National University of Computer and Emerging Sciences
Islamabad Campus

CY2002

Digital Forensics

Projects

Bitlocker Key Finder Tool

Submitted by: Aima Asghar, Maryam Shah, Noreen Mazhar
Roll number: 21i-2772, 21i-1570 ,21i-2768

Table of Contents

1. Overview

This tool, **BitLocker Key Finder**, is designed to help users locate and extract **BitLocker recovery keys** from various sources:

- System files.
- Live RAM (memory).
- Specific partitions.

It is primarily meant for **forensic investigations** or **recovery purposes** and works on both Windows and Linux operating systems.

2. Installation

Prerequisites

Before installing the tool, ensure:

- Python 3.9+ is installed.
- Administrator/root privileges are available (needed for partition or RAM scanning).
- Required Python libraries are installed.

Windows Installation

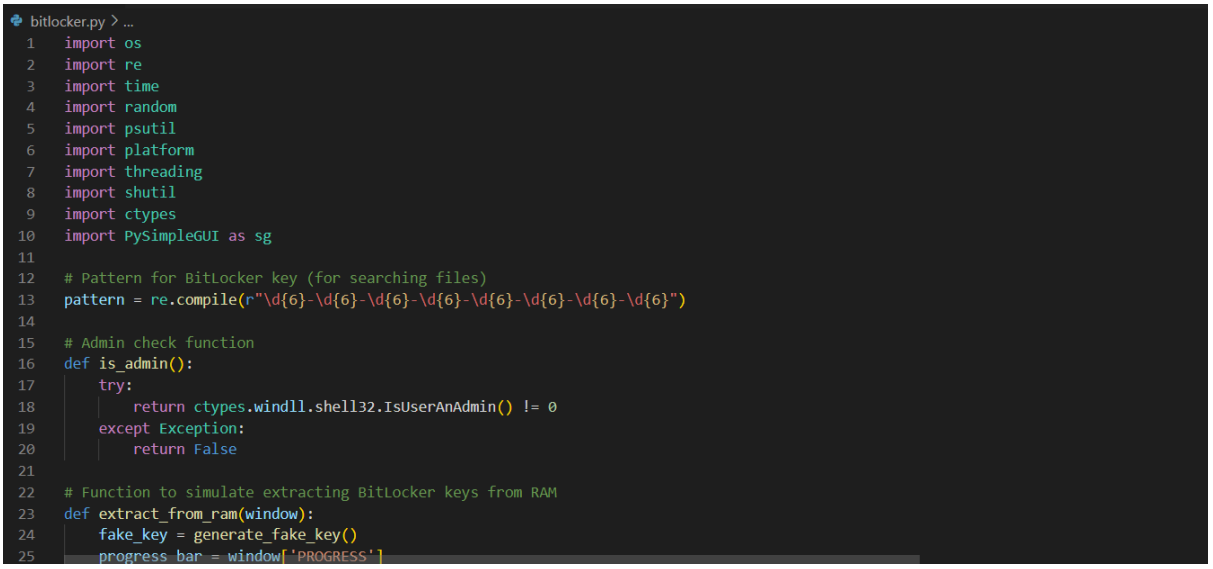
1. Install Python 3.9+ from Python.org.

During installation, check the box to **Add Python to PATH**.

2. Open Command Prompt and install the necessary libraries:
   ```
   pip install -r requirements.txt
   ```
3. Download the tool using Git:

   ```
   git clone https://github.com/bitlocker-key-finder.git

   cd bitlocker-key-finder
   ```



```python
import os
import re
import time
import random
import psutil
import platform
import threading
import shutil
import ctypes
import PySimpleGUI as sg

# Pattern for BitLocker key (for searching files)
pattern = re.compile(r"\d{6}-\d{6}-\d{6}-\d{6}-\d{6}-\d{6}-\d{6}-\d{6}")

# Admin check function
def is_admin():
    try:
        return ctypes.windll.shell32.IsUserAnAdmin() != 0
    except Exception:
        return False

# Function to simulate extracting BitLocker keys from RAM
def extract_from_ram(window):
    fake_key = generate_fake_key()
    progress_bar = window['PROGRESS']
```

Linux Installation

1. Update your package list and install Python:

```
sudo apt update
```

```
sudo apt install python3 python3-pip
```

1.

2. Install the required libraries:

```
pip3 install -r requirements.txt
```

3. Running the Tool

Windows

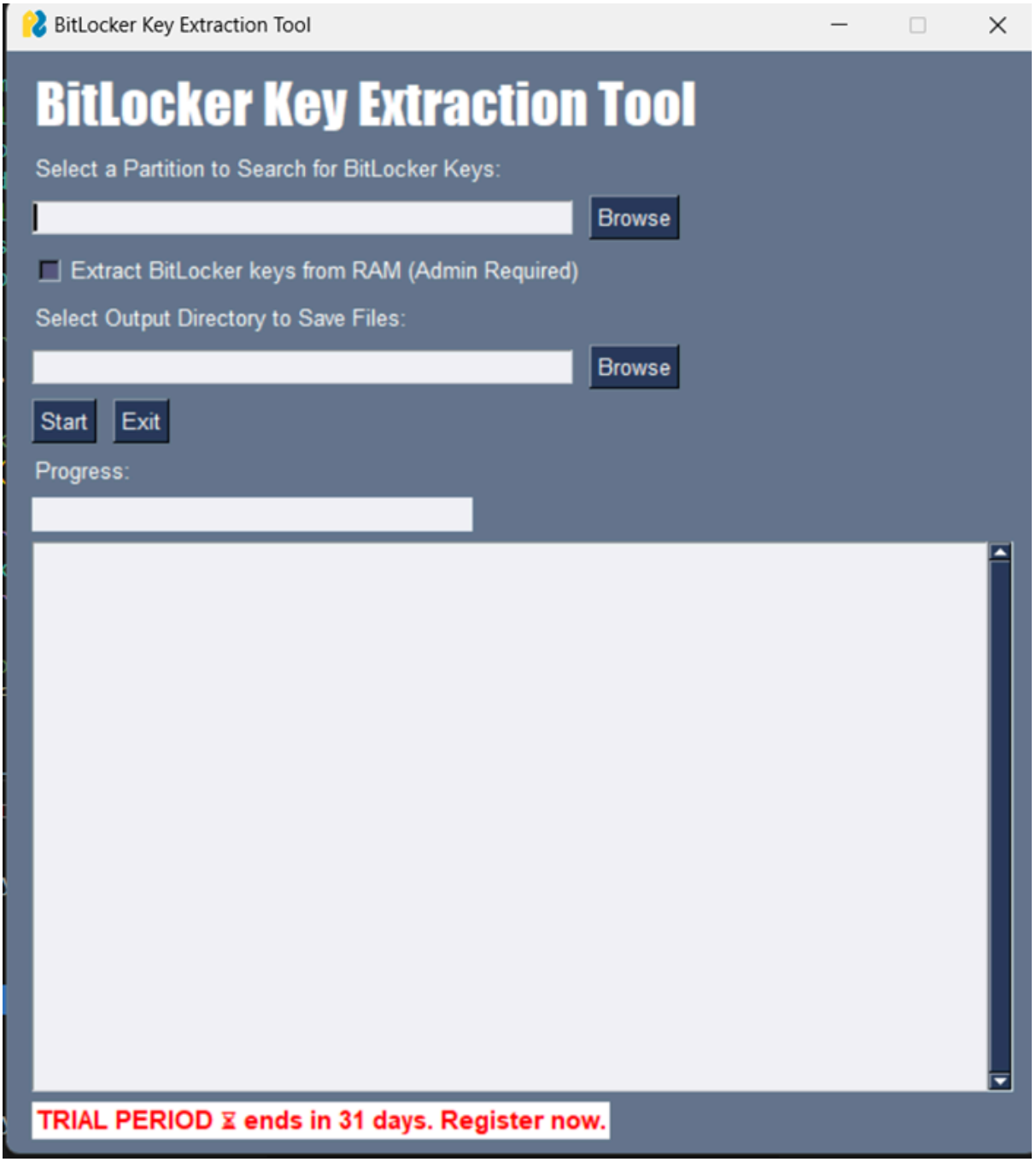
1. Open Command Prompt as **Administrator**.

2. Navigate to the tool directory:

```
cd path\to\bitlocker-key-finder
```

3. Run the tool:

```
python bitlocker.py
```



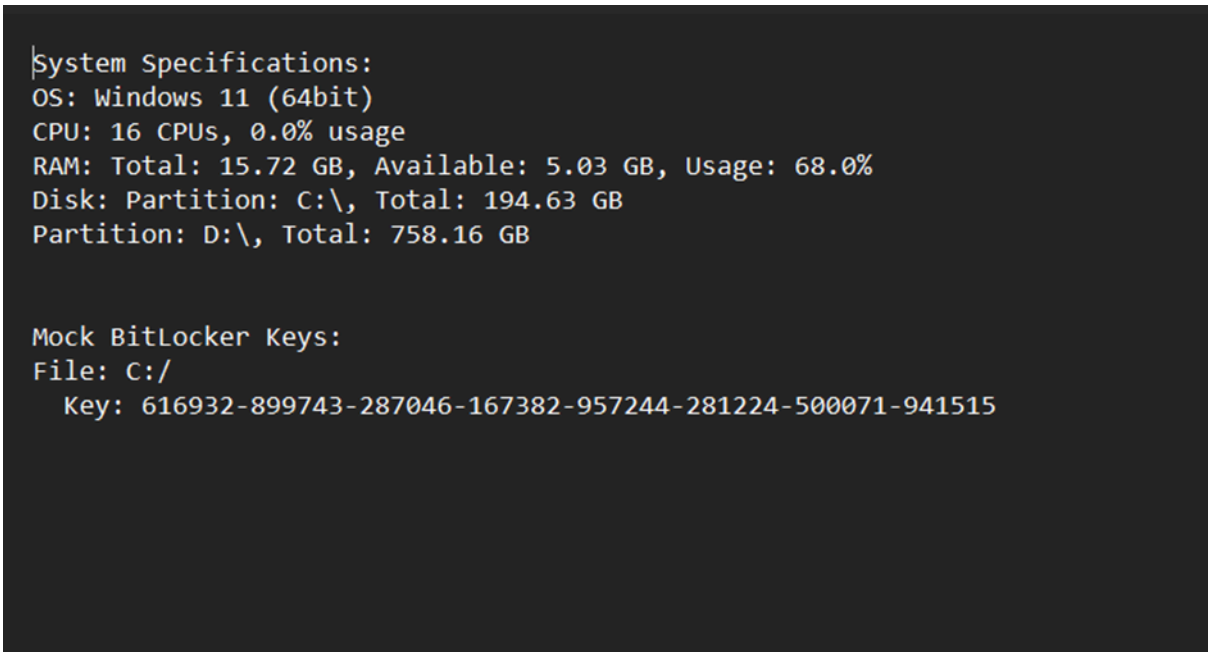
Linux

1. Open a terminal and navigate to the tool directory:
   ```
   cd path/to/bitlocker-key-finder
   ```
2. Run the tool with root privileges:
   ```
   sudo python3 bitlocker.py
   ```

4. Using the Tool

1. Scanning a Partition

- Use the **Partition Scan** option in the GUI or command-line interface.
- **On Windows**: Choose a drive like `C:\` or `D:\`.



- **On Linux**: Choose a partition like `/dev/sda1` or `/dev/sdb1`.
- Click "Start Scan" to begin the search.
- If keys are found, they are displayed in the output.

2. Searching Files

- Use the **File Search** option to scan specific directories or files.
- Supported file types include:
  - `.txt` files
  - `.bek` files
- The tool displays any detected recovery keys in the output window.

3. Live RAM Key Extraction

- Select **Live RAM Extraction** to scan the computer's active memory.
- **Requirements**:
  - On Windows: Must run the tool as an administrator.
  - On Linux: Run the tool with `sudo`.

5. Output Details

The tool displays results in the following format:

```
BitLocker Recovery Key:
123456-789012-345678-901234-567890-123456-789012-345678
```

- You can export the results to a `.txt` file using the "Save Keys" option.

6. Testing with Forensic Images

You can use the tool to scan forensic disk images:

1. **Mount the disk images**:
    - Use tools like Autopsy, SleuthKit, or OS-native mounting commands.
2. Choose an appropriate scan type:
    - For directories: Use **File Search**.
    - For partitions: Use **Partition Scan**.

7. Troubleshooting

Issue	Cause	Solution
Tool cannot access partitions/files	Insufficient permissions	Run as Administrator or with `sudo`.
No keys found	Incorrect path or no keys in the location	Verify the correct path/partition.
Errors during RAM extraction	Access restrictions or unsupported systems	Use elevated privileges or check system compatibility.
GUI crashes or freezes	Resource limitations or threading issues	Restart the tool and avoid multiple instances.

8. Frequently Asked Questions

Q1: What file types are supported?

The tool scans `.txt` and `.bek` files by default. You can modify it to scan other types.

Q2: Do I need elevated privileges?

Yes, you need admin/root privileges for:

- Partition scanning.
- Live RAM extraction.

Q3: Can it scan encrypted partitions?

The tool can only scan **accessible partitions**. Encrypted partitions must be unlocked first.