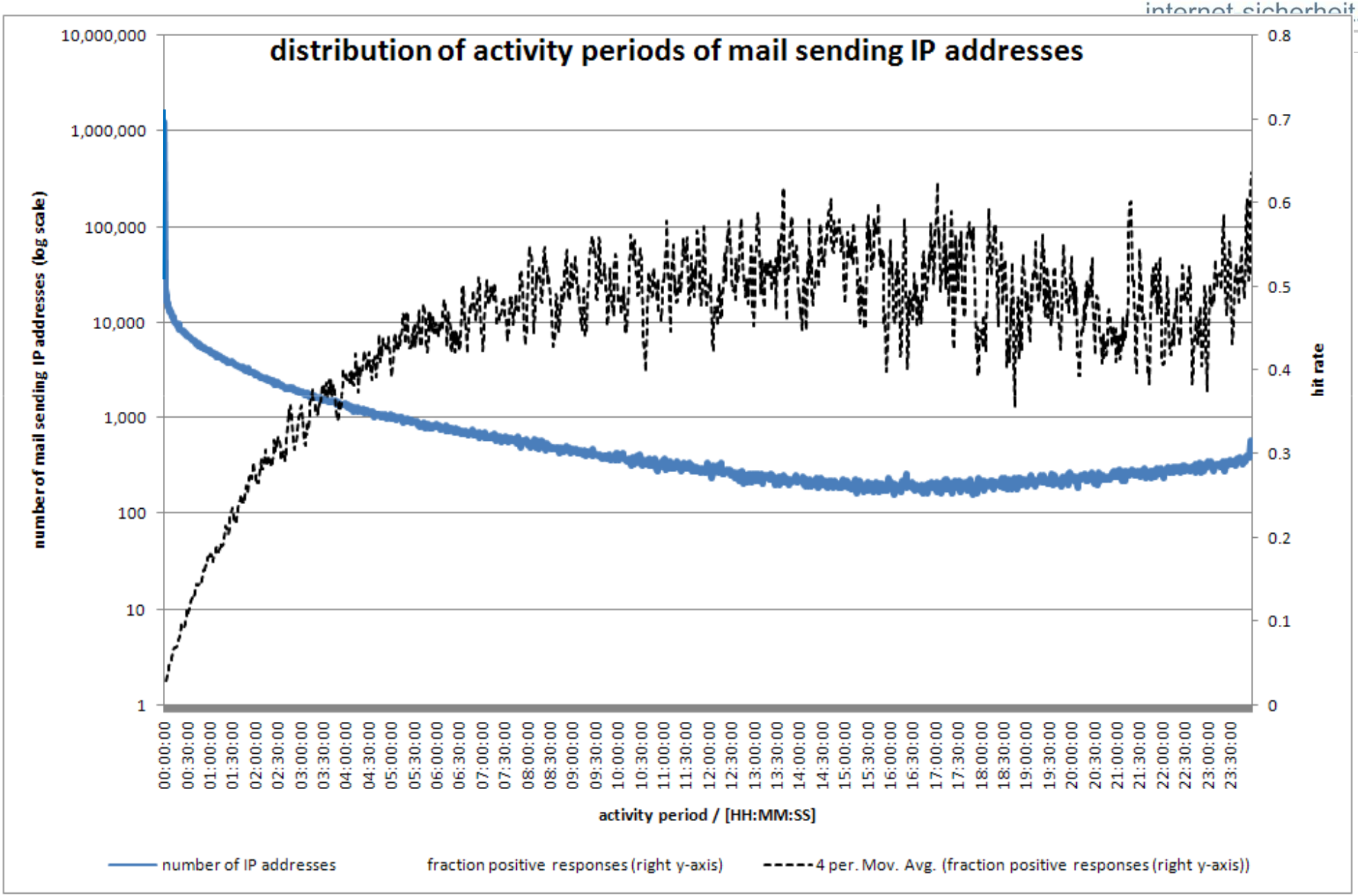
Reputation von IP-Adressen

- Theorie
  - 2^{32} = 4,2 Mrd. IPv4-Adressen
- Praxis
  - **1,872 Mrd. IPv4-Adressen advertised (Routing)**
  - **~75%** der advertised IPv4-Adressen sind **ohne Reputation!**
  - Statistisch: Nur jede 4. advertised IP-Adresse ist „bekannt“

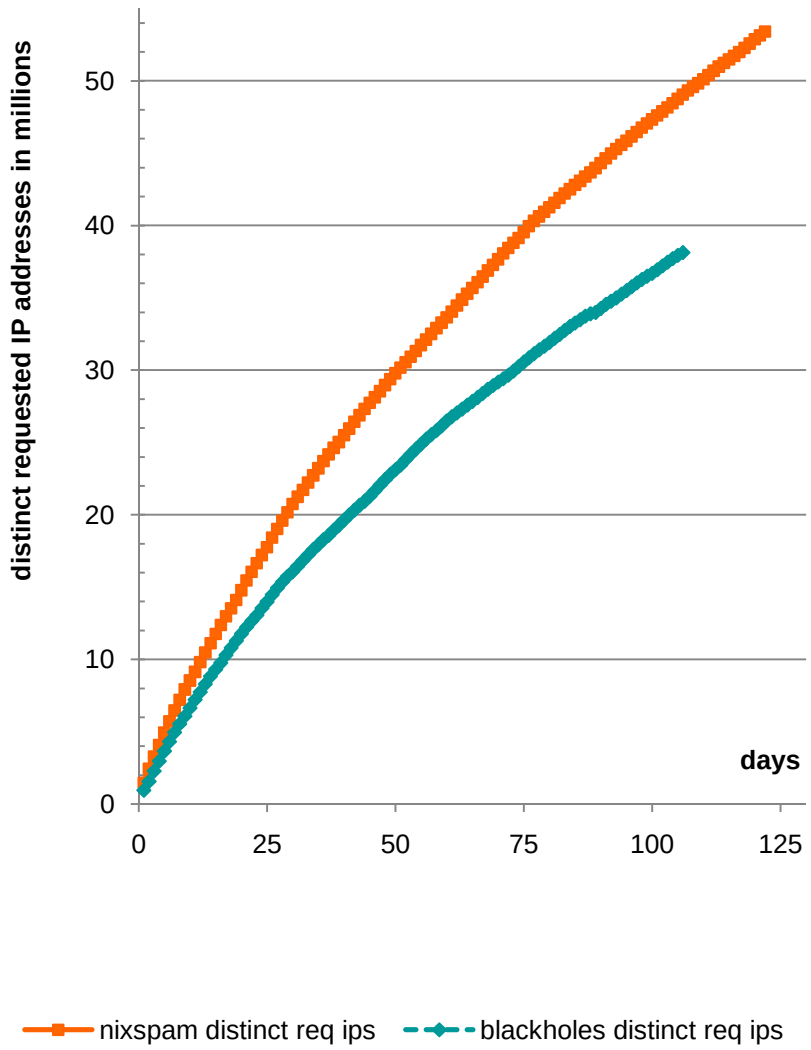




Verteilung der Aktivitätszeiträume von E-Mail-Quellen

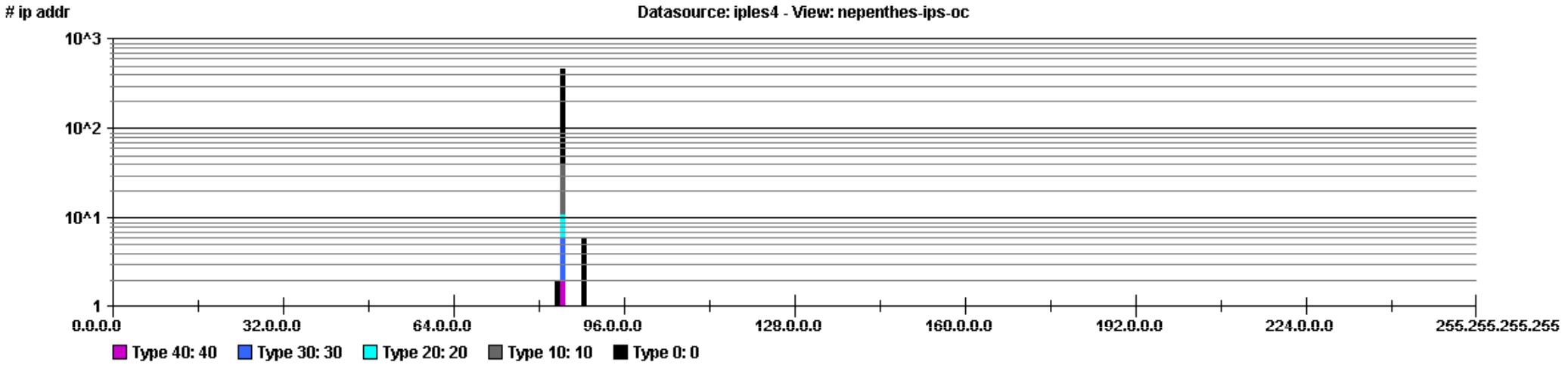


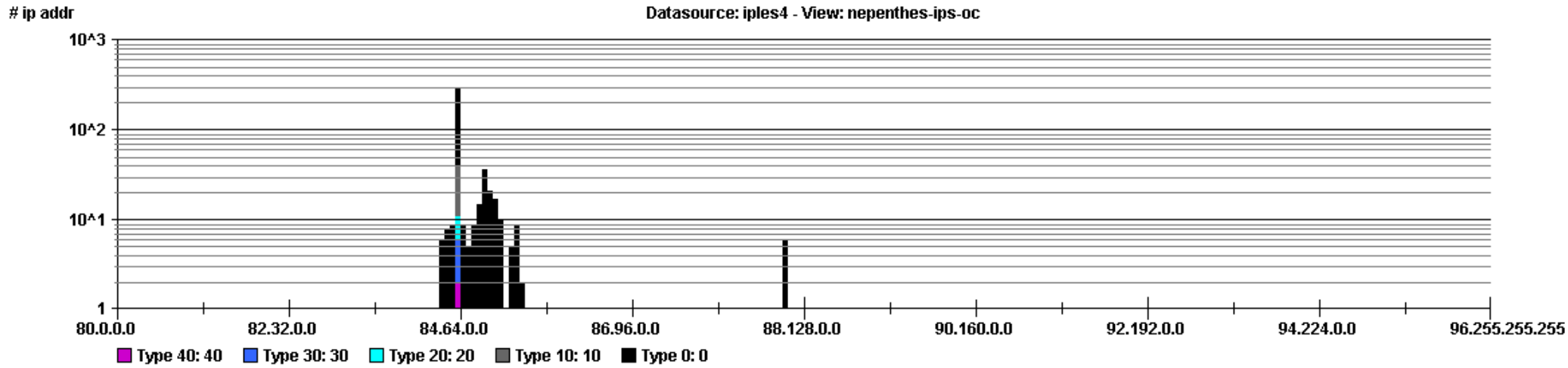
Eindeutigkeit von E-Mail-Quellen



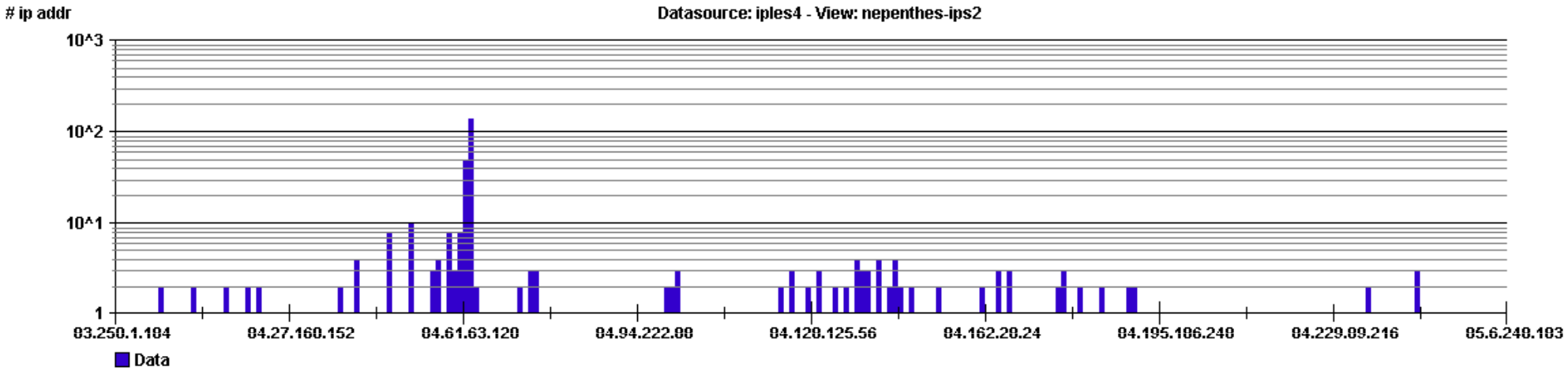
- 125-Tage-Zeitraum zeigt die „Einmaligkeit“ von IP-Adressen
- Mehr als **55 Mio. verschiedene IP-Adressen** von E-Mail-Quellen in 125 Tagen
- **12 Jahre** bis alle 1,8 Mrd. advertised IP-Adressen mind. 1 Mal genutzt wurden
- Orange line = Primärsensor
- Blue line = Sekundärsensor

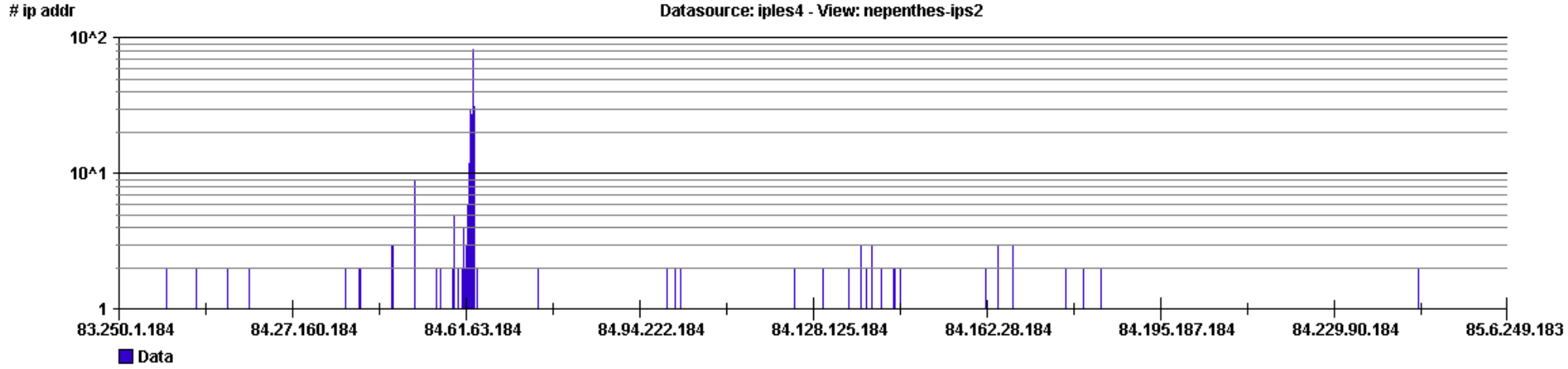
Infektionsquellen





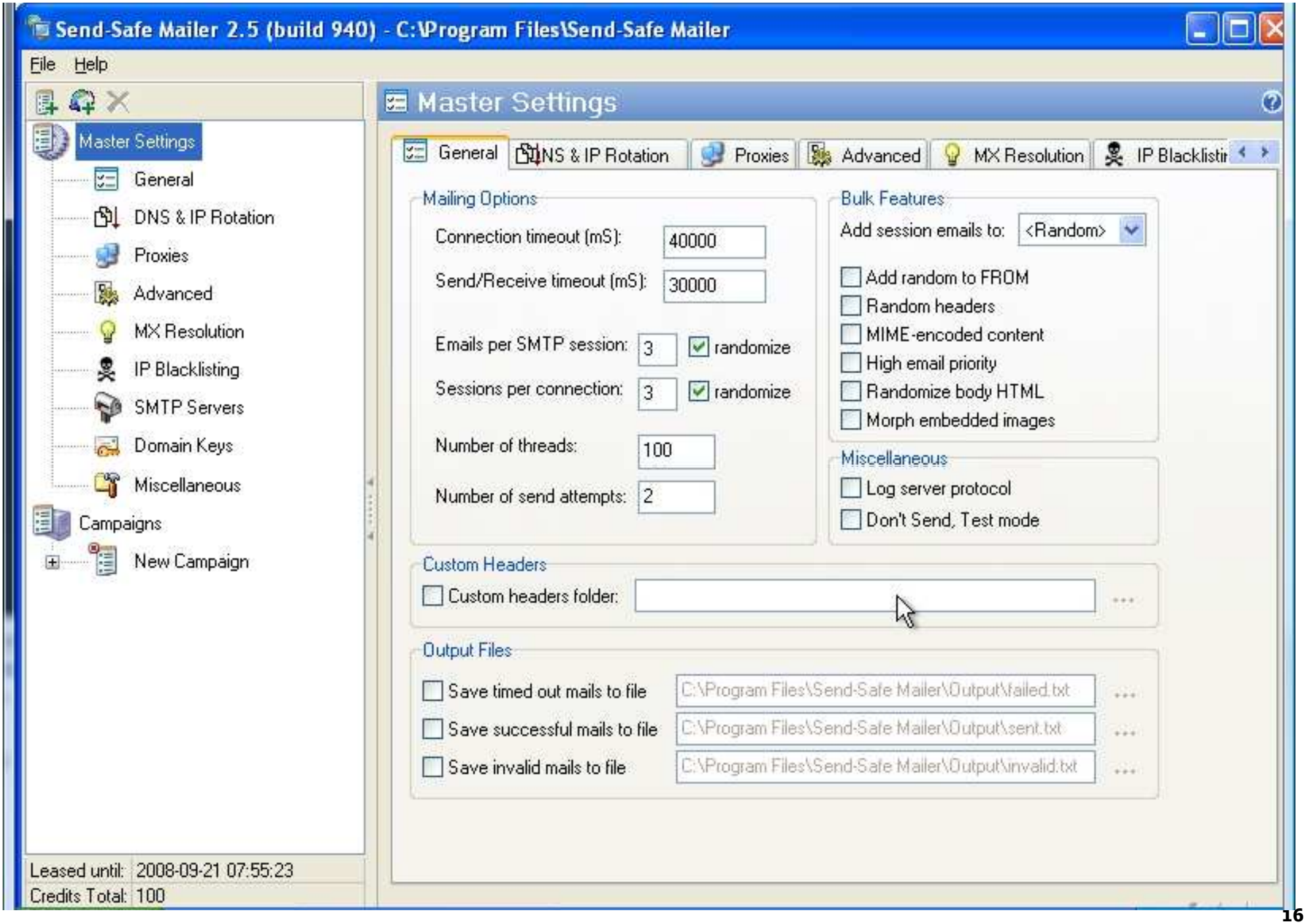
Infektionsquellen

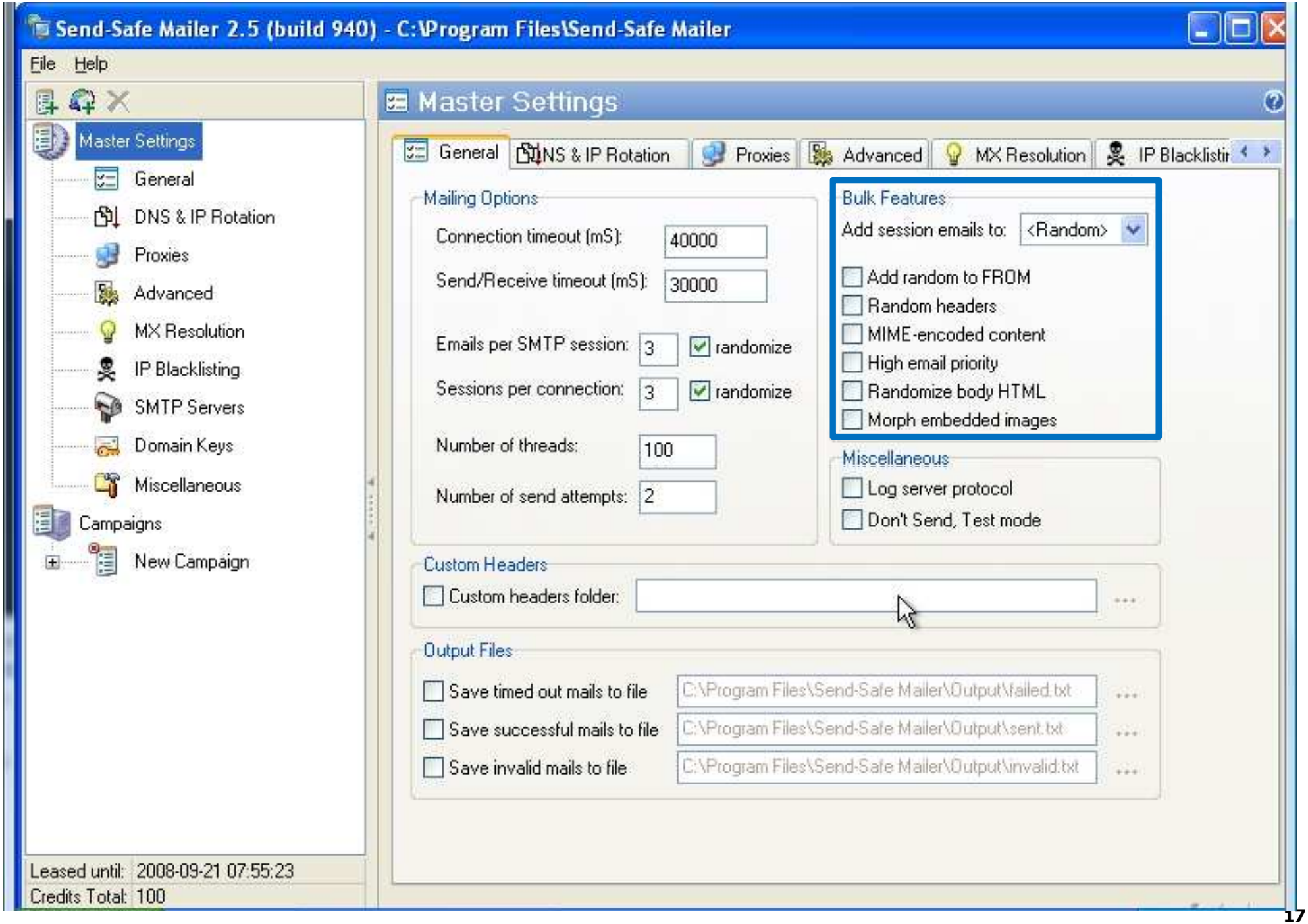


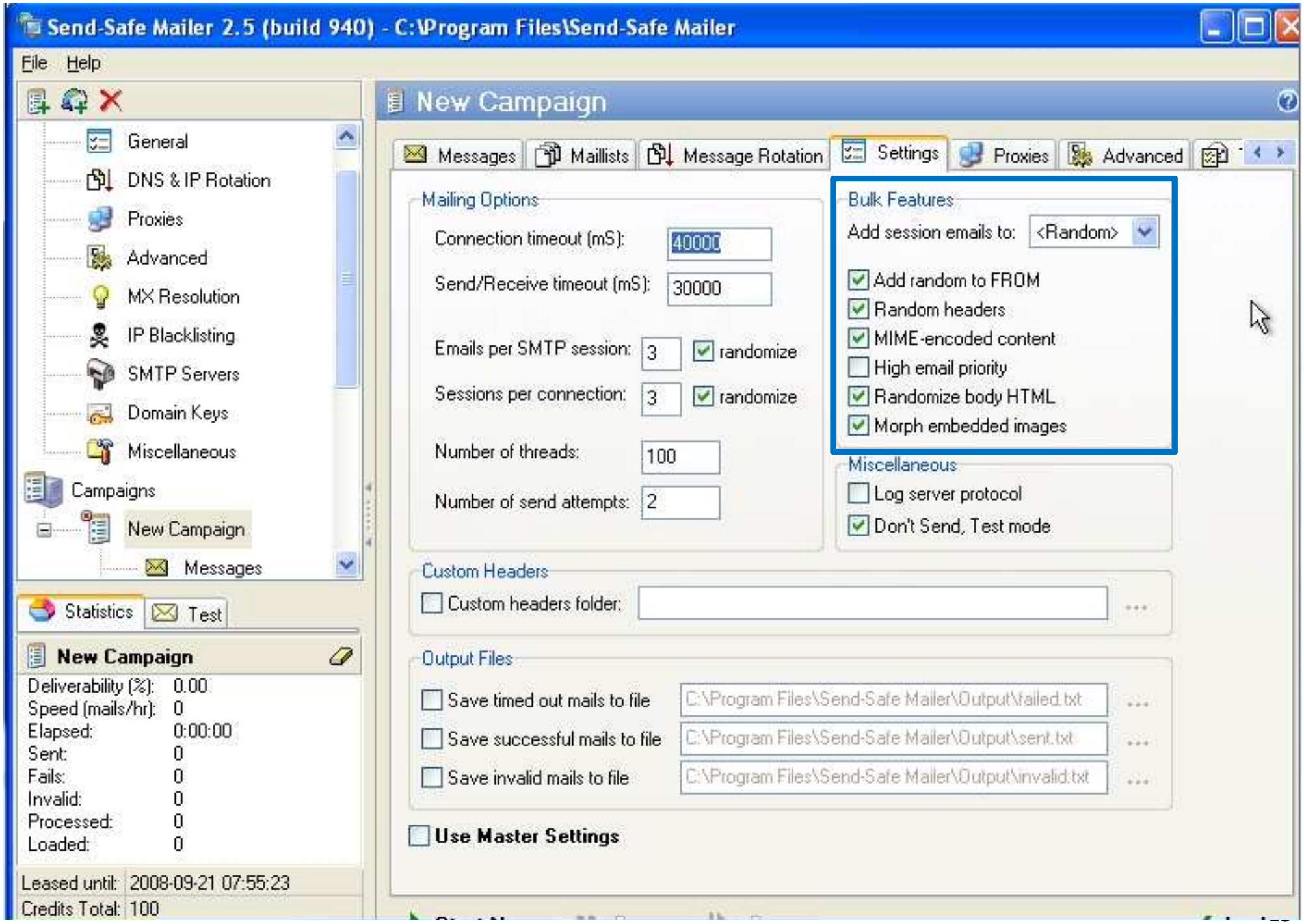


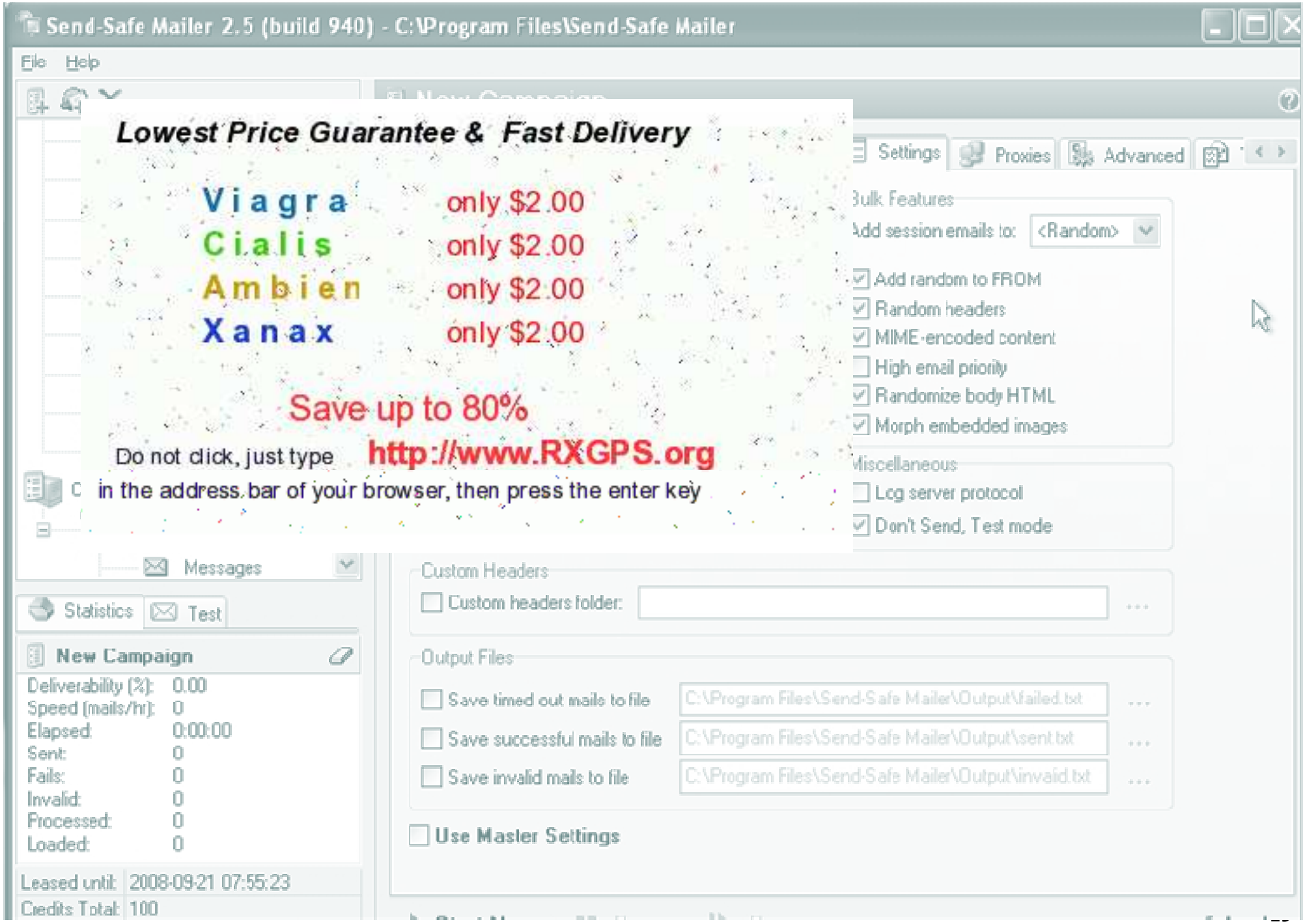
Inhalt

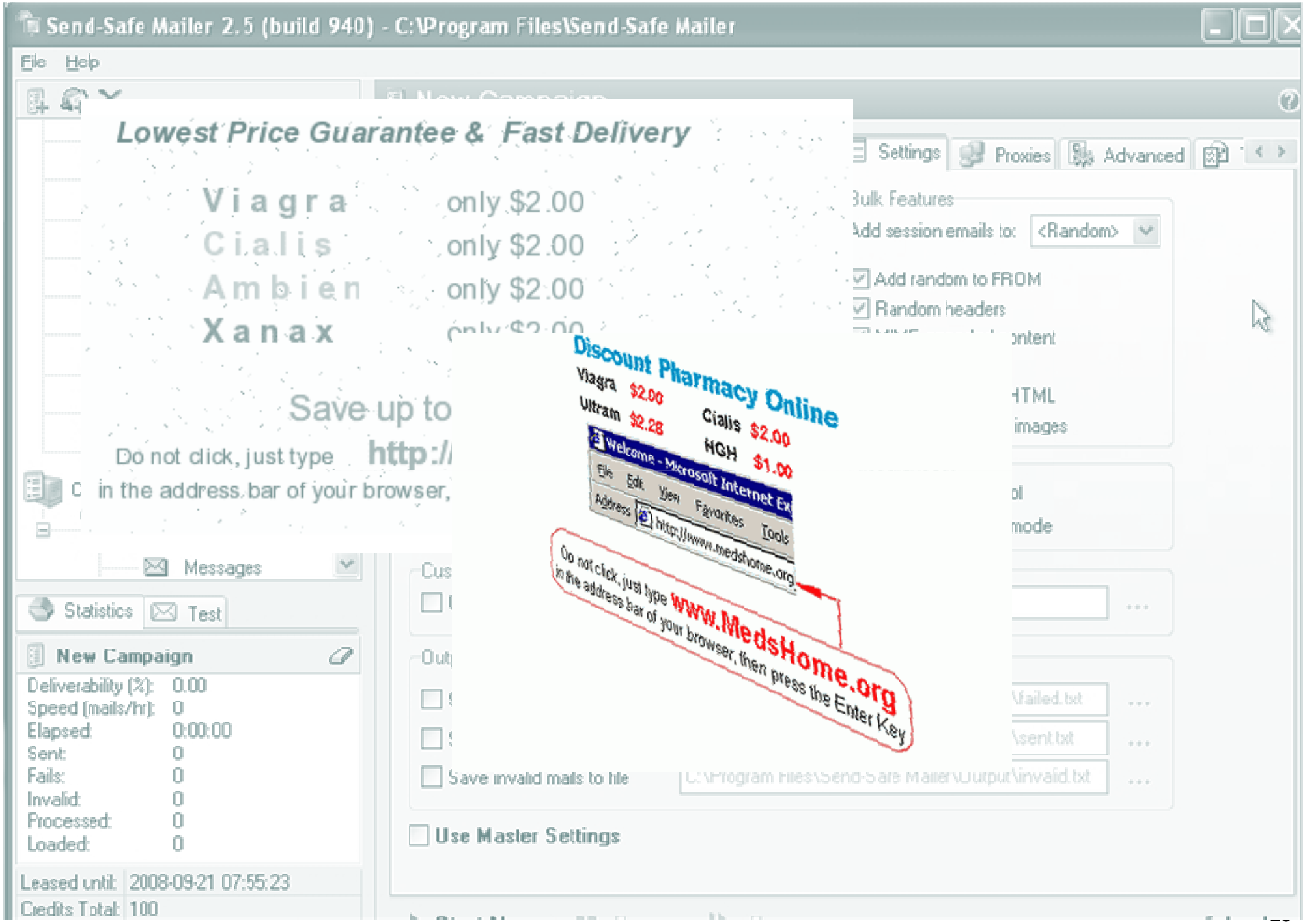
- Einleitung
- Aktuelle Spam-Entwicklung im Detail
- **Die Tools der Spammer**
  „Make money fast – the spammer‘s way“
- Botnet Security Mechanisms
- Fazit

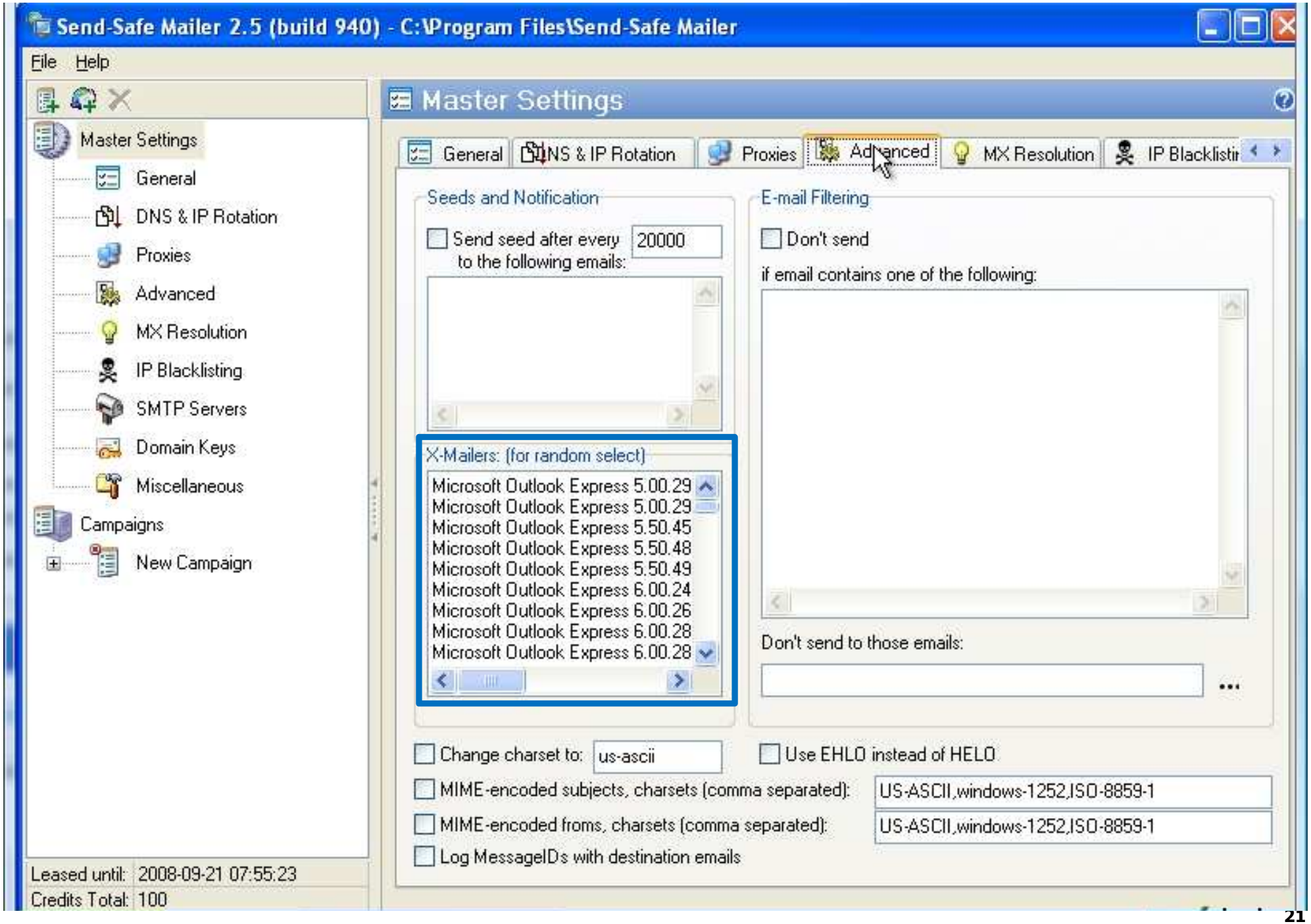


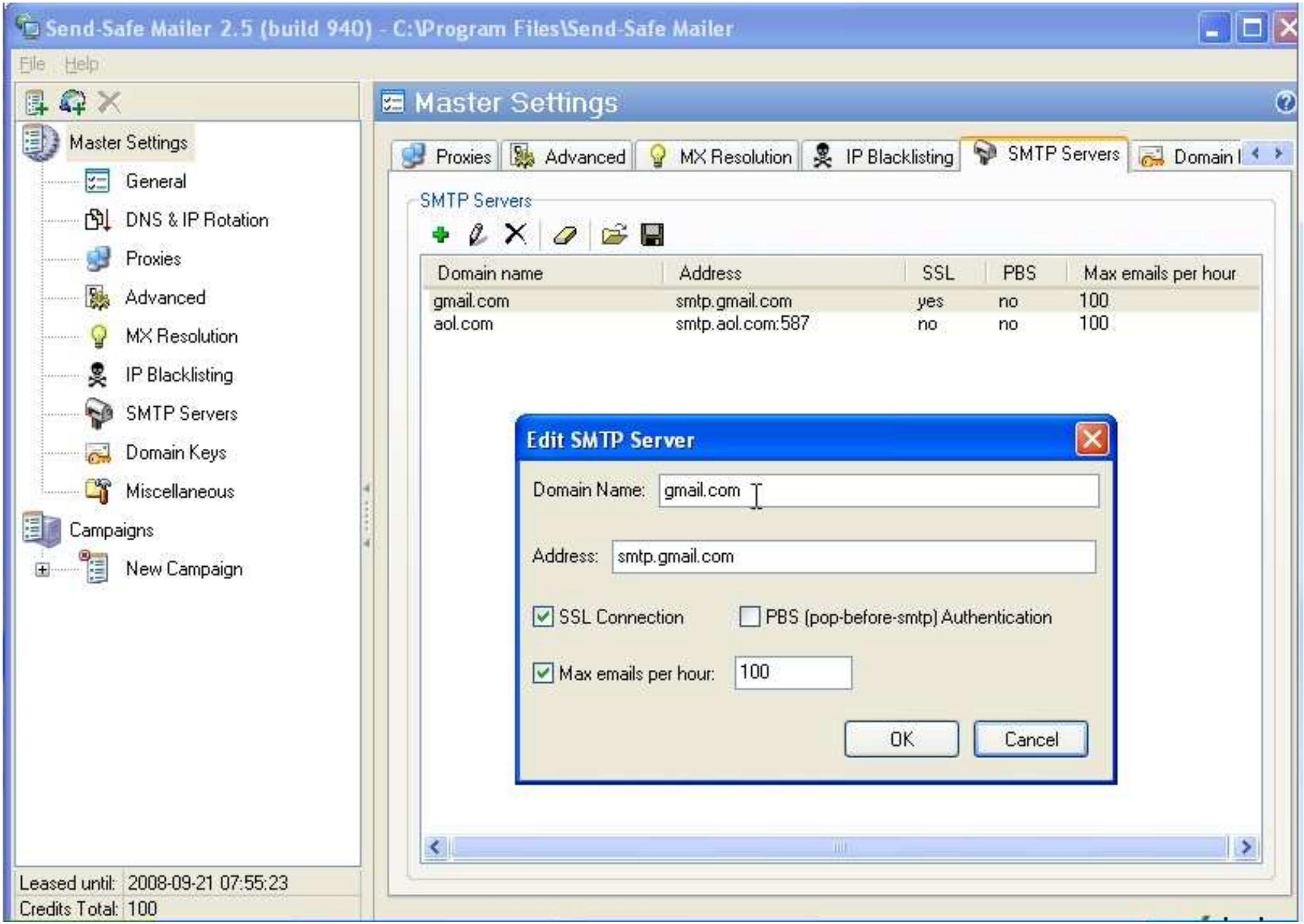


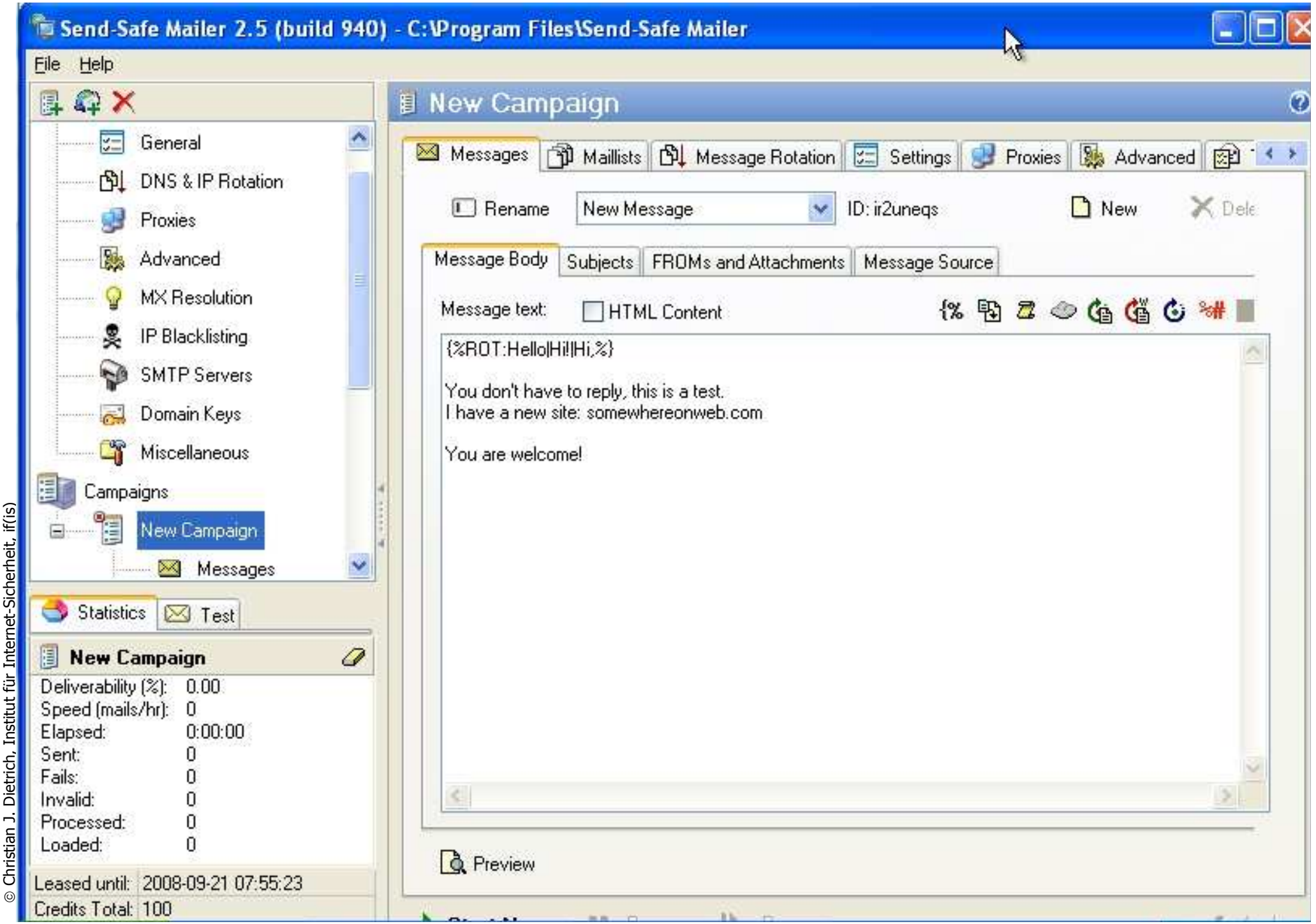


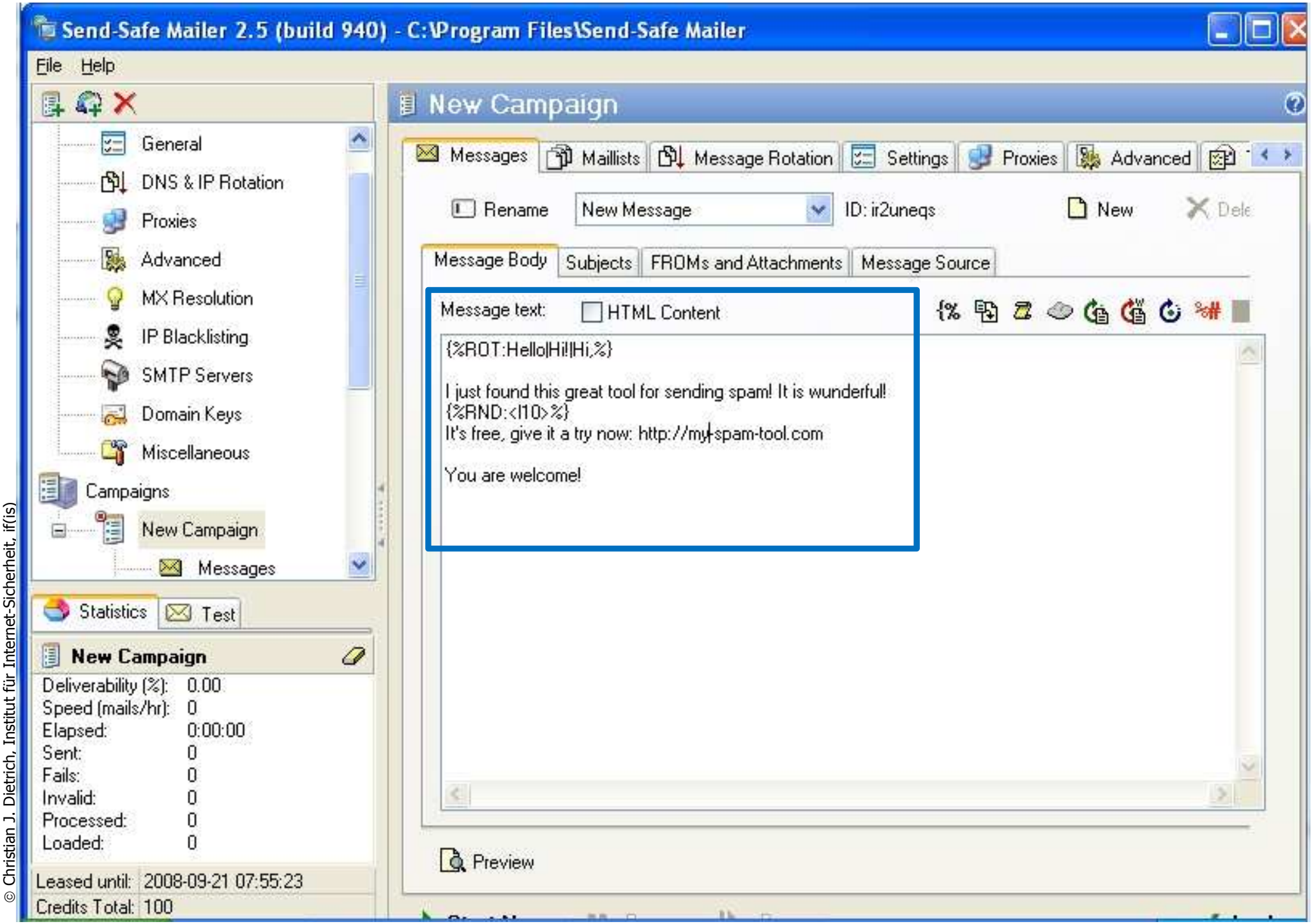


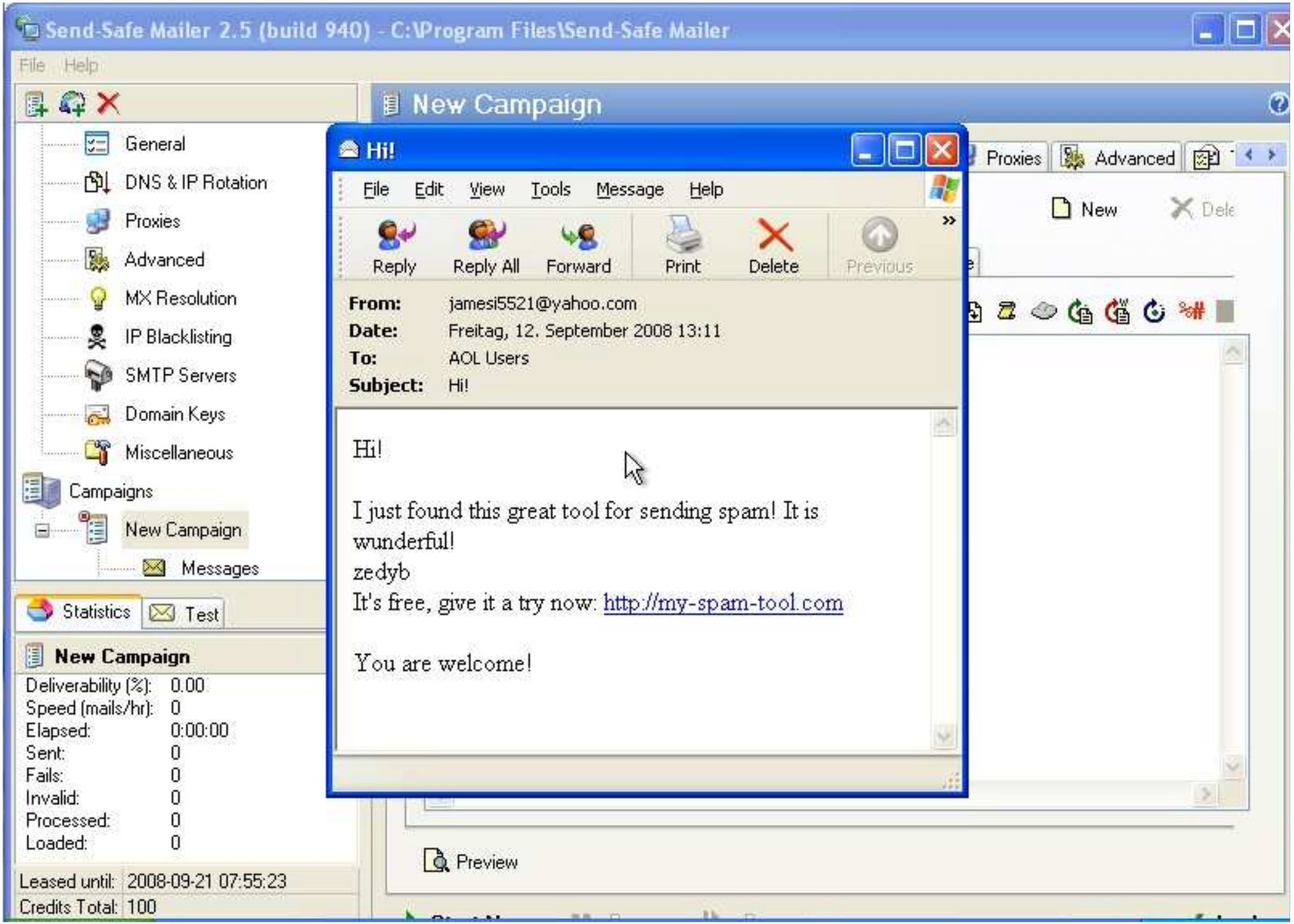


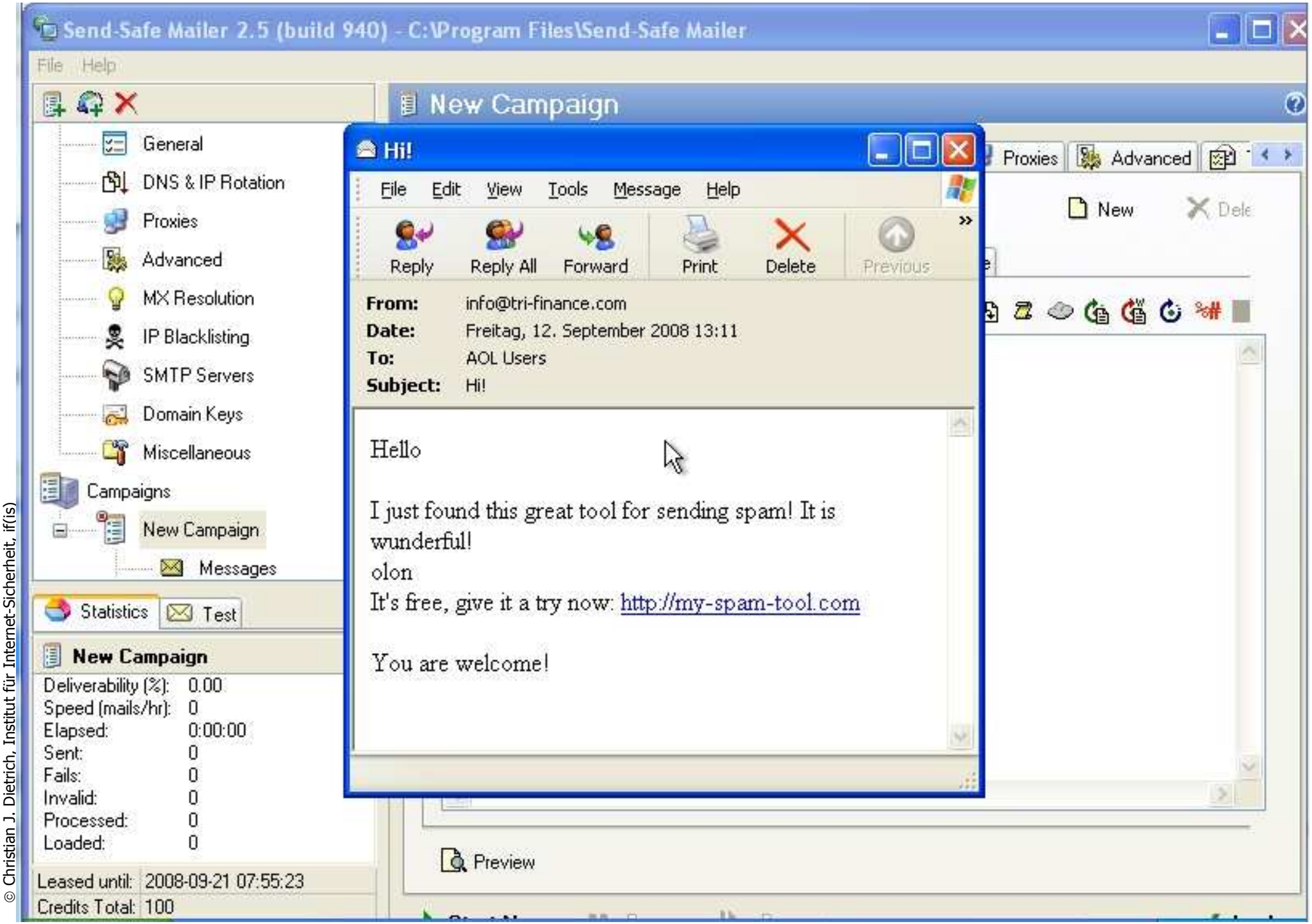


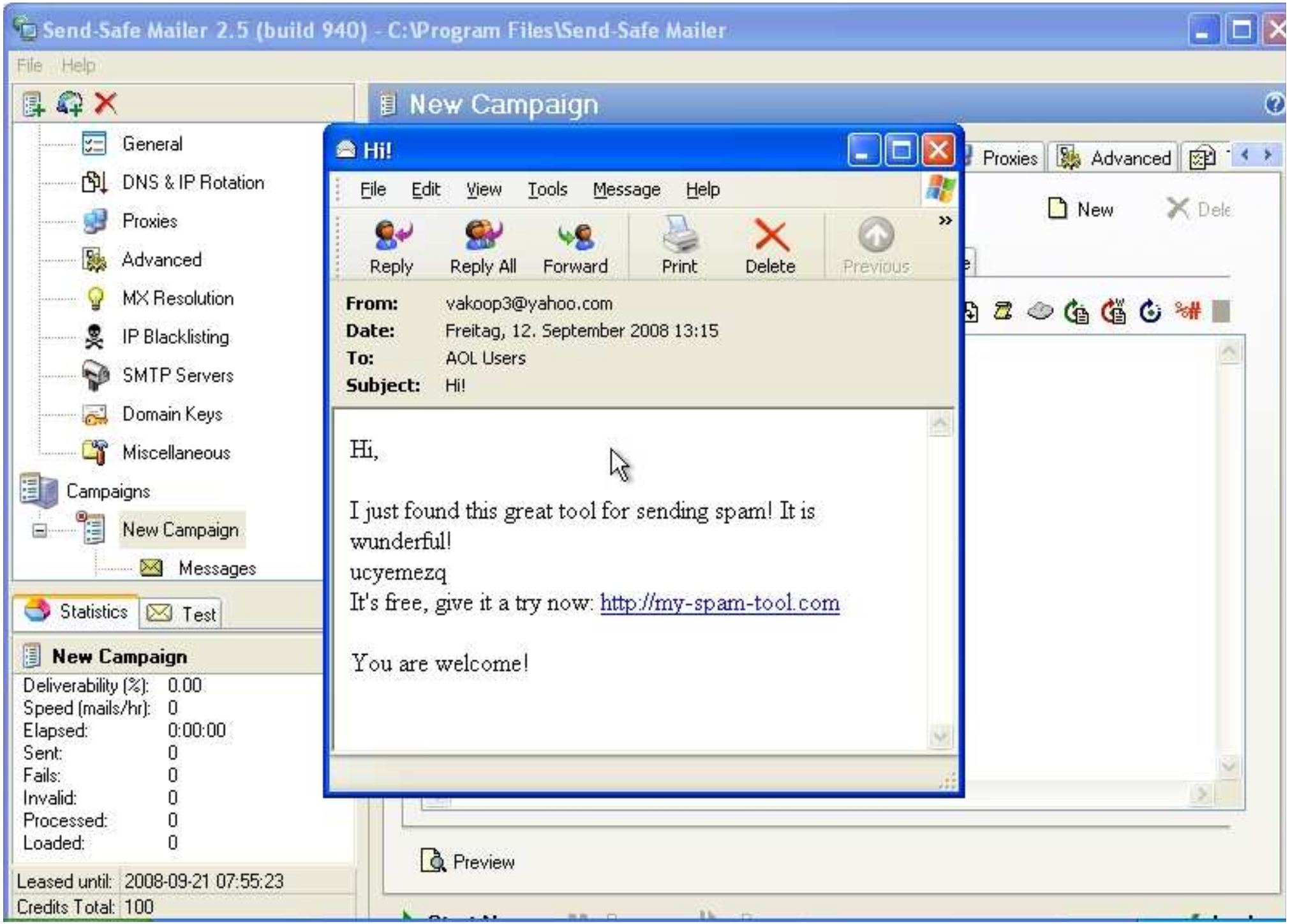


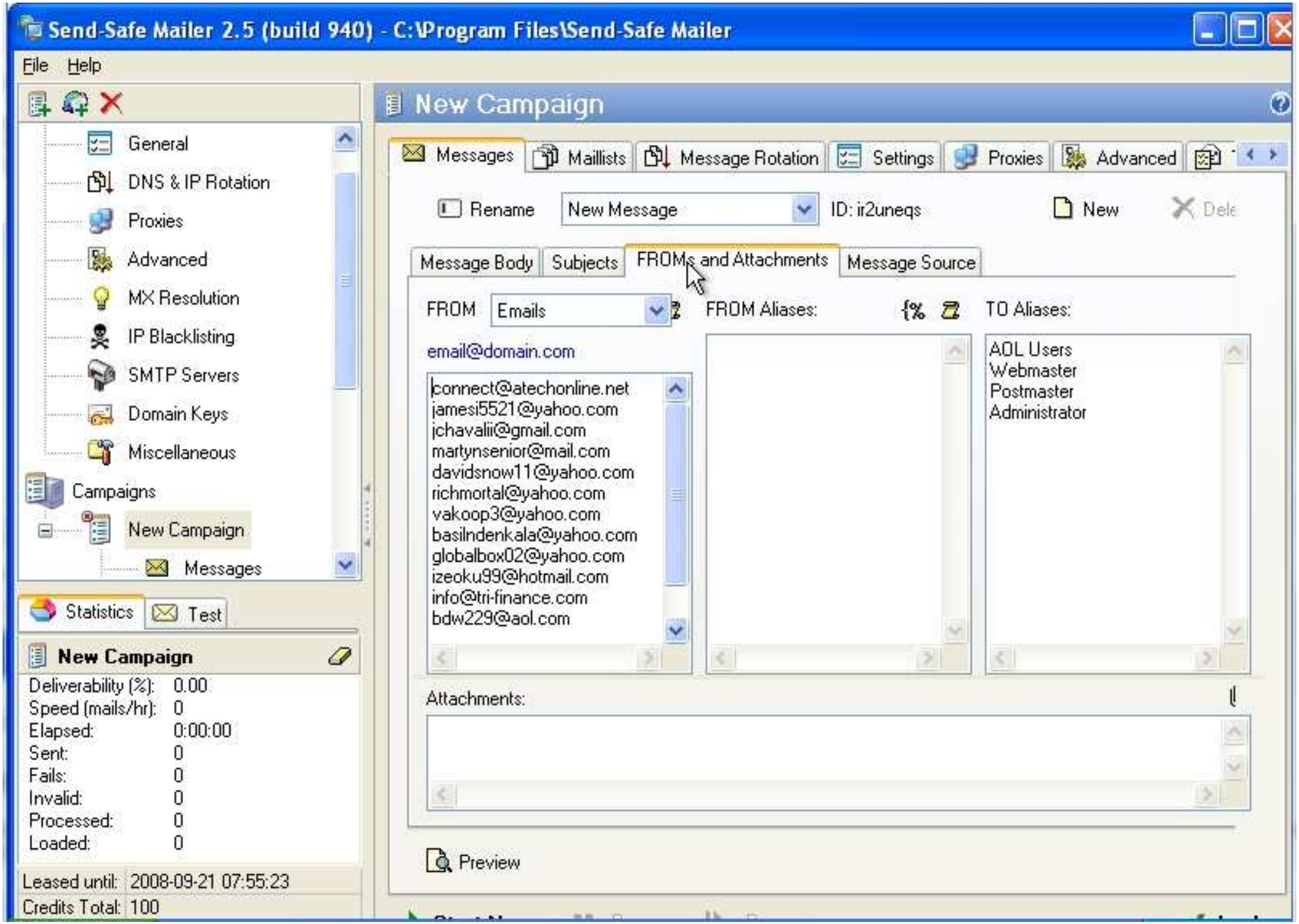


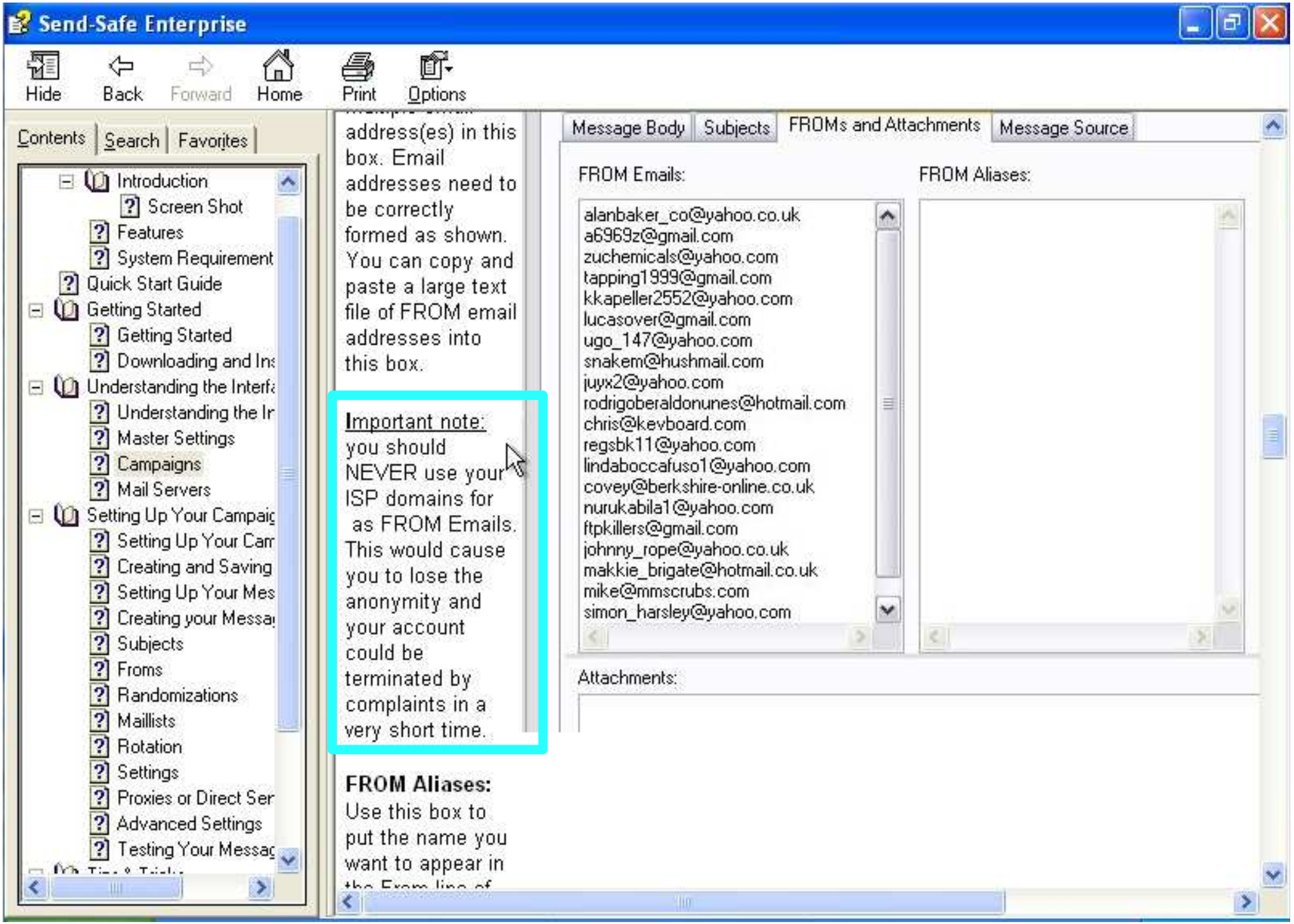


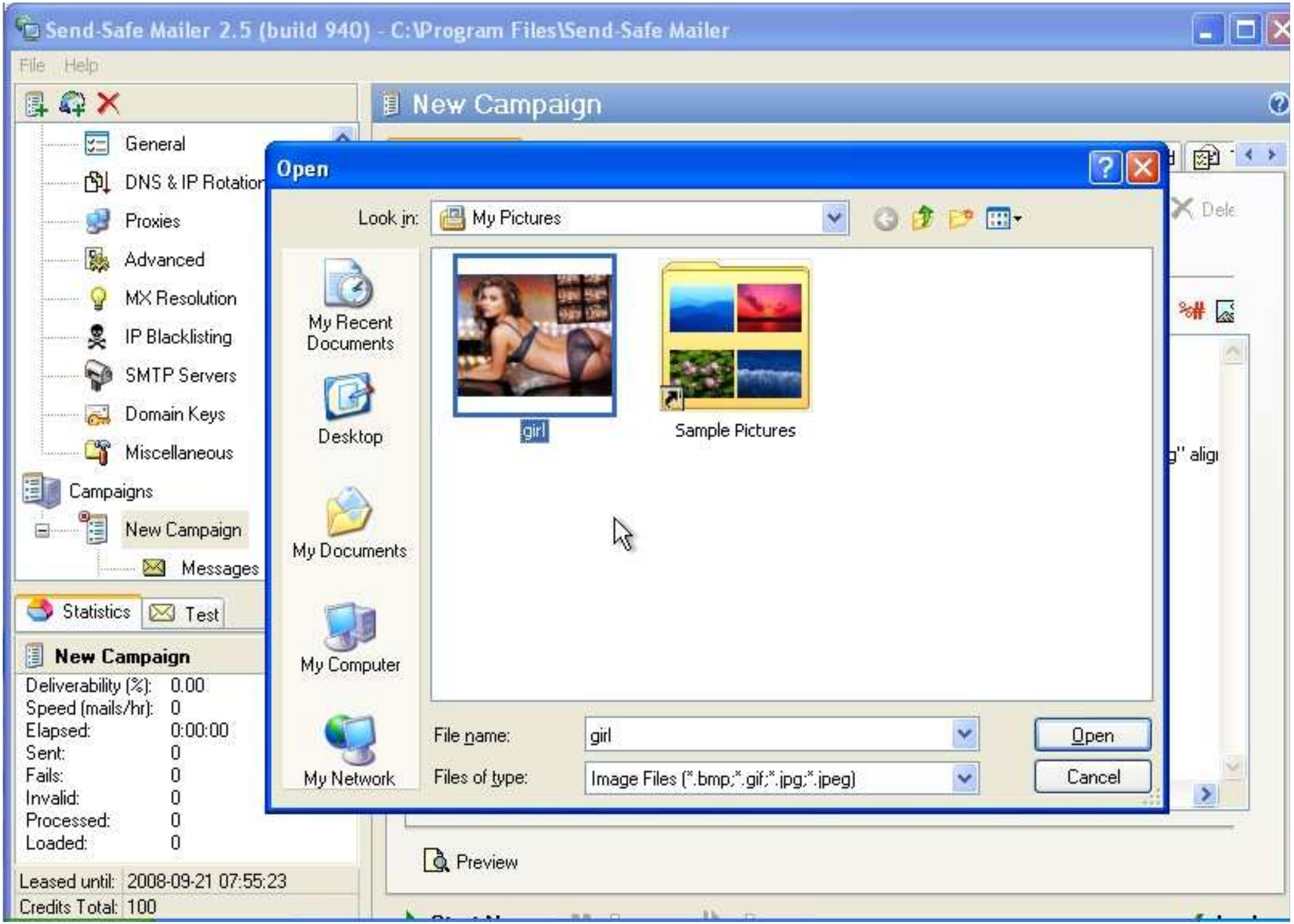


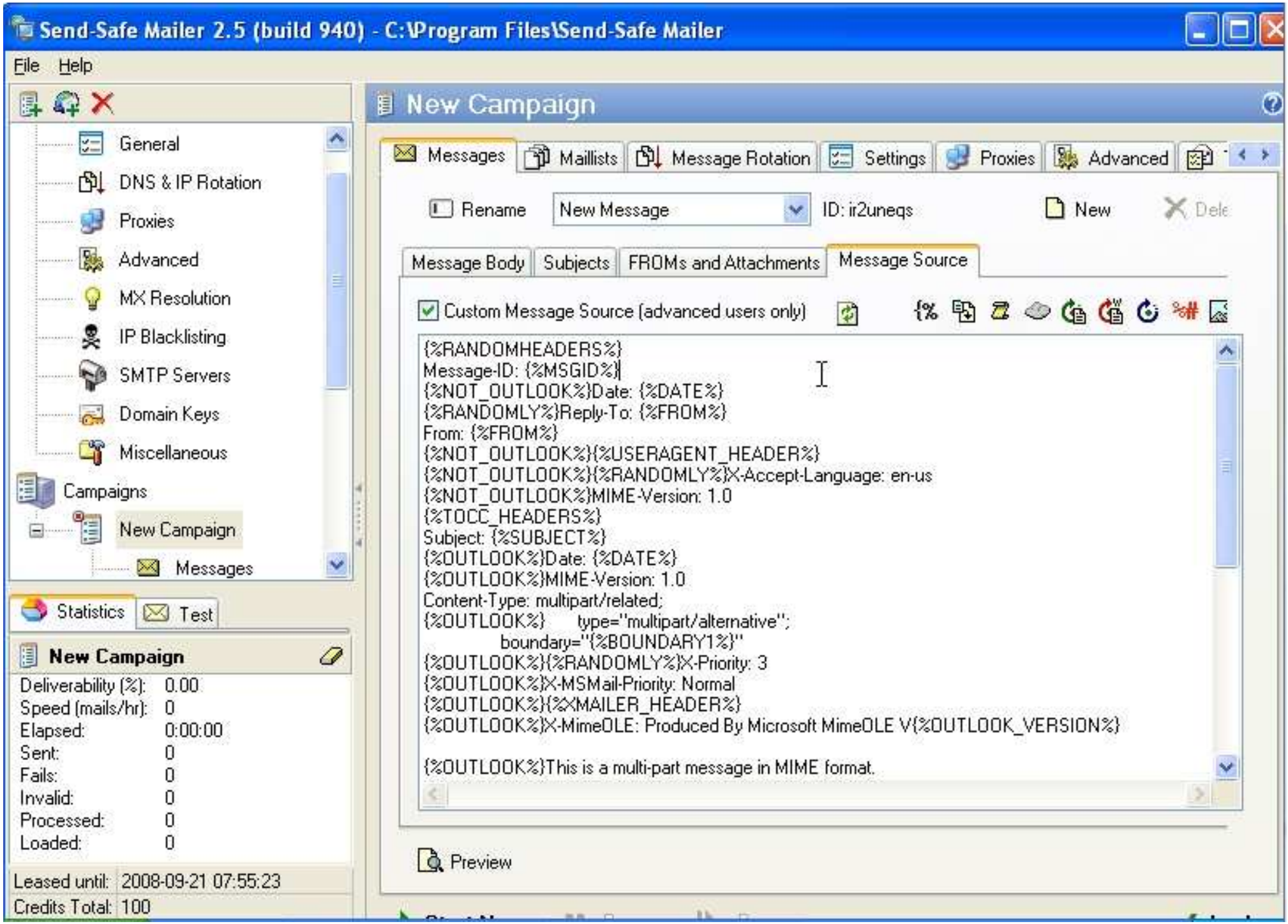


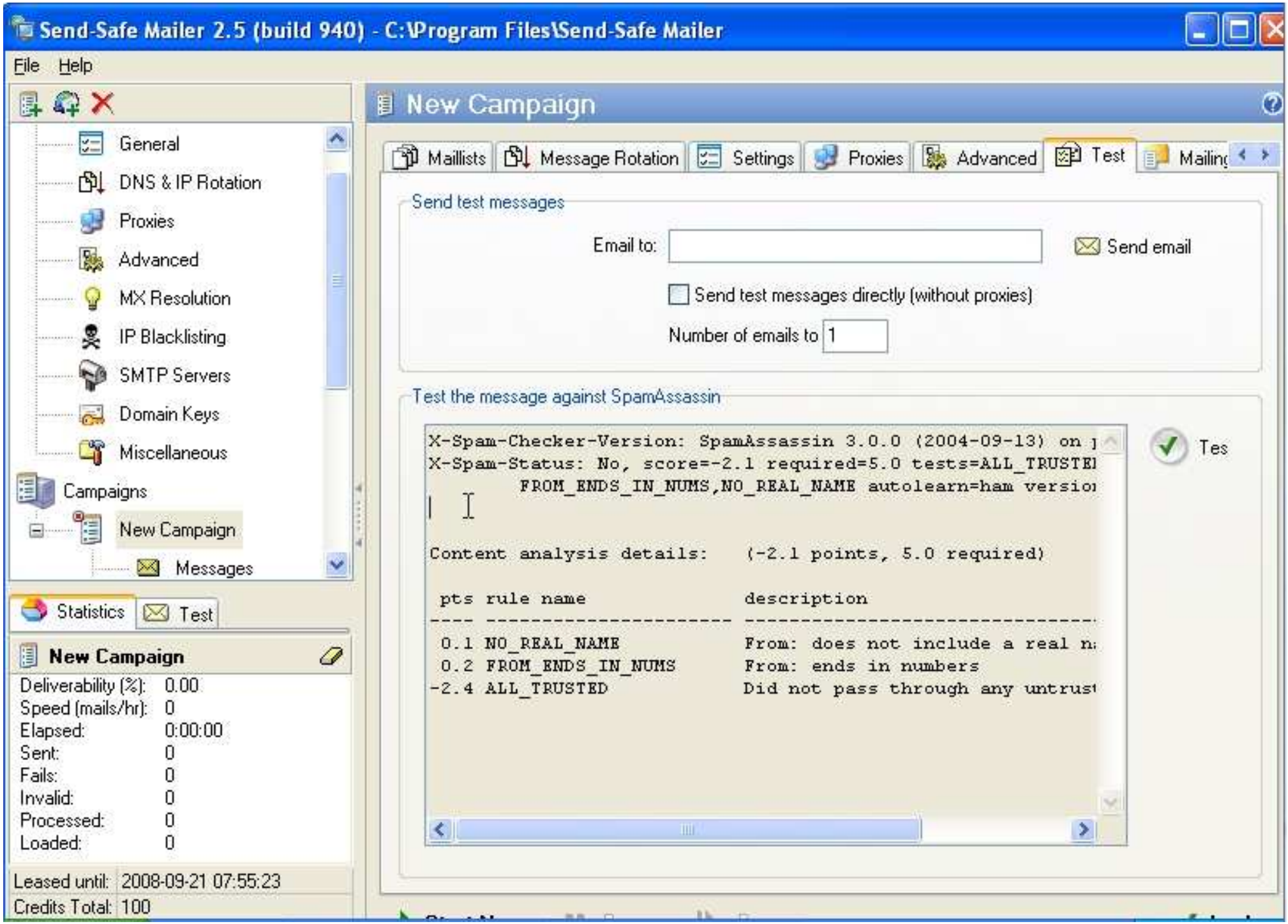












Inhalt

- Einleitung
- Aktuelle Spam-Entwicklung im Detail
- Die Tools der Spammer
  „Make money fast – the spammer‘s way“
- **Fazit**

Fazit

- Spam als (grober) Indikator für Botnetz-Aktivität
- „Professionalisierung“
  - Aufgaben (Captcha-Brechen)
  - Tools (Spamtools)
- Missbrauch legitimer Infrastruktur zum Spam-Versand
- Viel „Kreativität“
- Hybride Kommunikation der Bots (zentral und P2P)

E-Mail Sicherheit – aktuelle Entwicklungen und Trends

Vielen Dank für Ihre Aufmerksamkeit!

Fragen?

Christian J. Dietrich
dietrich [at] internet-sicherheit . de

Institut für Internet-Sicherheit
https://www.internet-sicherheit.de
FH Gelsenkirchen