

Live Response USB-Stick für Windows

Joël Spang

Lehrgebiet Datennetze, IT-Sicherheit, IT-Forensik



1. Einleitung & Motivation
2. Stand der Technik
3. Zielsetzung
4. Überblick der Software
5. GUI Komponenten
6. USB Anwendung
7. Zusammenfassung

- Was ist Live Response?
 - Teilgebiet der IT Forensik
 - Sicherung von flüchtigen Daten

- Was wird gesichert?
 - Inhalt des Hauptspeichers
 - Netzwerkinformationen (Verbindungen / Adapter)
 - Prozesslisten und Dienste
 - Allgemeine Systeminformationen
 - Benutzer & Benutzergruppen
 - Log Dateien

- Live Response oft essentiell
 - Flüchtige Daten von hoher Relevanz
 - Schadsoftware manifestiert sich nur auf laufendem System
 - Laufwerke unverschlüsselt

- Existierende Tools nicht ausreichend
 - Benutzerfreundlichkeit ist nicht Priorität
 - Eingeschränkte Erweiterbarkeit
 - Wenig Flexibilität bei Konfiguration

- Fokus: Windows Forensic Toolchest (WFT)
- Features
 - Datenaufnahme konfigurierbar
 - Ausführung der Tools automatisiert durch Engine
 - Detaillierte HTML-Berichte mit Prüfsummen
- Mängel
 - Konfiguration über Konsole
 - Keine GUI
 - Nur schwer erweiterbar
 - Keine vorgefertigten Konfigurationen

- Anforderungen an die Anwendung
 - Intuitive GUI
 - Konfiguration der Datensicherung soll vereinfacht werden
 - Vorbereitung eines Laufwerks automatisiert
 - Benutzung für First-Responders optimiert
 - Klare Anweisungen und Erklärungen
 - Konfigurationen
 - Leicht wiederverwendbar
 - Vorgefertigte Konfigurationen enthalten
 - Anwendung soll erweiterbar sein
 - Neue Tools sind einfach einzubinden

- LiveUSB besteht aus 2 separaten Anwendungen
 - GUI Anwendung
 - USB Anwendung

- LiveUSB besteht aus 2 separaten Anwendungen
 - GUI Anwendung
 - USB Anwendung



Rechner des Ermittlers

- LiveUSB besteht aus 2 separaten Anwendungen
 - GUI Anwendung
 - USB Anwendung



Rechner des Ermittlers

- LiveUSB besteht aus 2 separaten Anwendungen
 - GUI Anwendung
 - **USB Anwendung**



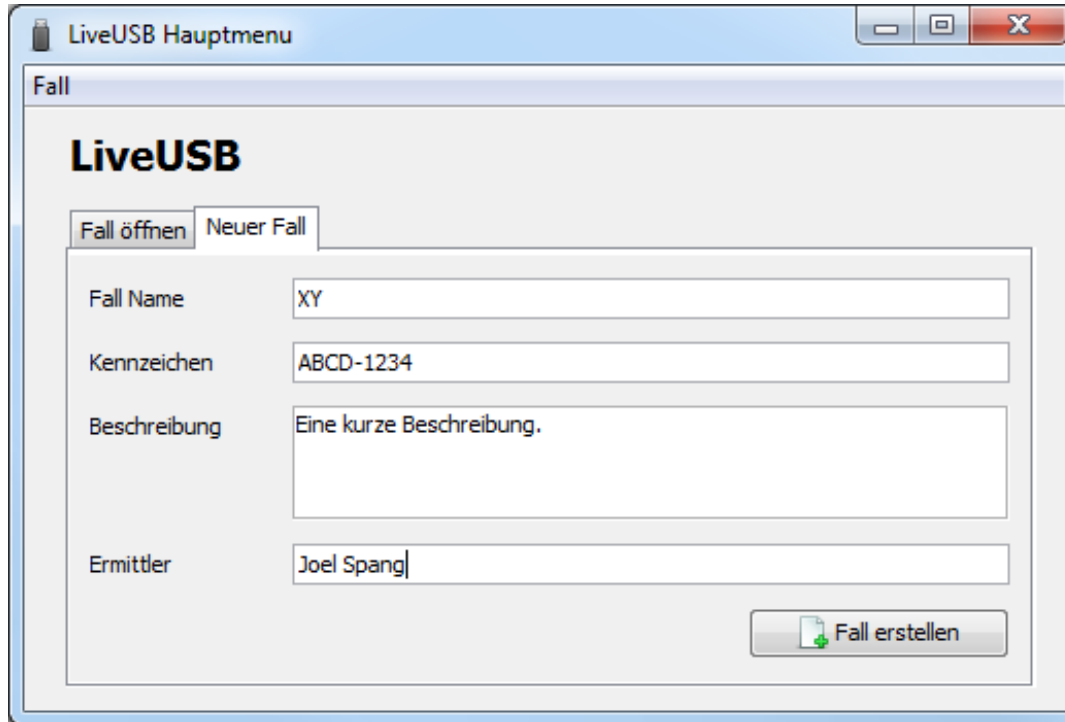
Rechner des Ermittlers



Zielsystem

■ Projektverwaltung

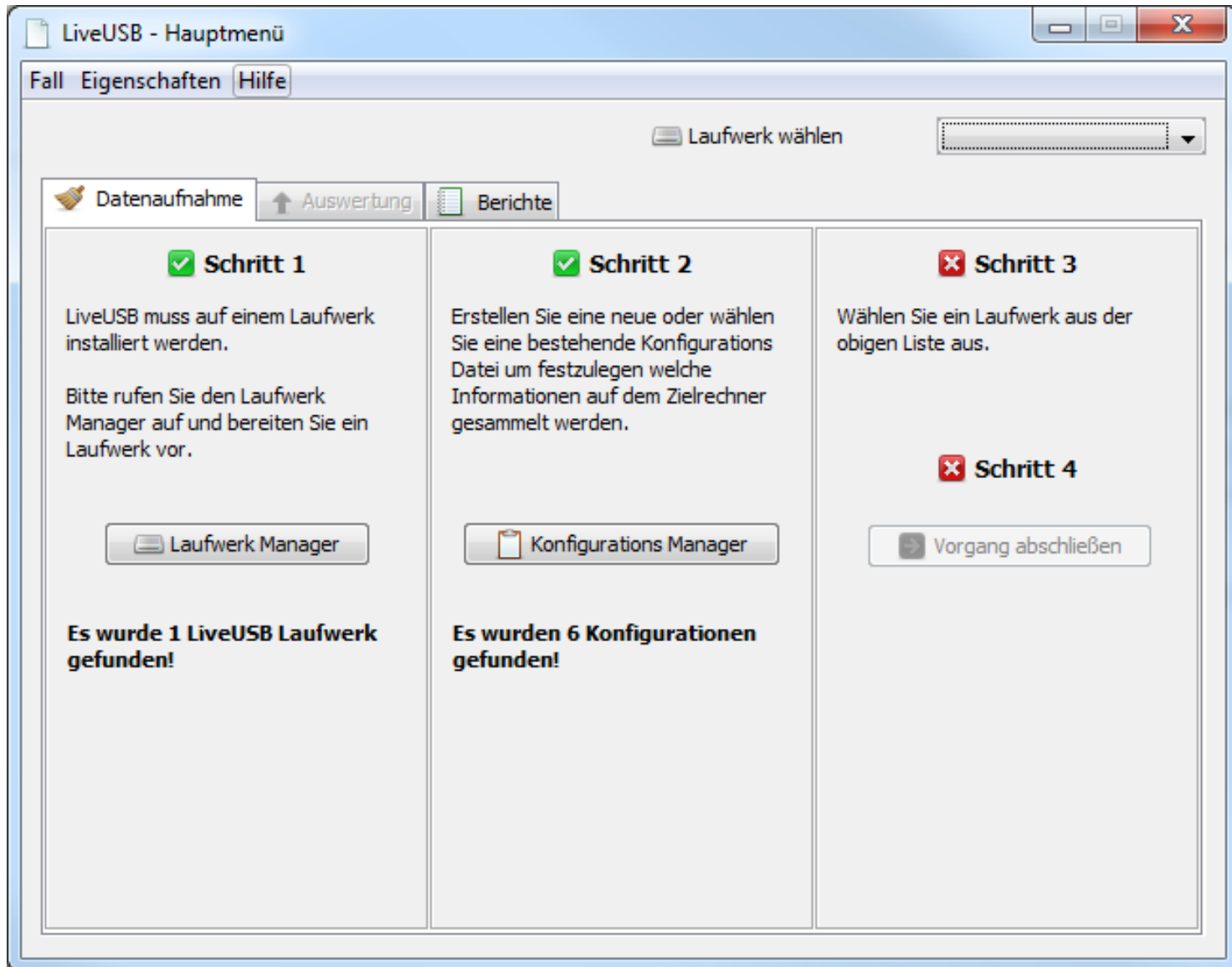
- Projekte bewahren Daten eines gleichen Falles auf
 - Gesammelte Daten (Quelldateien & Prüfsummen)
 - Erstellte HTML Berichte



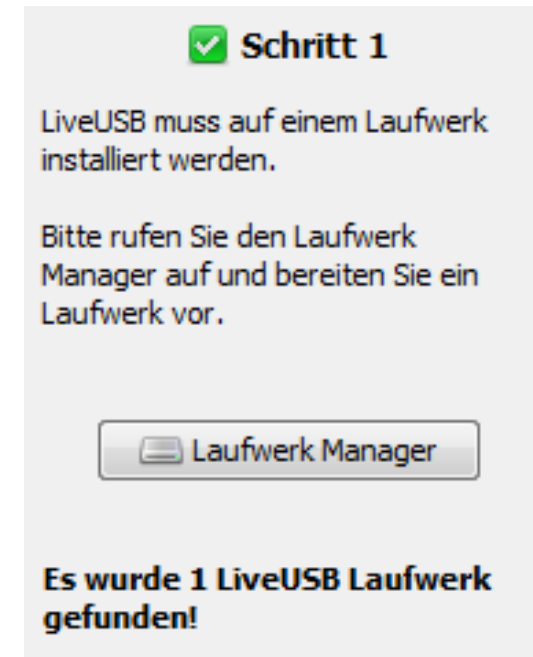
The screenshot shows a window titled "LiveUSB Hauptmenu" with a "Fall" tab. The main heading is "LiveUSB". There are two tabs: "Fall öffnen" and "Neuer Fall". The form contains the following fields:

Fall Name	<input type="text" value="XY"/>
Kennzeichen	<input type="text" value="ABCD-1234"/>
Beschreibung	<input type="text" value="Eine kurze Beschreibung."/>
Ermittler	<input type="text" value="Joel Spang"/>

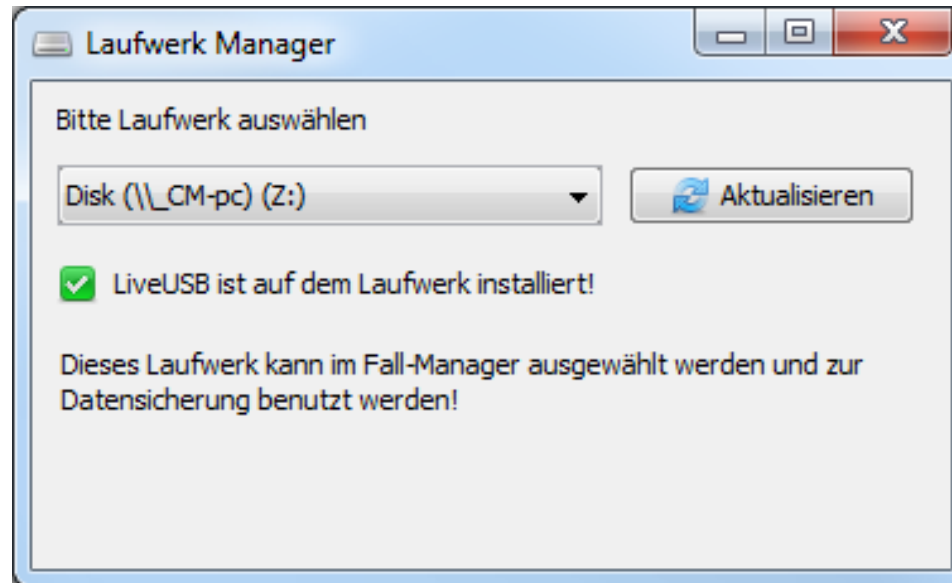
At the bottom right, there is a button labeled "Fall erstellen" with a green document icon.



- Hauptmenü
 - Bereitet eine Datenaufnahme in 4 Schritten vor
 - **Schritt 1: Vorbereitung eines Laufwerks**
 - Schritt 2: Erstellung von Konfigurationen
 - Schritt 3: Auswahl eines Laufwerks
 - Schritt 4: Synchronisation der Fall- und Konfigurationsdateien

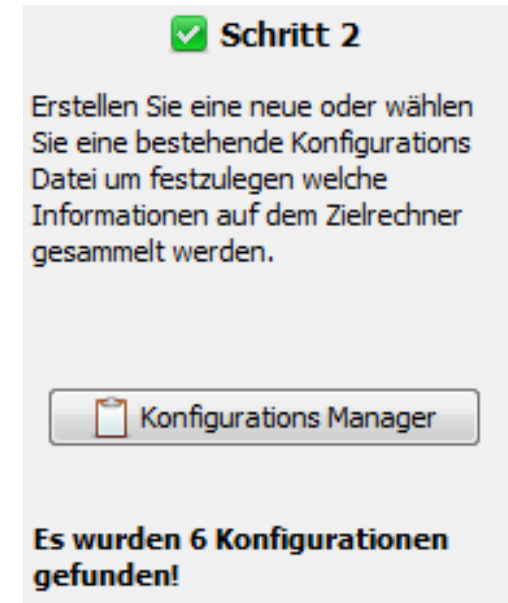


- Laufwerk-Manager
 - Bereitet Laufwerk für eine Datenaufnahme vor
 - Kopiert LiveUSB-Dateien und Tools auf das Laufwerk
 - Importiert gesammelte Dateien
 - Legt Quelldateien und Prüfsummen lokal ab

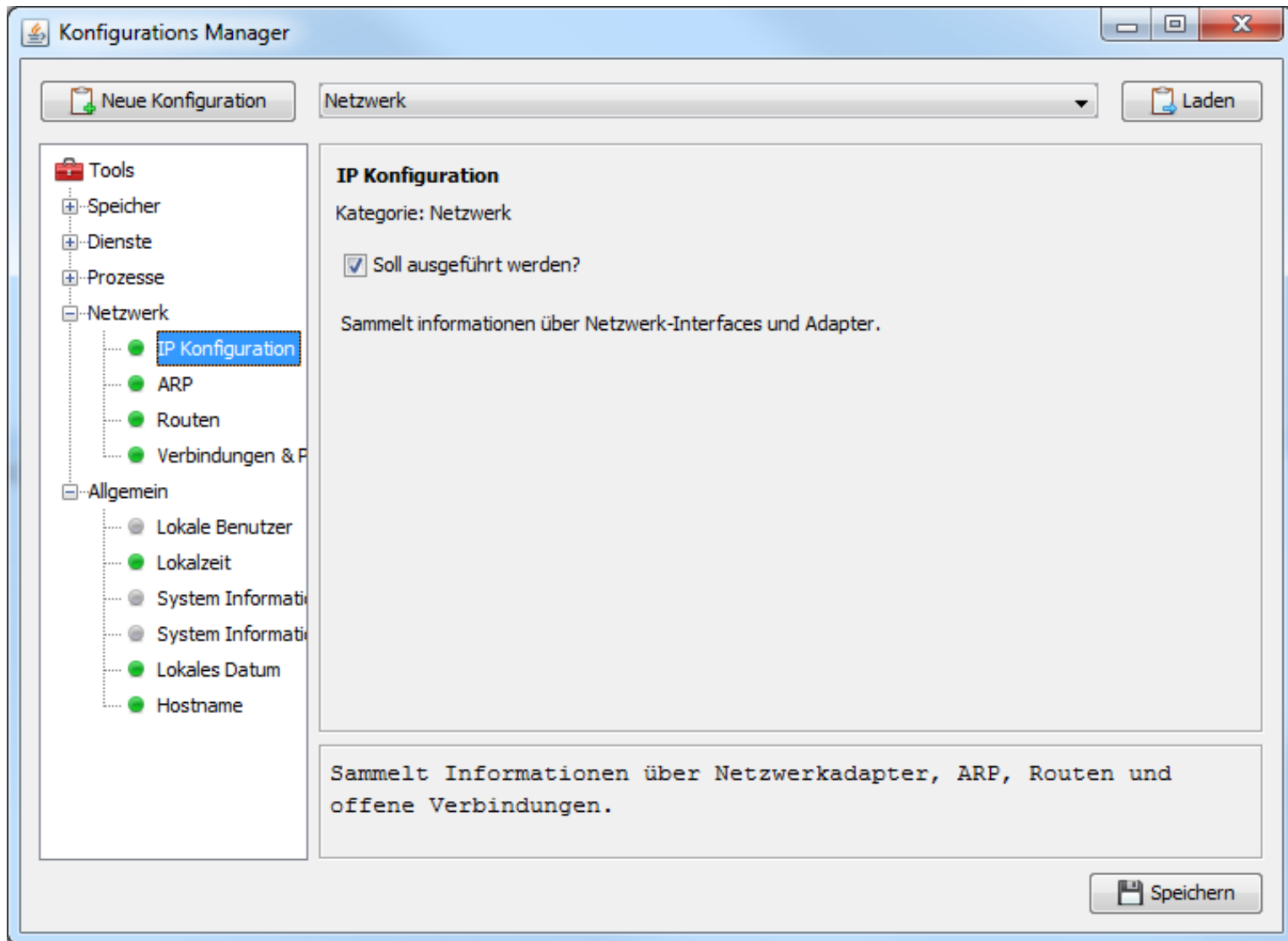


■ Hauptmenü

- Bereitet eine Datenaufnahme in 4 Schritten vor
- Schritt 1: Vorbereitung eines Laufwerks
- **Schritt 2: Erstellung von Konfigurationen**
- Schritt 3: Auswahl eines Laufwerks
- Schritt 4: Synchronisation der Fall- und Konfigurationsdateien

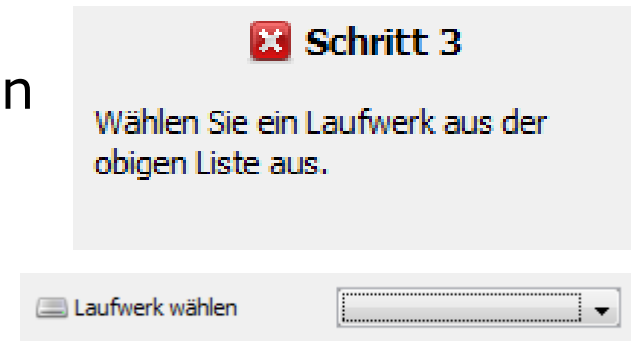


- Konfigurations-Manager
 - Erstellt und modifiziert Konfigurationsdateien
 - Konfigurationen legen fest, welche Tools ausgeführt werden
 - Legt Parameter für jedes Tool fest
 - Unterstützte Tools
 - Allgemeine Informationen
 - Datum / Zeit, OS Info, Benutzer & Gruppen
 - RAM Speicher
 - Prozesse, Dienste & Treiber
 - Netzwerk Informationen
 - Adapter / Interfaces, ARP, Routing, Ports, Remote Benutzer



■ Hauptmenü

- Bereitet eine Datenaufnahme in 4 Schritten vor
- Schritt 1: Vorbereitung eines Laufwerks
- Schritt 2: Erstellung von Konfigurationen
- **Schritt 3: Auswahl eines Laufwerks**
- Schritt 4: Synchronisation der Fall- und Konfigurationsdateien



- Hauptmenü
 - Bereitet eine Datenaufnahme in 4 Schritten vor
 - Schritt 1: Vorbereitung eines Laufwerks
 - Schritt 2: Erstellung von Konfigurationen
 - Schritt 3: Auswahl eines Laufwerks
 - **Schritt 4: Synchronisation der Fall- und Konfigurationsdateien**



- HTML-Berichte
 - Berichte werden aus Quelldateien der Datenaufnahme generiert
 - MD5 Prüfsummen gewährleisten Authentizität
 - Berichte enthalten
 - Name und Beschreibung der Tools
 - Gesammelte Daten und Ausgaben
 - Prüfsummen
 - Genutzte Konfigurationsdatei

LiveUSB Bericht

Navigation

 Startseite

 Konfiguration

Dienste

Lokale Dienste

Prozesse

Prozess Liste

Geladene DLLs

Datei Referenzen

Netzwerk

ARP

IP Konfiguration

Routen

Verbindungen & Ports

Allgemein

Lokale Benutzer

Lokalzeit

System Informationen


System Informationen (Erweitert)

Lokales Datum


Hostname

Prozess Liste

Erstellt eine Liste der laufenden Prozesse mit Prozess IDs.

 MD5 Hash:

 Prüfsumme OK.

 Datei Inhalt:

```
pmdump 1.2 - (c) 2002, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
- http://ntsecurity.nu/toolbox/pmdump/
```

```

0 - System idle process
4 - System
336 - smss.exe
456 - csrss.exe
540 - wininit.exe
548 - csrss.exe
596 - services.exe
612 - lsass.exe
620 - lsm.exe
712 - winlogon.exe
772 - svchost.exe
836 - nvsvc.exe
860 - nvSCPAPISvr.exe
904 - svchost.exe
972 - atiesrxx.exe
160 - svchost.exe
308 - svchost.exe
```

- LiveUSB besteht aus 2 separaten Anwendungen
 - GUI Anwendung
 - **USB Anwendung**

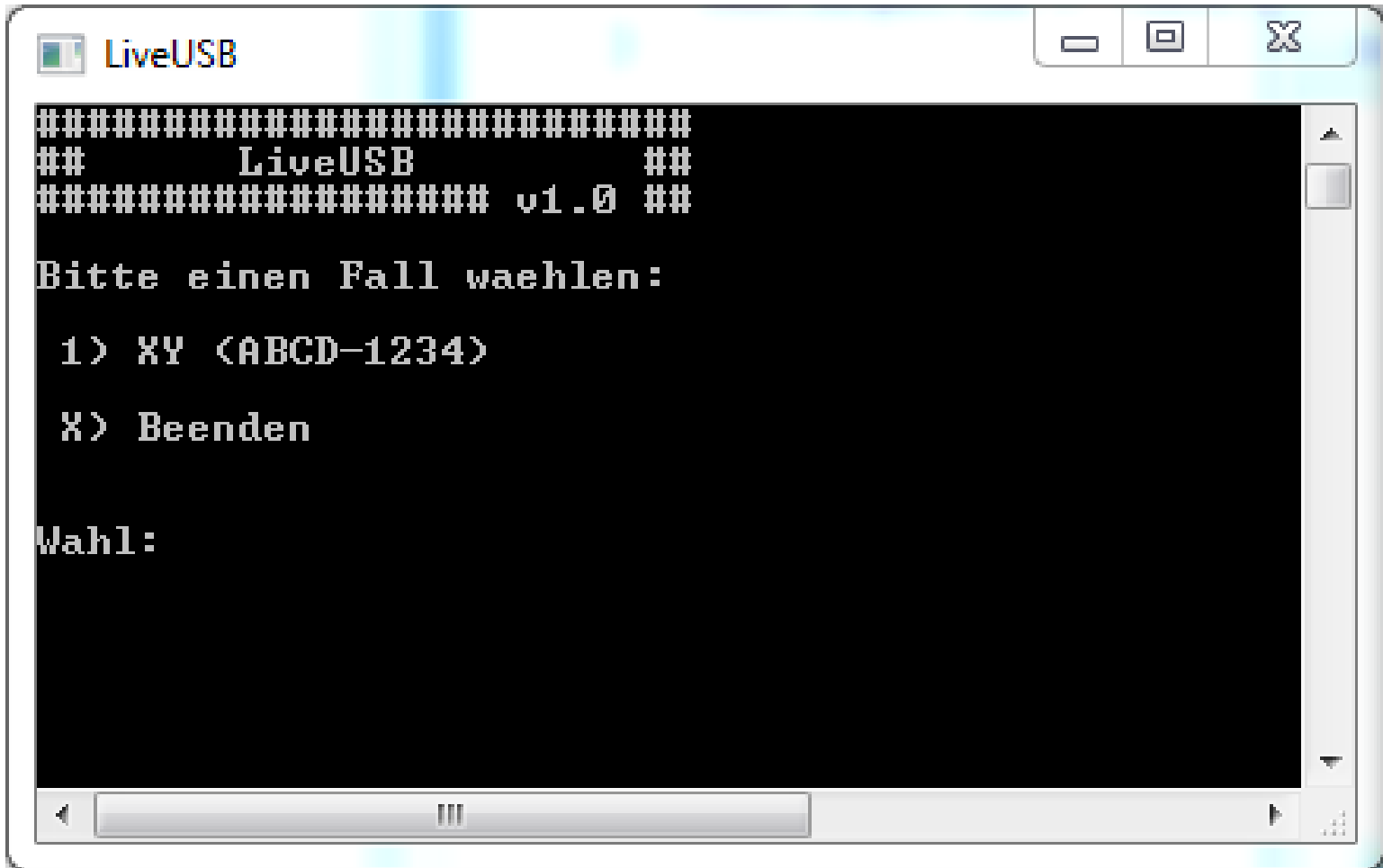


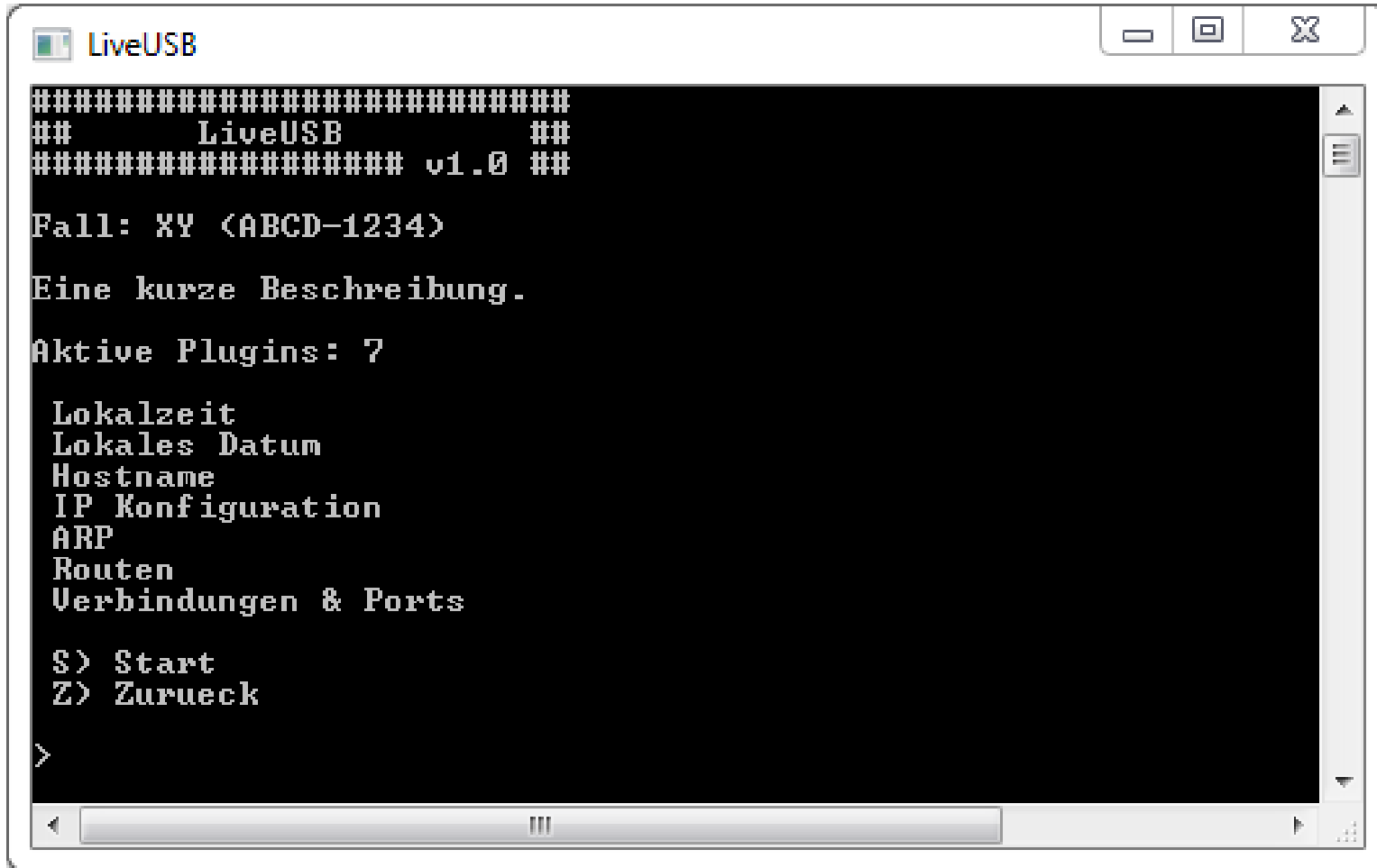
Rechner des Ermittlers

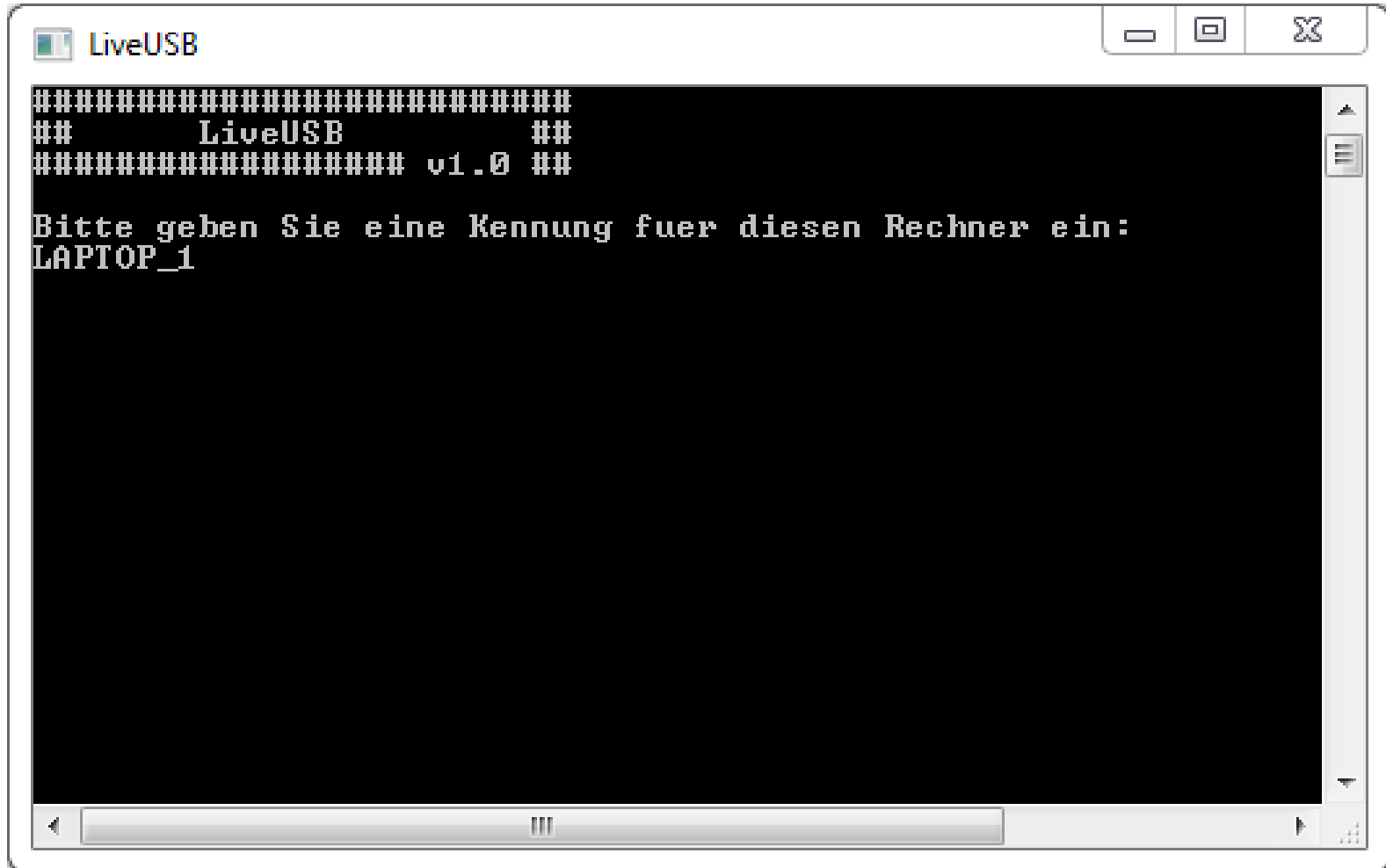
Zielsystem

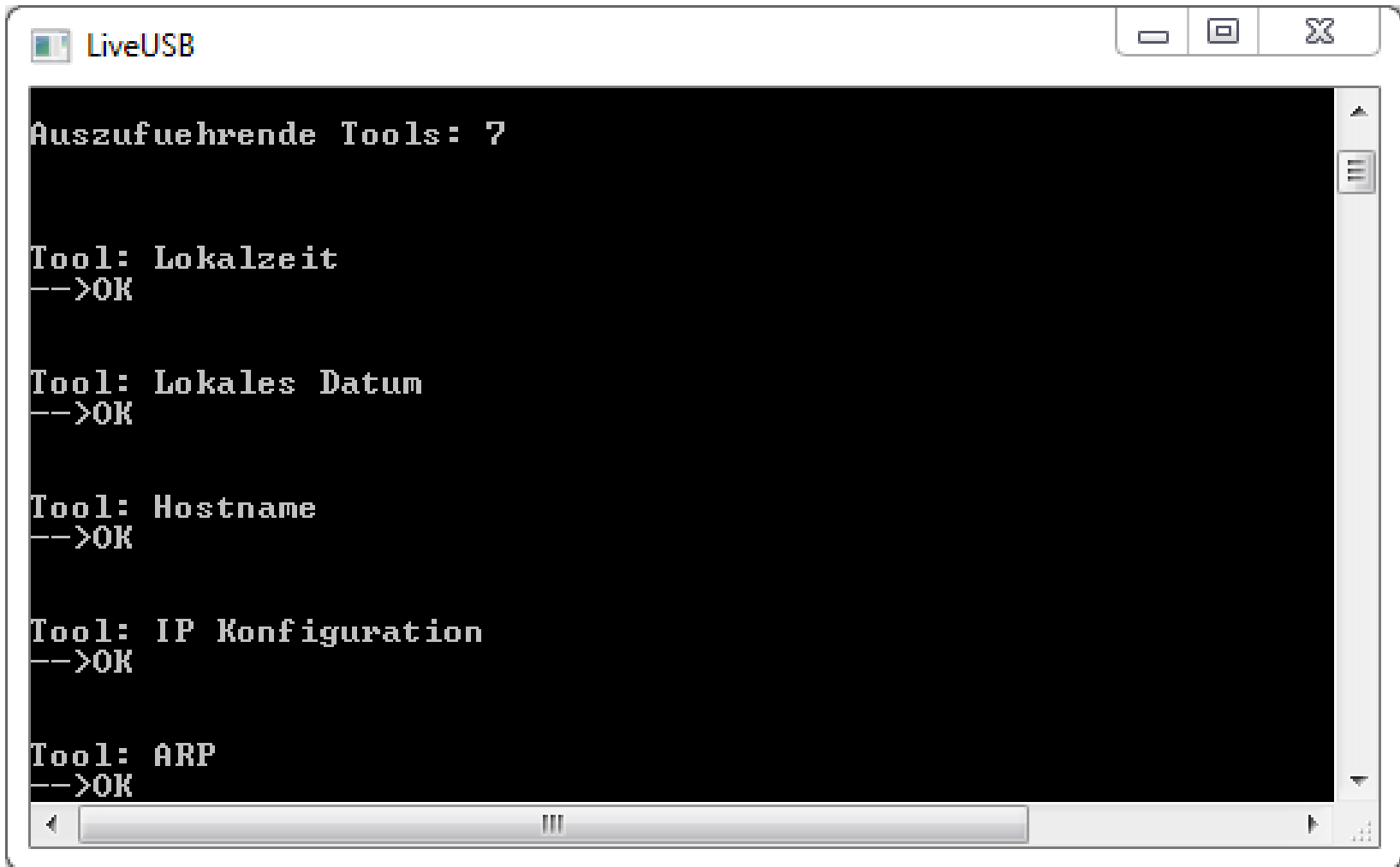
- Führt eigentliche Datenaufnahme durch
 - Liest Fall- und Konfigurationsdateien ein
 - Führt forensische Tools aus
 - Speichert Ausgabe der Tools auf Laufwerk ab
 - Erstellt Prüfsummen

- Benutzer kann Konfiguration frei wählen
 - Mehrere Datenaufnahmen eines Rechners möglich
 - Existierende Konfigurationen wiederverwendbar









- LiveUSB Anwendung
 - Erleichtert Konfiguration von Datenaufnahmen
 - Liefert intuitive GUI
 - Automatisiert viele Prozesse der Datensicherung
 - Generiert Berichte
 - Ist erweiterbar