Zeitschrift: Reihe Kriminologie / Schweizerische Arbeitsgruppe für Kriminologie = Collection criminologie / Groupe suisse de travail de criminologie

Herausgeber: Schweizerische Arbeitsgruppe für Kriminologie

Band: 21 (2003)

Artikel: Internet-Überwachung in der Praxis

Autor: Andres, Herbert

DOI: https://doi.org/10.5169/seals-1051095

HERBERT ANDRES

INTERNET-ÜBERWACHUNG IN DER PRAXIS

Zusammenfassung
Im Spannungsfeld zwischen den Erfordernissen eines wirksamen Datenschutzes und der vermehrten Nutzung des Internets für kriminelle und terroristische Zwecke erfuhr die für eine Internet-Überwachung eingesetzte Technik einen bemerkenswerten Wandel. Neben den Anstrengungen, eine einheitliche Überwachungstechnologie für die Strafverfolgung in verschiedenen Ländern zu realisieren, wird vermehrt an «Wanzen»-ähnlicher Software zur gezielten Überwachung von Personalcomputern geforscht. Während die staatlichen Überwachungssysteme einschliesslich deren Rechtsgrundlagen sich mehrheitlich auf den E-Mail-Verkehr beschränken, zeigen für wenig Geld im freien Markt erhältliche Programme, was technisch möglich wäre. Ein fiktives Fallbeispiel zeigt eine Überwachung des Computers einer Zielperson mittels eines Programms für die unbemerkte Aufzeichnung von E-Mails, besuchten Websites, Tastatureingaben und Bildschirminhalten.

La surveillance de l'Internet en pratique
Dans le cadre d'exigences contradictoires, à savoir celle d'une protection des données efficace et celle de la lutte contre l'utilisation accrue de l'Internet à des fins criminelles et terroristes, la technologie utilisée dans le but de surveiller l'Internet a subi des changements importants. A côté des efforts consentis pour mettre au point une technologie de surveillance uniforme pour les poursuites judiciaires dans différents pays, les recherches portent de plus en plus souvent sur des logiciels semblables à des mini-enregistreurs permettant de surveiller de manière ciblée les ordinateurs personnels. Alors que les systèmes étatiques de surveillance et leur base légale se bornent pour la plupart à traiter de l'échange de messages électroniques, certains programmes, en vente libre et relativement peu chers, nous dévoilent ce qui serait techniquement possible. Un exemple fictif présente la surveillance de l'ordinateur d'une personne cible au moyen d'un programme permettant d'enregistrer en toute discrétion des messages électroniques, les sites Internet consultés, les touches de clavier utilisées, ainsi que le contenu des écrans visualisés.

Im Spannungsfeld zwischen den Erfordernissen eines wirksamen Datenschutzes und der vermehrten Nutzung des Internets für kriminelle und terroristische Zwecke erfuhr die für eine Internet-Überwachung eingesetzte Technik einen bemerkenswerten Wandel. Am

Beispiel des amerikanischen Systems DCS-1000 («Carnivore») und eines frei erhältlichen Programms für die PC-Überwachung sollen nachfolgend die technischen Möglichkeiten von zwei Überwachungssystemen aufgezeigt werden.

DCS-1000 / Carnivore

Das für die Internet-Überwachung eingesetzte amerikanische Carnivore-System wird von der Bundesbehörde FBI als dritte Generation der eingesetzten Überwachungssysteme bezeichnet. Bereits anfangs der Neunzigerjahre setzte das FBI (wie auch die Behörden in anderen Ländern) sogenannte Paket-Analyse-Systeme ein, welche die im Internetverkehr ausgetauschten Datenpakete bei den Internet Service Providern (ISP's) mitlesen und in trivialer Form auswerten konnten. Die meisten Anwendungen stützten sich hierbei auf bereits verfügbare Produkte der technischen Netzwerkanalyse, die den Anforderungen der Ermittler jedoch oft nicht genügen konnten. Zudem wurden die datenschutzrechtlichen Auflagen meist nicht erfüllt. So wurden vielfach unselektiert grosse Datenmengen auf die Überwachungssysteme übertragen, die nichts mit der eigentlichen Zielperson zu tun hatten, was unweigerlich die Persönlichkeitsrechte anderer Internet-Benutzer tangierte.

1997 gab das FBI bekannt, «Omnivore» einzusetzen, ein Überwachungssystem der zweiten Generation. Omnivore wurde gezielt für die Überwachung des E-Mail-Verkehrs eingesetzt. Das System stützte sich dabei ausschliesslich auf die Überwachung der standardisierten, für den E-Mail-Verkehr verwendeten Protokolle und konnte keine E-Mails überwachen, die aus einem Internet-Café beispielsweise mittels Hotmail[1] oder GMX[2] versandt oder empfangen wurden. Auch Omnivore musste in den Rechnerräumen der ISP's instal-

1 http://www.hotmail.com
2 http://www.gmx.de

liert werden und führte oft zu Störungen des Netzwerkverkehrs und in einem Fall zu erheblichem Schaden bei einem Provider. Die Entwicklung von Omnivore wurde 1999 zu Gunsten eines modernen, modular aufgebauten Überwachungssystems eingestellt – der «Dragon Ware Suite». DragonWare sollte den Internetverkehr einer oder mehrerer Zielpersonen möglichst umfassend aufzeichnen. Darunter sollten nicht nur E-Mails, sondern auch transferierte Dateien oder besuchte Webseiten fallen. Teil der zurzeit hauptsächlich in der Terrorismusbekämpfung eingesetzten DragonWare Suite ist die Software «Carnivore», die auf einem Rechner mit Windows 2000-Betriebssystem eingesetzt wird. Carnivore wird über eine «Network Isolation Device»[3] mit dem Netzwerk des Providers verbunden. Selbst wenn es einem Hacker gelingen würde, in das Carnivore-System einzudringen[4], lässt diese Komponente den Abfluss von Daten nicht zu. Die aufgezeichneten Daten werden auf einem Wechseldatenträger gespeichert, der von FBI-Agents periodisch ausgetauscht wird. Carnivore wird als sogenannter «Packet Sniffer» bezeichnet, ein System, das aus dem Internet-Verkehr Datenpakete kopiert, nach bestimmten Vorgaben filtriert, aufzeichnet und für die Ermittler in eine verwertbare Form bringt.

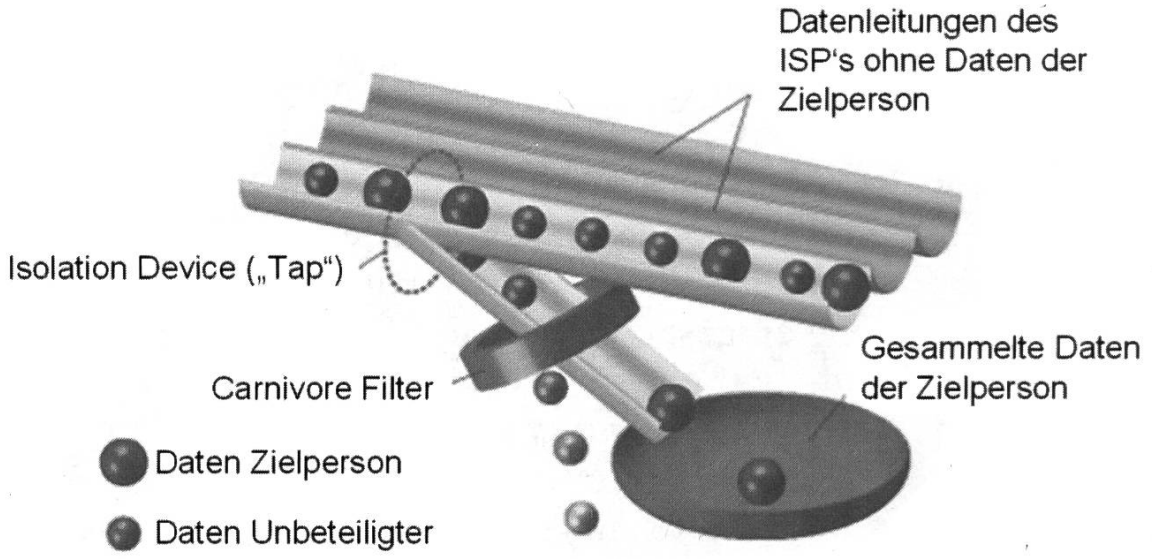
Carnivore wird, nachdem die rechtlichen Voraussetzungen für eine Überwachung erfüllt sind, beim von der Zielperson verwendeten Provider installiert. Bei dieser Installation wird in Zusammenarbeit mit dem Provider ein «Access Point» definiert, an dem möglichst viel Datenpakete der Zielperson und möglichst wenig Datenpakete Unbeteiligter durchfliessen.

---

3 Beispielsweise mittels des Shomiti Taps, der für die Entkopplung der Überwachungssysteme vom Netzwerk des Providers sorgt und Störungen des Netzwerkverkehrs verhindert.

4 Auf Grund fehlender TCP/IP-Stacks des Carnivore-Systems ist ein Eindringen von Hackern via Internet eher unwahrscheinlich. Gegen direkten Zugriff bestehen u.a. mechanische Sicherheitsmerkmale.

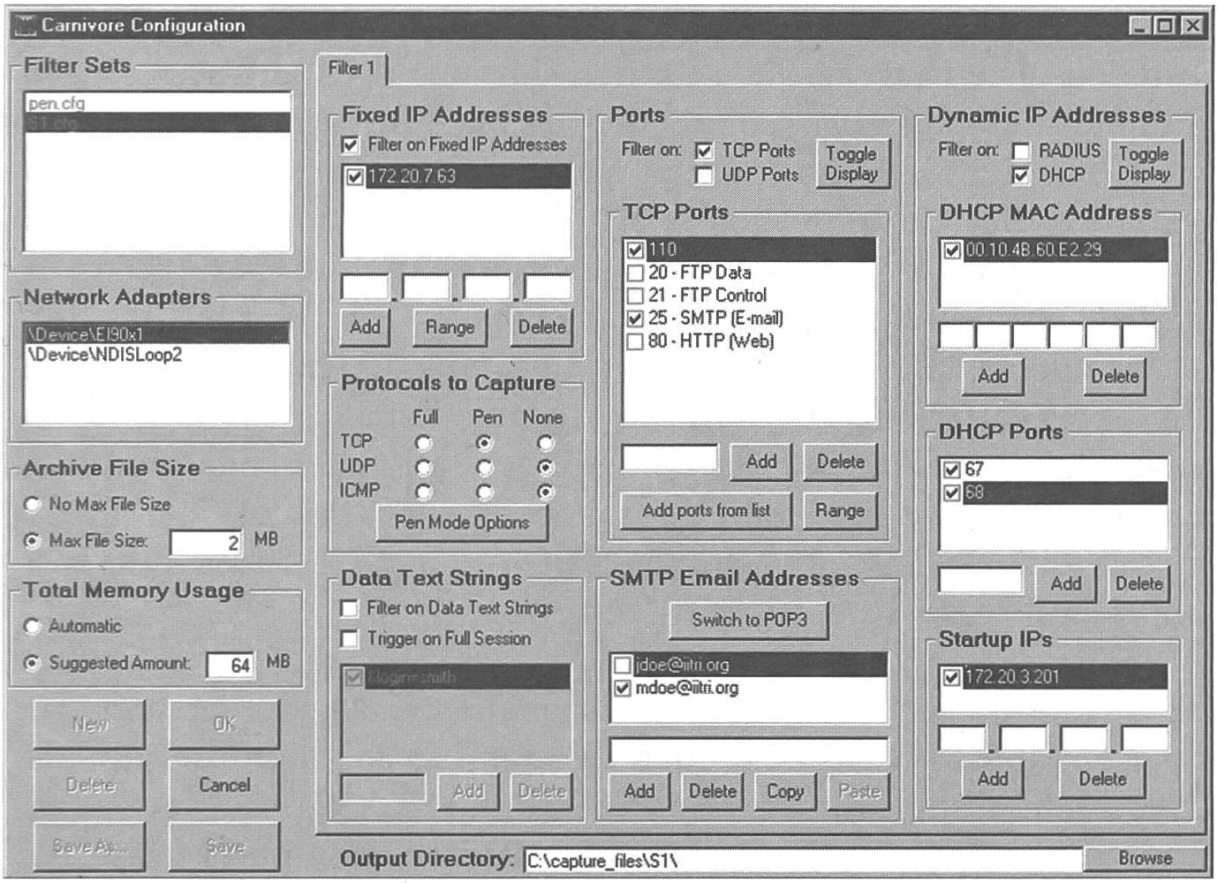
Abbildung 1 Darstellung der Carnivore-Funktion



Die Isolation Device «kopiert» die Datenpakete. Dabei werden auch Datenpakete Unbeteiligter berücksichtigt, die aber innerhalb der Carnivore-Filter verworfen werden, bevor sie den Speicher des Überwachungssystems erreichen.

Bestehen Anhaltspunkte, dass mehrere Provider involviert sind und /oder eine Zielperson beispielsweise von Internet-Cafés aus operiert, ist der Einsatz mehrerer Carnivore-Systeme oder der Einsatz der Systeme an den einzelnen Providern übergeordneten Datenleitungen möglich. Carnivore verfügt aber nicht über eine vergleichbare Kapazität und Rechenleistung, wie dies von global vernetzten Überwachungssystemen bekannt ist. Die Carnivore-Systeme lassen sich offensichtlich aufgrund dieser begrenzten Kapazität von einer überwachten Zielperson mittels der automatisierten Übertragung von sehr grossen und nichtssagenden Datenmengen ausschalten, sofern diese Zielperson von der laufenden Überwachung Kenntnis hat oder diese zumindest vermutet.

Abbildung 2 Bildschirmkopie der FBI Carnivore-Software mit erweiterter Konfiguration (Einstellungen der Parameter für die Überwachungsmassnahme)



Software zur Überwachung eines Personalcomputers

Während grosse Investitionen seitens der Justiz für die Überwachung des Internet-Verkehrs getätigt werden[5], sind für wenig Geld multifunktionale Programme frei erhältlich, die die Überwachung eines Personalcomputers, resp. des mittels des Personalcomputers geführten E-Mail- oder Chat-Verkehrs, der besuchten Websites, der

5 Über die Wirksamkeit der in der Schweiz operativ eingesetzten und auch für die Provider mit hohen Kosten verbundenen Überwachungssysteme bestehen kontroverse Meinungen. Nach Ansicht des Autors sind die Systeme bei entsprechender Fachkenntnis der Täterschaft nahezu wirkungslos. Zusätzlich verunmöglicht die in der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) angesetzte Frist von sechs Monaten für rückwirkende Ermittlungen bei Providern in vielen Fällen die Aufklärung von Straftaten.

kompletten Bildschirminhalte oder generell aller Tastatureingaben ermöglichen. Während der Einsatz dieser Programme rechtlich fragwürdig erscheint, ist eine zunehmende Verbreitung derartiger Überwachungs-Software im privaten Bereich und in Unternehmen festzustellen[6]. Die Beweggründe für den Einsatz der Überwachungsprogramme sind vielfältig – so möchte beispielsweise die Ehepartnerin wissen, ob der Gatte im Internet nach Informationen über die Neugestaltung des Gartens oder per E-Mail ein Treffen mit der Geliebten vereinbart. Auch der Arbeitgeber, der einen Angestellten verdächtigt, während der Arbeitszeit ausnahmslos im Internet zu surfen ist mit einer Überwachungssoftware bestens bedient und kann diesem seine Verfehlungen nachweisen. Sinnvoll mag auch die Überwachung der Internet-Aktivitäten der eigenen Kinder sein. Durchaus denkbar und in einzelnen Fällen bereits verwirklicht ist aber der Einsatz einer PC-Überwachungs-Software auch in Ermittlungsverfahren, sofern die Rechtslage diesen erlaubt.

Im Gegensatz zum vorgängig beschriebenen Carnivore-System oder anderen Überwachungssystemen ist beim Einsatz multifunktionaler Überwachungsprogramme wie «Spector», «STARR», etc. ein physischer Zugang zum zu überwachenden Personalcomputer nötig. Auf diesem ist die Überwachungssoftware zu installieren. Nach der Installation zeichnet die Software sämtliche Computer- und Internet-Aktivitäten auf. Um die aufgezeichneten Resultate der Überwachungssoftware einsehen zu können, ist ebenfalls wieder Zugang zum überwachten Computer nötig. Teilkomponenten der Überwachungssoftware können unter Umständen auch ohne Wissen der Zielperson über eine bestehende Netzwerkverbindung installiert werden.[7]

---

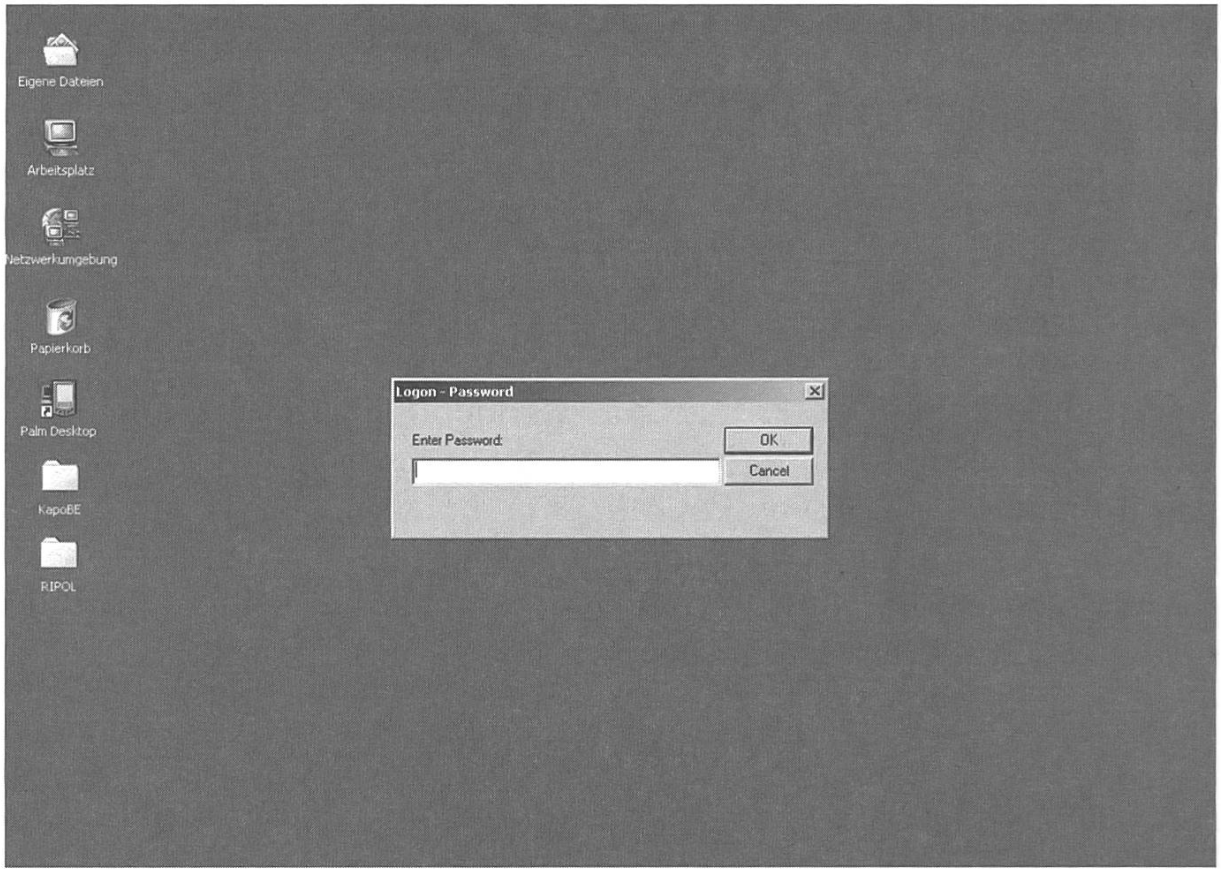
6 Unter http://www.elbtec.de/download/onlinecheck.php4 kann beispielsweise ermittelt werden, ob «Spector» auf einem Personalcomputer installiert ist oder nicht. Ein Versuch mit der aktuellen Version 4.0 Pro von «Spector» misslang – die Installation wurde nicht angezeigt. Der Betreiber der Website stellt jedoch eine zunehmende Anzahl positiver Analysevorgänge fest, was auf eine grössere Verbreitung der Überwachungssoftware schliessen lässt.

7 Eine «verdeckte» Installation ist u.a. unter Ausnutzung von Schwachstellen des auf dem Rechner der Zielperson eingesetzten Betriebssystems möglich.

Ein fiktives Fallbeispiel soll die technische Funktionsweise eines PC-Überwachungsprogramms im Einsatz für die Justiz aufzeigen: Peter W. aus Interlaken, einschlägig vorbestraft, wird dringend verdächtigt, Kinderpornographie herzustellen und im Internet zu verbreiten. Die Überwachung der privaten und geschäftlichen E-Mail-Adresse von Peter W. ist bereits eingeleitet und während rund 14 Tagen in Betrieb. Innerhalb dieses Zeitraums konnten keine sachdienlichen E-Mails ausgewertet werden. Ein Ermittler installiert über das Internet ein Überwachungsprogramm auf dem privaten PC von Peter W. Das Programm wird von aktuellen Schutzmassnahmen wie Virenscannern nicht erkannt,[8] Peter W. benutzt seinen PC weiterhin, ohne die Überwachungssoftware zu bemerken. Sporadisch verbindet sich der Ermittler mit dem PC von Peter W., um die aufgezeichneten Daten der Überwachungssoftware abzurufen. Der Zugang zur Überwachungssoftware ist passwortgeschützt, nur der zuständige Ermittler kann auf den PC der Zielperson zugreifen.

8 Die Umgehung von Schutzmassnahmen kann u.a. mittels der Kommunikation über «Well Known Ports» erreicht werden, über die beispielsweise auch Webseiten betrachtet werden.

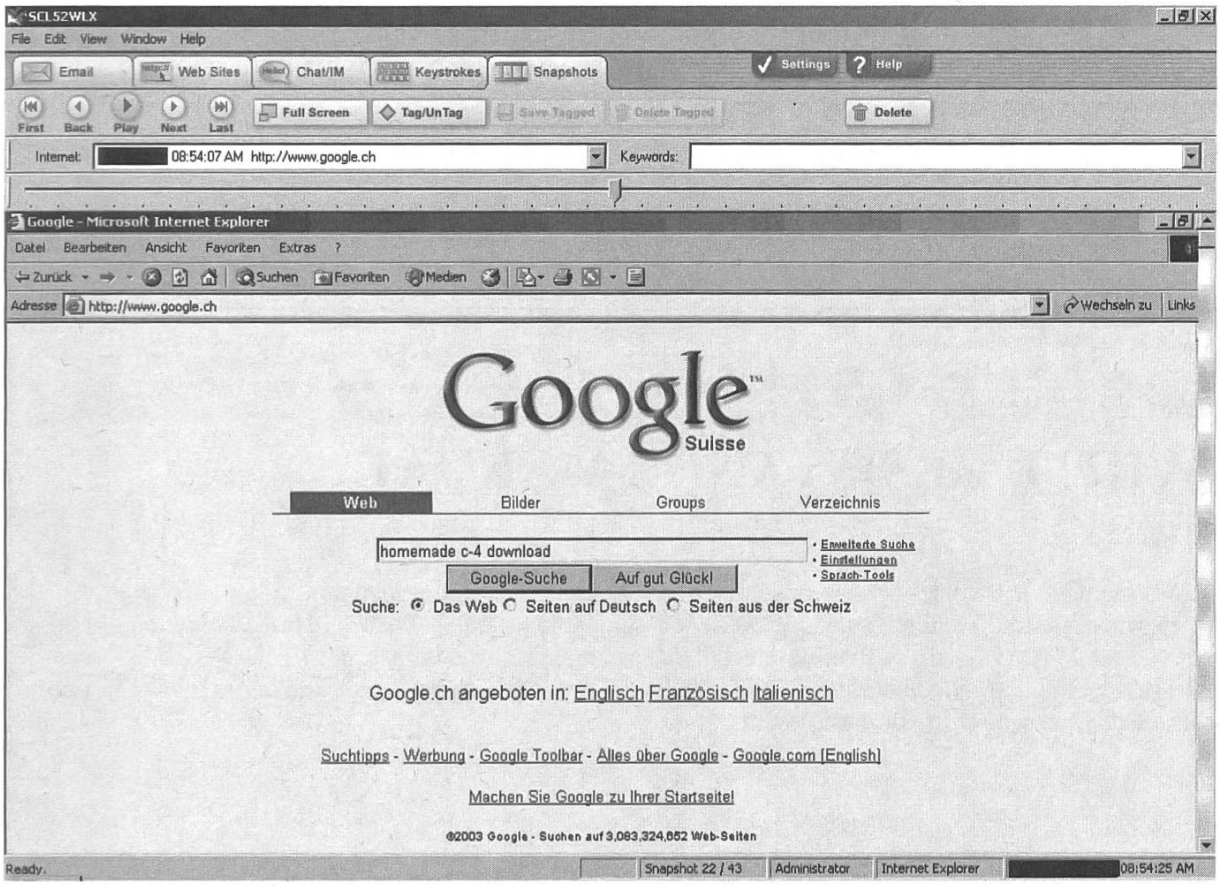
Abbildung 3 Verbindungsaufnahme vom Ermittler-PC mit dem PC der Zielperson



Die Überwachungssoftware auf dem PC der Zielperson verlangt ein Passwort zur Identifikation des Ermittlers.

Nach der Eingabe des korrekten Passworts erscheint die Benutzeroberfläche der Überwachungssoftware, die dem Ermittler Einblick in versandte und empfangene E-Mails, besuchte Webseiten, Chats, sämtliche Tastatureingaben und eine grosse Anzahl von Bildschirmkopien gewährt, die während der Überwachung automatisiert und in Zeitabständen von einigen Sekunden abgespeichert wurden.

Abbildung 4 Einblick in die überwachten Bildschirminhalte der Zielperson



Darstellung einer Eingabe in die Suchmaschine «Google» mit den Suchbegriffen «homemade», «C-4» und «download».

Abbildung 5 Darstellung einer vom überwachten PC aus besuchten Website mit dem «White Resistance Manual», welches u.a. Anleitungen zur Herstellung von Sprengstoffen und einfachen Schusswaffen enthält

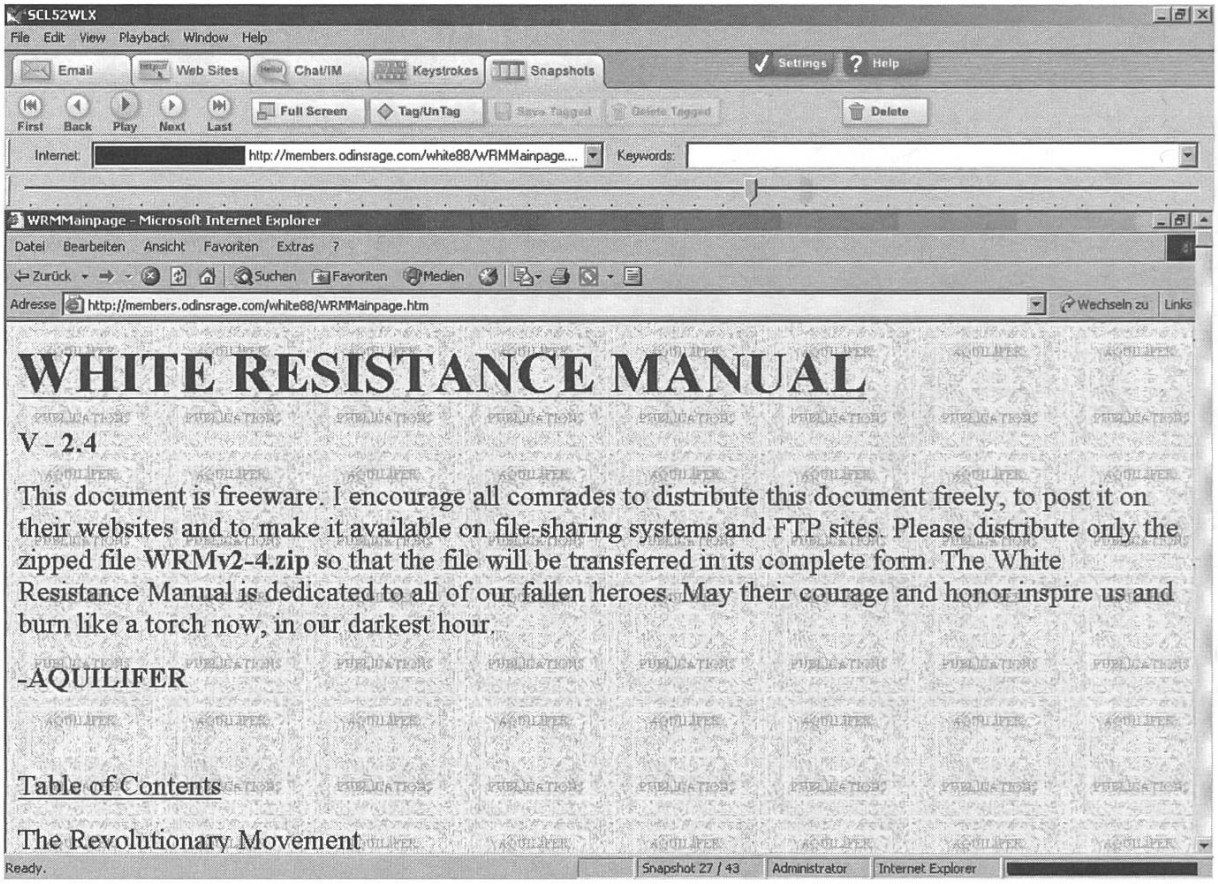


Abbildung 6 Aufgezeichnete Bildschirmkopie mit empfangenem E-Mail, in welchem die Bestellung einer «Sprengkapsel N54» bestätigt wird.

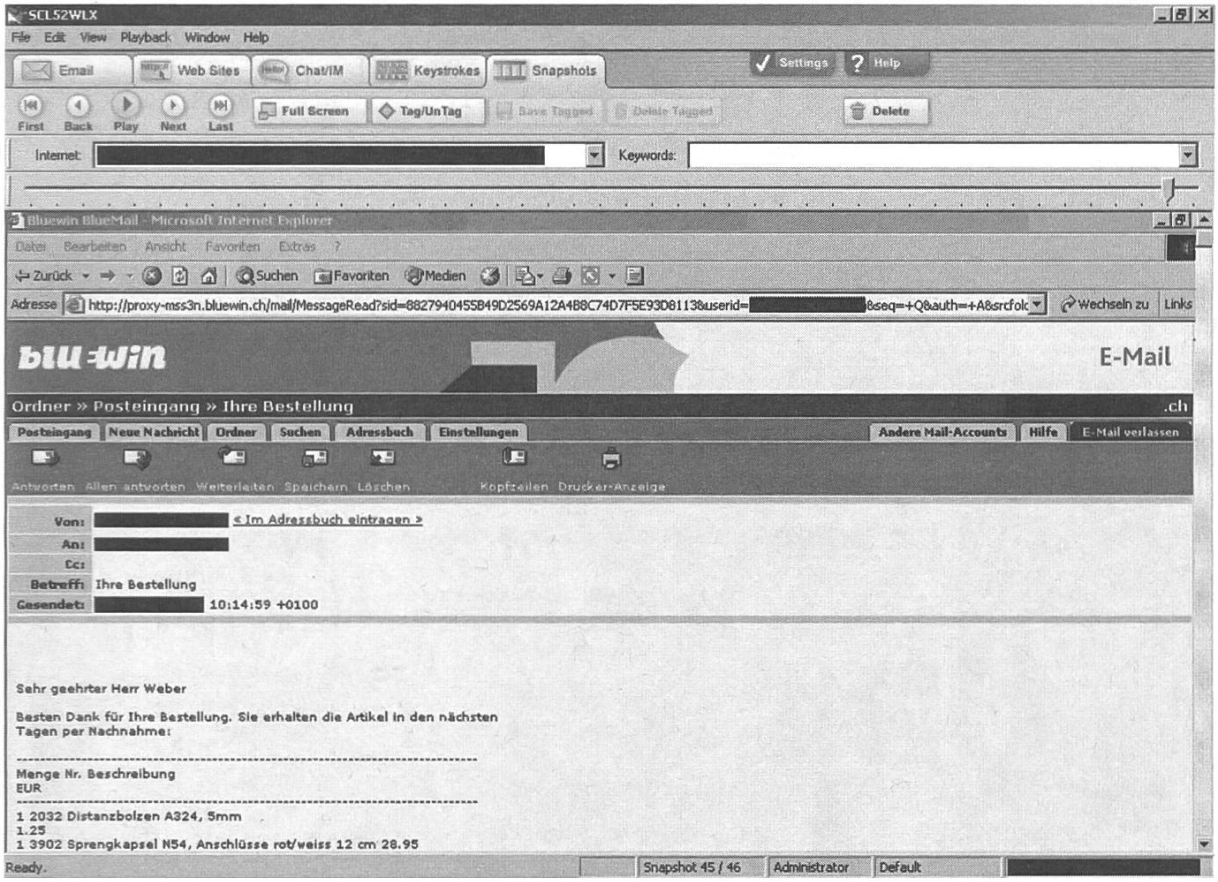


Abbildung 7 Aufgezeichnete Bildschirmkopie mit Internet-Website, auf der das Buch «Homemade C-4» (Anleitung zur Herstellung eines Sprengstoffs) bestellt werden kann.

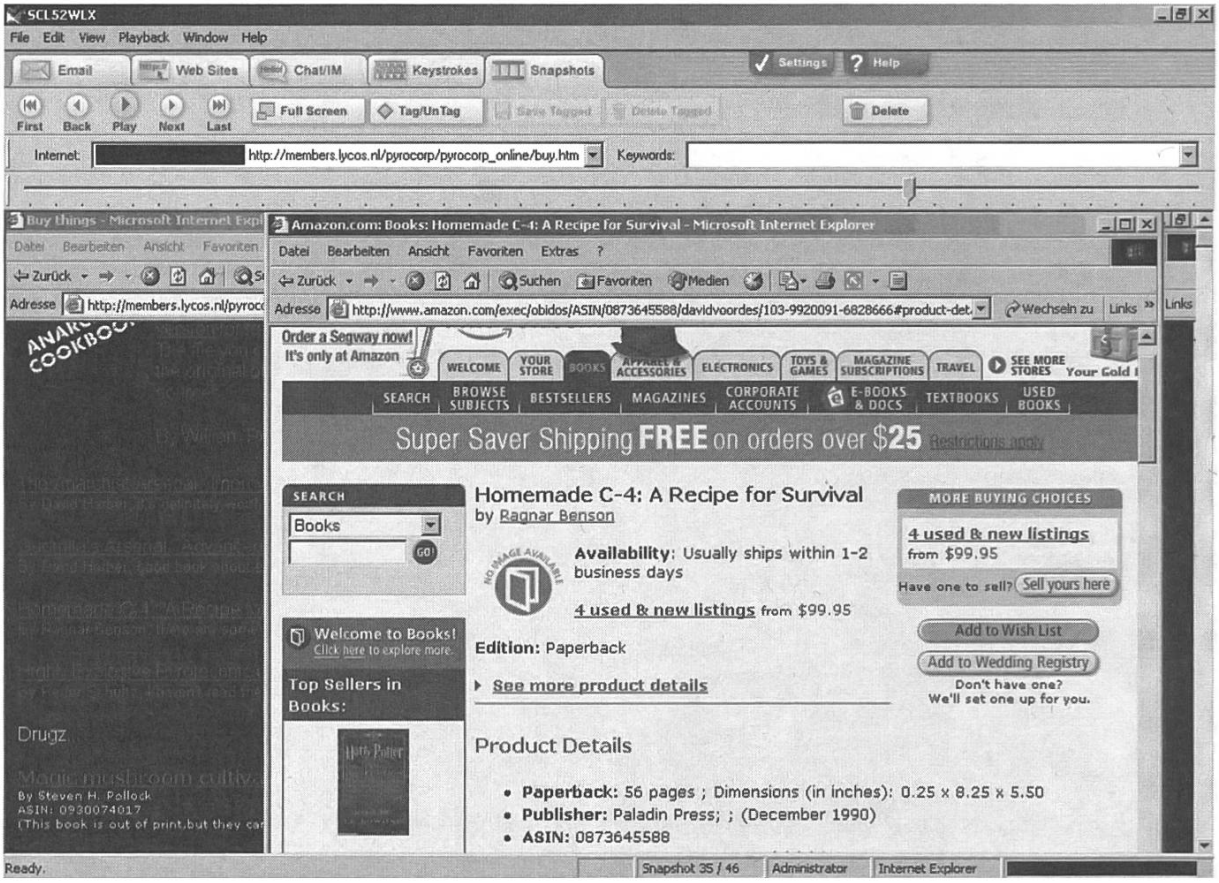
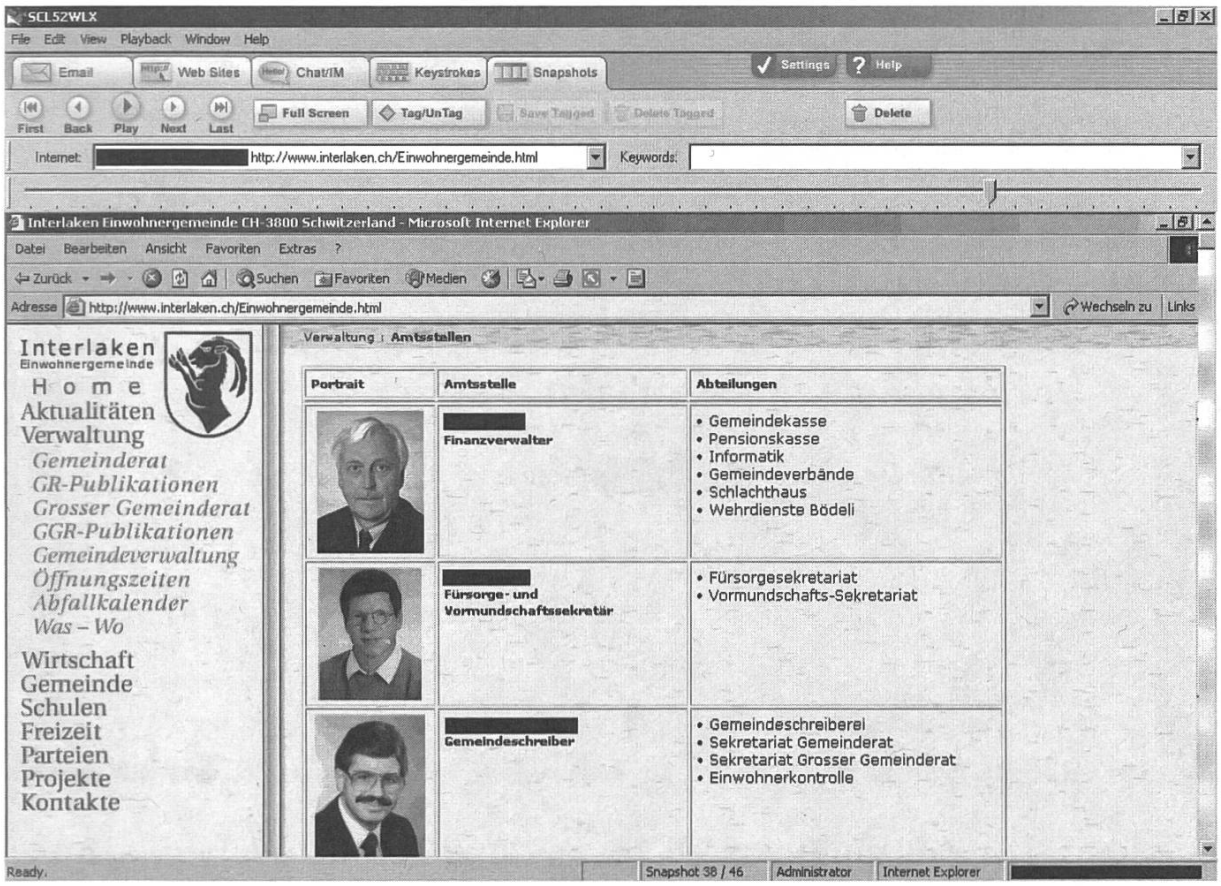
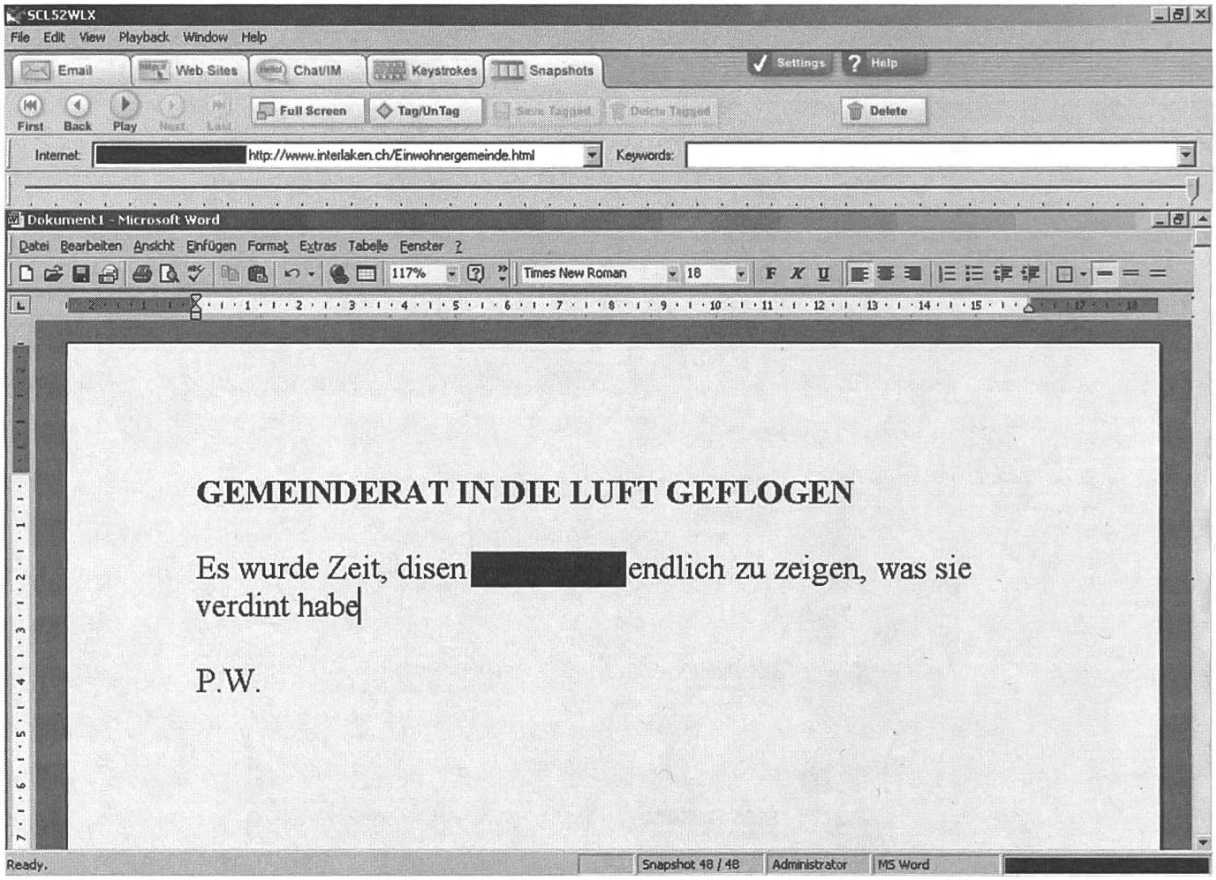


Abbildung 8 Aufgezeichnete Bildschirmkopie der Überwachungssoftware mit besuchter Internet-Website, auf der Mitglieder der Gemeindeverwaltung Interlaken vorgestellt werden.



Die angefertigten Bildschirmkopien des überwachten PC's erlauben dem Ermittler auch Einblick in bearbeitete Dokumente. So kann beispielsweise die Entstehung eines Textdokuments mitverfolgt werden, welches vermutlich als Bekennerschreiben dienen soll:

Abbildung 9 Aufgezeichnete Bildschirmkopie der Überwachungssoftware mit Textverarbeitungsdokument.



Die über den Zeitraum von 30 Tagen durchgeführte Überwachung des Personalcomputers von Peter W. zeigte der Polizei, dass dieser vom Vorwurf der Herstellung von Kinderpornographie vermutlich entlastet wird, dass jedoch umgehend eine Hausdurchsuchung wegen eines geplanten Attentats auf Mitglieder des Gemeinderats von Interlaken durchzuführen ist.

Das fiktive Beispiel «Peter W.» zeigt eine Variante der verfügbaren Überwachungstechnologie, deren Einsatz rechtlich sicher nicht unproblematisch ist. Erste Erfahrungen mit vergleichbaren Systemen zeigten aber, dass innert kurzer Zeit und mit wenig Aufwand sowohl belastende wie auch entlastende Indizien in Ermittlungsverfahren gesammelt werden konnten. Oftmals hätten diese Erkenntnisse mit-

tels herkömmlicher Überwachung[9] des E-Mail-Verkehrs nicht gewonnen werden können.

Blick in die Zukunft

Es ist davon auszugehen, dass erfolgreiche Internet-Überwachungsaktionen zukünftig möglichst direkt an den Informatikmitteln der Zielpersonen anzusetzen sind, sofern keine intelligente und leistungsfähige Überwachung der übertragenen Datenpakete zur Verfügung steht. Überwachungseinrichtungen, die auf Protokollen der Server inländischer Provider basieren, sind wertlos, wenn beispielsweise im E-Mailverkehr von einer Täterschaft ausländische Dienstanbieter benutzt werden oder der Versand von E-Mails über ungeschützte Mailserver Unbeteiligter im fernen Ausland erfolgt. Anpassungen der Überwachungsgesetzgebung an die niemals statisch zu erfassende, rasante technische Entwicklung und vor allem die Ausdehnung geltender Fristen sind daher zu begrüssen.

9 Insbesondere versagen herkömmliche Überwachungssysteme (auch Carnivore) bei verschlüsselten E-Mails, weshalb das FBI innerhalb des Projekts «Magic Lantern» den Ansatz des Direktzugriffs auf den Personalcomputer einer Zielperson verfolgt. S. hierzu auch http://usgovinfo.about.com/library/weekly/aa121401a.htm