測試與評估表

Magic Wormhole

1. 工具概述

姓名:	Magic Wormhole
類別:	文件傳輸
目的:	提供 library 和 CLI, 以便使用者可以將任意大小的檔案和目錄從一台電腦發送到另一台電腦
測試日期:	2025年4月2日
文件翻譯日期:	2025年8月7日
地位:	已部署 ☑ 營運中 - 積極運作/維護 ☐ 測試中 - 目前正在評估或試行 ☐ 不活躍/棄用 - 不再維護或運行
部署架構:	☐ 獨立軟體 - 完全在本地運行(例如, 在電腦上運行並且不依賴外部伺服器) ☐ 具有獨立伺服器和用戶端元件的本機主機服務 - 自行執行後端/前端(例如, 後端可以在本機網路上, 也可以在雲端自行託管) ☑ 由第三方託管的本機用戶端服務 - 您在裝置上安裝用戶端, 但它連接並依賴遠端伺服器(例如, Signal:安裝應用程式(用戶端), 但 Signal 的伺服器處理訊息中繼等) ☐ 由第三方託管但也可以自行託管的服務
版本:	在 0.6.3 中

2. 安裝和設定

作業系統相容性	MacOS、Linux、Windows
安裝手冊:	Yes
安裝步驟:	1. 以管理員身分開啟終端機:

	a. Windows：右鍵單擊開始>”命令提示字元（管理員）","**Windows PowerShell**（管理員）“，或者 ”終端（管理員）」。 b. macOS/Linux：打開終端。 2. 安裝 Wormhole： a. 請按照上述文件中針對您的作業系統的安裝說明進行操作。 3. 接受下載： a. 當提示您接受下載時，請輸入 ”**y**“ 或者 ”**a”**。
提及是否需要命令列設定或特殊配置	整個工具是一個命令列工具，雖然操作起來可能有點複雜，但不需要特殊配置。儘管使用命令列作為文件傳輸的介面，但它使用起來相對容易。
常見安裝問題及修復：	● 用戶在使用 Magic Wormhole 時經常遇到的一個問題是傳輸後如何定位下載的檔案。預設情況下，檔案會保存在終端機的目前工作目錄中。使用者需要了解系統的檔案路徑和目錄結構，才能知道下載檔案的保存位置。 ● 當使用者共用檔案時，一個常見問題是如何正確地將檔案路徑複製到終端。要發送文件，必須在蟲洞發送 命令。
使用者文件：	Yes
所需的技術知識	中

3. 測試與評估

類別	細節	分數
操作功能：	功能 ● Magic Wormhole 能夠有效地實現設備之間的安全文件傳輸，同時實施強大的安全措施。它採用結構化協議，包含郵箱伺服器、中轉中繼和擴展協議，以促進加密的點對點通訊。即使在網路中斷的情況下，該系統也能確保可靠的資料傳輸。 ● 未發現任何損壞的特徵 ☐ 該工具基本上無法使用，存在許多損壞的功能和缺陷。 ☐ 一些功能損壞或出現錯誤 ☐ 小錯誤或問題 ☐ 基本功能正常，幾乎沒有錯誤或沒有錯誤 ☑ 功能齊全，無任何錯誤	3.3

	網路依賴: ● 沒有離線功能，必須連接到中繼伺服器 在地化和語言支持 ● 僅提供英語 ● 社群似乎沒有致力於語言在地化 移動無障礙 ● 不適用於行動設備，需要電腦才能使用終端機發送檔案。	
非技術用戶的可用性	易於安裝和部署 ● 需要 4 個步驟 ● 需要使用命令列 ● 維護良好的設定指南和常見問題解答 ● 具有廣泛的安裝、使用和安全訊息 ● 安裝耗時不到 2 分鐘 ● 對於新用戶來說，弄清楚 Tor 等蟲洞支援的可用標籤/功能可能比較困難。 使用者入門體驗 ● 擁有廣泛的文檔，包括安裝、實施和支援、tor 支援等。 ● https://magic-wormhole.readthedocs.io/en/latest/ 所需的技術經驗水平 ● Yes，唯一令人生畏的部分是導航終端，但這並不難。 ● 嚴重依賴終端機中的命令列	4.3
安全和隱私強度	加密標準 ● Magic Wormhole 代碼包含 16 位熵，因此暴力猜測的可能性極小（機率為 65,536 分之一）。 ● 如果當局控制網路或郵件伺服器，則可能會被封鎖。 審查彈性 ● 配置 Tor 後，可以在審查或監視嚴格的地區使用 ● 不包含內建規避工具 漏洞：抵禦已知威脅的能力 ● 如果攻擊者攔截流量並重複猜測代碼，則可能引發中間人 (MitM) 攻擊。較長的代碼 (--code-length=4) 可以降低此風險。 ● Magic Wormhole 的集合伺服器是單點故障 (SPOF)，容易受到 DoS 攻擊，攻擊者可以暴力破解銘牌來破壞金鑰交換，但該協定包含一個「許可」功能，允許工作量證明挑戰（例如 HashCash）來緩解此類攻擊。 與已知標準的比較	4.6

	● 與 TLS 或 PGP 等更強大的系統相比，Magic Wormhole 中使用 16 位元程式碼稍微不安全。 ● Magic Wormhole（NaCl「秘密盒子」）中使用的加密技術強大可靠，適合小型、快速的通信 資料最小化 ● 僅處理必要的資料（檔案傳輸詮釋資料）。 隱私權政策的可近性和清晰度 ● 隱私權政策明確了資料處理，並提供了更安全和私密的考慮。 ● https://github.com/magic-wormhole/magic-wormhole-protocols/security/policy	
維護/永續性	社群支持 ● 社群很活躍，並且定期更新。 ● 這是e輕鬆獲得協助和提出問題，或從開發人員那裡找到解決方案 開發活躍狀態 ● 每月至少更新一次 ● 最後更新於2024年12月 ● 開發團隊對好的變化反應迅速。 資金和贊助 ● 沒有明確的政府資金 ● 似乎是由個人完成的，這可能支持中立 ● 整體財務穩定	3.0
性能/有效性和可靠性	測試環境設定： ● 裝置**:** 惠普 Envy x360 ○ 第 13 代Intel® i7 CPU ○ 16 GB RAM ● **Windows 11** ● 網路：4G網絡 使用者體驗觀察 ● 發送文件的載入時間較短 ● 使用電腦終端發送文件時回應略有延遲 速度和反應能力： ● 近乎即時的設定和初始化 ● 發送方和接收方輸入密碼/指令後，傳輸立即開始。 ● 使用過程中是否有明顯的延遲或延遲？ 資源使用： ● 對於小檔案傳輸來說最小，但對於大檔案傳輸來說會增加（1-5%的CPU使用率）。 ● 小檔案：10-50MB RAM，大檔案可達 200MB+ RAM。 網路效能：	4.5

	● 如果透過直接點對點 (P2P) 傳送，則會佔用全部可用頻寬。如果使用中繼伺服器，速度可能會因擁塞而變慢。 ● 延遲：較小檔案約為 3-20 毫秒，中等檔案約為 10-50 毫秒，較大檔案約為 100 毫秒以上，具體取決於中繼伺服器的使用情況（Tor）。 ● 頻寬使用量對於點對點連接來說是最大的，但受到中繼的限制（如果使用 Tor） 可靠性 ● 許多人相信 Magic Wormhole 是安全可靠的，並且在 Github 上有一個龐大的開發團隊協助改進該工具。	
部署注意事項：	開源與透明度： ● Yes，程式碼在 Github 上開放，可供獨立驗證 雲端部署與本地部署： ● 無需 AWS/Azure 即可在本地運行。 依賴項： ● 需要 Python，但不依賴 Docker 或資料庫 ● 依賴關係有明確記錄 部署後維護 ● 部署後易於維護。 ● Yes，修改 UI 很容易，但加密演算法可能需要更高的專業知識。 合併/可持續性： ● 此專案開放貢獻 ● 如果有好的更改，則將更改提交到主儲存庫相對容易。	
4. 測試場景		
如何使用（基本）	發送文件： ● 若要將文件傳送到另一台電腦，請輸入：**wormhole send [filename/filepath]** ○ 例如：wormhole send “C:\Users\person\abc.txt” ● 發送時將產生接收者需要的 “magic-code”。 接收文件： ○ 若要從另一台電腦接收文件，請輸入：**wormhole receive [magic-code]** ○ “magic-code” 由發送者提供。 ○ 預設情況下，wormhole receive [magic-code] 將檔案保存在目前目錄中 ■ 若要將檔案儲存到特定目錄或重新命名，請使用標籤：**--output-file [filename/filepath]**	

- 重新命名：
  - 例如：wormhole receive 7-chicken-monster --output-file "C:\Users\person\Downloads\received_file.txt”
  - 確保在重命名時接收的檔案保留其原始檔案類型（例如，如果檔案是 .png，則它應該保持為 .png）。
- 選擇目錄：
  - 例如：wormhole receive 23-purple-dragon --output-file "C:\Users\person\Downloads\”

```
PS C:\Users\npson> wormhole send "C:\Users\npson\Downloads\123.txt"
Sending 23 Bytes file named '123.txt'
Wormhole code is: 74-asteroid-spaniel
```

```
On the other computer, please run:

wormhole receive 74-asteroid-spaniel

ERROR:  Key confirmation failed. Either you or your correspondent
typed the code wrong, or a would-be man-in-the-middle attacker guessed
incorrectly. Try sending the file again.
PS C:\Users\npson>
```

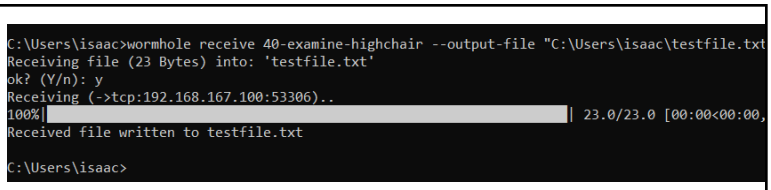
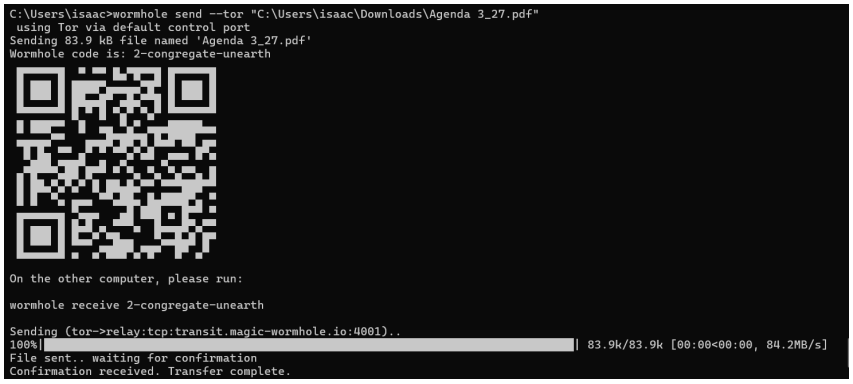
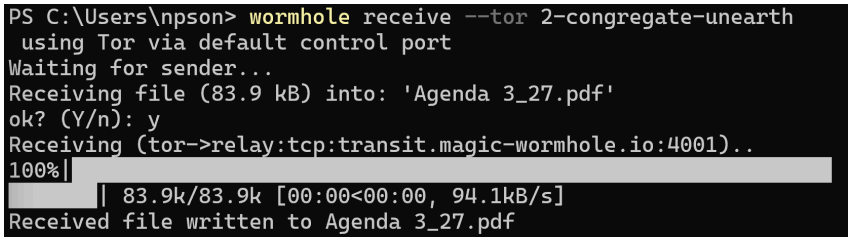
- 圖 *1*：編寫錯誤的 “magic-code” 會導致這種情況，這表示在錯誤輸入程式碼和防止攻擊者時具有安全性。

```
PS C:\Users\npson> wormhole send "C:\Users\npson\Downloads\123.txt"
Sending 23 Bytes file named '123.txt'
Wormhole code is: 40-examine-highchair
```

```
On the other computer, please run:

wormhole receive 40-examine-highchair

Sending (<-192.168.161.179:54771)..
100%|                                                                                | 23.0/23.0 [00:00<00:00, 22.8kB
/s]
File sent.. waiting for confirmation
Confirmation received. Transfer complete.
```

	•  圖 *2*: 上面的兩張圖片來自兩台不同的筆記型電腦, 顯示了檔案是如何發送到另一台筆記型電腦的。
透過 **Tor** 中繼網路使用魔法蟲洞	• 使用**--tor**命令列中的標誌, 以及圖 3 和圖 4 所示的參數, 用於透過 Tor 的中繼網路路由流量。這將隱藏用戶的 IP 位址, 從而實現匿名。 1. 要使用此功能, Tor 必須正在運行。  圖 *3*: 使用 Tor 的中繼網路透過蟲洞發送檔案以保持匿名。  圖*4*: 使用 Tor 的中繼網路透過蟲洞接收檔案以保持匿名。
5. 見解和建議	
主要發現	優勢: • 易於使用, 具有簡單的命令列介面, 用於文件和文字傳輸。 • 使用 PAKE(密碼認證金鑰交換)進行安全金鑰協商。訊息已加密, 伺服器無法讀取內容。 • 適用於不同的作業系統 • 支援文字、文件和目錄傳輸, 並提供 API 和庫支援以整合到其他應用程式。

	● 能夠使用 Tor 中繼網路匿名傳輸文件 弱點: ● 傳輸檔案時 IP 位址可能會洩露，但可以透過 Tor 使用 Magic Wormhole 來解決這個問題。 ● 預設中繼伺服器沒有正常運作時間保證，這可能會導致連線問題。 ● 蟲洞代碼中預設的 16 位熵使得攻擊成為可能（機率為 65,536 分之一） ● 預設中繼伺服器沒有正常運作時間保證，這可能會導致連線問題。 ● 難以自行託管/部署。
建議的改進	● 為技術和非技術用戶建立快速視訊教學和互動式文件。 ● 透過將 16 位元 PAKE 代碼增加到 32 位元或更多，可能的代碼數量呈指數級增長，使得暴力攻擊變得更加困難。 ● 魔法蟲洞目前使用固定的字典，以提高使用者可讀性。擴展字典或使用更長的短語可以在保持可用性的同時提高安全性。 ● 發送額外的驗證步驟（如電子郵件確認或二級金鑰）可以進一步加強安全性。 ● 雖然 secretbox 對於小消息來說是安全的，但整合額外的加密握手（如 TLS，用於傳輸安全性）或利用 Signal 的雙棘輪演算法進行前向保密可以進一步提高安全性。
替代工具:	● Croc ● Send
授權	GNU AGPL V3
成本/資源影響	總成本: ● Magic Wormhole 完全免費使用
為什麼這對威權環境中的公民社會有用？	● 跨平台和點對點:一個非政府組織的個人可以透過點對點傳輸輕鬆地將文件發送到另一個國家的非政府組織。它還支援多個平台，使其能夠在各種設備和作業系統上使用。 ● 隱私:魔法蟲洞不會洩露任何詮釋資料，這對於舉報人或在壓制環境中共享資料的個人來說是理想的選擇 ● 安全文件傳輸:Magic-wormhole 具有端對端加密功能，可用於與記者或法律團隊共用文件、媒體或其他報告。 ● 繞過審查:魔法蟲洞不依賴集中式基礎設施，在受限網路中具有更強的彈性。 ● 避免監視:文件端對端加密並直接在對等點之間傳輸