秘密 真相 鑑識

AUTHOR-LIST: 王旭正 楊中皇
分類: 科學普通讀物 (SCIENCE BOOK)
PUBLICATION: 2012

2012

Secret, Truth, and Forensics

第三章 妙妙妙的整數

整數，生活中隨處可見，也時常用到，是再熟悉不過的數字。就一般人來說，任何數字的變化與應用，都是從整數出發，以為整數是數字的根。但有一派研究整數的人卻不這麼認為哦，在這些人的觀點裡，質數才是所有數字的根，並非整數也。這一派學者認定大於 1 的任何正整數，除了本身是質數外，非質數的數字也可由質數的乘積求得。原來，整數之中還存在如此巧妙的關係，那質數到底是什麼呢，就讓我們展開質數之旅，好好認識一下它！

3.1 質數的奧妙

你知道什麼是質數(Prime)嗎？所謂「質數」，是指任何大於1的整數，除了1和本身以外，沒有其它的因數，即是「質數」，否則稱為合數(Composite)。舉個例，2、3、5、7、11、13等，這些數字除了1和本身以外，你無法找到其它因數的存在，那麼我們會將此數稱為質數；如果還未了解，舉個反例，4、6、8、9、10、12等，這些數除了1和本身以外，是不是還有其它因數2、3、5存在，這些非質數的數，我們稱為合數。質數是一個很奇特的數字，它在數學上有很多的研究及應用，但可別以為只有在數學上才有質數的存在，自然界中，看似平常無奇的生命週期，卻藏著質數的應用，這樣的發現除了讓人驚奇外，卻也深深佩服自然的運作法則，是這麼的偉大卻平實。

蟬，大家對它的瞭解，就是在夏天裡聽到它們在伏在樹上，當中午人們正昏昏欲睡時，發出“唧唧鳴鳴”的喧鳴聲。夏天是蟬最活躍的季節。雄雌蟬交尾後，雌蟬會用它堅硬的產卵管刺入樹枝內產卵，蟬卵孵化成幼蟲後，便會離開生長的樹木掉進土裡，利用前腳挖入土壤，靠著吸取植物汁液成長，經過幾次蛻變脫皮後鑽出土壤，羽化成蟲。等交配季節一到，雄蟬就會利用歌聲吸引雌蟬進行交尾，繁衍下一代後便死去，形成蟬的生命週期。蟬的生命週期和質數有什麼關聯呢？你有這個疑問吧。

原來，位於食物鏈最底層的蟬，天敵眾多，此對生存造成了很大的威脅，為了種族生命的延續，牠們必須躲避天敵的攻擊，既然是天敵，註定無法反擊天敵的侵略。從生物演化論中，動物為了適應周遭環境，會進行演化，蟬面對狩獵者，牠們選擇躲避天敵，那怎麼躲避呢？想想看，如果你是蟬，會用什麼方式躲避？挖洞，還是學會能抗敵的防身術，其實答案很簡單，避開與天敵出現在同一時間，此時質數的觀念在蟬的生命週期可見一斑，還記得剛剛提到的質數概念嗎，質數是除了1和本身無其它因數的數，所以蟬誕生的週期若能選在質數週期，例如 3、5、7、11、13、17年等，則在該質數時間點上，除非相同的生命週期，否則該時間點內的天敵相對能減少許多。蟬利用了質數性質有效地避開與天敵同一時間誕

生於世上，大大增加生存的機會，你說自然界是不是很奇妙。世上真有蟬的生命週期是質數週期嗎？位於北美洲獨有的布魯德X蟬（Brood X）即屬於質數生命週期的蟬，它的生命週期高達17年，只為減少與天敵在世上相遇的機會，增加生命延續的可能，故有「質數蟬」之稱。

由自然界的生命演化，我們瞭解質數的奧妙，但僅由質數蟬認識質數，如同瞎子摸象，只知其一不知其二。我們需要對質數有更完整的認識，多方面的瞭解。過往不少數學家對質數進行許多的研究，譬如最大的質數是多少？該如何找出質數？讓我們站著巨人的肩膀上一探質數的全貌吧。

你能琅琅上口的質數有多少呢？2、3、5、7、11、13…，繼續唸下去何處是終點？一開始，你可能還可以應付，但隨著十萬位數、千萬位數，甚至是億萬位數，相信已不是那麼簡單可以確定數字是否是質數，到底哪個數才是最大的質數？還是質數是無限多個？可否給一個完整的證明？這個問題，西元300年前，著名的希臘數學家歐幾里得(Euclid)給了我們答案，在他的著作「幾何原本」中提到質數是否有限制的問題，且用數學理論證明質數有無窮多個。歐幾里得(Euclid)的證法是一種「矛盾證法」，他的論述重點在於「預先任意給定幾個質數，則有比它們更多的質數」條件下，反證有無限個質數，證明如下：

【證明】

假設質數是有限多個

令P是一個最大質數

Q為所有小於或等於P質數的乘積

$Q+1$表示Q除以任何質數均餘1，$Q = 2 \times 3 \times 5 \times 7 \times \ldots \times P + 1$

由上述可知

Q亦是質數且大於P

但命題假設質數是有限個且P為最大質數

上述證明得知Q是質數且大於P

命題假設不成立

故質數有無窮多個

這是一個很聰明的證法，利用矛盾反證質數有無窮多個，且質數存在於從 2 開始一連串質數相乘加 1 之中，但不一定是 $2 \times 3 \times 5 \times 7 \times \ldots \times P + 1$。在無窮多個質數中，我們需要一套有效找尋的方法，幫助我們快速找出質數。二千多年以前，一位古希臘數學家埃拉托斯特尼（Eratosthenes）針對找尋質數方法進行探究，他以土法煉鋼的方式，在一張羊皮紙上寫上自然數列之後，逐一將 2 的倍數、3 的倍數、5 的倍數等數字挖掉，因而找出首幾個質數。請想像一下，你手上有一大把的沙石，若想將石子留下去掉沙子，你會怎麼做？是不是拿塊布，戳幾個如沙子般大小的洞，將沙石包裹住，然後左右搖一搖，沙子不就順著洞漏出，而石子因洞口太小被保留了下來，埃拉托斯特尼法(sieve of Eratosthenes)也像是這般

原理，羊皮紙上將質數倍數的數字依序刪掉，如同篩子般將非質數的合成數去掉，篩選出質數，這雖然很費工，但卻不失為有效找出質數的好辦法。舉例說明埃拉托斯特尼法(sieve of Eratosthenes)，以找尋 1 至 60 以內的質數為例：

1. 列出範圍內所有質數。

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60

2. 找出範圍內 2 的倍數、3 的倍數、5 的倍數、7 的倍數等。

   2 的倍數：2、4、6、8、10、12、14、16、18、20、22、24、26、28、30、32、34、36、38、40、42、44、46、48、50、52、54、56、58、60。

   3 的倍數：3、6、9、12、15、18、21、24、27、30、33、36、39、42、45、48、51、54、57、60。

   5 的倍數：5、10、15、20、25、30、35、40、45、50、55、60。

   7 的倍數：7、14、21、28、35、42、49、56。

   11 的倍數：因剛找 2、3、5、7 的倍數時，便將 11 的倍數刪去了，接下應找 11×11＝121，但這已超出範圍了。

3. 將上述提到非質數因子刪除，留下質數。

	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47			
		53						59	

4. 利用「埃拉托斯特尼法(sieve of Eratosthenes)」，可以有效率地找出 1 至 60 範圍內所有質數，共 16 個：2、3、5、7、11、13、17、19、23、29、31、37、41、47、53、59。

這只是一個開端，後來也有許多數學家提出相關尋找方法，其中相當著名的，是 17 世紀初法國數學家馬林梅森尼(Marin Mersenne,1588~1648)，他提出了梅森尼質數(Mersenne Primes)。梅森尼最早接觸的是神學，1609 年開始在索邦大學鑽研神學，1611 年加入天主教行乞修士會，也就是後來的修道院，並成為法國天主教米尼瑪派教士。但他未放棄學業，仍繼續在尼就（Nigeon）與莫克斯（Meaux）接受教育。1614 年開始，在法國納維爾天主教修道院貢獻所學直到 1618 年，隔年返回法國巴黎並將自己的房子修建成修道院，漸漸地科學家往此修道院聚集，互相討論科學，成為了當時科學家聚會場所和資訊交換中心，後來此修道院被稱作「梅森尼學院」，日後更成為法蘭西學院核心人物像是費馬(Pierre de Fermat, 1601-1665)、帕斯卡(Pascal,1623–1662)、伽桑狄(Gassendi,1592–1655)等大數學家的開會處所。

梅森尼所發現尋找質數的方法其實相當的簡單，它只有短短一個式子 $2^n - 1$，梅森尼是如何得出計算此質數公式的呢，它的推導過程如下：

【推導】

1. 假設有一多項式 $x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \ldots\ldots + x + 1)$。此多項式涉及因式分解，不在本書討論範圍，我們只需知道多項式是成立的。

2. 令 $x^n - 1$ 是質數，因質數只有除了 1 和本身外，並無其它因數，由上式可知 $x - 1$ 必定等於 1。

3. 因 $x-1=1$，則 $x = 2$。

4. 當 $n = ab$ 並且 $a \leqq b$ ，又令 $x = 2^a$ ，
   則 $2^n - 1 = (2^a)^b - 1$
   $= x^b - 1$
   $= (x - 1)(x^{b-1} + x^{b-2} + \ldots\ldots + x + 1)$ 。

5. 如果 $2^n - 1$ 是質數，那麼 $x - 1$ 必定又要等於 1 。由此得 $2^a = 2$ ，即 $a = 1$。

6. 因 $a = 1$，則 $n = 1 \times b$，可知 $n=b$，符合質數條件：1 和本身以外無其它因數。故 n 必定是質數。

7. 因 n 為質數是在假設 2^n-1 為質數條件下成立，故可得 2^n-1 為質數且 n 為質數，質數公式由此可證。

綜合上述結果，梅森尼提出一條計算質數的公式：2^n-1 ，其中 n 為質數。利用質數公式，我們嘗試代入數字計算是否所得數字確為質數。

$n=2$，$2^2-1=3$ 為質數；

$n=3$，$2^3-1=7$ 為質數；

$n=5$，$2^5-1=31$ 為質數；

$n=7$，$2^7-1=127$ 為質數；

$n=11$，$2^{11}-1=2047=23\times89$，檢驗發現，2047 除了 1 和本身因數外，還包括 23 和 89 二個因數。

梅森尼質數在代入 2、3、5、7 等質數時，雖計算的結果都為質數，但當 n=11 時，所得出的結果 2047 卻能分解成 23 × 89 二個因數，並不符合質數條件。由上檢驗可知，梅森尼質數是計算質數方法，但卻是屬於計算質數的「必要」條件，非是「充分」條件，無法完全滿足所有條件；亦即，在某些情況下，梅森尼質數計算出來的結果，不一定是質數。

結果雖不是完美，但梅森尼在於尋找質數的研究為後人開了一條大路，他用盡一生時間找出所有的質數，並建立質數公式 2^n-1，雖然質數公式後來檢驗無法完全滿足所有的條件，但現今我們仍會使用到梅森質數公式，主要原因在於現今電腦系統採用二進制，以 0 和 1 構成數位世界，質數公式剛好符合電腦二進制需求，配合現代電腦高速運算能力，找尋的質數越來越大。資料顯示，2008 年找出的最大質數是由美國洛杉磯加州大學的數學團隊找出一個有一千三百萬位數的質數，他們運用 75 台安裝 windows XP 作業系統的電腦，算出第 46 個梅森尼質數，它是 2 的 4 千 3 百 11 萬 2 千 6 百 9 次方減 1($2^{43112609}-1$)，也是該團隊第八次發現新的質數。

長期和梅森尼書信往來討論數學問題的數學家費馬（Pierre de Fermat）在 1640 年提出過一條類似的質數公式。費馬是十七世紀最偉大的數學家之一，素有「業餘數學家之王」的稱號，雖然他在近三十歲時才開始認真專研數學，但他在數學領域的成就著實不凡。費馬質數公式為 $P=2^{2x}+1$，論證如下：

【證明】

1. 令 $n=ab$ ，且 b 是一個奇數。

2. 當 $x = 2^a$ ，則 $2^n + 1 = (2^a)^b + 1 = x^b + 1 = (x + 1)(x^{b-1} - x^{b-2} + \ldots\ldots - x + 1)$，由於 $2^n + 1$ 涉及因式分解，不在本書討論範圍，我們只需知道多項式可分解如上式。

3. 上式要成立，*b 必須*為奇數。

4. 由 $2^n + 1 = (x + 1)(x^{b-1} - x^{b-2} + \ldots\ldots - x + 1)$得知，在 *x* 不等於 0 情形下，$2^n + 1$ 結果並不是質數。

5. 欲使 $2^n + 1$ 是質數成立時，則 *n* 必定不能有奇因子存在，即 *n* 必定是 2 的乘冪。由此可知，費馬的質數公式為 $P=2^{2x} + 1$。

由費馬質數公式所產生的數值，是否一定是質數呢？我們經由土法鍊鋼方式逐一驗證：

x=0 時，*n*=1，$P_0 = 2^1 + 1 = 3$；

x=1 時，*n*=2，$P_1 = 2^2 + 1 = 5$；

x=2 時，*n*=4，$P_2 = 2^4 + 1 = 17$；

x=3 時，*n*=8，$P_3 = 2^8 + 1 = 257$；

x=4 時，*n*=16，$P_4 = 2^{16} + 1 = 65537$。

x=5 時，*n*=32，$P_5 = 2^{32} + 1 = ??$

當 *x* 為 0、1、2、3、4 時，由於數值不大，容易檢驗數值是否為質數，至 x=4 時，所得的數皆為質數。但當 *x*=5 時，*n* 為 32，所得的數並非質數。為什麼 x=5 在當時未被檢驗出是合數呢？原因是，以費馬當時的環境，要計算 2^{32} 是相當耗時費力，可說是不可能的任務。因為這個數字實在太大了，很難以證明 *x*=5 時，代入質數公式所得到的數是否為質數或是合數，就連費馬本人也只驗證到 x=4，*n*=16。於是費馬根據前幾項數值驗證過後皆為質數，便猜測只要是利用這個公式計算出來的數值，一定是質數，而費馬質數公式也成為有名的費馬猜想。

最先證明費馬猜想的人，是十八世紀瑞士大數學家歐拉（Euler，1707~1783）。1732 年，歐拉針對費馬猜想提出驗證方法，證明利用費馬質數公式所產生的自然數不全是質數，證明如下：

【證明】

1. 令 $a = 2^7$ 且 $b = 5$，
   則 $a - b^3 = 3$。

2. 因 $1 + ab - b^4$
   $= 1 + (a - b^3)b$
   $= 1 + 3b$
   $= 2^4$

3. 故 $2^{32} + 1$
   $= (2a)^4 + 1$
   $= 2^4a^4 + 1$
   $= (1 + ab - b^4)a^4 + 1$
   $= (1 + ab)a^4 + (1 - a^4b^4)$
   $= (1 + ab)(a^4 + (1 - ab)(1 + a^2b^2))$。

4. 由 $1 + ab = 641$ 可知 641 可整除 $2^{32} + 1$，故 $2^{32} + 1$ 不是質數。

現今電腦計算速度飛快，找出 $2^{32}+1$ 的因數不是難事，$2^{32}+1 = 4294967297 = 641 \times 6700417$，這樣的結果直接否定 $2^{32} + 1$ 為質數的看法，但未結束，透過電腦傑出的運算能力，試著從費馬質數公式中是否還能找出其它質數。結果，目前只限於 $x = 0$、1、2、3、4 共 5 個質數，沒有其它質數能由費馬質數公式產生，另外也無數學家能提出數學方法證明費馬質數公式只有 5 個質數。

找尋質數現今不再只是單純數學問題，密碼學家利用找尋質數的困難，將此概念運用在密碼學上，建構出強韌安全的密碼系統。它的應用是將兩個很大的質數相乘，並從大質數相乘後的大整數反向找出相乘的兩質數，我們由梅森質數及費馬質數檢驗知道，兩質數相乘是相當容易，但若要將合數積反向推估是由哪兩質數相乘，難度是很高的，所以根據大數分解的困難度，密碼系統的安全性高低便建立在找尋質數難易度上。像是 Diffie-Hellman 密鑰交換、RSA 加密、ElGamal 數位簽章等皆是利用大數分解困難度建構密碼系統。故當破密者欲解開密碼系統取得加密資訊時，需要花上很長時間計算才能解密，將這樣的困難度運用在密碼學上，就能大大提升密碼系統的安全性。密碼學和數學已是息息相關密不可分，意料之外的，數學家們鑽研數學問題不再只是單純數學問題，也實際運用在生活上，形成保護重要資料的幕後功臣。

3.2 有趣的質數

介紹至此，你是不是對質數有點著迷了。它的魅力絕對不止於此，就像尋寶一樣，我們沿著前人畫下的地圖幻想著質數寶藏前去，尋寶過程隨時都能有新發現，這些發現衍生出新的故事，寶藏依然還在尋找。3576863126462165676291 37，你能從中找出任何規律嗎？很難看得出來吧，向你揭開謎底，此一長串的數字是可以由左至右依序拿掉一位數，仍然是質數的最大質數。請你再試一個質數73939133，與上一質數相反，73939133是從反方向由右至左依序拿掉一位數，仍然是質數的最大質數，如表3-1所示，質數的規律是不是很迷人呢。

表3-1　質數的規律

質數	
由左至右拿掉一位數	由右至左拿掉一位數
3576863126462165676291 37	73939133
576863126462165676291 37	7393913
76863126462165676291 37	739391
6863126462165676291 37	73939
863126462165676291 37	7393
63126462165676291 37	739
3126462165676291 37	73
126462165676291 37	7
26462165676291 37	
6462165676291 37	
462165676291 37	
62165676291 37	
2165676291 37	
165676291 37	
65676291 37	
5676291 37	
676291 37	
76291 37	
6291 37	
291 37	
91 37	
1 37	
37	

7	

質數能有今天的成果，是憑著數學家對它的熱情，付出了時間、精力，莫不想對質數有更一番徹底的研究。還記得費馬猜想嗎？質數性質的猜想還有一位數學家提出，為哥德巴赫猜想(Goldbach Conjecture)。哥德巴赫（Goldbach，1690-1764），他原本是法律系畢業的學生，之後才專研醫學和數學。1725 年旅居俄國，因才華出眾，被推薦出任彼得堡科學院院士和兼任秘書。1742 年，他被德國任命為駐莫斯科外交公使。在遊歷歐洲期間，哥德巴赫認識許多數學家，像是戈特弗里德·威廉·萊布尼茨（Gottfried Wilhelm Leibniz）、白努利（Bernoulli）家族等，一群數學家，試著想像，他們熱烈討論數學的畫面，是不是也想加入呢，一起探討數學，哥德巴赫也就如此，更加引發他對數學的興趣，由其是數論的研究，他貢獻更是顯著，哥德巴赫猜想便是其一。

1942 年哥德巴赫對奇數 = 奇數 + 奇數 + 奇數這一數學常理感到興趣，利用一些數字測試之後，發現一個更完美的現像，奇數 = 質數 + 質數 + 質數，如表 3-2 所示。

表 3-2　奇數與質數的關聯表示

質數	計算式			
9	=3+3+3			
11	=3+3+5			
13	=3+3+7	=3+5+5		
15	=3+5+7	=5+5+5		
17	=3+3+11	=3+7+7	=5+5+7	
19	=3+3+13	=3+5+11	=5+7+7	
21	=3+5+13	=3+7+11	=5+5+11	=7+7+7
23	=3+3+17	=3+7+13	=5+5+13	=5+7+11
...	...	...	...	...

經過無數的檢驗，證實奇數與質數存在這般奧妙的規律，哥德巴赫非常高興的寫了信，將發現的現象告訴他的好友，同為數學家的歐拉。信中寫著：「任何一個不小於 9 的奇數均可寫成三個質數之和。」詢問歐拉這是否是一般現像，想請歐拉證明或否定他所發現的規律。歐拉的回信中說：「任何不小於 9 的奇數都可寫成三質數之和，我無法針對你的發現提供嚴謹證明，但我相信這是正確的結論。」另外歐拉也提出類似的規律：任何不小於 6 的偶數也可寫成二質數之和。

由於古人對偶數的定義有不同看法，2 既是偶數也是質數，但當時 2 是不是偶數、質數無法有統一認定，所以 4 = 2 + 2 與 7 = 2 + 2 + 3 可以表示成兩質數與

三質數之和，但此命題內，二者均被排除在外，未列入命題之中。三質數之和及二質數之和，因偶數排除在外而獲得解決，此兩道問題後來便就是有名的「哥德巴赫猜想 (Goldbach Conjecture)」。

哥德巴赫猜想是近代三大數學難題之一(四色猜想、費馬最後定理、哥德巴赫猜想)，從發表以來的 200 多年仍無人能證明它，這實在是一大挑戰，不過數學家就是憑著對數學的熱情，儘管困難，仍然不斷嘗試證明哥德巴赫猜想。歷年欲征服哥德巴赫猜想的數學家們，終於經歷無數次的計算與檢驗下，有了成果。率先提出哥德巴赫猜想的證明方法，是 1920 年挪威數學家布郎（Brun）。

布郎對「任何不小於 6 的偶數都可寫成二質數之和」提出證明方法，他不直接證明一個偶數等於二個質數相加，而是利用循序漸進的方式，提出名為「9+9」的定理：「一個偶數可以寫成兩個數字之和，其中每一個數字最多只有 9 個質因數」。定理「9+9」的提出，使哥德巴赫猜想的證明往前跨了一大步，提供日後研究哥德巴赫猜想證明的數學家們一個新的方向。朝著此方向努力下，有關證明哥德巴赫猜想的方法發表不少，如 1924 年德國數學家拉德馬赫(Hans Rademacher,1892-1969)證明了(7+7)；1932 年，英國數學家愛斯特曼(Estermann)證明了(6+6)；1938 年，蘇聯數學家布赫斯塔勃(A. A. Buchstab)證明了(5+5)，於 1940 年，他又證明了(4+4)，遵循布郎方法證明哥德巴赫猜想的方法整理如表 3-3：

表 3-3　證明哥德巴赫猜想的相關定理方法

年代	數學家	定理
1920 年	挪威布郎	9+9
1924 年	德國拉德馬赫	7+7
1932 年	英國愛斯特曼	6+6
1938 年	蘇聯布赫斯塔勃	5+5
1940 年	蘇聯布赫斯塔勃	4+4

1941 年是數學家突破哥德巴赫猜想證明關鍵的一年。1941 年，蘇聯數學家林尼克(Yu. V. Linnik)發明了「大篩法」，證明每一個充分大的數可以用兩個質數和 2 的數次方來表示。1948 年，匈牙利瑞尼(Alfred Renyi,1921-1969)採用了林尼克的方法，提出了(1+c)，c 代表某一個大數目。1962 年，中國的潘承洞證明了一個偶數必定可以寫成一個質數加上一個由 5 個因子所組成的合成數。後人將其簡記為(1+5)。1963 年，中國的王元和潘承洞分別證明了(1+4)。1965 年，蘇聯的維諾格拉道夫(A. I. Vinogradov)證明了(1+3)。1966 年，中國的陳景潤證明了(1+2)，這一證明的提出，已離哥德巴赫猜想只剩一步的距離，200 多年的努力眼看夢想即將實現，但這一步的距離，直到今日還未有人能跨出，無法突破(1+2)，這亦是世上目前對「哥德巴赫猜想」證明的最佳結果。以大篩法為基礎提出哥德巴赫猜想證明數學家如表 3-4：

表 3-4　以大篩法為基礎的哥德巴赫猜想證明

年代	數學家	定理
1941 年	蘇聯林尼克	大篩法
1948 年	匈牙利瑞尼	1+c，c 是大數目
1962 年	中國潘承洞	1+5
1963 年	中國王元和潘承洞	1+4
1965 年	蘇聯維諾格拉道夫	1+3
1966 年	中國陳景潤	1+2

孿生質數

孿生的兄弟，你會聯想到什麼？臉蛋長的一樣、聲音一樣、肢體動作一樣等等，他們長得非常的相像，當然不會完全一樣，還是有所差別，只是很小。為什麼突然提到孿生兄弟，難道與質數有關嗎？

在無窮的質數中，存在所謂「孿生兄弟」的質數，二者的差距也是很小，發現此現象的數學家就是歐幾里得，在他的著作「幾何原本」中，提到此質數現像，在「無窮多的質數 p 中，p+2 也是質數」，即 (p，p+2) 兩數符合二者最小差距為 2 且都為質數的規則下，p、p+2 便稱為「孿生質數」，例如 (3，5)、(5，7)、(11，13) …等。在無窮盡的質數中，總共有多少對孿生質數呢？看似簡單的問題，實際上卻是相當不易，從歐幾里得時代開始直到現在，還沒有人能夠完全證明孿生質數是否無窮多個。這看似簡單卻又不簡單的問題，也形成有名的「孿生質數猜想(Twin Prime Conjecture)」。讓我們來試試能否從 10000 個自然數中，找出所有的孿生質數，看看這些孿生質數的個數變化是否存在著我們不知道的規律。

我們以 100 個數為一個範圍，每 1000 個數為一組，看看各組間的孿生質數個數有什麼變化，表列如表 3-5。

表 3-5　孿生質數

範圍：1~1000 共 10 組

範圍	孿生質數	個數
1~100	(3,5)，(5,7)，(11,13)，(17,19)，(29,31)，(41,43)，(59,61)，(71,73)	8
101~200	(101,103)，(107,109)，(137,139)，(149,151)，(179,181)，(191,193)，(197,199)	7
201~300	(227,229)，(239,241)，(269,271)，(281,283)	4

301~400	(311,313)，(347,349)	2
401~500	(419,421)，(431,433)，(461,463)	3
501~600	(521,523)，(569,571)，(599,601)	3
601~700	(617,619)，(641,643)，(659,661)	3
701~800		0
801~900	(809,811)，(821,823)，(827,829)，(857,859)，(881,883)	5
901~1000		0
小計		35

範圍：1001~2000 共 10 組

範圍	孿生質數	個數
1001~1100	(1019,1021) ， (1031,1033) ， (1049,1051) ， (1061,1063) ，(1091,1093)	5
1101~1200	(1151,1153)	1
1201~1300	(1229,1231)，(1277,1279)，(1289,1291)	3
1301~1400	(1301,1303)，(1319,1321)	2
1401~1500	(1427,1429)，(1451,1453)，(1481,1483)，(1487,1489)	4
1501~1600		0
1601~1700	(1607,1609)，(1619,1621)，(1667,1669)，(1697,1699)	4
1701~1800	(1721,1723)，(1787,1789)	2
1801~1900	(1871,1873)，(1877,1879)	2
1901~2000	(1931,1933)，(1949,1951)，(1997,1999)	3
小計		26

範圍：2001~3000 共 10 組

範圍	孿生質數	個數
2001~2100	(2027,2029)，(2081,2083)，(2087,2089)	3
2101~2200	(2111,2113)，(2129,2131)，(2141,2143)	3
2201~2300	(2237,2239)，(2267,2269)	2
2301~2400	(2309,2311)，(2339,2341)，(2381,2383)	3
2401~2500		0
2501~2600	(2549,2551)，(2591,2593)	2
2601~2700	(2657,2659)，(2687,2689)	2
2701~2800	(2711,2713)，(2729,2731)，(2789,2791)	3
2801~2900	(2801,2803)	1
2901~3000	(2969,2971)，(2999,3001)	2
小計		21

範圍：3001~4000 共 10 組

範圍	孿生質數	個數
3001~3100		0
3101~3200	(3119,3121)，(3167,3169)	2
3201~3300	(3251,3253)，(3257,3259)，(3299,3301)	3
3301~3400	(3329,3331)，(3359,3361)，(3371,3373)，(3389,3391)	4
3401~3500	(3461,3463)，(3467,3469)	2
3501~3600	(3527,3529)，(3539,3541)，(3557,3559)，(3581,3583)	4
3601~3700	(3671,3673)	1
3701~3800	(3767,3769)	1
3801~3900	(3821,3823)，(3851,3853)	2
3901~4000	(3917,3919)，(3929,3931)	2
小計		21

範圍：4001~5000 共 10 組

範圍	孿生質數	個數
4001~4100	(4001,4003)，(4019,4021)，(4049,4051)，(4091,4093)	4
4101~4200	(4127,4129)，(4157,4159)	2
4201~4300	(4217,4219) ， (4229,4231) ， (4241,4243) ， (4259,4261) ，(4271,4273)	5
4301~4400	(4337)	1
4401~4500	(4421,4423)，(4481,4483)	2
4501~4600	(4517,4519)，(4547,4549)	2
4601~4700	(4637,4639)，(4649,4651)	2
4701~4800	(4721,4723)，(4787,4789)，(4799,4801)	3
4801~4900		0
4901~5000	(4931,4933)，(4967,4969)	2
小計		23

範圍：5001~6000 共 10 組

範圍	孿生質數	個數
5001~5100	(5009,5011)，(5021,5023)，(5099,5101)	3
5101~5200		0
5201~5300	(5231,5233)，(5279,5281)	2
5301~5400		0
5401~5500	(5417,5419)，(5441,5443)，(5477,5479)	3
5501~5600	(5501,5503)，(5519,5521)	2

5601~5700	(5639,5641)，(5651,5653)，(5657,5659)	3
5701~5800	(5741,5743)	1
5801~5900	(5849,5851)，(5867,5869)，(5879,5881)	3
5901~6000		0
小計		17

範圍：6001~7000 共 10 組

範圍	學生質數	個數
6001~6100	(6089,6091)	1
6101~6200	(6131,6133)，(6197,6199)	2
6201~6300	(6269,6297)，(6299,6301)	2
6301~6400	(6359,6361)	1
6401~6500	(6449,6451)	1
6501~6600	(6551,6553)，(6569,6571)	2
6601~6700	(6659,6661)，(6689,6691)	2
6701~6800	(6701,6703)，(6761,6763)，(6779,6781)，(6791,6793)	4
6801~6900	(6827,6829)，(6869,6871)	2
6901~7000	(6947,6949)，(6959,6961)	2

範圍：7001~8000 共 10 組

範圍	學生質數	個數
7001~7100		0
7101~7100	(7127,7129)	1
7201~7300	(7211,7213)	1
7301~7400	(7307,7309)，(7331,7333)，(7349,7351)	3
7401~7500	(7457,7459)，(7487,7489)	2
7501~7600	(7547,7549)，(7559,7561)，(7589,7591)	3
7601~7700		0
7701~7800	(7757,7759)	1
7801~7900	(7877,7879)	1
7901~8000	(7949,7951)	1
小計		13

範圍：8001~9000 共 10 組

範圍	學生質數	個數
8001~8100	(8009,8011)，(8087,8089)	2

8101~8200		0
8201~8300	(8219,8221)，(8231,8233)，(8291,8293)	3
8301~8400	(8387,8389)	1
8401~8500	(8429,8431)	1
8501~8600	(8537,8539)，(8597,8599)	2
8601~8700	(8627,8629)	1
8701~8800		0
8801~8900	(8819,8821)，(8837,8839)，(8861,8863)	3
8901~9000	(8969,8971)，(8999,9001)	2
小計		15

範圍：9001~10000 共 10 組

範圍	孿生質數	個數
9001~9100	(9011,9013)，(9041,9043)	2
9101~9200	(9239,9241)，(9281,9283)	2
9201~9300		0
9301~9400	(9341,9343)	1
9401~9500	(9419,9421)，(9431,9433)，(9437,9439)，(9461,9463)	4
9501~9600		0
9601~9700	(9629,9631)，(9677,9679)	2
9701~9800	(9719,9721)，(9767,9769)	2
9801~9900	(9857,9859)	1
9901~10000	(9929,9931)	1
小計		15

總計 1~10000 範圍內，共有 205 個孿生質數

根據 1~10,000 所統計出的孿生質數，以 100 為組距畫成圖表，觀察質數個數的變化，嘗試從中尋找規律。如圖 3-1 所示，孿生質數的分佈圖中，從 1~100 範圍內有 8 個孿生質數，之後逐漸下降，似乎有遞減的趨勢；但到 801~900 時又出現 5 個孿生質數，之後孿生質數個數穩定的在 0 到 5 之間起伏，遞減的趨勢似乎不見了。以 100 為組距的統計圖中，觀察分佈圖曲線的起伏趨勢，孿生質數似乎是無窮盡的。

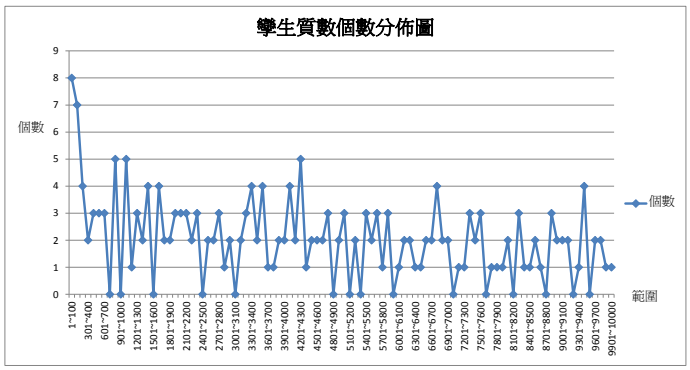


圖 3-1　以 100 為組距的統計圖

接著，我們以 1000 為組距，將 1~10000 的質數個數畫成圖表，再觀察個數的變化是否有規律。如圖 3-2 所示，孿生質數的分佈圖中，孿生質數的個數從 1~1000 範圍內有 35 個孿生質數，減少至 1001~2000 範圍內的 26 個，孿生質數個數逐漸遞減。從圖 3-2 可知，隨著整數愈多，每間隔 1000，孿生質數個數愈少，似乎有遞減的趨勢，若照此趨勢下去，孿生質數個數最後會到盡頭等於零？是否表示孿生質數並非無窮多？

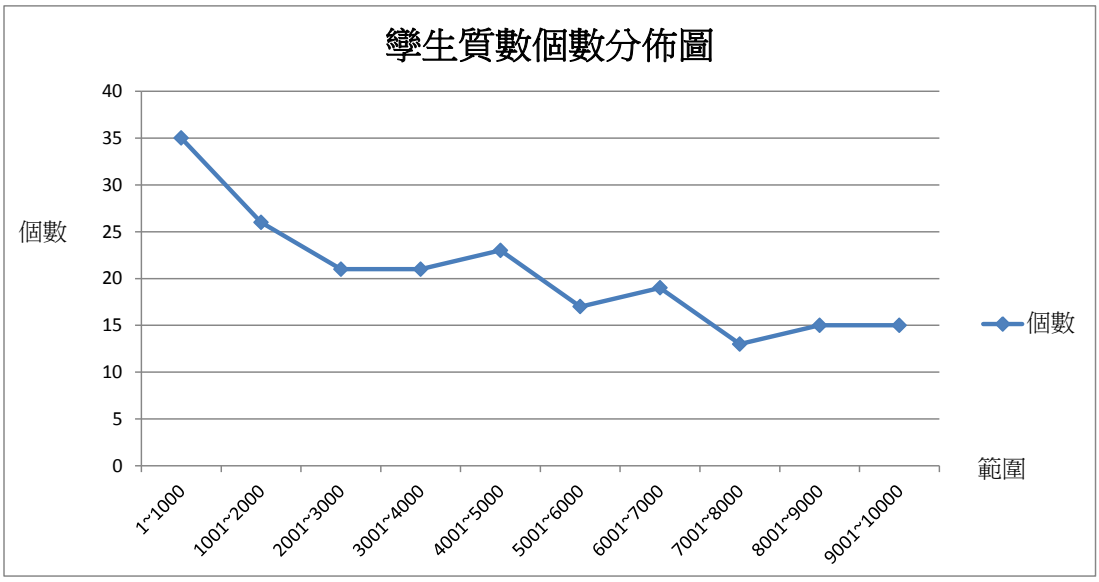


圖 3-2　以 1000 為組距的統計圖

以上我們從 1~10000 個整數，分別以組距 100 和 1000 作分析，嘗試找出孿生質數分佈的規律，從分佈情形判斷孿生質數是否無窮多。結果發現，從二者曲線的走勢來看，以組距 100 為分組的統計中，所得到的結論是孿生質數似乎無窮

多；以組距 1000 為分組的統計中，孿生質數個數有遞減的趨勢，最終似乎會等於 0。但這些結論，只是從無窮多的整數中，以 10000 個整數去找出孿生質數的個數分佈規律，且得出的結論是完全相反，更加說明孿生質數個數的變化是不易猜測。你可以往 10,000 以後的孿生質數再做統計，挑戰「孿生質數猜想」，雖然不簡單，但卻是個使你更加了解孿生質數的好機會。

3.3 質數魔術方陣與螺旋圖

質數魔術方陣

在第二章已經介紹過魔術方陣，一般的魔術方陣中，要求每一行、每一列甚至是對角線數字之和，都必須相等。而方陣愈大或提供的線索愈少，解開魔術方陣的難度也相對增加。上一章初步對魔術方陣有瞭解後，我們將擴大魔術方陣的應用，讓方陣中的數字不只是單純的整數數字，我們將數字限定為質數範圍，唯有符合質數的數字才能填入魔術方陣中，完成的方陣稱為質數魔術方陣。同魔術方陣的遊戲規則，亦即每一行、每一列、和對角線上的數字之和必須相等，唯一不同的地方是，數字需是質數的，是不是覺得很刺激阿，動手作看看，能否產生出完整的質數魔術方陣。如圖 3-3 所示為 3 階質數魔術方陣的例子：

(一)

157	13	211
181	127	73
43	241	97

(二)

191	17	239
197	149	101
59	281	107

圖 3-3　質數魔術方陣

質數魔術方陣不像一般魔術方陣，它填入的數字須是質數，非是任何數字均可填入，特別注意的是，除了填入數字必須符合質數的規定外，質數定義中，2是不能填入方陣中，也一定不會出現在質數魔術方陣。原因在於 2 雖是質數，但同時具有偶數性質，若在行列之和中出現 2，則該行列和的奇偶性質與其它行列和的奇偶性質必定不同，在此狀況下是沒辦法組成質數魔術方陣。如圖 3-4 所示，3 階魔術方陣中，當 2 所在的行列有 1 個偶數、2 個奇數，其和為偶數。第一列之和為偶數＋奇數＋奇數，其和為偶數，其它行列 3 個數字都是奇數，其和是奇數，任何一行列和必定不相等，無法構成魔術方陣。故質數 2 必定不會出現在質數魔術方陣中。

偶	奇	奇
奇	奇	奇
奇	奇	奇

圖 3-4　奇偶行列的魔術方陣

若我們要找尋 1~100 整數中，符合質數魔術方陣的條件會有多少個呢？經由我們的計算，可以知道 1~100 整數中質數魔術方陣只有一個，如圖 3-5 所示。但若嚴格的去定義，1 並非是質數，若將 1 排除掉，1~100 整數中，則全無符合質數魔術方陣的條件。

7	73	31
61	37	13
43	1	67

圖 3-5　質數魔術方陣

一般而言，質數魔術方陣不像魔術方陣，有規律可循，只要依序填入數字就可輕鬆完成，但質數魔術方陣只能辛苦地用土法鍊鋼的方式一個一個填入試誤。與魔術方陣不同點在於質數魔方陣將數字限定為質數，這樣的條件下，增加了質數魔術方陣完成的困難度，倘若利用電腦破解質數魔術方陣，也考驗著程式設計者的能力，只能設計良好的程式演算法，藉由加快程式檢驗的速度，縮短完成質

數魔術方陣的時間外，別無他法。無論是人工計算或是程式運算，在無通用的破解方法下，考驗著挑戰者的運算能力，可見質數真的是特別的數字。

質數螺旋圖

質數螺旋圖是數學家不經意發現的質數現象，在 1963 年，美國數學家烏蘭(Stanislaw Ulam,1906-1986)參加數學會議時，台上演講者滔滔不絕演講著質數論文，但內容卻枯燥無味無法引起烏蘭的興趣。在閒悶之於，烏蘭拿著演講者發的講義，開始在背面空白處塗鴨畫畫，一開始烏蘭只是隨意在紙張上編寫自然數，但就在他書寫過程中，忽然發現所編寫的自然數螺旋表中，似乎潛藏著一些規律，隱隱覺得規律是由質數所散發，仔細探究後，他驚覺地發現質數很有規矩的排列在一條直線上，宏觀來看，直線構成奇特的圖形而且不斷的重複著，自然數螺旋表愈大，奇特的圖形愈清晰可見，令人感到興趣的是，無論數字的範圍多大，這種現象依然存在。後人把烏蘭所發現的質數現象，稱為烏蘭螺旋，而質數螺旋圖也成為 1964 年 3 月美國科學雜誌的封面。

烏蘭所編寫的自然數螺旋表，從 1 開始，圖陣的中心先填入，從 1 的正上方填入 2，以逆時針方向螺旋狀依序填入自然數，、3、4、5…，一層一層的往外擴充，構成自然數螺旋圖，如圖 3-6 所示。接著將質數標示出來，可明顯發現烏蘭現像，即質數會排列在一條直接上，如(31,13,37,43,73)、(5,19,41,71)或(67,19,7,23,47,79)等，如圖 3-7 所示。烏蘭認為這是質數於自然數螺旋圖的規律，並不是隨機發生或偶然巧合。

100	99	98	97	96	95	94	93	92	91
65	64	63	62	61	60	59	58	57	90
66	37	36	35	34	33	32	31	56	89
67	38	17	16	15	14	13	30	55	88
68	39	18	5	4	3	12	29	54	87
69	40	19	6	1	2	11	28	53	86
70	41	20	7	8	9	10	27	52	85
71	42	21	22	23	24	25	26	51	84
72	43	44	45	46	47	48	49	50	83
73	74	75	76	77	78	79	80	81	82

圖 3-6　烏蘭螺旋圖

若僅保留質數，將非質數刪除，呈現的規律就更明顯，如圖 3-6 所示：

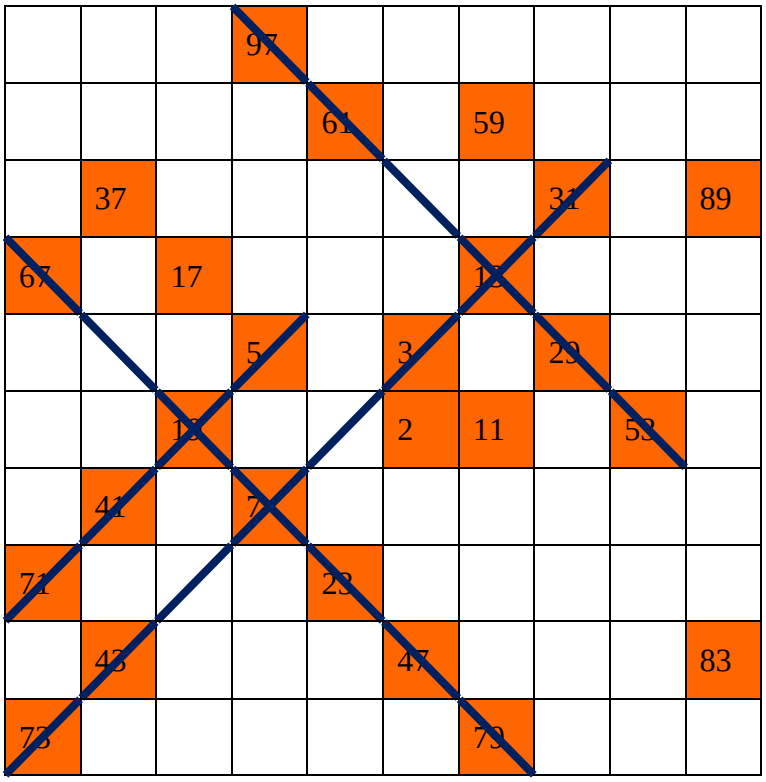


圖 3-7　呈現規則的烏蘭螺旋圖

若將自然數螺旋圖放大到 200＊200 的空間，內含 40000 個數字，並將質數以黑點表示，斜直線的排列將更為明顯，如圖 3-8 所示：

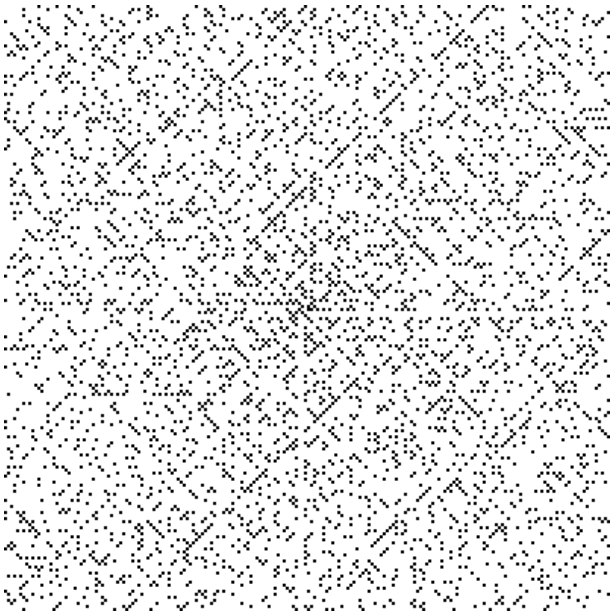


圖 3-8　200*200 空間的烏蘭螺旋圖

第九章 現代數位放大鏡

9.1 現代福爾摩斯

著名的美國影集—CSI 犯罪現場，這一部影集是描述一組 CSI 刑事鑑識科學家如何運用鑑識技巧順利偵破多起刑事犯罪的鑑識過程，如圖 9-1 所示。透過影集 CSI 犯罪現場，讓人一窺刑事案件偵辦過程精彩可倫的鑑識技術，瞧上劇中所用鑑識科學的專業工具及知識，真是讓人驚奇連連。在精彩的劇情下，可以很明白看出，鑑識人員除了具備專業知識外，還需有見微知著能力。經由收集的證據中，抽絲剝繭還原刑案現場經過，如指紋的採集、血跡/DNA 的鑑識進而鎖定嫌犯或採集現場遺留的玻璃碎片、彈殼還原彈道，這些皆是鑑識人員運用最先進的技術，加上多門專業知識而完成。其實，除了這些實體的證據之外，在資訊化時代，CSI 鑑識人員採證的另一項重點，即是蒐集虛擬的證據，這些虛擬的證據存在何處呢？就是大家每天生活幾乎離不開的資訊產品，而電腦更是最重要的鑑識來源。

圖 9-1　　CSI 犯罪現場影集

究竟對電腦進行鑑識可取得什麼樣的證據呢？首先，先請您想像一下以下的情境：

①今天逛了好多遊戲網站，功課都沒有做了，萬一被爸媽發現了，可就大事不妙了！

②這張照片實在拍的好難看，萬一被弟弟看到了一定會被笑，還是趕快刪掉吧！

③跟小美傳了好多簡訊，萬一明天手機被隔壁小華拿來看到就糗了，該怎麼辦呢？

相信大家想到的解決方法就是把所有相關的紀錄、檔案、簡訊，一律刪、刪、刪，全部丟到資源回收桶再清空吧？！如此一來，爸媽不會知道、弟弟不會發現、小華就不會看到，這樣秘密就不會被發現了。

但是，這樣子真的就安全了嗎？其實並不一定喔！就如同 CSI 犯罪現場裡的鑑識人員一樣，總是能在最微小的跡證當中尋找最大的可能。在現實生活當中，就算在電腦或者是手機上刪除了一些紀錄或檔案，鑑識人員還是有可能讓這些檔案紀錄重見天日的！

為什麼鑑識人員要特別把檔案和紀錄復原回來呢？這樣執行檔案刪除的動作不就失去意義了嗎？而且究竟鑑識人員用什麼方法，把已刪除掉的紀錄還原的呢？我們要再請您思考一下，下列的幾種情境：

①下課回來，馬上迫不及待地打開電腦，連上網路，昨天跑跑卡丁車又輸給小華了，小華最近技術變得那麼好，一定有在偷練，今天一定要再加緊練習，再不趕緊追，就輸大了。但是登入遊戲之後，咿？怎麼好像怪怪的.....我買的卡丁車怎麼不見了，還有金幣、裝備、寶物也都不見了！這下該怎麼辦才好，到底發生了什麼事。

②在網路拍賣上看到好喜歡的鞋子，是當季最流行的長靴，價錢比外面商店賣的還便宜好多喔！賣家說是因為清倉所以在大特價，庫存數量只剩下最後兩雙了，不趕快下標訂購怎麼行呢，免得被人搶標，那當然毫不猶豫地先下標訂一雙了！依賣家提供的帳戶將錢匯過去之後，滿懷期待能趕快穿上長靴去逛街，但，為什麼已經過了快一個月，鞋子都還沒有寄來呢？打賣家的手機變成了空號，寄發郵件過去也沒回應.....。

③小華剛剛在即時通密我，要我先幫他買遊戲點卡，再將帳號密碼傳給他就可以了。小華說是家裡沒人要顧家，所沒法出門才麻煩我，小華平常跟我就是麻吉，而且購買遊戲點數的錢，他說明天上學就會馬上還，麻吉有事相託，不幫這點小忙說不過去。但是隔天在學校遇到小華，為什麼他說他從來沒有要我幫他買點卡過呢？那昨天的那個”小華”又是誰呢？

④今天一早打開信箱收信，有一封 Google 寄來的信，上面寫著要重新檢測帳號安全性，必須輸入自己的帳號密碼，過了幾天，同學跟我說，我一直用自己的電子郵件地址寄垃圾信給大家，怎麼會這樣？

上述的情境在網路普及的現在時有所聞，和傳統的詐騙行為不同的是，受害

者損失的財產並不一定是金錢、飾品等實品，也有可能是線上遊戲的虛擬裝備、寶物、點數卡的帳號密碼等等，嫌犯改變以往的詐騙模式，變換了詐騙平台，轉用電腦和網路作為進行詐騙，獲取不當利益。為了遏止此種新型的詐騙行為，我國的刑法增訂了"妨害電腦使用罪"，對於電腦犯罪的相關行為制訂了罰則，如表 9-1 所列。

表 9-1　中華民國刑法(節錄)

條號	條文內容
第 358 條	無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。
第 359 條	無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。
第 360 條	無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。
第 361 條	對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。
第 362 條	製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。
第 363 條	第三百五十八條至第三百六十條之罪，須告訴乃論。

事實上，線上遊戲中所使用的帳號、角色、裝備、虛擬金幣等，都是電磁紀錄的一種，若利用不當方法，如密碼破解、側錄等而取得別人的帳號密碼，都是犯法的行為。這麼嚴重的問題，當然不能漠視，故此國家在刑法罪章訂定了相關法律條文，意旨嚇止非正當使用電腦的非法者。電腦紀錄非實品資料，一旦調查人員遇上相關電腦犯罪問題，該如何找出關鍵跡證，還原事件。在影集 CSI 犯罪現場中，鑑識人員憑藉著指紋、腳印、細小的痕跡，拼構出犯罪過程，釐清事件脈絡，並且佐為證據，逮捕非法的犯罪者。但是在電腦世界中，並無所謂的指紋、腳印、血液等實體證據，鑑識人員又該如何蒐集證據，不讓罪惡逍遙法外，繩之以法呢？

關鍵就在於遭刪除的檔案和紀錄喔！其實，經由一般方式刪除的檔案紀錄，是可以經由特殊方法復原的！而該如何復原這些檔案，又該如何讓這些檔案變成有效的證據，這些便是鑑識人員展現專業的地方了，搜尋關鍵跡證！在 CSI 犯罪現場當中，鑑識人員們就像是現代版的福爾摩斯，利用各種鑑識工具，在

犯罪現場尋找蛛絲馬跡，釐清事件來龍去脈。數位鑑識涵面廣泛，在下面的章節當中，先提出數位證據以及數位鑑識的概念和特性，唯先了解數位資料特性，才能進一步明瞭如何進行鑑識，否則，一個不注意則會破壞了數位證據，影響其證據力。接著以案例說明數位鑑識過程，透過案例操作，介紹以電腦、網路及手機的鑑識方法，進一步明白鑑識人員是如何在這些裝置中蒐集證據，最後，說明數位鑑識的敵手，反鑑識的概念，一來一往之間攻詰，深刻了解鑑識的精彩之處。

9.2 數位證據說話了嗎

什麼是數位證據，與數位鑑識間關係又為何牽扯一起。概念上數位證據是指：「電子儲存媒體內的數位資料，包括文字、聲音、圖片 、檔案、程式等，透過鑑識工具，將儲存於數位媒體中的資料進行萃取，經由萃取出的數位跡證，能還原事件，說明數位媒體上執行過哪些程緒。經由萃取的數位跡證可於法庭上提供加強非法者犯罪事實的證據。」在法庭之上，數位證據是否與原始的紀錄相同、是否曾遭人為因素竄改抑或其它因素變更原始內容，以及該證據能證明什麼是最受到關注的焦點。因此，要如何從這些新科技產物中取得法庭所需之證據，用以證明被告有罪或是無罪，就有所謂的電腦鑑識（Computer Forensics）或稱之為數位鑑識（Cyber Forensics）的科學技術領域發展，其目的在於專門負責蒐集、檢驗及分析數位證據。藉由保存電腦犯罪證據，並透過電腦採集有意義的證據資訊或從片斷資料描繪事件的大略情形以進行現場重建。至於數位證據和我們所知道的實體證據有什麼相異之處呢？一般來說，數位證據具有下列幾項特性：

1、原始狀態保持不易

在電子媒體上，資料與紀錄都是以 0 與 1 的方式存在檔案系統中，因此複製檔案的內容與原始資料是完全相同，且修改也相對容易，不像是一般的實體證據，有明確清晰的連結，如果要竄改偽造的話也得耗費一番功夫。因數位資料有易複製特性，若要判別萃取的資料是否為原始檔案內容，需經一番驗證，很難當下判斷為原始檔案，而使得該類證據易遭質疑。

2、難以確定完整性與來源性

由於數位證據易於複製與修改，若要直接聯結案件與嫌犯的關係較於困難。且其不似生物跡證具有極佳的單一性，如 DNA、指紋，可提供犯罪關係的鎖定。因不具單一性，使數位證據在個化方面的確定性較被難與認可。

3、不易察覺與解讀

數位資料是一種電磁紀錄，無法直接用眼察視資料，是需藉由媒體設備

和軟體才能讀取，顯示電磁紀錄中的數位資料，有些數位資料甚至需要用特殊的演算法方能解讀。

四、不易蒐集

以現今硬碟儲存容量來說，幾乎皆以 Gb（Gigabytes）的方式來計算容量，儲存大量資料已不是問題，而伴隨電腦媒體的普及，也產生越來越多的資料，又透過網路的傳播，資料變得且多且廣。如何在網際網路以及儲存媒體中，從大量的儲存資料裡蒐集真正有用的資料，是數位鑑識工作的一項重要議題。

9.3 鑑識陣線聯盟

在本節中，我們將以實際模擬案例的方式，介紹數種常見的數位鑑識軟體及鑑識操作方法，如從電腦磁碟、網際網路及最熱門的智慧型手機等不同鑑識平台上，說明如何以適當的方法萃取完整的數位跡證，期能使讀者對於數位鑑識進行的過程更為了解。

9.3.1 電腦磁碟

假設嫌犯在隨身碟當中儲存了非法圖片，內容記載了犯罪現場的相關資訊，為確保資訊不被偵查人員知悉，嫌犯將整個隨身碟進行了格式化，企圖湮滅證據，如圖 9-2 所示。

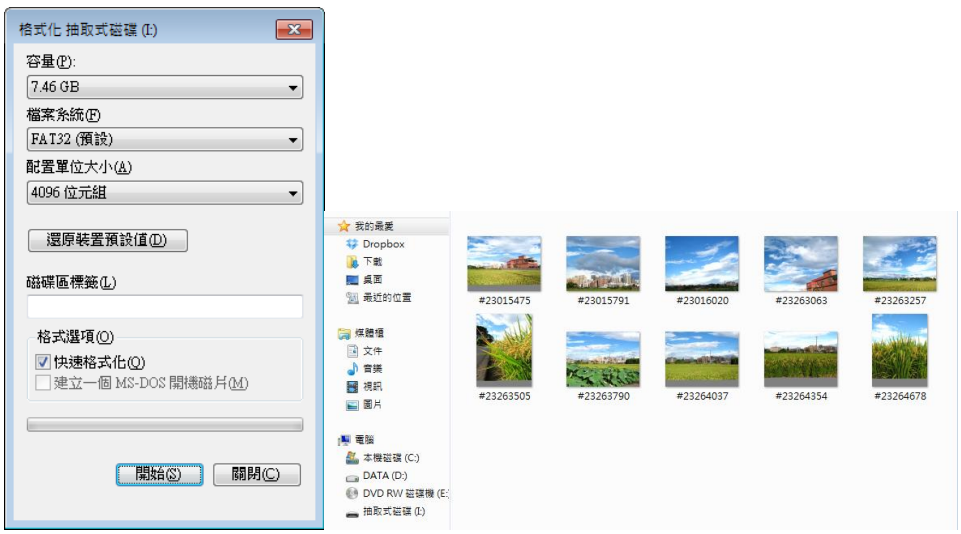


圖 9-2　格式化的隨身碟

在一次搜查中偵查人員取得了該隨身碟並且交由鑑識人員，在鎖定要鑑識對

象的系統環境後，開始著手進行鑑識工作，利用鑑識人員隨行準備的鑑識工具軟體—FinalData，進行對磁碟進行掃描。由鑑識軟體掃描內容中，發現有一些已遭嫌犯刪除的檔案和文件，鑑識人員判斷，這些資料極為是有可能儲有非法資訊的檔案，遂以進行回復，如圖 9-3 所示。

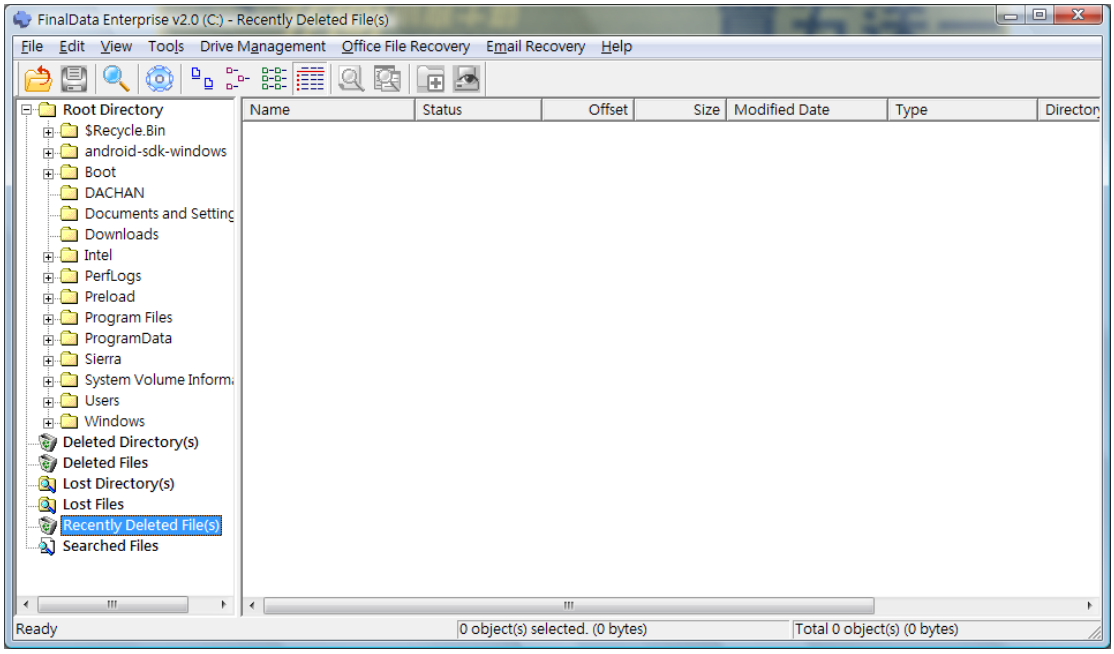


圖 9-3　資料還原軟體—FinalData 操作介面

進行回復檔案後，鑑識人員點選檢視回復的資料，如圖 9-4。發現遭刪掉的圖片雖被成功還原，但有些圖片並不完整。但從連續的幾個檔案當中，還是看得出來，確實是剛才被嫌犯刪除的圖片沒錯。

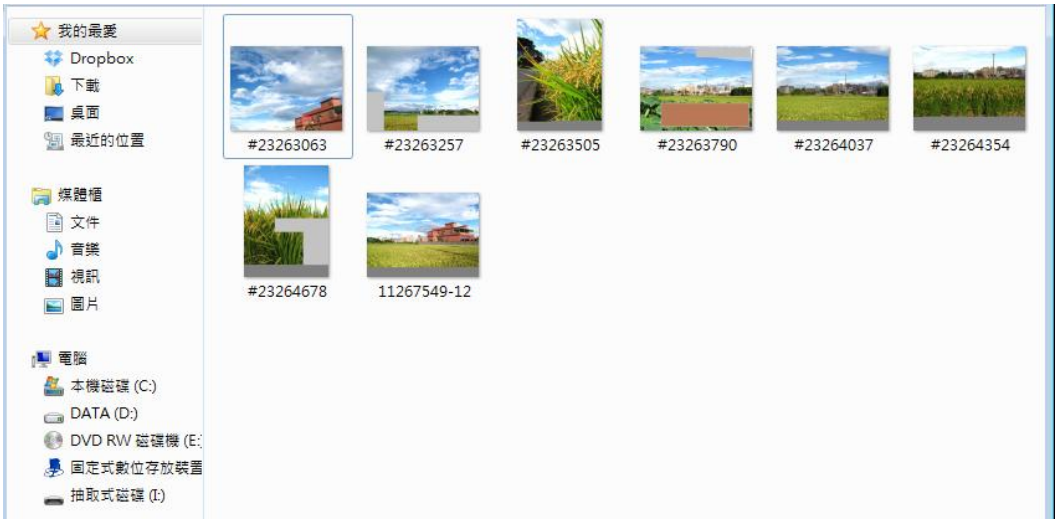


圖 9-4　執行 FinalData 還原隨身碟資訊

這是怎麼辦到的呢？圖片不是明明已經被刪除了嗎？江湖一點絕，裡頭所涵原理這般如下：在電腦系統當中，系統使用者的資料是儲存於磁碟中，為了方便理解檔案儲存系統，且將磁碟比喻為「收納盒」，而收納盒由無數個「收納格」所組成，平常生活中，會將裝飾品、信件、鑰匙鎖頭等物品存放於收納格中，收納格看似便利，但卻存在一個問題，待日子一久或擺放的東西會越來越多，找尋物品就成為了頭痛的問題。所以，為此解決棘手的問題，很直觀地會將物品依性質分類，更進一步的，會在收納格外貼上註記的標籤紙，等到需要某項物品時，可以很快地找出，而不是茫茫地翻找，毫無頭緒。依此觀念，回到我們的主題，遭到刪除的圖片，為何還能復原呢？電腦中，使用者所見的檔案圖示，並非是的檔案內容，這些檔案圖示就是上述所稱的「標籤」，所以使用者將圖片丟入資源回收桶並執行清除命令的動作，像是只將貼於收納格外的標籤」撕掉了一樣，物品依然在收納格中，並無被刪除。很明顯的，檔案依然是在電腦中，只是因缺少了索引標籤，暫時無法找到該檔案。而檔案會被真正的移除，在於電腦空間若不夠，則會將無「標籤」的檔案作移除動作，重新存入新的檔案，再度貼上新的標籤。利用檔案系統的管理特性，數位鑑識人員便能夠有機會透過工具軟體回復被刪除檔案，此原理實為重要！所以，這裡可以很明白的知道，在檔案被刪除後，如果硬碟沒有經過重組（收納格的擺放太雜亂了，全部檔案抽出來好好擺整齊）、格式化（把收納格的所有標籤撕掉，檔案倒出來），原則上都還是可以找回被刪除的檔案。

9.3.2 網路瀏覽器與世界接軌的接窗口

網路不再是遙遠陌生的名詞，透過網路可以接收很多資料，當然也可以上傳，隨著網路的普及，從鑑識角度上，可從網路紀錄的鑑識，了解使用者在網路上的瀏覽活動。

你是否有這樣的經驗，有時候在登入過 facebook、gmail 後，下次開機重啟網頁要點選帳號/密碼登入時，居然不用再次輸入帳號密碼就能登入了？或者是已經讀取過的網頁，下次重新開啟時顯示速度似乎特別快呢？！

以 Internet Explorer 為例，在使用者以瀏覽器為瀏覽網頁的環境下，會產生三種記錄，分別是：History、Cookies、Temporary Files，以下將說明他們的功用分別為何：

1、History(歷史紀錄)

網路管理中，為方便使用者再度拜訪該網頁，瀏覽器會將瀏覽網頁的活動及相關網頁內容記錄下來，而這些紀錄也就是 History(歷史紀錄)了。以鑑識人員的角度看來，歷史紀錄可以了解使用者造訪過哪些網站、進行過什麼活動，進一步從紀錄中找出有利的證據。很像一本記事簿，將瀏覽紀錄詳細寫在記事簿中，供使用者查閱。

2、Cookies

Cookies?難道是可以吃的餅乾嗎？並不一樣喔！Cookies 是使用者在讀取網頁內容時，瀏覽器為減少與遠端溝通的時間，將瀏覽的資料與認證資訊保存於電腦中，待下次重新讀取網頁時，便大大減少重新存取網頁內容的時間，例如會員的登入、曾經瀏覽過的影片、文章，而將這些資訊暫時儲存在 Cookies 裡面。所以很明顯的看出，網站就可以運用 Cookie，將使用者習慣的操作模式記錄下來，讓使用者免於多花心力再度登入、重新設定的好處，Cookies 雖然如此般的便利性，卻也造成資訊安全上的隱憂，如果 Cookies 裡面的資料遭到惡意取用，那使用者的一些個人資料，如帳號、密碼，以及使用網頁瀏覽器的習慣，就會被盜用，因此為了安全起見，目前很多的 Cookies 檔案都已經經過加密處理，無法輕易地被讀取。

3、Temporary Files（暫存檔）

一個吸引大家瀏覽的網頁，內容可能含有多樣的多媒體設計，或者是觸動人心的文字內容，這些吸引你點取瀏覽的網頁由文字、圖片、聲音、動畫等元素構成。如圖 9-5 中，所顯示的是使用者點選造訪過的網頁，這些網頁中的文字圖片等多媒體檔案，瀏覽器會以暫存檔方式儲存在本地端的電腦，如圖 9-6 所示。此功能好處在於，下次若要再讀取該網頁時，就無需耗費額外時間在從網路上下載同同內容的網頁，而可以馬上從暫存檔當中讀取出來了！這也就是為什麼當我們再度開啟曾經瀏覽過的網頁時，感覺讀取速度好像特別快的原因。

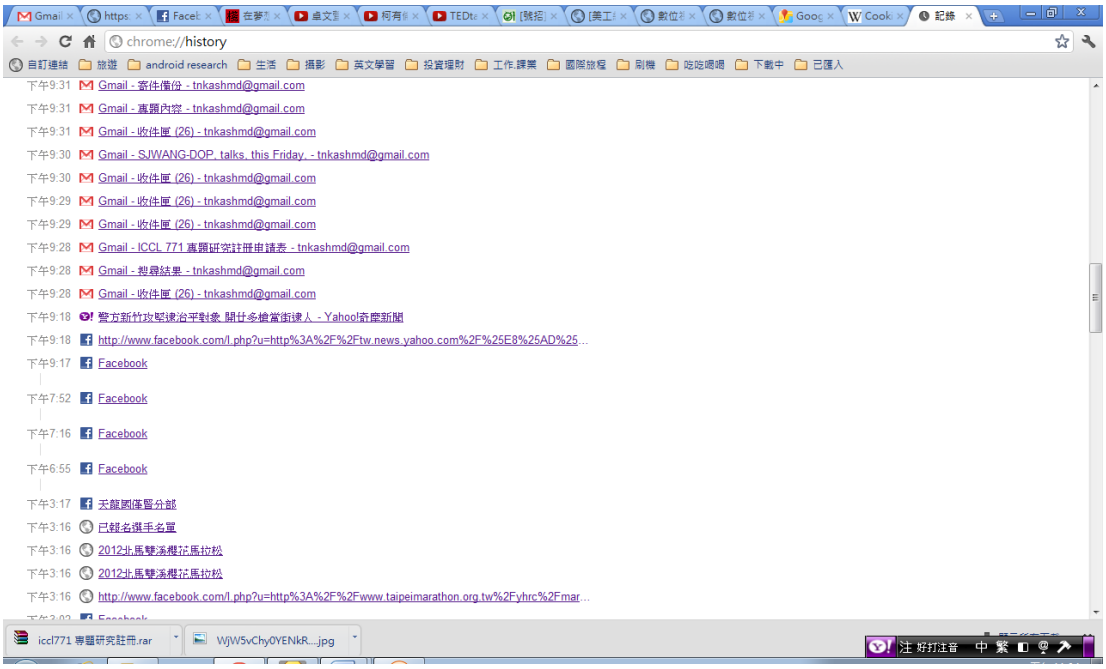


圖 9-5　Google 瀏覽器 Chrome 的歷史紀錄畫面

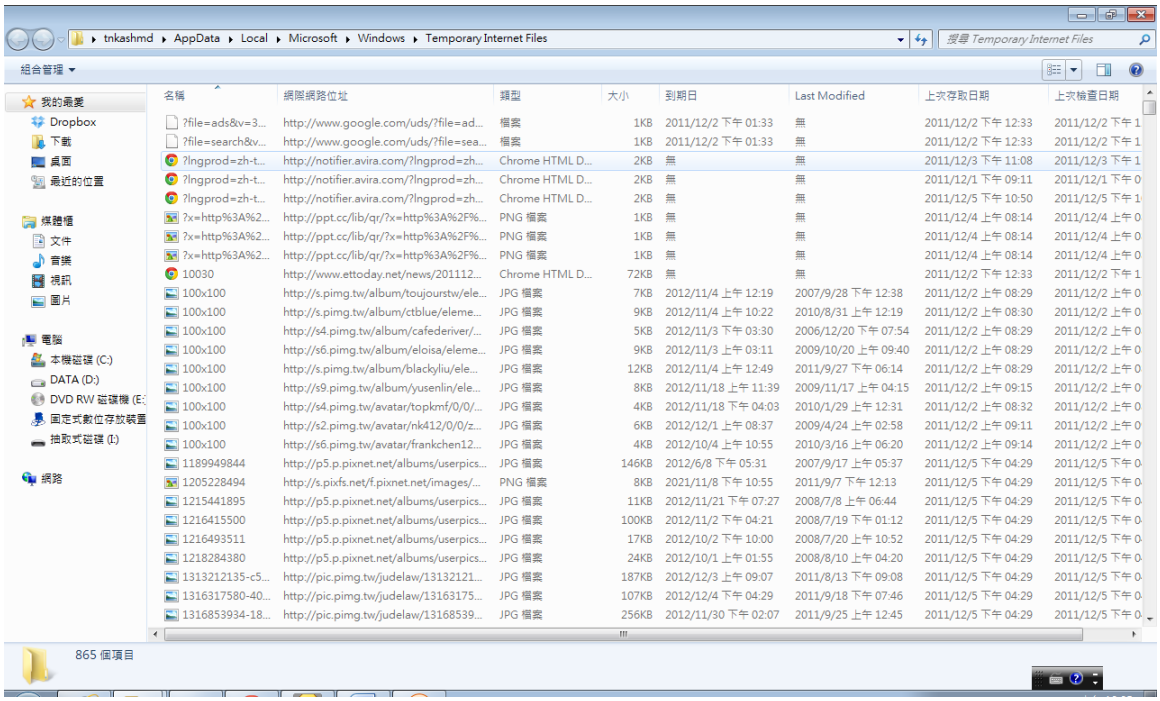


圖 9-6　電腦當中儲存 Temporary files 的資料夾

由上述的三種網頁紀錄中，可以很明瞭地知道，若鑑識人員對電腦系統進行鑑識時，如果想要了解使用者曾經造訪過哪些網站，最直接的方式，當然就是檢視 History(歷史紀錄)、Cookies、Temporary Files（暫存檔）三種檔案。所以鑑識網頁紀錄目的莫過於想知道使用者的瀏覽行為，如造訪過哪些網頁，下載過哪些檔案，甚至是在網路服務中所使用的帳號/密碼。

當然，鑑識人員在進行檢視時，可能會發現這些網頁紀錄內容早就已經遭到刪除了，這些刪除網頁紀錄的程緒可由系統設定時間點自動刪除或者是使用者透過瀏覽器手動清除，但如同我們前面提到過的「收納盒」概念，鑑識人員還是可以運用一些特殊的技術和工具，回復被刪除的歷史紀錄。

9.3.3 網際網路無所遁形

網際網路的發展帶來了便利，但卻也像是雙面刃，造成不少的負面結果，下列是兩則摘錄自網路的新聞案例：

案例一：

四十五歲的台東市男子黃顯誠今年五月十三日晚間涉嫌寄送標題為「刺殺密令」的電子郵件到總統府民意信箱，信件署名收件人為「總統」，內容為「馬英九：有人花錢指派我、欲刺殺你；作事習慣！先行通知」，台北地檢署昨依恐嚇危害安全罪將黃某聲請簡易判決。檢警是案發後根據ＩＰ位址發動搜索，在黃某

電腦內發現另一文件記載「現任台灣總統馬英九我以天六本身之名敕令所有妖魔鬼怪全力刺殺相片本人到死為止」檔案，黃某到案後坦承不諱。

案例二：

綽號「阿龍」的蔡姓少年涉嫌在網路上虛擬成立「雷龍幫」招募幫眾，被警方查獲。前晚，又有人在臉書上冒用雷龍幫之名 PO 文「閃尿？閃你媽，明天血祭新聞和條子」，恐嚇意味濃厚，昨天「阿龍」出面喊冤，強調是盛名之累，被人冒用，警方初步調查，應該有人冒用雷龍幫之名 PO 文，將透過 IP 追查搞鬼的人。

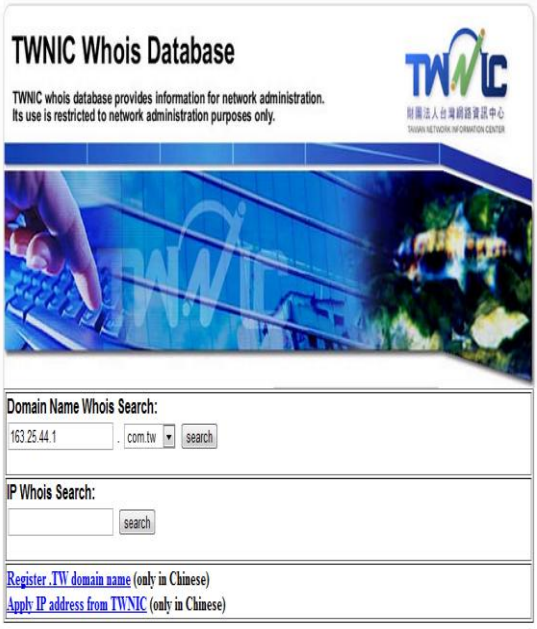
上面的兩則新聞，都是有關於冒名或者是匿名，在網路上發表恐嚇、威脅的留言或信件，遭到警察人員查獲。兩則新聞當中，都提到了利用 IP 位址追查嫌犯，究竟 IP 位址是什麼，又具有什麼功用呢？

IP(Internet Protocol)是 TCP/IP 協定的基礎，它是一種協議，裡頭內容描述資料封包於交換網路時該如何運作，如網際網路的定址方式、資料傳送路徑及單位等。IP 在 TCP/IP 協議中是網路層的主要協議，如同使用者使用網路時，所能代表他們的地址一樣，它的任務是根據來源主機和目的主機的地址傳送資料。為此目的，IP 協議描述了網路定址的方式和傳送資料時應該如何被包裝的內容。第一個架構的主要版本，現在稱為 IPv4，迄今仍然是最主要的網際網路協議，但此遇上了一個難題，當初未想到網際網路使用人數增加如此迅速之多，導致 IPv4 所提供的 IP 數量已即將不敷使用，目前世界各地正在積極部署 IPv6，它是能提供更多定址的新網際網路協議，解決 IPv4 定址數量不足的問題。

每個網際網路的使用者，在連線至網際網路時，都會被分配到 ISP(Internet Service Provider,網際網路服務提供者)所提供的一個 IP 位址，這串 IP 位址就代表著使用者在網路上的身分辨認。IP 位址又分為浮動式以及固定式，固定式代表每次與 ISP 連線時，所分配到的 IP 都是相同的，而浮動式 IP 則是隨著每次連線而有所不同，並無固定的 IP 位址。鑑識人員如果想要追查在網站中留言或者撰寫文章的發文者究竟是從何處所傳，只要取得發文者的 IP 位址（如部落格、社群網站、bbs、e-mail 等）並且分析發文時間是哪位網際網路用戶在什麼地點，被分配到這個 IP 位置上網，就可以獲知確切的電腦所在位置了，如圖 9-7。如果再搭配剛才我們介紹過的電腦磁碟、網路瀏覽器的鑑識方式，找到相關的上網紀錄或者是恐嚇郵件的存檔，那就罪證確鑿囉！

圖 9-7　BBS 登入畫面

現在，我們來驗證看看，為什麼 IP 位址就像是代表網際網路使用者的地址呢。首先我們連到 TWNIC whois 的網站（http://whois.twnic.net.tw），這個網站是由財團法人台灣網路資訊中心(TWNIC)所有，是一個非營利性的財團法人機構，也是國內目前唯一統籌網域名稱註冊及 IP 位址發放之超然中立非營利性的組織，除提供國內完整之網路服務外，更積極參與各項國際相關網路會議。我們輸入想要查詢的 IP 位址在 IP Whois Search 欄位後，可以查詢到 IP 所屬的使用單位以及組織的聯絡方式，如圖 9-8 所示。所以說，IP 位址確實可以代表網路使用者的身分，也能夠被追溯，查詢擁有者和使用者。



IP代理發放單位網段:163.13.0.0-163.28.255.255	
Chinese Name	教育部
Netname	TANET-NET
Organization Name	Ministry of Education Computer Center
Street Address	12F, No 106, Sec.2,Hoping E. Rd.,
Admin. Contact	chuang@mail.moe.gov.tw
Tech. Contact	tanetadm@moe.edu.tw
Spam. Contact	tanetadm@moe.edu.tw
用戶單位:163.25.0.0/16	
Netname	T-TYRC.EDU.TW-NET
Registered Date	1992-05-17
Admin. Contact	abuse@ncu.edu.tw
Tech. Contact	abuse@ncu.edu.tw

圖 9-8、TWNIC Whois IP 查詢網頁

不過實際上，有關於 IP 位置的鑑識當然並不是這麼簡單。有心人士為了隱匿自己的 IP 位址，還可以利用一種稱之為虛擬私人網路(Virtual Private Network，VPN)的技術，在 VPN 環境下，使用者可以偽裝為其它 IP 的位置。這一項技術的研發，使鑑識人員在追查 IP 位址時，往往發現 IP 位址居然來自外國，追其原因都是這些偽裝技術的應用。除此之外，無線區域網路 WiFi 的盛行，有心人士也可能透過破解無線區域網路的加密而連上網際網路，進而仿冒他人的 IP 位置發送訊息。故此，當鑑識人員追查到 IP 位置時，無線區域網路的原本主人就變成了無辜的苦主了。諸如這些問題，都是鑑識人員在進行鑑識工作時，必須考量及克服的難題，這實在是當初設計網際網路始料未及的麻煩。

9.3.4 行動娛樂握於手中—智慧型手機

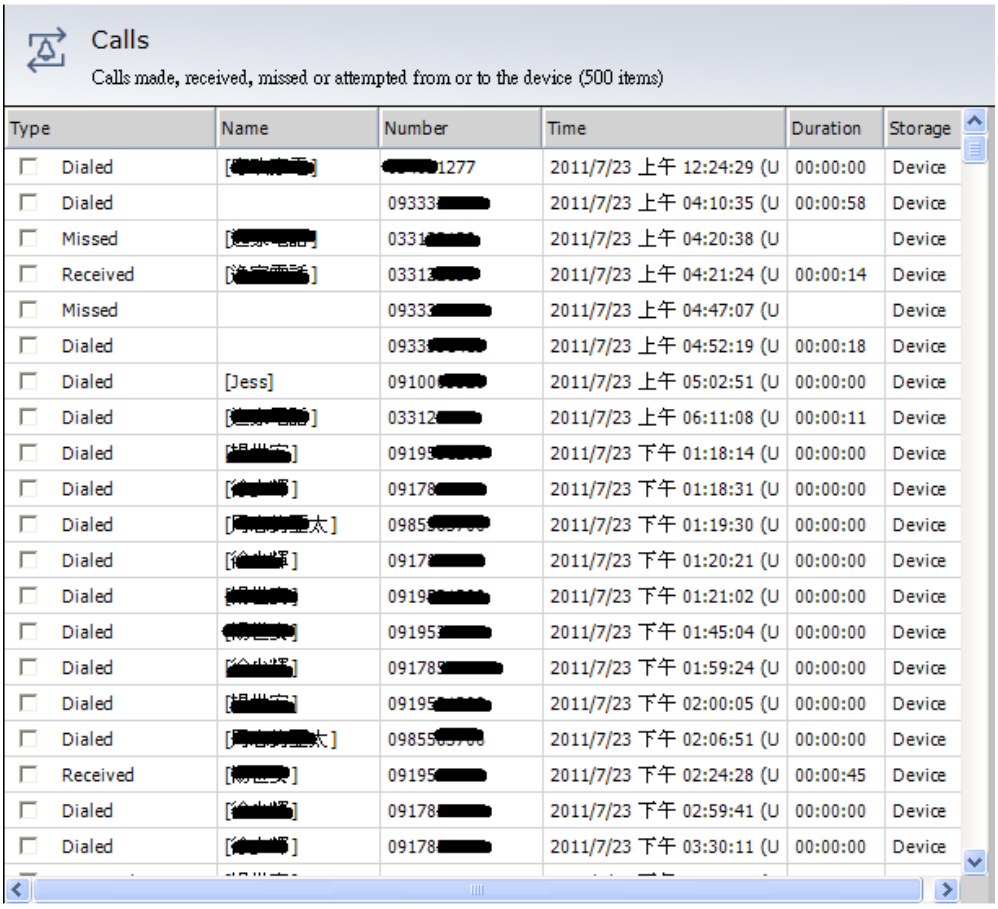
接下來，我們要把介紹的對象，從電腦當中移到另一個同樣也是生活中不可或缺的科技產品，那就是最近相當熱門智慧型手機了！手機剛被發明時俗稱“黑

金剛”，故其意無非就是它的大小就和一個黑色大盒子一樣，又大又笨重，當時的功能也只能用來打電話。漸漸地隨科技發展，手機的外觀愈薄愈精小，功能上設計出更貼近生活的工具，發送簡訊、計算機、通訊簿、行事日曆、小遊戲等附加功能。一直到現在，手機除了基本的通訊功能之外，還融合了個人掌上型電腦 PDA 的功能，能夠上網、聽音樂、記事、拍照，儼然就是一台電腦的智慧型手機，聰明的您一定想到了，剛剛討論的是電腦系統的鑑識方式，那智慧型手機是不是也有什麼鑑識方式呢？沒錯！智慧型手機的鑑識，正是目前積極研究的領域，我們就來看看，智慧型手機到底有什麼有趣的鑑識內容呢。

圖 9-9　功能多元、便利的智慧型手機

如果您有一本筆記本，裡面記錄著朋友、家人的聯絡方式和地址、夾著同學們寄給您的信件、您重要的記事及去過的地方等資訊，這麼多私密的紀錄，一旦被其他人打開來看，您的「底細」豈非就全部都洩露出來了，隱私不保。智慧型手機扮演的就是這樣的一個角色，可以完成很多事，如上網瀏覽訊息、照相、編緝聯絡簿，衍然一機在手，萬事 OK。但有一好無兩好，事情總是很難有那麼完美，試想儲有那麼多個人資訊的智慧型手機若被有心人竊走或者不小心掉落，那訊息不就全外漏了，所以使用智慧型手機還是要相當謹慎，才能用的安心。但話說既然智慧型手機這麼的方便，當然嫌犯也有可能使用它進行非法活動。基於這樣的可能性，依鑑識立場來說，若能將智慧型手機的資訊萃取出來，對於取得數位證據又多了一項有力的管道。所以面對這樣的挑戰，智慧型手機鑑識是刻不容緩的鑑識議題。

手機最基本的功能，就是撥打電話，大部分的手機都會記錄下來使用者撥打接收通話的時間、號碼，這些資料對鑑識人員來說，是非常具有參考價值的資料。因為一旦了解使用者習慣撥打的號碼，掌握了通話的頻率和次數，那麼分析使用者經常往來的對象，就不是那麼困難了。透過鑑識工具軟體 XRY，將手機連接到電腦上進行分析，可以整理出如圖 9-10 的資料。



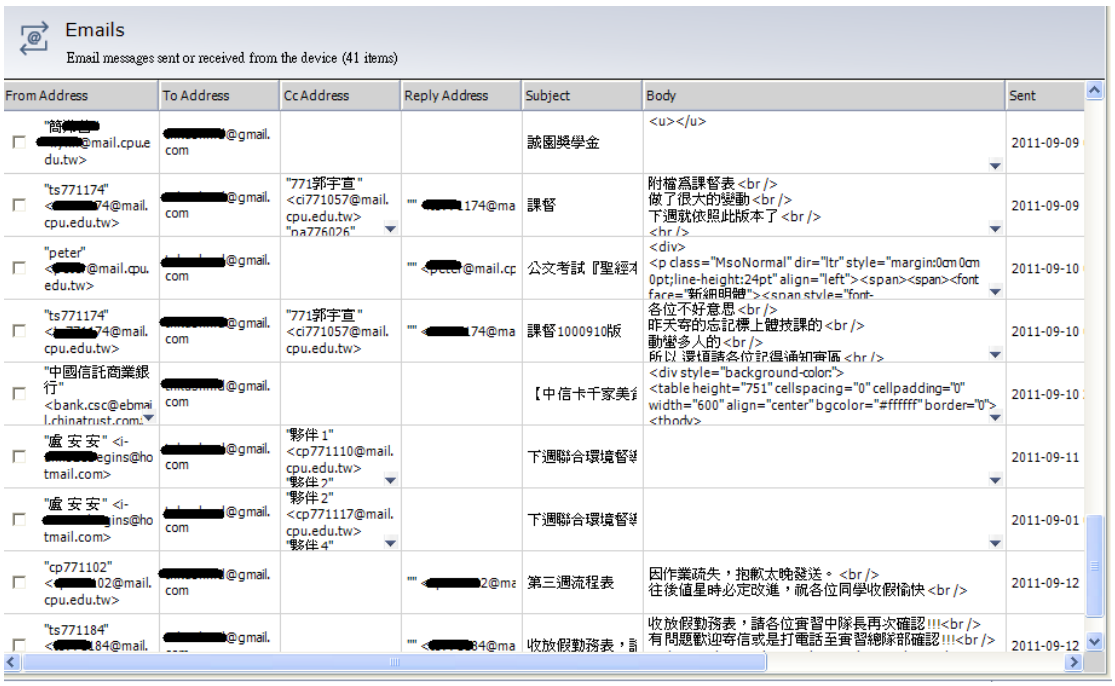
Calls

Calls made, received, missed or attempted from or to the device (500 items)

Type	Name	Number	Time	Duration	Storage
Dialed	[redacted]	[redacted]1277	2011/7/23 上午 12:24:29 (U	00:00:00	Device
Dialed		09333[redacted]	2011/7/23 上午 04:10:35 (U	00:00:58	Device
Missed	[redacted]	0331[redacted]	2011/7/23 上午 04:20:38 (U		Device
Received	[redacted]	0331[redacted]	2011/7/23 上午 04:21:24 (U	00:00:14	Device
Missed		0933[redacted]	2011/7/23 上午 04:47:07 (U		Device
Dialed		0933[redacted]	2011/7/23 上午 04:52:19 (U	00:00:18	Device
Dialed	[Jess]	0910[redacted]	2011/7/23 上午 05:02:51 (U	00:00:00	Device
Dialed	[redacted]	0331[redacted]	2011/7/23 上午 06:11:08 (U	00:00:11	Device
Dialed	[redacted]	0919[redacted]	2011/7/23 下午 01:18:14 (U	00:00:00	Device
Dialed	[redacted]	0917[redacted]	2011/7/23 下午 01:18:31 (U	00:00:00	Device
Dialed	[redacted]	0985[redacted]	2011/7/23 下午 01:19:30 (U	00:00:00	Device
Dialed	[redacted]	0917[redacted]	2011/7/23 下午 01:20:21 (U	00:00:00	Device
Dialed	[redacted]	0919[redacted]	2011/7/23 下午 01:21:02 (U	00:00:00	Device
Dialed	[redacted]	0919[redacted]	2011/7/23 下午 01:45:04 (U	00:00:00	Device
Dialed	[redacted]	0917[redacted]	2011/7/23 下午 01:59:24 (U	00:00:00	Device
Dialed	[redacted]	0919[redacted]	2011/7/23 下午 02:00:05 (U	00:00:00	Device
Dialed	[redacted]	0985[redacted]	2011/7/23 下午 02:06:51 (U	00:00:00	Device
Received	[redacted]	0919[redacted]	2011/7/23 下午 02:24:28 (U	00:00:45	Device
Dialed	[redacted]	0917[redacted]	2011/7/23 下午 02:59:41 (U	00:00:00	Device
Dialed	[redacted]	0917[redacted]	2011/7/23 下午 03:30:11 (U	00:00:00	Device

圖 9-10　利用 XRY 鑑識通話記錄

傳送簡訊也是大家會利用手機上常用功能之一，簡訊除了可傳送文字外，也附加表情圖案，此功能深受使用者的喜愛。由於近年無線網路發展，收發訊息除透過手機內簡訊功能外，還藉由手機無線上網，從網路上收發電子郵件。這些電子郵件和簡訊的內容，相信大家很明瞭，這是相當重要的數位證據，如圖 9-11。經由鑑識分析訊息內容，可以了解手機的主人最近有什麼活動，跟哪些人聯絡過什麼事情，在哪些時間、地點，馬上就可以掌握的一清二楚。



Emails

Email messages sent or received from the device (41 items)

From Address	To Address	Cc Address	Reply Address	Subject	Body	Sent
"簡[redacted]@mail.cpu.edu.tw>	[redacted]@gmail.com			誠園獎學金	<u></u>	2011-09-09
"ts771174" <[redacted]74@mail.cpu.edu.tw>	[redacted]@gmail.com	"771郭宇宣" <ci771057@mail.cpu.edu.tw> "na776026"	"" [redacted]174@ma	課督	附檔爲課督表 做了很大的變動 下週就依照此版本了 	2011-09-09
"peter" <[redacted]@mail.cpu.edu.tw>	[redacted]@gmail.com		"" <peter[redacted]@mail.cp	公文考試『聖經神	<p class="MsoNormal" dir="ltr" style="margin:0cm 0cm 0pt;line-height:24pt" align="left"><font face="新細明體"><span style="font-	2011-09-10
"ts771174" <[redacted]74@mail.cpu.edu.tw>	[redacted]@gmail.com	"771郭宇宣" <ci771057@mail.cpu.edu.tw>	"" [redacted]74@ma	課督1000910版	各位不好意思 昨天寄的忘記標上體技課的 動蛍多人的 所以 還值請各位記得通知審區 	2011-09-10
"中國信託商業銀行" <bank.csc@ebmail.chinatrust.com>	[redacted]@gmail.com			【中信卡千家美食	<table height="751" cellspacing="0" cellpadding="0" width="600" align="center" bgcolor="#ffffff" border="0"> <tbody>	2011-09-10
"盧 安 安" <i-[redacted]egins@hotmail.com>	[redacted]@gmail.com	"夥伴 1" <cp771110@mail.cpu.edu.tw> "夥伴 2"		下週聯合環境督導		2011-09-11
"盧 安 安" <i-[redacted]ins@hotmail.com>	[redacted]@gmail.com	"夥伴 2" <cp771117@mail.cpu.edu.tw> "夥伴 4"		下週聯合環境督導		2011-09-01
"cp771102" <[redacted]02@mail.cpu.edu.tw>	[redacted]@gmail.com		"" <[redacted]2@ma	第三週流程表	因作業疏失，抱歉太晚發送。 往後值星時必定改進，祝各位同學收假愉快 	2011-09-12
"ts771184" <[redacted]84@mail.	[redacted]@gmail.		"" <[redacted]84@ma	收放假勤務表，請	收放假勤務表，請各位實習中隊長再次確認!!! 有問題歡迎寄信或是打電話至實習總隊部確認!!! 	2011-09-12

圖 9-11　利用 XRY 鑑識收發過的電子郵件

有些人可能會想到：「如果我把這些簡訊和電子郵件刪掉，別人不就看不到了嗎？」還記得「收納盒」的概念嗎？如果將手機經過特殊的處理方式，以及使用適當的鑑識工具軟體，還是可以回復這些遭到刪除的資料！

當我們開車到一個陌生的地方時，人生地不熟的，仰賴的是安裝在車上的導航系統，經由 GPS 定位車子目前所在的位置，並將其位置資訊讀入導航的地圖中，聰明的導航系統便會為駕駛人規劃出最短、最方便的路徑，防止駕駛人在陌生的地方迷路，智慧型手機上多有此功能。手機上的 GPS 角位導航是另一項十分熱門的功能。目前智慧型手機，一般來多以採用 Google map 的地圖資料，如圖 9-11，利用手機基地台或者是 GPS 定位手機目前的所在經緯度，方便我們利用手機進行導航、找路、找商店，甚至可以與好朋友們分享自己目前所在的位置！

導航定位系統（如 Google Map）如同網路瀏覽器一樣，有儲存紀錄的功能。它會將曾經在系統上定位過的經緯度記錄會留在手機內。記錄功能，可說是鑑識的好朋友，透過鑑識軟體操作，將定位過的地點經緯度從紀錄中萃取出來並列表分析，如圖 9-12。如此就可以一目了然，掌握手機的主人曾經去過哪些地方了！

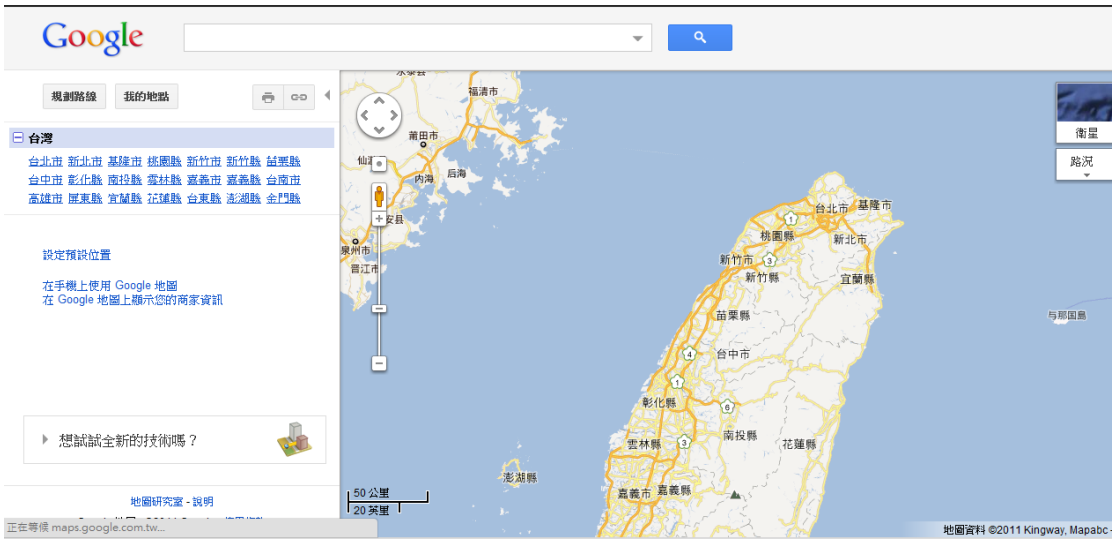


圖 9-11　Google 公司提供之 Google Map

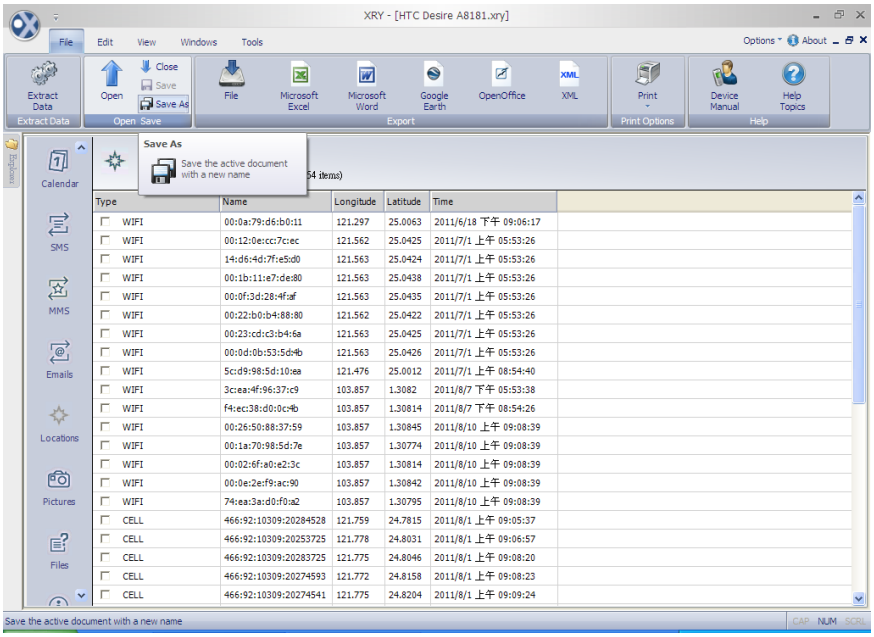


圖 9-12　使用 XRY 鑑識智慧型手機內之定位系統使用記錄

小小的一支智慧型手機，居然可以告訴我們這麼多資訊，這都是拜科技進步之賜，但在了解這些鑑識技術之餘，我們也必須知道個人資訊產品保管的重要性，這些東西一旦遺失而遭人拾獲，手機內的資訊，無論是已存在的還是過往已刪除的資料，都可能隨著個人隱私一起流露出來。

9.4 鑑識是敵是友？

俗話說「道高一尺、魔高一丈」，在 CSI 影集當中，嫌犯在犯案過後，總是想盡辦法，企圖把留下來的證據銷燬、偽造，故佈疑陣，妨礙鑑識人員採證分析，擾亂偵查方向。在數位鑑識的工作當中，會不會遇到這種難題呢？答案是會的。正因為數位證據易於改變、複製的特性，鑑識人員在進行鑑識工作時，需詳加確認數位證據的完整性，如萃取的數位證據是否於原本的證據一致、是否遭到竄改、所欲萃取的數位證據是否已經被隱藏或者是刪除。而採取各種手段防止數位證據的鑑識行為，我們稱之為「反鑑識(Anti-forensics)」。

反鑑識的作為是「任何在鑑識工作過程當中，嘗試干涉對證物的取用和存取的動作，意圖擾亂鑑識工作」。反鑑識的運作主要透過下列三個策略進行：

一、對資料的攻擊

對潛在有可能的證物進行刪除或者竄改，讓這些資料變得無法理解，而導致該證物在法庭上失去證據效力。

二、對工具的攻擊

反鑑識利用目前電腦鑑識工具漏洞或其它弱點，從被鑑識物中試圖更改鑑識作為，以產生偽造的鑑識結果或報告。

三、對分析者的攻擊

反鑑識透過產生大量無意義資料來混淆視聽，或者是事後強烈質疑鑑識工作的有效度和可信度，來對鑑識工作者造成困擾。

目前已有數種技術，可達成反鑑識的目的，藉以干涉數位鑑識工作，以下就列出幾個例子，作與參考：

1、資料加密（Encryption）

將資料透過私鑰加密方法如 RC4、DES 等方法，或是透過公鑰加密如 RSA 等方法，成為旁人無法理解或者是不具有金鑰的人無法探究的密文內容。

2、資料隱藏（Steganography）

將資料隱藏在平常電腦中較無用處且不起眼的儲存位置，或是透過一些演算法將資訊隱藏在某個檔案或圖片中。這些被隱藏的資料，有可能是圖形、文字、聲音、HTML 檔，甚至是磁碟內的資料。透過資料隱藏技術，使得數位鑑識人員無法由直觀發現變化的部份，來達到隱藏資訊的目的。

3、資料抹除

對攻擊者來說，為了要避免被追蹤出身分，最好的方法就是刪除掉所有關於他在電腦上的活動紀錄了。但是前面我們提到過，如果僅僅是將資料刪除，資料還是有可能被還原，唯一可以根除的方式，就是「除了撕掉標籤外，也要把收納盒內的檔案確實移除」，那這項工作該如何辦到呢？一些軟體設計師，為徹底刪除資料，避免隱私外漏，開發出相關抹除資料的軟體，如「eraser」。執行 eraser 進行抹除資料時，eraser 會將欲抹除的資料依預先設定的或者是隨機產生的資料覆寫數次，達到確實刪除資料的目的。如此一來，如果還想利用 FinalData 復原資料的話，就會有困難了，如圖 9-13 所示。

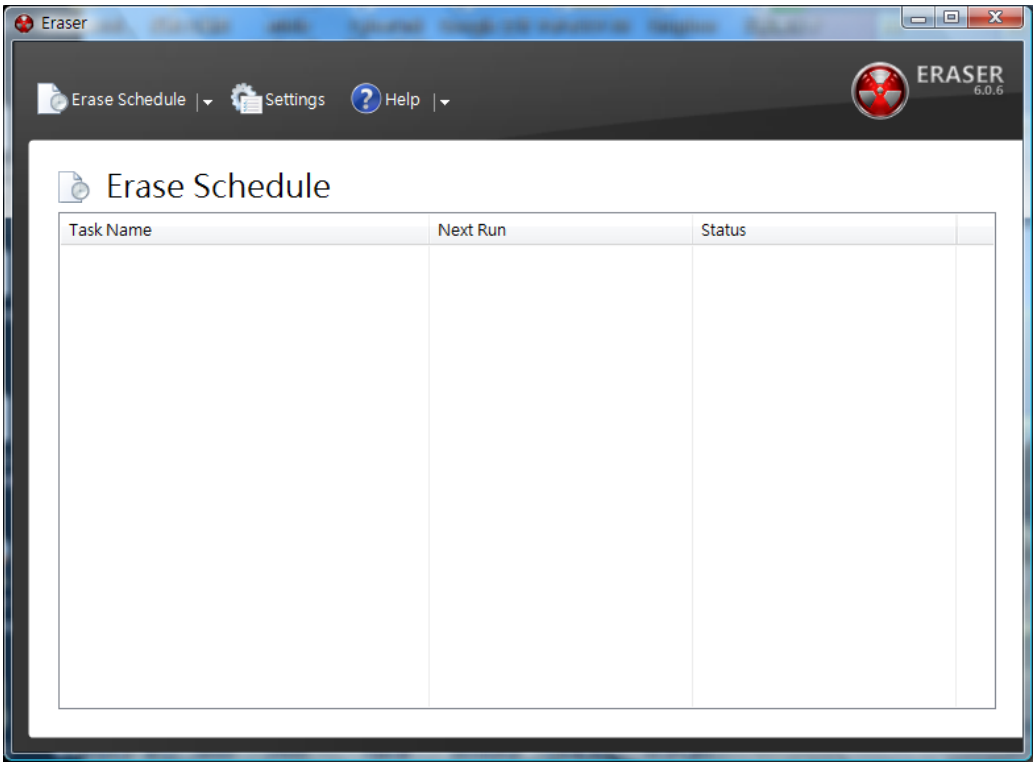
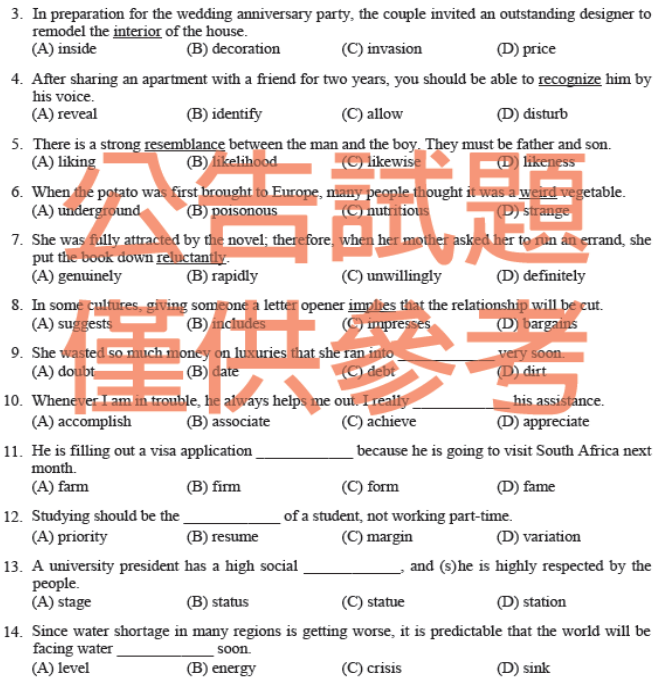


圖 9-13　資料抹除軟體 eraser 操作介面

不同於銷毀傳統鑑識證據的手段，反鑑識雖然對電腦鑑識工作帶來了難題，卻也在生活中提供了不少用途，在現實生活中，存在惡意程式從政府機關、企業公司或者是個人電腦中竊取機密檔案，並透過電子郵件、網路空間或者是可攜式儲存裝置傳遞檔案。因此，為了避免機密檔案被惡意程式存取，減低資料外流的威脅，會選擇採用資訊保密的策略，例如在公司當中，會監控員工的電子信箱、側錄與分析內部網路封包、禁止登入社群網路等，藉此阻止非正當使用電腦的工作者。

此外，前面反鑑識作法中，所提到的資料隱藏技術，還可應用在數位浮水印上。數位浮水印的用處在於宣告著作版權，它的作法是將有版權的檔案上加入著作權者個人資訊，以防他人偽造複製。數位浮水印又分為可視(Visible)浮水印和

不可視(Invisible)浮水印二種，前者是將原始圖片檔，加上肉眼能辨別的擁有者資料，如果要移除數位浮水印，一定會嚴重的破壞原始圖片檔的資訊，如圖 9-14；後者則將圖片檔加上我們肉眼所看不見的浮水印，整張圖片檔的外觀和細節內容並沒有發生顯著的變化，如圖 9-15，而除了銷毀這張圖檔外，沒有任何其他的方法可以將數位浮水印移除，如果有違反著作權的盜用時，我們可以透過特別的方法從中取出隱藏的浮水印，藉以辨識著作權資訊。從上面的例子當中，我們可以知道，反鑑識帶來的影響，是一體兩面的，正所謂水能載舟亦能覆舟，如果能善加利用這些特性的話，能夠解決我們生活當中許多的難題，提供許多助益呢！



3. In preparation for the wedding anniversary party, the couple invited an outstanding designer to remodel the interior of the house.
(A) inside (B) decoration (C) invasion (D) price

4. After sharing an apartment with a friend for two years, you should be able to recognize him by his voice.
(A) reveal (B) identify (C) allow (D) disturb

5. There is a strong resemblance between the man and the boy. They must be father and son.
(A) liking (B) likelihood (C) likewise (D) likeness

6. When the potato was first brought to Europe, many people thought it was a weird vegetable.
(A) underground (B) poisonous (C) nutritious (D) strange

7. She was fully attracted by the novel; therefore, when her mother asked her to run an errand, she put the book down reluctantly.
(A) genuinely (B) rapidly (C) unwillingly (D) definitely

8. In some cultures, giving someone a letter opener implies that the relationship will be cut.
(A) suggests (B) includes (C) impresses (D) bargains

9. She wasted so much money on luxuries that she ran into _____ very soon.
(A) doubt (B) date (C) debt (D) dirt

10. Whenever I am in trouble, he always helps me out. I really _____ his assistance.
(A) accomplish (B) associate (C) achieve (D) appreciate

11. He is filling out a visa application _____ because he is going to visit South Africa next month.
(A) farm (B) firm (C) form (D) fame

12. Studying should be the _____ of a student, not working part-time.
(A) priority (B) resume (C) margin (D) variation

13. A university president has a high social _____, and (s)he is highly respected by the people.
(A) stage (B) status (C) statue (D) station

14. Since water shortage in many regions is getting worse, it is predictable that the world will be facing water _____ soon.
(A) level (B) energy (C) crisis (D) sink

圖 9-14　可視型浮水印

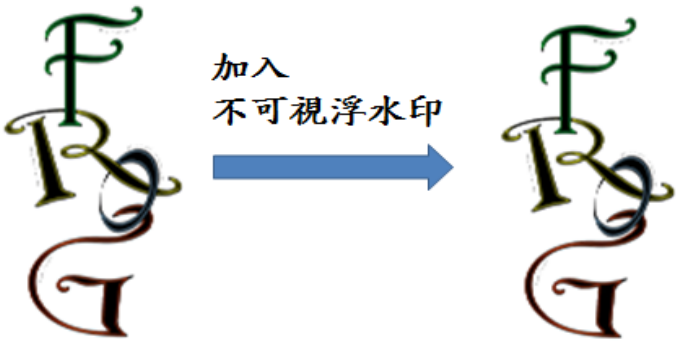


圖 9-15　添加不可視浮水印