**⚙Digisuraksha project 2025**

**Tool Name: USB Keylogger**

### **1. History**

USB keyloggers have been in use since the early 2000s as hardware-based surveillance tools. Originally used by security agencies and penetration testers, they have become easily accessible and are used both for ethical hacking and malicious purposes. With the rise of USB devices, attackers started exploiting the universal plug-and-play functionality, making it possible to intercept keyboard inputs without detection.

### **2. Description**

A USB Keylogger is a hardware device that plugs in between a keyboard and a computer. It captures keystrokes as they are typed and stores them in internal memory or sends them to a remote location. It operates passively without altering the data, making it difficult to detect by conventional antivirus solutions.

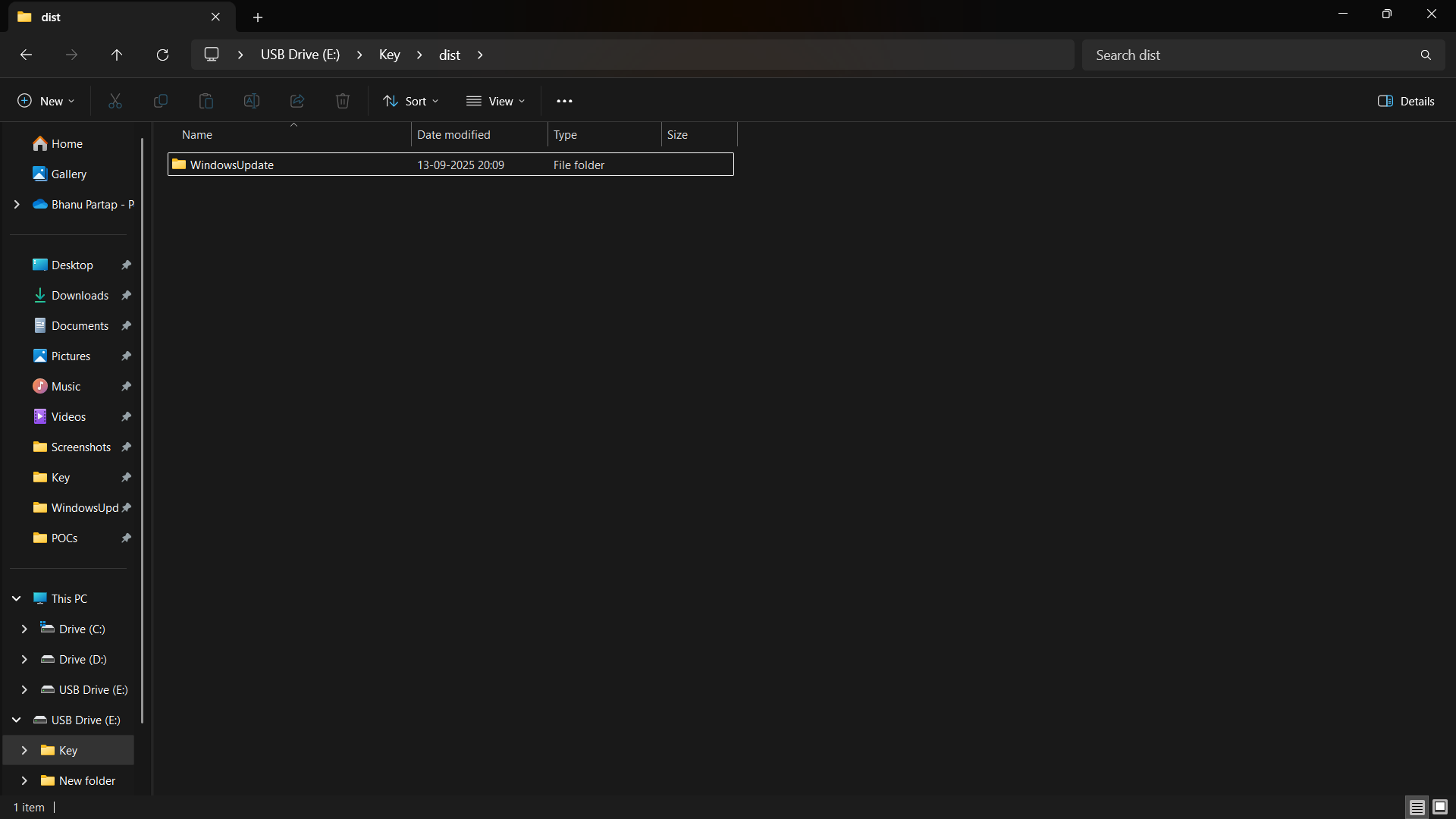
### **3. Key Features**

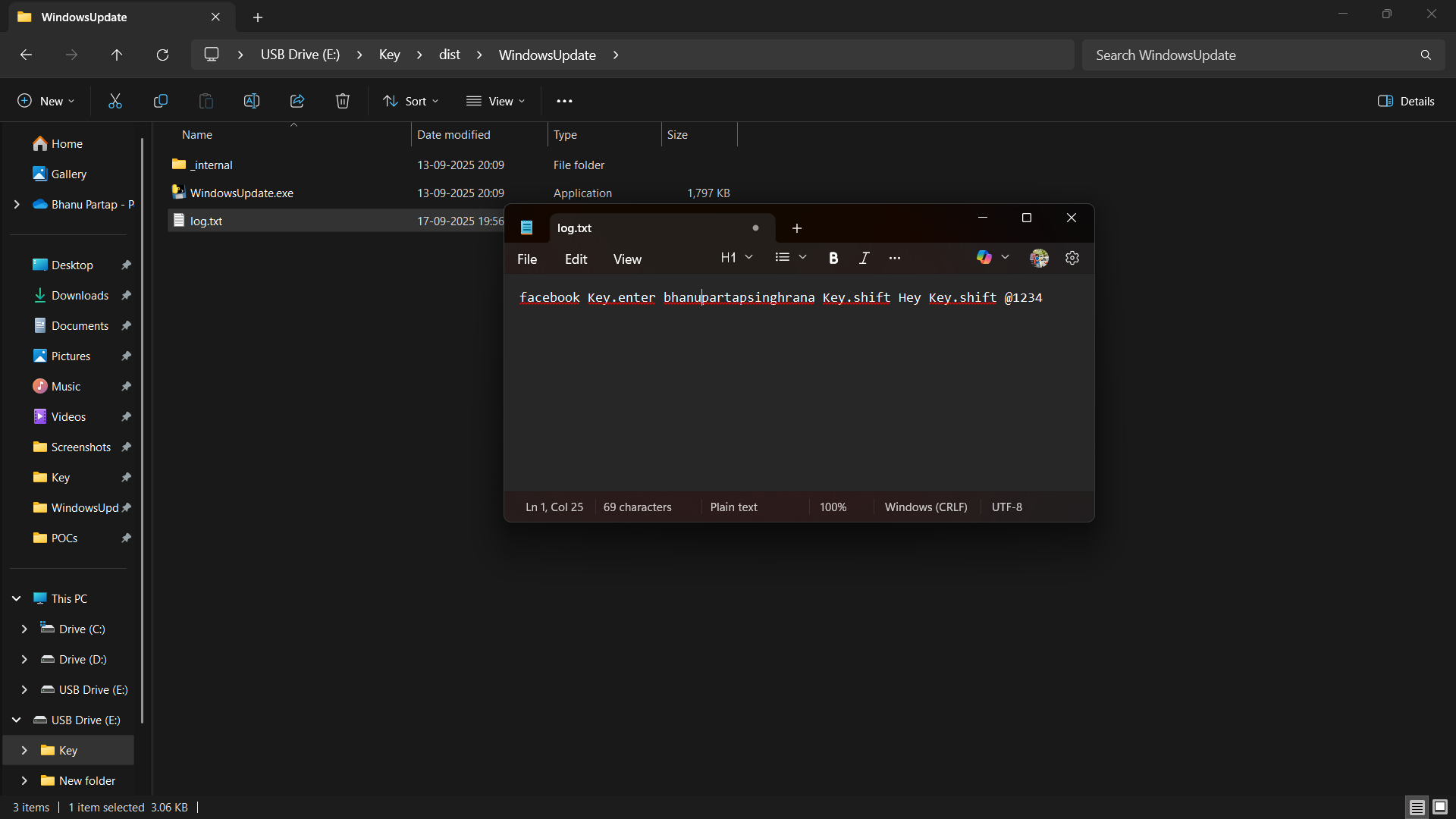
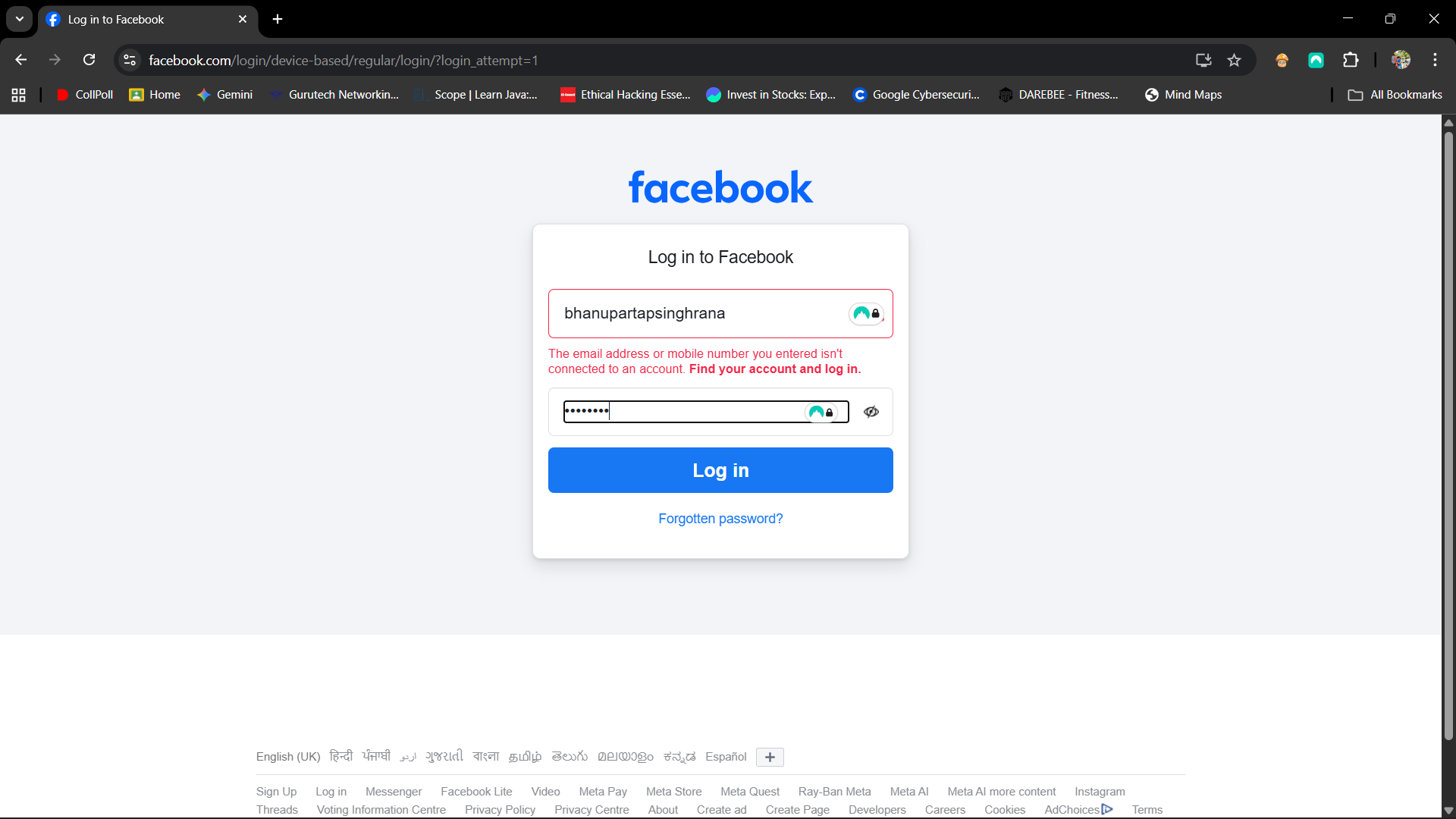
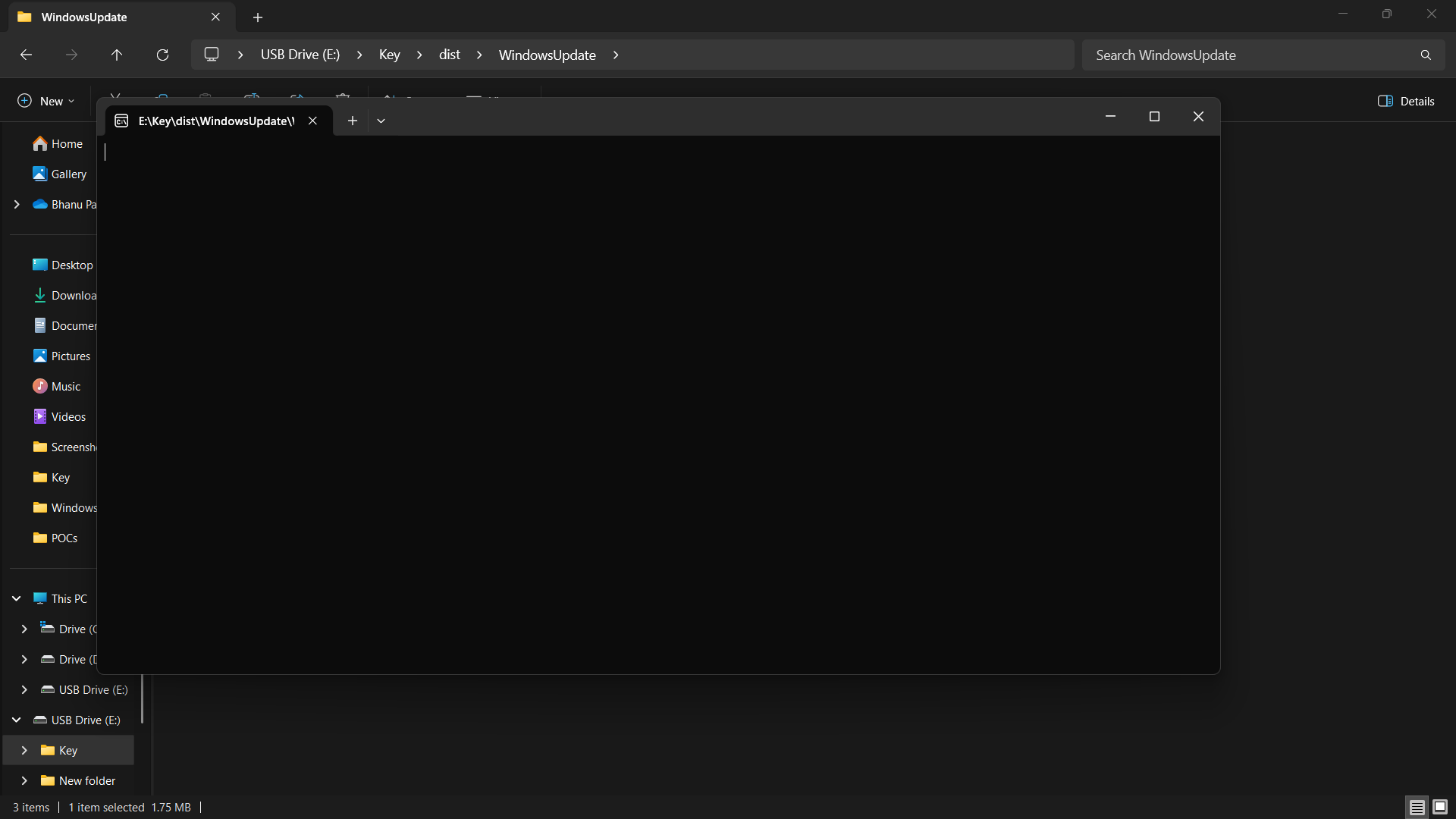
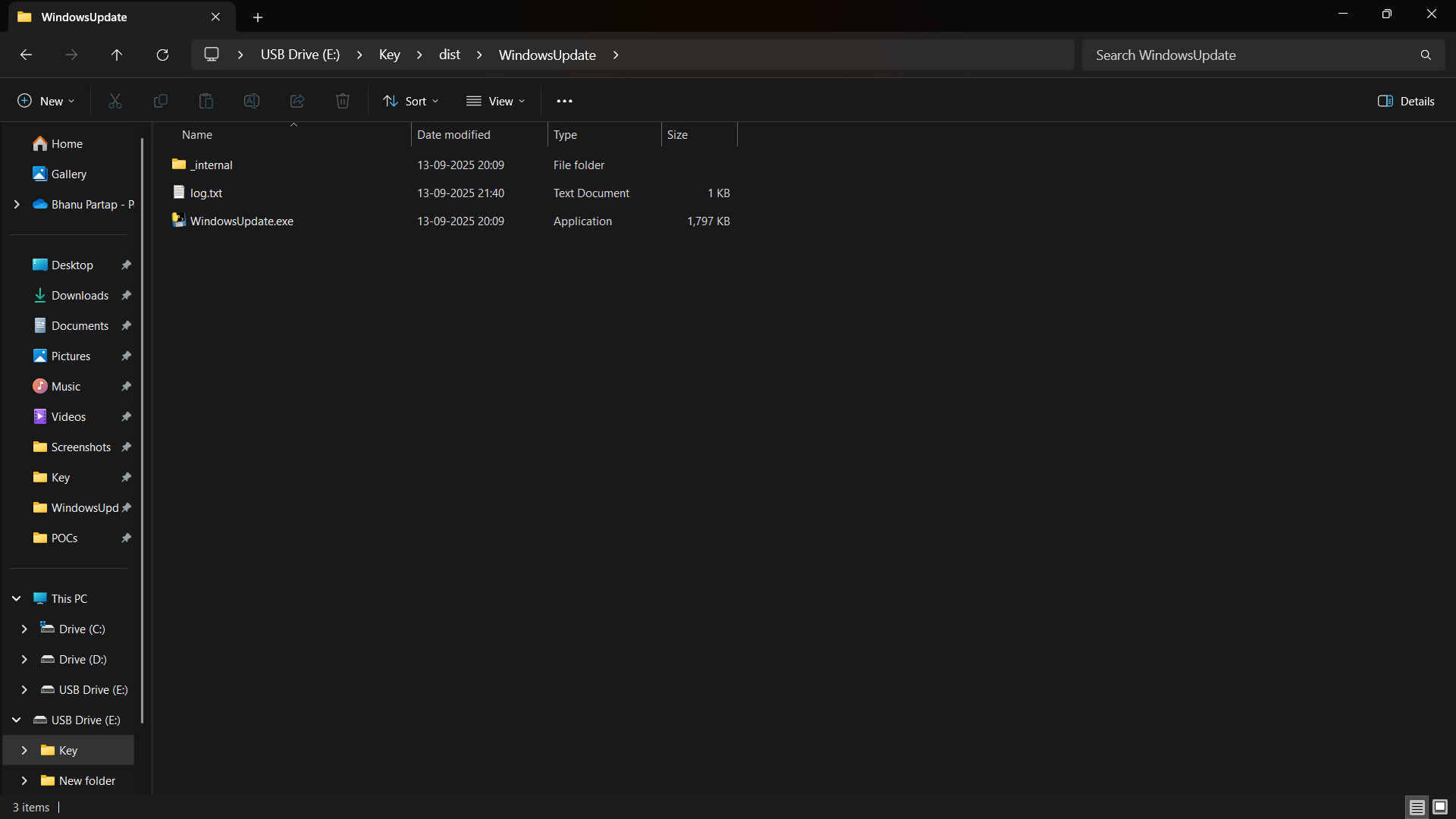
* **Plug-and-play**: Requires no software installation.
* **Stealth operation**: Works silently without alerts.
* **Data storage**: Can store thousands of keystrokes.
* **Encryption support**: Some models encrypt logged data.
* **Low power consumption**: Operates without external power.
* **Portable**: Compact and easy to conceal.
* **Compatibility**: Works with USB keyboards and multiple operating systems.
* **Write protection**: Prevents detection by some scanning tools.
* **Time-stamped logging**: Records the exact time of each keystroke.
* **Remote access** (in advanced models): Sends data via Wi-Fi or Bluetooth.

### **4. How Will This Tool Help**

* **Penetration testing**: Simulate real-world attacks to improve security posture.
* **Forensic analysis**: Help track user behavior in investigations.
* **Monitoring**: Used by organizations to monitor internal misuse (only with consent).
* **Training**: Teach cybersecurity students about hardware-level threats.
* **Vulnerability assessment**: Expose unsecured endpoints.

### **5. POC Images**





* A USB keylogger device between keyboard and computer
* Screenshot of logged data
* Diagram showing data capture process

### **6. 15-Liner Summary**

1. USB keyloggers are hardware devices that capture keystrokes.
2. They plug in between the keyboard and computer.
3. Originally used by security experts, they are now accessible to attackers.
4. They don’t require installation and operate silently.
5. They store data internally or send it remotely.
6. Compatible with most USB keyboards and OS platforms.
7. Some models encrypt data to avoid detection.
8. Used for penetration testing and security research.
9. Helps organizations monitor insider threats.
10. Assists forensic teams in tracking activity.
11. Can bypass antivirus and firewall protections.
12. Offers time-stamped logging for better analysis.
13. Portable and easy to deploy discreetly.
14. Ethical use requires legal consent.
15. Awareness and proper countermeasures are crucial.

### **7. Best Case Scenarios**

* Performing security assessments in controlled environments.
* Teaching cybersecurity students about physical access risks.
* Testing defenses in a simulated cyberattack setup.
* Monitoring authorized personnel for policy compliance.
* Investigating insider threats in forensic cases.

### **8. When to Use**

* During authorized penetration testing.
* In cybersecurity training labs.
* For forensic investigations.
* While demonstrating vulnerabilities in corporate workshops.
* When assessing physical security protocols.

### **9. Flaws**

* **Ethical risks**: Can be misused for spying or stealing sensitive information.
* **Limited storage**: May overflow if not retrieved regularly.
* **Detection risks**: Advanced systems may detect unauthorized devices.
* **Physical access required**: Must be plugged in manually.
* **Legal implications**: Unauthorized use is illegal in many regions.
* **Encryption limitations**: Some models do not encrypt data.
* **Compatibility issues**: May not work with wireless or specialized keyboards.

### **10. Good Things About It**

* Simple and effective hardware solution for keylogging.
* Requires no software footprint, making detection harder.
* Excellent tool for educating users on physical threats.
* Portable and cost-effective for security demonstrations.
* Useful in forensic investigations and ethical hacking exercises.
* Encourages organizations to strengthen endpoint protection.
* Helps build awareness around physical access vulnerabilities.