

網路安全的理論與實務

楊中皇 著

第十四章 AIDE與wxChecksums

<http://crypto.nknu.edu.tw/textbook/>

金 禾 圖 書

伴 您 學 習 成 長 的 每 一 天



- － 系統稽核軟體簡介
- － 安裝方法
 - AIDE
 - wxChecksums
- － 使用介紹
 - AIDE
 - wxChecksums



系統稽核軟體發展歷史

- AIDE 的發展承繼自 Open Source Tripwire。而 wxChecksums 是以跨平台視窗程式發展工具 wxWidgets 所開發，除了提供 Linux 系統的版本外，亦可以在 Windows 系統上安裝使用
- 最重要的共同功能就是可以偵測出被改變的檔案與入侵偵測系統主要的不同是，系統稽核著重於檢驗系統檔案的「完整性」



- 系統稽核軟體能在最短時間內查出異常的系統檔案，幫助系統管理者進一步追蹤並修復影響系統運作的檔案
- 這些系統稽核軟體所用來檢驗檔案完整性的技術，主要是以雜湊函數演算法，針對檔案運算出一組雜湊值作為檔案的檢查碼（**checksum**），以此來檢核比對檔案是否遭到修改



- AIDE主要支援的Unix-like系統
 - Linux
 - FreeBSD
 - NetBSD
 - OpenBSD
 - Apple Mac OS X
 - Solaris
 - IBM AIX
 - HP-UX
 - Cygwin



- wxChecksums對於大多數的Linux系統及Windows系統均提供支援
- 有別於AIDE僅具有命令列模式的操作方式，wxChecksums除了可在命令列操作外，還具備友善的視窗使用介面
- 如果要在Linux系統上使用wxChecksums，必須事先安裝X Window，並使用Gnome或KDE視窗環境，才能安裝執行wxChecksums的視窗模式

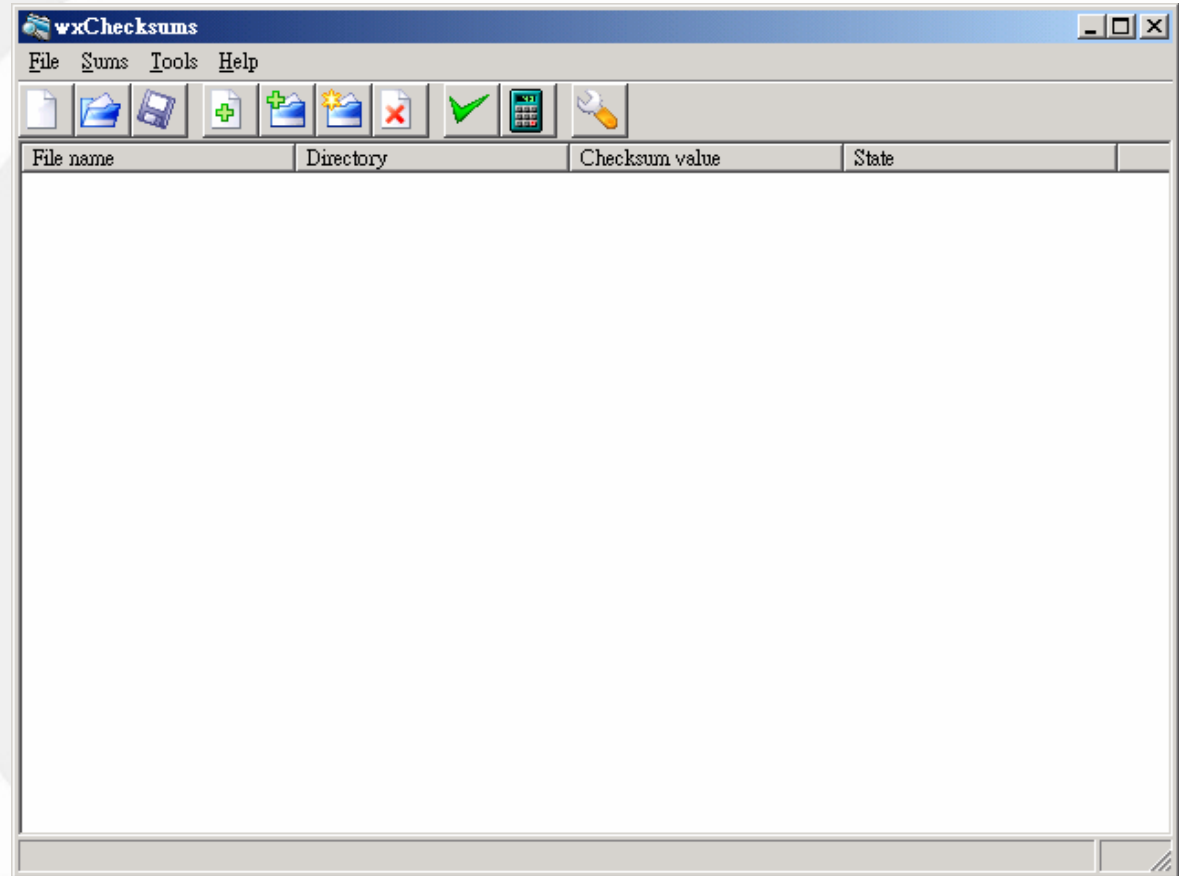


安裝方法 - AIDE

- 安裝AIDE最新版0.10版，RPM套件安裝的指令如下：
 - `rpm -ivh aide-0.10-2.1.fc3.rf.i386.rpm`
- 以Tarball套件安裝的話，首先要安裝Mhash，這是一套雜湊函數的函數庫，安裝指令如下：
 - `tar xvfz mhash-0.9.2.tar.gz`
 - `cd mhash-0.9.2`
 - `./configure`
 - `make`
 - `make install`
- 之後再安裝AIDE：
 - `tar xvfz aide-0.10.tar.gz`
 - `cd aide-0.10`
 - `./configure --with-config_file=/usr/local/etc/aide.conf`
 - `make`
 - `make install`



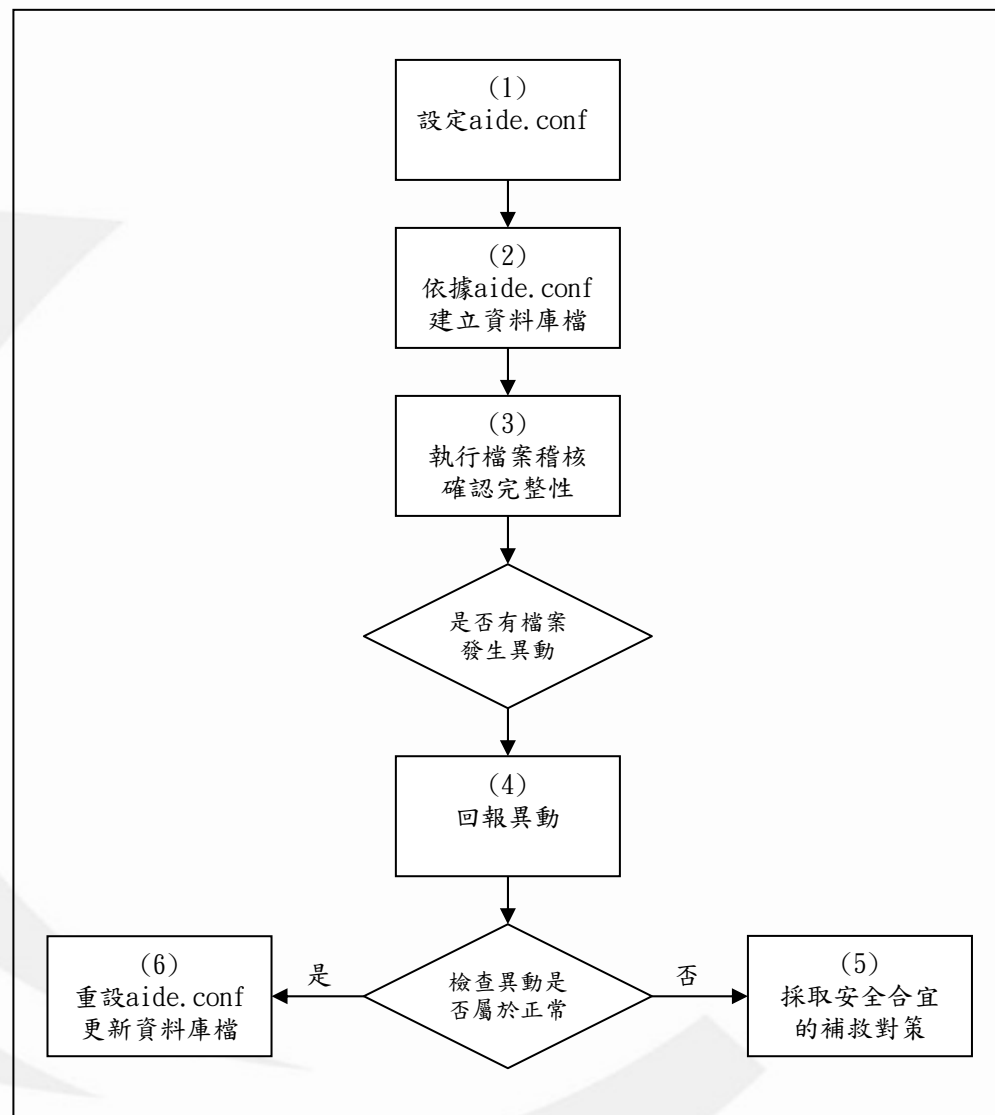
- wxChecksums 迄今最新的版本是 1.2.0，以官方網站上所專為 Windows 系統提供的安裝檔案安裝於 Windows XP
- 安裝過程非常容易，幾乎不需要更改任何設定，執行的主畫面如右圖





使用介紹 - AIDE

- 右圖是使用**AIDE**時的應用流程
- 系統管理者應將其視為例行性工作，定期稽核系統中重要目錄及檔案，以避免發生安全漏失，影響系統的正常運作





設定aide.conf檔

AIDE的稽核設定參數

#p: permissions	存取權限
#i: inode	檔案索引節點
#n: number of links	檔案鏈結數
#u: user	擁有檔案的使用者
#g: group	擁有檔案的使用者群組
#s: size	檔案大小
#b: block count	檔案區段計算
#m: mtime	檔案最後修改時間
#a: atime	檔案最後存取時間
#c: ctime	檔案建立時間
#S: check for growing size	檢查檔案大小的變動程度
#md5: md5 checksum	雜湊函數演算法
#sha1: sha1 checksum	雜湊函數演算法
#rmd160: rmd160 checksum	雜湊函數演算法
#tiger: tiger checksum	雜湊函數演算法
#R: p+i+n+u+g+s+m+c+md5	R參數代表同時設定這9個參數
#L: p+i+n+u+g	L參數代表同時設定這5個參數
#E: Empty group	空群組
#>: Growing logfile p+u+g+i+n+S	變動的log檔檢查參數
#haval: haval checksum	雜湊函數演算法
#gost: gost checksum	雜湊函數演算法
#crc32: crc32 checksum	雜湊函數演算法



設定aide.conf檔(說明)

- 通常參數的運用可以直接對目錄設定一組檢查參數，如下：
 - /etc p+i+u+g+md5
- 設定的位置並無限制，但建議設在aide.conf檔案的最下方，以方便和原先的預設內容區別。較有彈性的運用則是定義一個參數群組，再將群組名稱設定給欲執行稽核的目錄。aide.conf預設已經定義兩個群組，分別是All及Norm，設定的參數如下：
 - All=R+a+sha1+rmd160
 - Norm=s+n+b+md5+sha1+rmd160
- 如果要對某個目錄以某個參數群組作稽核，設定如下：
- /sbin Norm
- /etc Norm
- 若要忽略對某個目錄的檢查，只要在設定的目錄或檔案前加上!驚嘆號：
 - !/var/log



- 建立資料庫檔的指令為：
 - `aide -init`
- 自動產生的資料庫檔預設名稱為[aide.db.new](#)，將其更名為[aide.db](#)，這是AIDE預設的存取檔名
- 使用者亦可自行定義資料庫檔名，將資料庫更名之後，同時也要修改[aide.conf](#)檔存取資料庫的路徑設定
- 以vi編輯[aide.conf](#)檔如下內容：
 - `database=file:@@{TOPDIR}/doc/aide.db`
 - `@@{TOPDIR}`是引用TOPDIR這個變數的值，預設為
`/root/aide-0.10`
- 系統管理者需要注意資料庫檔的存放是否與[aide.conf](#)組態相同，否則會無法執行稽核。



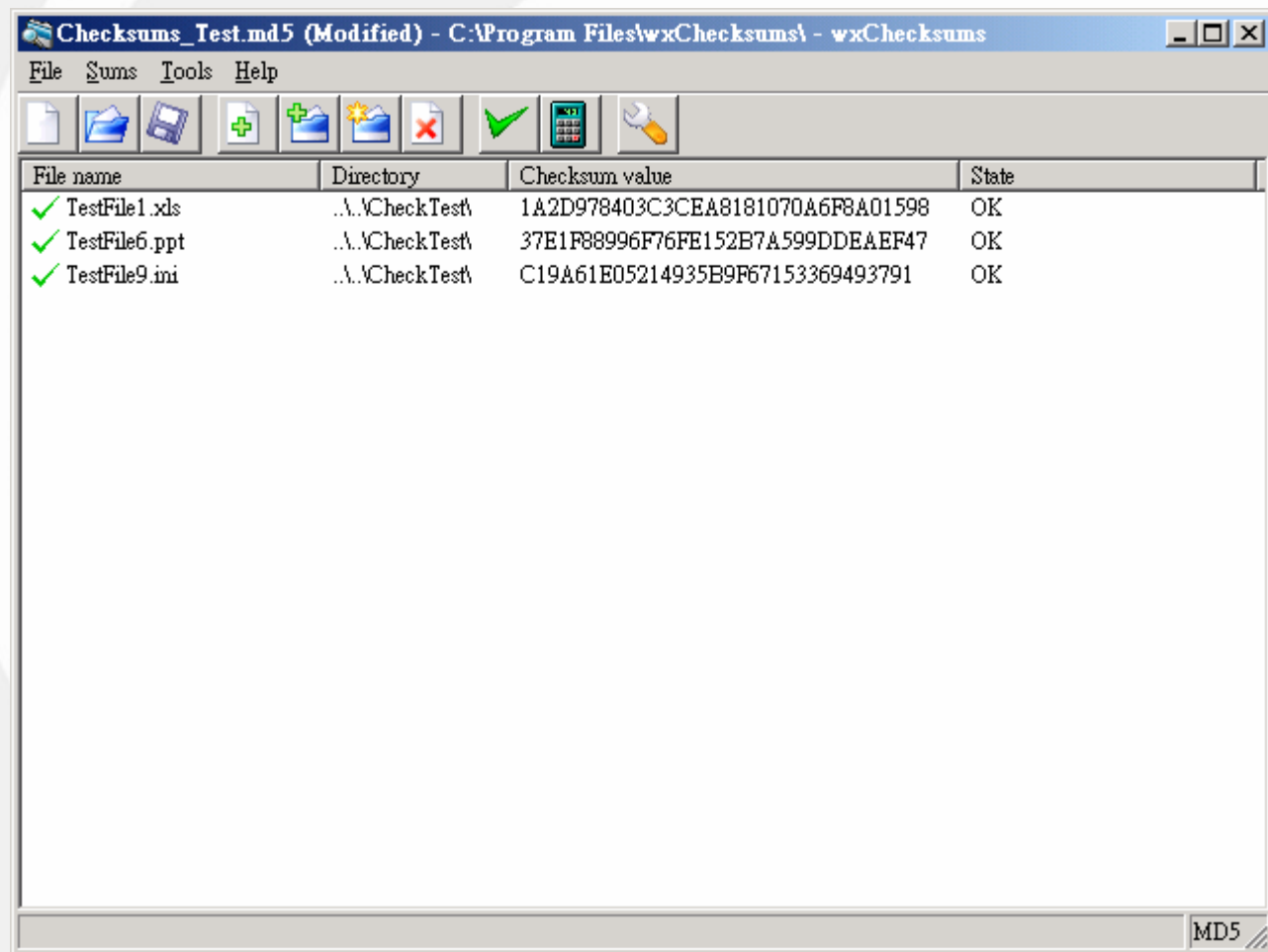
- 稽核檔案的指令為**--check**，在建立資料庫檔之前，在**aide.conf**中設定以下參數檢查/etc目錄：
 - /etc p+s+n+g+sha1
- 再使用**--init**指令建立資料庫檔後，爲了測試，在執行**--check**指令之前，先修改/etc/passwd檔的權限如下：
 - **chmod 664 /etc/passwd**
- 再執行稽核指令：
 - **aide --check**
- 就會回報異動訊息



- 在確認異動的檔案是屬於正常的變更之後，就可以執行**--update**指令更新資料庫檔：
 - **aide --update**
 - 實際上**--update**指令在更新時還會再進行一次**--check**指令的動作。
- 系統管理者如果針對同一群的目錄及檔案進行兩次不同參數的稽核，且將資料庫檔分別以不同的檔名儲存（前提是必須在**aide.conf**檔中增加設定），事後若需要比對兩個資料庫檔的異同，可以使用**--compare**指令如下：
 - **aide --compare**




- 建立新的檢查碼檔案
 - wxChecksums只有兩種雜湊函數檢查碼檔格式可以選擇，分別是MD5及SFV
 - 使用者可自訂欲儲存的目錄路徑
- 開啓並檢視既有的檢查碼檔
- 儲存啓用中的檢查碼檔
- 加入欲計算檢查碼的檔案





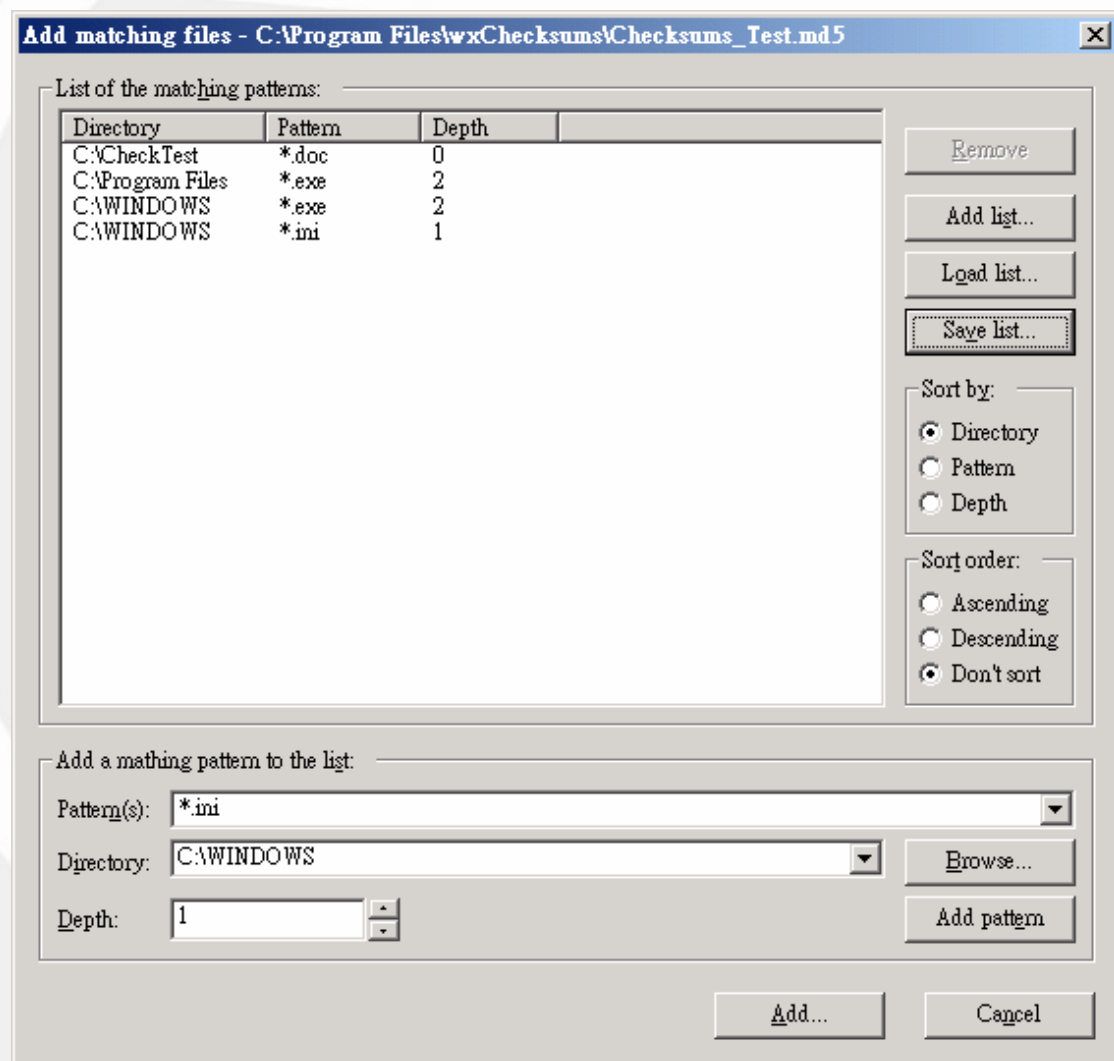
Checksums_Test.md5 (Modified) - C:\Program Files\wxChecksums\ - wxChecksums

File Sums Tools Help



File name	Directory	Checksum value	State
✓ TestFile1.xls	..\CheckTest\	1A2D978403C3CEA8181070A6F8A01598	OK
✓ TestFile10.ini	..\CheckTest\	1854CD17BBF81FD660BEC672B8669995	OK
✓ TestFile11.txt	..\CheckTest\	77C54C2BE84A17973D706390DD7965C1	OK
✓ TestFile12.txt	..\CheckTest\	77C54C2BE84A17973D706390DD7965C1	OK
✓ TestFile2.doc	..\CheckTest\	FF2943594E6071A89CF6B9B65F7EC0F1	OK
✓ TestFile3.doc	..\CheckTest\	10602CAFA40CDEE6B1B59C8267EBD579	OK
✓ TestFile4.exe	..\CheckTest\	755596EED318F23AC4F1FFCA94E0E43B	OK
✓ TestFile5.exe	..\CheckTest\	A9B4DA3A2DEC4D9C616685EB95005F2B	OK
✓ TestFile6.ppt	..\CheckTest\	37E1F88996F76FE152B7A599DDEAEF47	OK
✓ TestFile7.pdf	..\CheckTest\	200EC98F3EA2B66D6AC43156484D0300	OK
✓ TestFile8.pdf	..\CheckTest\	02400839397EDDC33323045467EB2DB4	OK
✓ TestFile9.ini	..\CheckTest\	C19A61E05214935B9F67153369493791	OK

MD5



- **[List of the matching patterns:]**：列出設定的樣本清單；顯示的樣本資料包含目錄（**Directory**）、樣本條件（**Pattern**）及目錄搜尋層級（**Depth**）
- **[Remove]**：移除選取的樣本
- **[Add list...]**：加入某個wpf檔的樣本清單
- **[Load list...]**：載入一個wpf檔的樣本清單
- **[Save list...]**：將設定的樣本清單儲存成wpf檔
- **[Sort by:]**：設定樣本清單依目錄、樣本條件或目錄搜尋層級排序顯示
- **[Sort order]**：設定樣本清單排序方式



- **[Pattern(s):]**：設定樣本條件，所謂的樣本條件，就是設定欲過濾的檔案，過濾條件的設定主要是以部分檔名或副檔名加上萬用字元“*”或“?”
- **[Directory:]**：設定欲檢查的目錄，一次只能增加一個
- **[Depth:]**：設定欲檢查的目錄的搜尋層級
 - 0表示沒有限制
 - 1表示只對該目錄的作檔案檢查，不包含底下的子目錄
 - 2表示對該目錄及其下一層的目錄作檔案檢查，下兩層以下的目錄則不在搜尋範圍
 - 依此類推



- **[Add pattern]**：將所設定的樣本條件增加到清單
- **[Add...]**：針對樣本清單的條件逐一作搜尋，計算所有符合條件的檔案暨檢查碼，並將檢查碼新增到使用中的檢查碼檔。



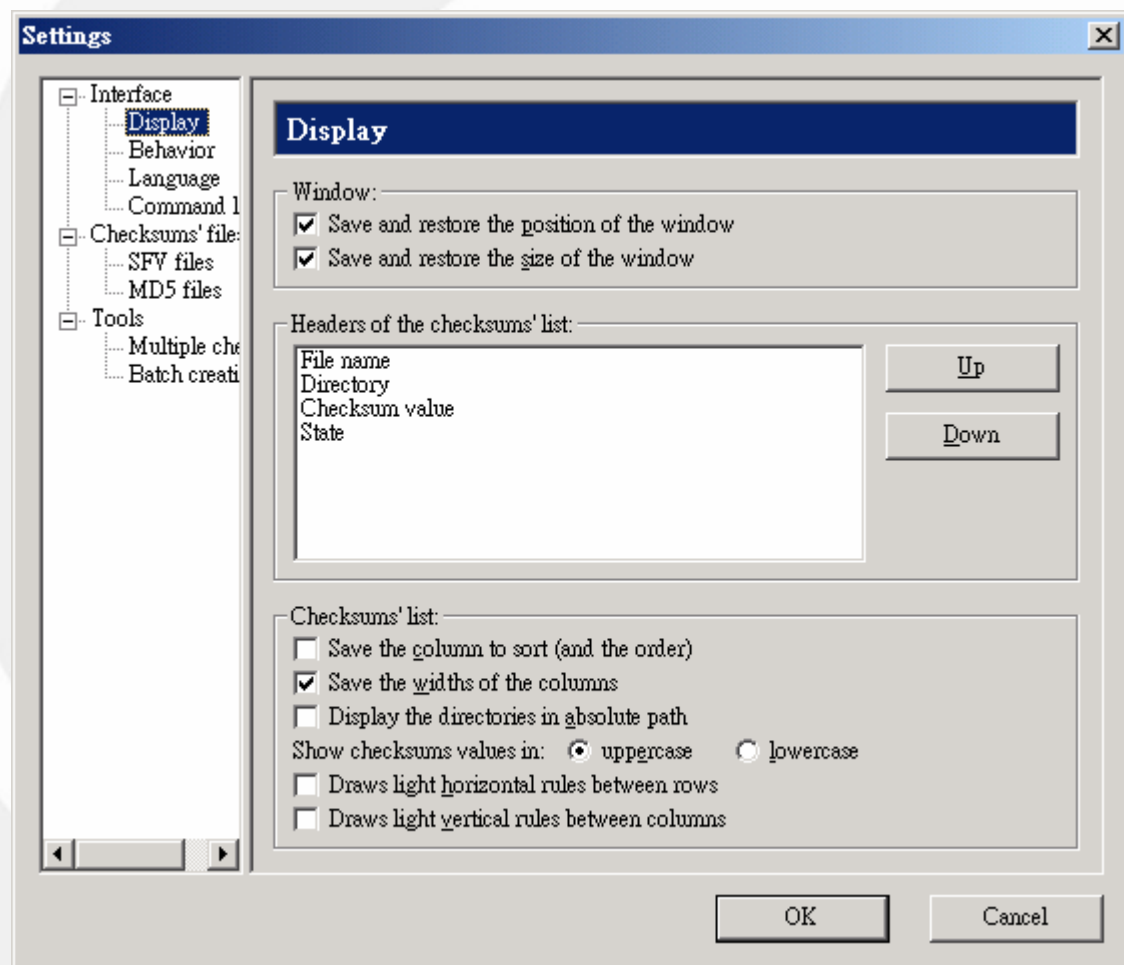
檔案稽核的檢查結果

Checksums_Test.md5 - C:\Program Files\wxChecksums\ - wxChecksums

File Sums Tools Help

File name	Directory	Checksum value	State
✓ TestFile1.xls	..\CheckTest\	1A2D978403C3CEA8181070A6F8A01598	OK
✓ TestFile10.ini	..\CheckTest\	1854CD17BBF81FD660BEC672B8669995	OK
✗ TestFile11.txt	..\CheckTest\	77C54C2BE84A17973D706390DD7965C1	Checksums differ
✓ TestFile12.txt	..\CheckTest\	77C54C2BE84A17973D706390DD7965C1	OK
✓ TestFile2.doc	..\CheckTest\	FF2943594E6071A89CF6B9B65F7EC0F1	OK
✓ TestFile3.doc	..\CheckTest\	10602CAFA40CDEE6B1B59C8267EBD579	OK
✓ TestFile4.exe	..\CheckTest\	755596EED318F23AC4F1FFCA94E0E43B	OK
? TestFile5.exe	..\CheckTest\	A9B4DA3A2DEC4D9C616685EB95005F2B	File not found
✓ TestFile6.ppt	..\CheckTest\	37E1F88996F76FE152B7A599DDEAEF47	OK
✓ TestFile7.pdf	..\CheckTest\	200EC98F3EA2B66D6AC43156484D0300	OK
✓ TestFile8.pdf	..\CheckTest\	02400839397EDDC33323045467EB2DB4	OK
✓ TestFile9.ini	..\CheckTest\	C19A61E05214935B9F67153369493791	OK

MD5





- 可針對wxChecksums的各項使用作細節設定
 - [Display]：定義視窗及檢查碼資訊的呈現方式
 - [Behavior]：設定wxChecksums的操作行為
 - [Language]：選取wxChecksums使用的介面語言，預設有英文及法文兩種
 - [Command line]：定義於命令列執行指令後的操作模式，可選擇是否以視窗介面顯示執行結果
 - [SFV files]：設定SFV檔的讀寫參數
 - [MD5 files]：設定MD5檔的讀寫參數
 - [Multiple check]：設定批次稽核的執行參數
 - [Batch creation]：設定批次建立檢查碼檔的執行參數



批次稽核

Check multiple checksums' files

List of files to check:

File name	Directory
Checksums_Test.md5	C:\Program Files\wxChecksums
Checksums_Test2.md5	C:\Program Files\wxChecksums
Checksums_Test3.md5	C:\Program Files\wxChecksums

Add...
Remove
Add list...
Load list...
Save list...

Sort by:
☒ File name
☐ Directory

Sort order:
☐ Ascending
☐ Descending
☒ Don't sort

Search for some files to check:

Named:

Look in: Browse...

Depth:

Search and add

Check Cancel

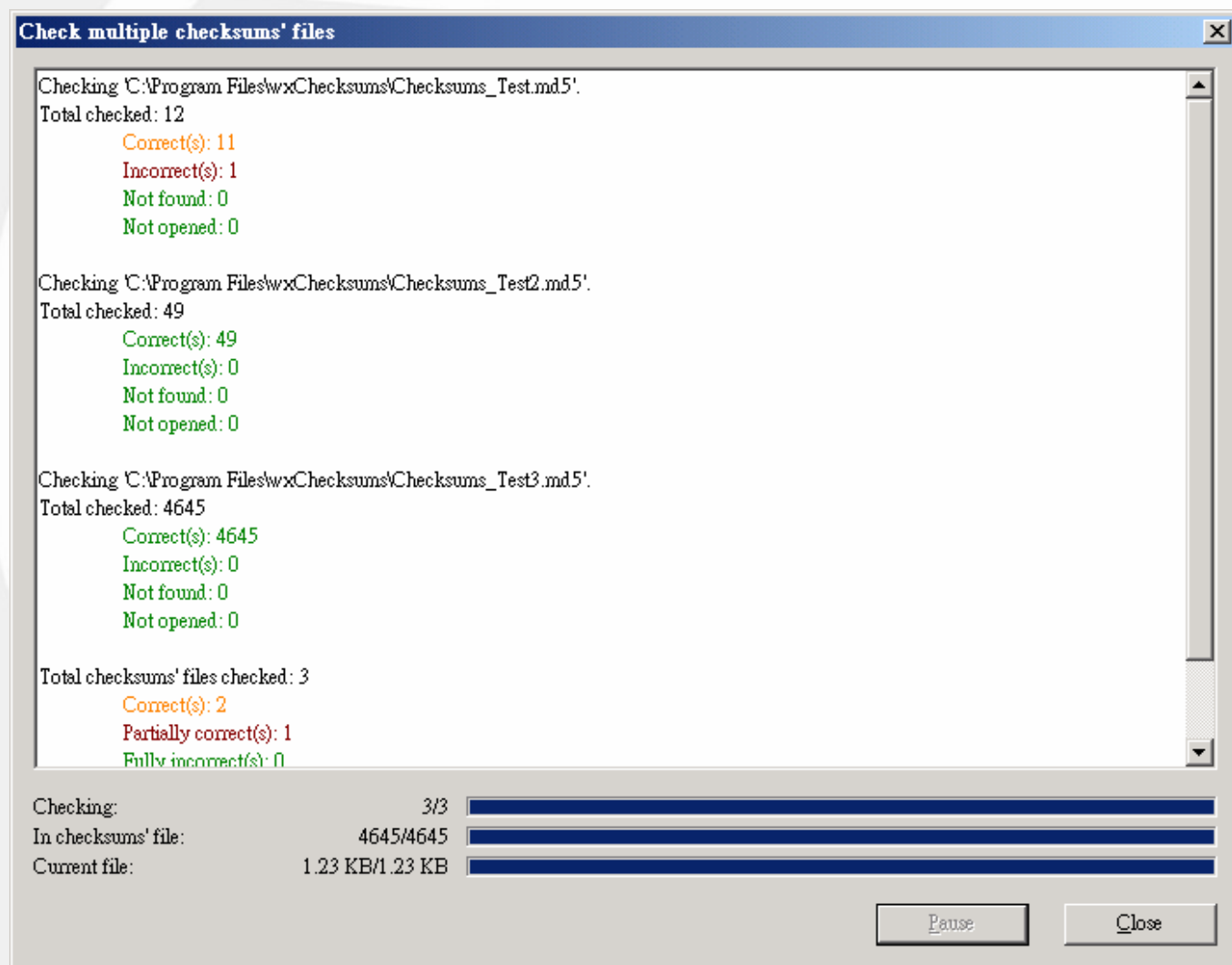


批次稽核說明

- **[List of files to check:]**：列出欲稽核的檢查碼檔清單
- **[Add...]**：新增檢查碼檔
- **[Remove]**：移除選取的檢查碼檔
- **[Add list...]**：加入某個檢查檔清單
- **[Load list...]**：載入一個檢查檔清單
- **[Save list...]**：將目前設定的檢查檔清單儲存成lst檔或txt檔
- **[Sort by:]**：設定檢查檔清單依檔案名稱或目錄排序顯示
- **[Sort order]**：設定檢查檔清單遞增或遞減排序，或不排序
- **[Named:]**：設定篩選的檢查碼檔名
- **[Directory:]**：設定欲搜尋的目錄
- **[Depth:]**：設定目錄的搜尋層級
- **[Search and add]**：依所設定的目錄及篩選條件搜尋檢查碼檔，並增加到清單
- **[Check]**：執行批次稽核



批次稽核的測試執行結果





批次建立檢查碼檔

Batch creation of checksums' files

List of files from which the checksums' files will be created:

File name	Directory
TestFile2.doc	C:\CheckTest
TestFile3.doc	C:\CheckTest
TestFile7.pdf	C:\CheckTest
TestFile8.pdf	C:\CheckTest

Add...
Remove
Add list...
Load list...
Save list...

Sort by:
☒ File name
☐ Directory

Sort order:
☐ Ascending
☐ Descending
☒ Don't sort

Search for some files:

Named:

Look in: Browse...

Depth:

Search and add

Create the following types of checksums' file:

☐ SFV ☒ MD5

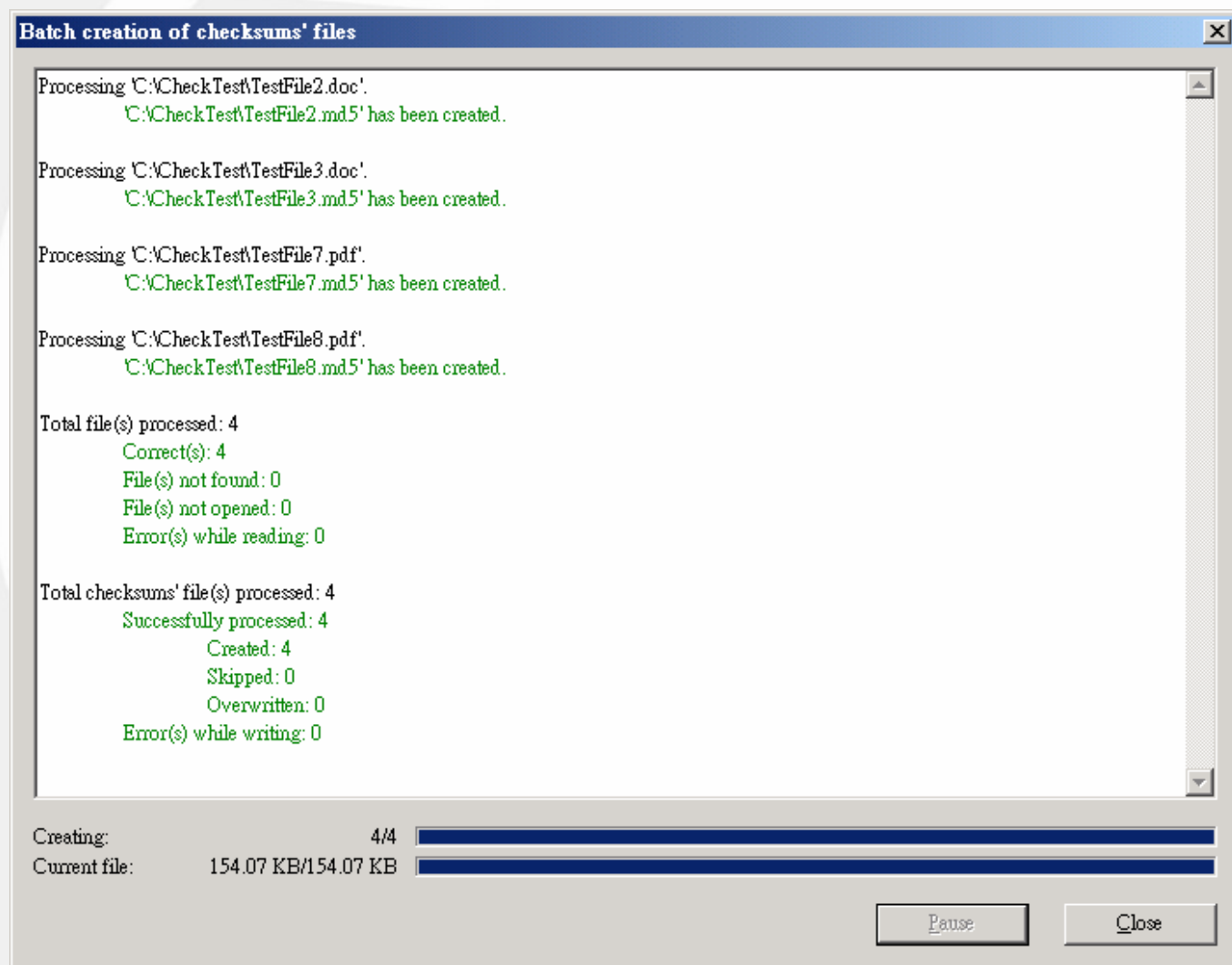
Options...

Create Cancel



批次建立檢查碼檔(說明)

- **[List of files from which the checksums' files will be created:]**：預備建立檢查碼檔的檔案清單
- **[Add...]**：新增欲建立檢查碼檔的檔案
- **[Remove]**：移除選取的檔案
- **[Add list...]**：加入某個檔案清單
- **[Load list...]**：載入一個檔案清單
- **[Save list...]**：將目前設定的檔案清單儲存成lst檔或txt檔
- **[Sort by:]**：設定檔案清單依檔案名稱或目錄排序顯示
- **[Sort order]**：設定檔案清單遞增或遞減排序，或不排序
- **[Named:]**：設定篩選的檔案名稱
- **[Directory:]**：設定欲搜尋的目錄
- **[Depth:]**：設定目錄的搜尋層級
- **[Search and add]**：依設定的目錄及篩選條件搜尋檔案，並增加到清單
- **[Create the following types of checksums' file:]**：選擇檢查碼檔建立格式
- **[Options...]**：可開啓建立檢查碼檔的進階設定
- **[Create]**：批次產生檢查碼檔





- Julien Couot, *wxChecksums 1.2.0 Manual*, <http://sourceforge.net/projects/wxchecksums/>, 2004
- Michael D. Bauer, *Building Secure Servers with Linux*, O'Reilly, 2002
- Rami Lehti, "The Aide manual", <http://www.cs.tut.fi/%7Erammer/aide/manual.html>
- 伊原秀明著, 蘇秉豐譯, *Tripwire for Linux 系統稽核*, O'Reilly, 2001年