3. IT-Forensik Workshop an der FH Aachen

Vortrag "Anti-Anti-Forensik"

Martin Wundram, Hendrik Adam
{wundram|adam}@digitrace.de

Bildquelle: mpavlov / Clipdealer

Agenda

I. Was ist Anti-Forensik?

II. Beispiele für Anti-Forensik

III. Kategorisierung von Maßnahmen der Anti-Forensik

IV. Anti-Anti-Forensik: Was können wir tun?

V. Lessons learned

VI. Fragen?

Begrüßung

Über uns

- Schwerpunkte: IT-Sicherheit und IT-Forensik

DigiTrace
Kompetenz in IT-Forensik

- Martin Wundram: *Von der IHK zu Köln öffentlich bestellter und vereidigter Sachverständiger für Systeme und Anwendungen der Informationsverarbeitung*

TG TRONICGUARD

- Hendrik Adam: *Seit 2013 im Team von DigiTrace und TronicGuard, forscht und arbeitet im Bereich IT-Forensik*
- Gleichermaßen Aufträge von Polizei/StA/Gerichten, Unternehmen und Privatpersonen
- Weitere Infos: www.tronicguard.com und www.digitrace.de

Begrüßung

Motivation des Themenkomplexes "Anti-Forensik"

- Wie wäre es, IT-Sicherheit und IT-Forensik zu kombinieren? Die eigenen Werkzeuge der IT-Forensik Stresstests und Angriffen unterziehen?
- Sind diese Werkzeuge so robust und zuverlässig, wie wir es erwarten?
- Erster Vortrag 2011 beim 28C3 in Berlin (Chaos Communication Congress des Chaos Computer Club)
- Bereits existierende Forschungsarbeiten (zwei Beispiele):
    - *“Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem“*, Ryan Harris, 2006
    - *„Counter Forensics“*, Noemi Kuncik und Andy Harbison, Digital Forensics Magazine, 2010
        - Data Destruction, File Deletion, Re-Formatting, Defragmentation

Was ist Anti-Forensik?

Storytelling

Was ist Anti-Forensik?

Storytelling – Fazit dieser Geschichte

- Eigentlich nicht neu: IT-Forensik bedient sich komplexer Techniken, um oft enorm umfangreiche Datenbestände auf oft viele Sachverhalte zu untersuchen.
    - Forensik-Software ist oft komplex und arbeitet selten fehlerfrei
    - “Viele Kurven, aus denen man fliegen kann.“
- Eigentlich auch nicht neu: Anti-Forensik ist bereits mit einfachsten Maßnahmen möglich
- Anti-Anti-Forensik war hier zwar nicht einfach, aber mit Bordmitteln möglich (intensive Suche nach gelöschten Daten, + Auffälligkeiten in Zeitstempeln und Dateinamen). Leicht hätte man die entscheidenden Hinweise übersehen können
- Im vorliegenden Fall hätte eine „sichere“ Datenlöschung möglicherweise eine Aufklärung des Falls verhindert

Was ist Anti-Forensik?

Storytelling

Bildquelle: treenabeena - Fotolia.com

Was ist Anti-Forensik?

Storytelling – Fazit dieser Geschichte

- IT-Forensik-Software hat maßgeblichen Anteil an der Gewinnung und Beurteilung von Erkenntnissen über Sachverhalte
- Als IT-Forensiker könnte man dazu verleitet sein, Ergebnissen ungeprüft zu vertrauen und technische Hintergründe außer Acht zu lassen
- Die Korrektheitsanforderungen an IT-Forensik-Software sind daher besonders hoch
- Letztlich Gefahr, dass Einrede wegen grundsätzlicher und kaum zu entkräftender Bedenken erhoben wird. Selbst wenn dies im konkreten Fall gar nicht zutrifft.

Was ist Anti-Forensik?

Definition

- ***Jeder Kompromittierungsversuch zur Reduktion der Verfügbarkeit oder Nützlichkeit von Beweisen für den IT-forensischen Auswerteprozess***
  (angelehnt an Definition von Ryan Harris)

- Es gibt im Wesentlichen Maßnahmen der **Datenvermeidung** und **Datenverschleierung/Datenvernichtung** (können unbemerkt und unbemerkbar bleiben) und **aktive Angriffe** (können und führen oft zu erkennbaren Unregelmäßigkeiten)
- In diesem Vortrag: Fokus auf Angriffe gegen Werkzeuge der IT-Forensik

Was ist Anti-Forensik?

Angriffspunkte im IT-Forensik-Prozess

- **Vereinfachte Prozesssicht:**
  - **Identifizierung → Sicherstellung → Analyse → Präsentation**

- Mögliche Zielressourcen:
  - Beweismittel
  - Werkzeuge
  - Forensiker

Was ist Anti-Forensik?

Angriffspunkte im IT-Forensik-Prozess

- Einige Motivationsfragen aus Sicht der IT-Forensiker:
  - Ist jeder Handlungsschritt dokumentiert und nachvollziehbar?
  - Kennt die Gegenseite sich in einem Teilgebiet besser aus als wir?
  - Wurde etwas unverdächtig Erscheinendes nicht weiter untersucht?
  - Haben Zeitdruck und übereiltes Arbeiten ein gründliches Vorgehen verhindert? War man abgelenkt?
  - War das Auswertesystem mit dem Internet oder internen Netz verbunden?
  - Hat man sich auf nur ein Werkzeug verlassen?
  - **SOLL <!-> IST**

Was ist Anti-Forensik?

Wann und warum kommt Anti-Forensik zum Einsatz?

- Wenn der Verdacht oder die Vermutung besteht, dass relevante Systeme zukünftig einer IT-forensischen Auswertung unterzogen werden:
  - Cracker verwischt Einbruchsspuren
  - Downloader verwischt Downloadspuren
  - Registry-Cleaner und Disk-Wiper um Spuren der Erstellung z.B. einer gefälschten Rechnung zu beseitigen
  - Person verschlüsselt alle persönlichen Daten
  - Das ist wohlbekannt
  - **Neu sind**: Direkte Angriffe gegen Werkzeuge der IT-Forensik
    - Wann werden solche Maßnahmen der Anti-Forensik aktiv? → Wenn der “Spürhund angeschlagen hat“

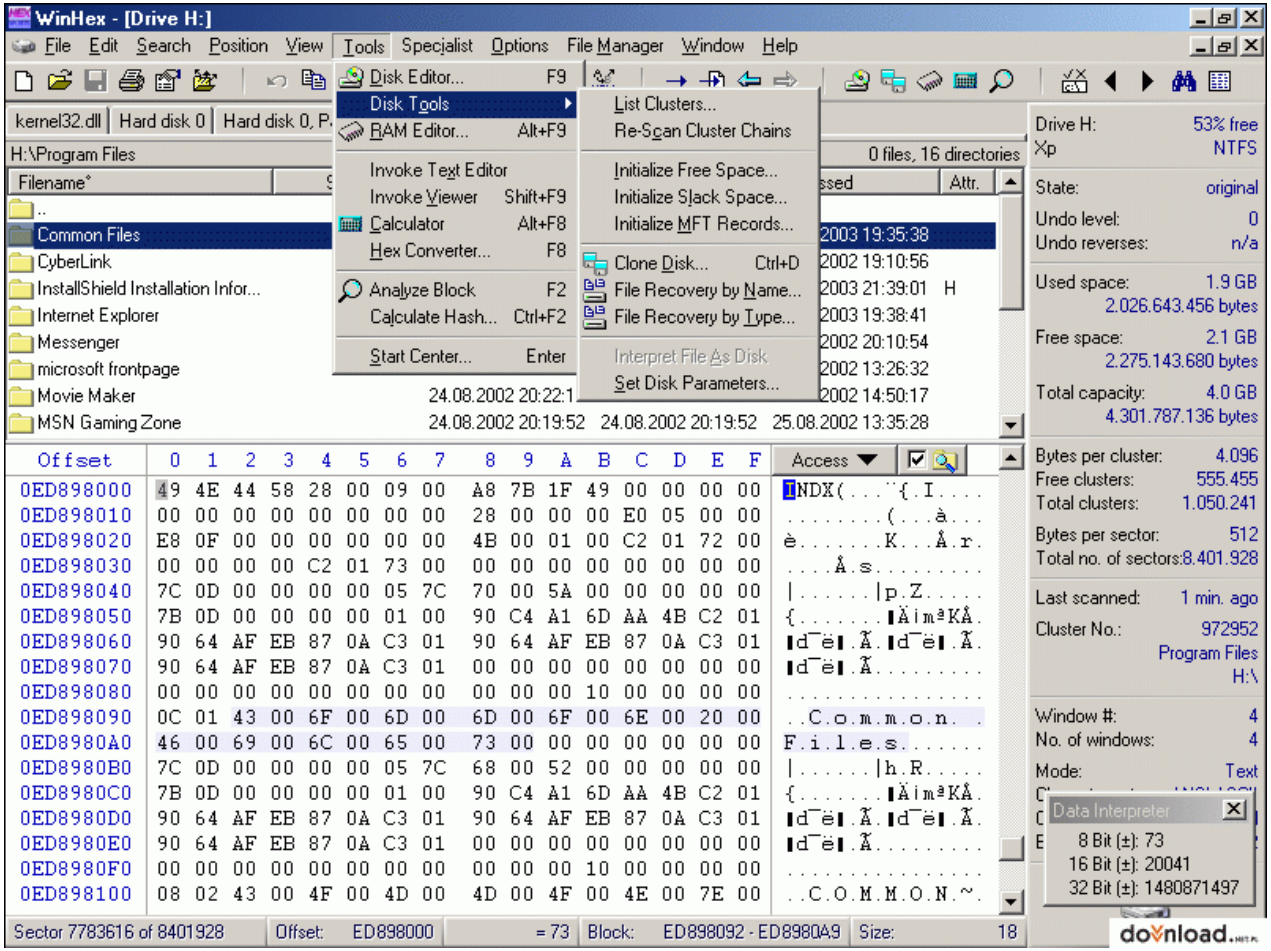
Beispiele für Anti-Forensik

Kritische XSS-Schwachstelle in X-Ways Forensics

- Sehr verbreitet in Deutschland und auch in anderen Ländern
- Insgesamt gute und wertvolle Software
- Ein mittlerweile gefixtes, aber ernsthaftes Problem:
  - XSS-Klassiker, oder nach Artur Janc „**Resident XSS**“
  - In einem toten Asservat kann HTML/JavaScript-Code abgelegt werden
  - X-Ways baut diesen Code in eigene HTML-Berichte ein
  - Resultat:
    - Verstecken von Spuren
    - Hinzufügen von gefälschten Spuren
    - Angreifen des Auswerte-PC und anderer PC

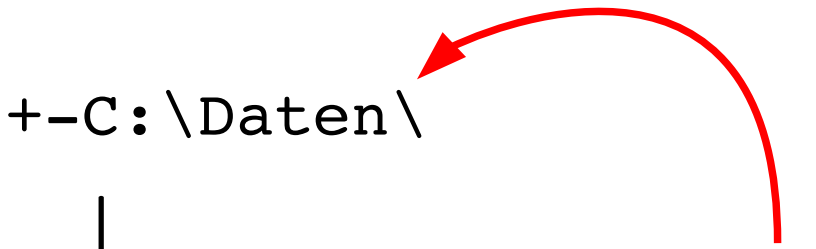
Beispiele für Anti-Forensik

Kritische XSS-Schwachstelle in X-Ways Forensics



Beispiele für Anti-Forensik

Verzeichnis-Schleifen

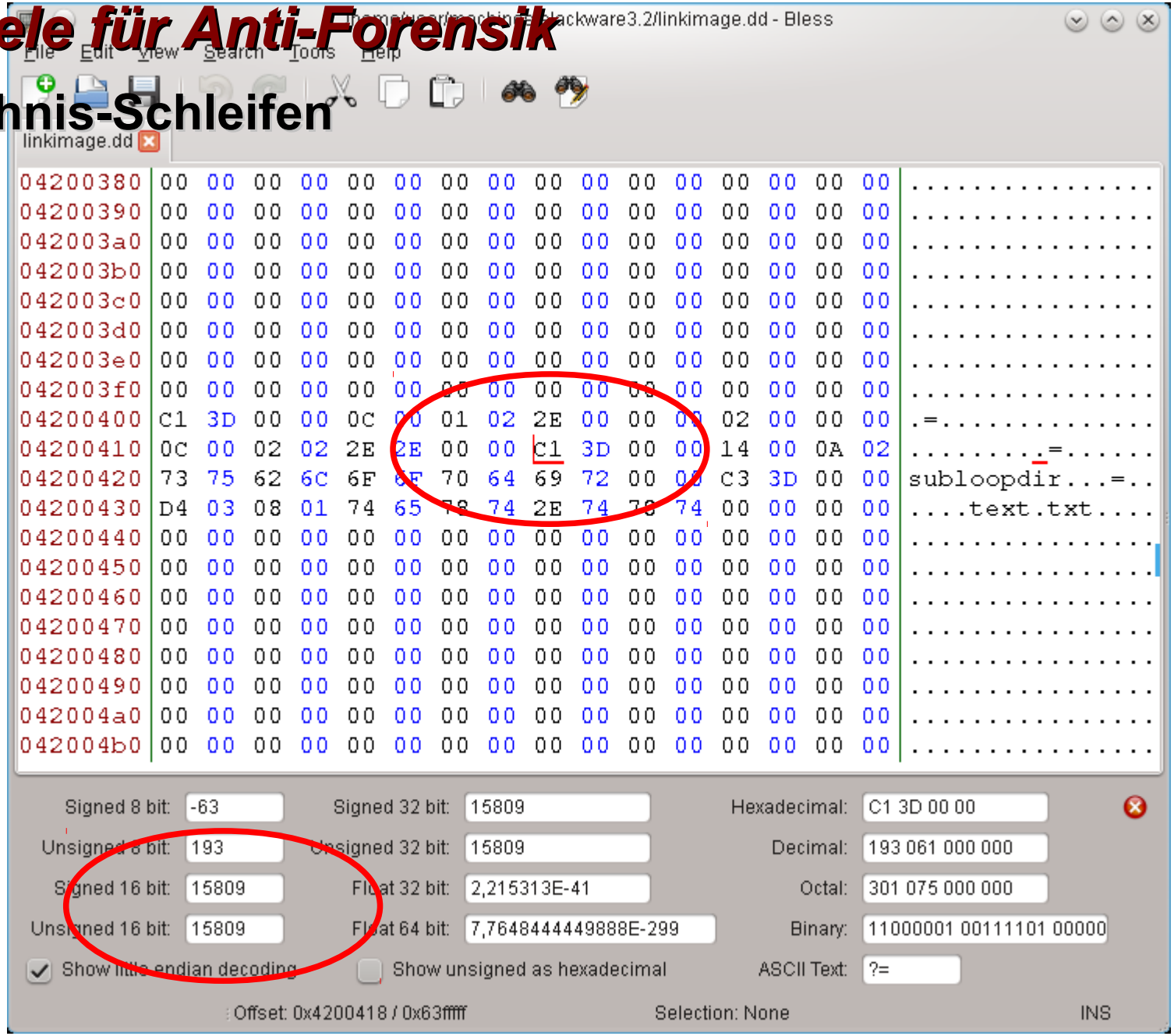


```
+-C:\Daten\
  |
  +-Unterverzeichnis\
  |
  +-Inhalte.txt
```

```
+-C:\Daten\
  |
  +-Unterverzeichnis\
  | |
  | +-Unterverzeichnis\
  | | |
  | | +-Unterverzeichnis\
  | | +-Inhalte.txt
  | |
  | +-Inhalte.txt
  |
  +-Inhalte.txt
```

Beispiele für Anti-Forensik

Verzeichnis-Schleifen



Beispiele für Anti-Forensik

How to own your write blocker in less than two hours

Beispiele für Anti-Forensik

Anti-Forensic-Rootkit

- Ausgangssituation: Live-Forensik an einem präparierten Linux-System
- Nutzt bekannte Rootkit-Technik und Schnittstellen des Linux-Kernels zur Erfüllung von antiforensischen Tätigkeiten
- Unterstützt dabei subtile als auch offensive Angriffe
- Ist in der Lage:
    - Hash-Summen zu manipulieren
    - Memory-Dumps zu verändern
    - Datei als 'Falle' zu setzen, um RAM der Maschine kontrolliert zu löschen.
    - USB-Devices zu beobachten und ggf. anzugreifen

Beispiele für Anti-Forensik

"Self-Anti-Forensik"

- **Produkt A**: ~30% der Firefox-History (SQLite-Datenbank!) wurden kommentarlos übersehen
- **Produkt B**: „Fehler 42 in Komponente XY bei Auswertung MFT. OK klicken für Weitermachen“ → großer Teil der Dateien wurde nicht angezeigt, unter anderem die Outlook-.PST mit entlastenden Spuren!
- **Produkt C** (Live-Forensik-Tool): Reproduzierbarer Absturz bei Sicherung des DNS-Cache, weitere Auswertung nicht möglich

Kategorisierung von Maßnahmen der Anti-Forensik

Angriffsziel / Zielsetzung	**Untersuchung vermeiden/verhindern**	**Untersuchung verzögern**
Auf das Asservat bezogen	Festplatte wipen; Registry wipen; Steganographie; full disk encryption; ...	Große Mengen Pr0n, ungewöhnliche Hardware, ...
Auf den Auswerter bezogen	Präkontamination mit Auswerterdaten	Zeitstempel manipulieren
Auf das Auswertesystem bezogen	Code injection Angriffe; buffer overflows; directory loop Angriffe	ZIP-Bomben, Hashes von Dateien verändern (Hash-Datenbanken!)

Anti-Anti-Forensik: Was können wir tun?

Alle Anti-Forensiker und jedes Wissen über Anti-Forensik wegsperren

Bildquelle: YuriArcurs / Clipdealer

Anti-Anti-Forensik: Was können wir tun?

Problembewusstsein bilden

- IT-Forensiker müssen sich mit dem Themenkomplex beschäftigen, denn:
  - Täter tun dies bereits ebenfalls
  - IT-Forensik und IT-Sicherheit wachsen zusammen
  - Live-Forensik wird zunehmend wichtiger, und nicht selten gibt es „nur einen Versuch“
  - Jedes Szenario ist hypothetisch bis es eintritt
  - Forensik-Software kann auch ohne externe Einflüsse unzutreffende Ergebnisse liefern
  - Es ist nie verkehrt, vorbereitet zu sein

Anti-Anti-Forensik: Was können wir tun?

Zeit und Ressourcen sowie bessere Software

- Eng getaktete Bearbeitungszeiten und hoher Vorgangsdruck = wenig Zeit und Ruhe für außergewöhnliche und scheinbar gewöhnliche Fälle
- Mindestens zwei verschiedene Werkzeuge verwenden
- Wenigstens bei Auffälligkeiten und Programmfehlern
- Zeit und Gelegenheit zum Austausch mit Kollegen

Anti-Anti-Forensik: Was können wir tun?

Zeit und Ressourcen sowie bessere Software

- **Zuverlässigere und genauere Software**
  - Entwicklung **robuster** Programme
  - Auffälligkeiten deutlich melden, mehr Debug-Informationen
  - **Prüfroutinen**, die auf erkannte Maßnahmen der Anti-Forensik und andere Auffälligkeiten deutlich hinweisen
  - Heuristiken, die bestimmte Angriffe abwehren
- *Forensische Software sollte nicht bloß auf das Finden von Spuren, sondern auch auf Robustheit geprüft werden*

Anti-Anti-Forensik: Was können wir tun?

Grundlagen/Theorie und Schulungen

- Hintergründe und Informatik/Theorie verstehen
  - Das Starten von automatischen Routinen reicht nicht mehr aus
  - Nicht jeder kann oder will Programmierer und Informatiker werden, aber Theorie und Grundlagen sind essentiell
  - Zusammenhänge und Techniken werden immer komplexer
- Schulungen, die nicht nur in die fachliche Breite sondern auch in die Tiefe gehen
- Anti-Forensik muss Bestandteil der Ausbildung von IT-Forensikern sein
- **Mehr Verständnis über Roh-Daten und Artefakte erlangen**
- Weniger Fokussierung auf einzelne Tools und deren Bedienung

Anti-Anti-Forensik: Was können wir tun?

Aktive Forschung und gemeinsamer Dialog

- Intensive Forschung in Bezug auf Angreifbarkeit und Robustheit von IT-Forensik-Software ist notwendig
- Offener Dialog führt letztlich zu besserer Software und treffsicheren Prozessen
- Individuelle organisatorische Schwachstellen dürfen und sollen verborgen bleiben

Ausblick, Entwicklung in der Zukunft?

Lessons learned

- IT-Forensik im Vergleich zu IT-Sicherheit noch eher „ungefestigt“
- Alte Hüte (XSS) sehen hier wieder aus wie neu
- Anforderungen an korrekte Arbeitsweise und korrekte Ergebnisse sind sehr hoch
- Auch kleine Probleme (entlastende Datei übersehen?) können fatale Folgen haben
- Vermutlich warten viele weitere Probleme in Forensik-Software darauf, gefunden zu werden...
- IT-Forensiker und Software-Hersteller müssen aufmerksamer und genauer arbeiten
- **Logs auswerten und Software auf Logging prüfen**

Fragen? / Kontakt

Fragen? Anregungen? Hinweise? :-)

- Kontakt:
  - Martin Wundram
  - wundram@tronicguard.com, wundram@digitrace.de
  - Telefon: 0179 / 213 82 67
  - Hendrik Adam
  - adam@digitrace.de
  - Www.tronicguard.com Www.digitrace.de
  - Standorte: Dormagen/Düsseldorf und Köln