## 目標讀者

不論公家機關或私人機構的數位鑑識實驗室，負責電腦系統（包括 Linux）鑑識作業的工作人員都能從本書得到啟發。從事件應變團隊轉換到鑑識工作的人愈來愈多，還有大型機構裡的電腦鑑識人員、法律事務所、稽核單位和顧問公司等的鑑識和電子搜索技術人員、來自執法機構的傳統鑑識人員，這些都是本書的潛在讀者，儘管本書主要目標是為想提升 Linux 分析技能的有經驗數位鑑識人員而寫，但其他人也能從書中得到滿滿知識。

經驗豐富的 Unix 和 Linux 管理員，若想學習數位鑑識分析和調查技巧，本書絕對是最佳的學習教材，可以幫助這些系統管理員轉換到數位鑑識領域，或者可利用書中的鑑識手法增進故障排除功力。

安全專家也可從本書得到啟發，藉由評估預設安裝的 Linux 系統之資訊風險，可促成安全驅動的程序變革，包括減少儲存在系統上的資料量以達到資訊保密的目的；然而，為了達成鑑識目的，可能因日誌紀錄或稽核資料要求而增加系統儲存的資料量。

注重隱私的人也會發現本書的用處，因為它明白指出 Linux 系統上的大量個人機敏資料之保存位置，人們可利用書中知識來降低個人資料暴露的可性能，增進系統隱私保護能力（可能導致部分功能無法發揮或喪失系統的便利性）。

Linux 應用程式和發行版的開發人員也可從本書找到靈感，本書點出預設組態下的潛在隱私和安全問題，有助於開發人員建立更安全牢固的組態來保護使用者。

令人遺憾的，鑑識社群從事的活動，犯罪分子也一樣感到興趣。每本數位鑑識書籍皆因此產生不良副作用，惡意行為者總是尋找攻擊系統和破壞安全性的新方法，鑑識分析技術也無法逃避，因此，筆者會在適當時機說明反鑑識議題，鑑識人員必須瞭解操縱或破壞證據的反鑑識技術。

## 必備基礎知識

為了發揮本書最大效益，接下來將依照讀者已具有的技能，說明所需的必備知識：

- 具備數位鑑識知識，但對 Linux 瞭解有限的人。
- 具備 Linux 知識，但對數位鑑識瞭解有限的人。



碁峰 www.gotop.com.tw

## 資料流程圖

鑑識分析需要確認跡證位置和重建過去的活動軌跡，為達成任務目標，就必須知道所關心的資料（潛在證據）之流動路徑及儲存位置。本書使用資料流程圖說明資料在程式、服務程序、主機或其他資料處理系統（透過網路）之間的傳遞情形，與證據採集有關的檔案和目錄也列在流程圖裡。

圖 1 是一套虛構系統的資料流程圖，藉以說明資料流程圖在本書的使用方式，每一個方塊代表資料的來源或目的（如檔案、程式或其他電腦），線條則表示資料流的關聯性（讀取／接收或寫入／發送）。

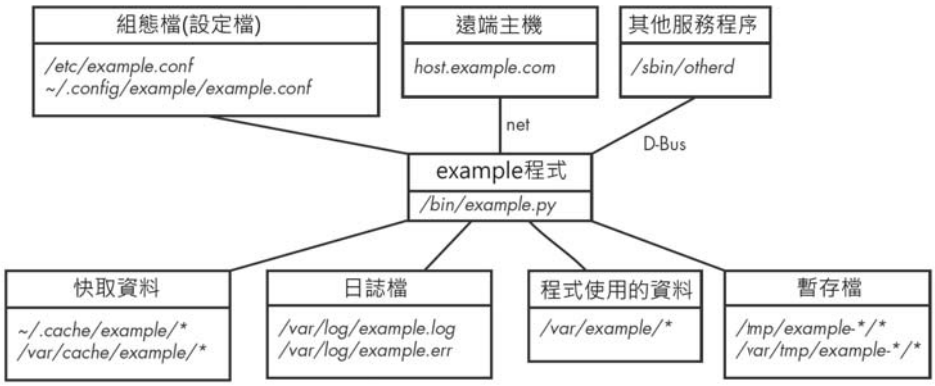


**圖 1：一套虛構系統的資料流程圖**

在此範例系統裡，程式（*example.py*）是流程圖的核心，正和遠端主機及服務程序交換資料，包括組態案、日誌檔、暫存檔和快取資料。

某些流程圖還會加上箭頭來指示資料流向，而不是僅僅表達資料間的關聯。當某些細節毋須表現出來時，有時會以一個方塊代表多個程式所組成的資料，以簡化流程圖。

注意，書中所提供的流程圖並非完整的資料關聯，只是配合該節討論主題，就數位鑑識角度所列出的潛在證據而已。透過這樣的資料流程圖，有助以視覺化方式呈現 Linux 系統上的潛在證據位置。

撰寫本書給筆者帶來很多歡樂，也希望讀者從書中得到愉悅。對於鑑識人員和資安事件應變人員，期盼你們能滿載 Linux 系統的分析知識而歸；對於 Linux 工程師和愛好者，希望數位鑑識調查技巧能協助你們順利除錯和排除系統故障。



碁峰 www.gotop.com.tw

圖 2-1 是 Linux 核心及其子系統的架構總覽[4]。

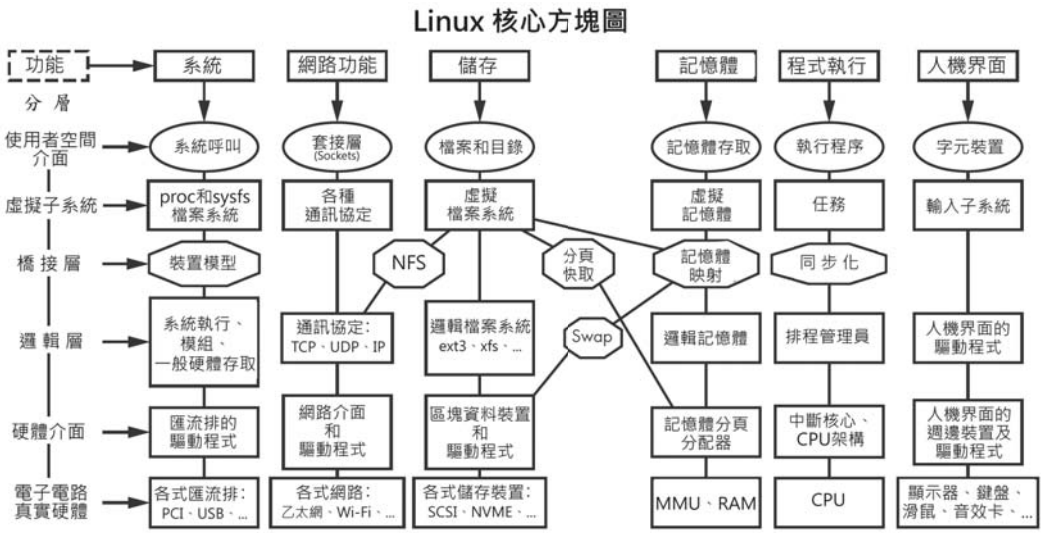


圖 2-1：Linux 核心架構（修改自 *https://github.com/makelinux/linux_kernel_map/*）

這些年來，系統核心已加入許多新功能：利用 cgroup 和命名空間處理先進的執行程序隔離是構成容器的基礎能力；像 btrfs 之類的新式檔案系統是專門為 Linux 系統而設計，btrfs 檔案系統整併之前個別元件（如 RAID 或 LVM）裡常見的儲存功能，提供快照、子卷冊和其他卷冊管理功能；nftables 的新防火牆技術具備更快、更有效率的運作方式和更易理解的規則集，正逐漸取代傳統的 iptables；WireGuard 等新的 VPN 技術逐漸取代陳舊的 IPsec 和 OpenVPN 標準。

當電腦開機時，系統核心會由開機引導程序（bootloader）載入及執行，開機引導程序的技術已從傳統的 MBR（磁區 0 的 BIOS 功能）轉變成更高階的 UEFI（使用 GPT 分割區、UEFI 二進制檔和 EFI 變形的韌體），運行過程中，系統核心可以被動態地改變和設定，並藉由可載入（loadable）的核心模組來加入更多功能，執行系統關機時，核心會在最後程序才被停止。

本書將從數位鑑識調查的角度介紹這些新技術。

4. 此插圖是由 Constantine Shulyupin 所繪制的原始圖片修改而成，並受 GNU 通用公眾授權條款 3.0 保護。



碁峰 www.gotop.com.tw

之樹狀結構，人們熟悉帶有目錄的完整檔案「路徑」（如 */some/path/file.txt*），其實並不儲存於任何地方，而是透過遍歷檔案和根（/）目錄之間，從具有連結的目錄檔案名稱計算出來的。

區塊和 inode 的配置狀態儲存在位元對應（bitmap）裡，並在建立或刪除檔案時進行更新，從圖 3-2 可看出這些分層的抽象概念。

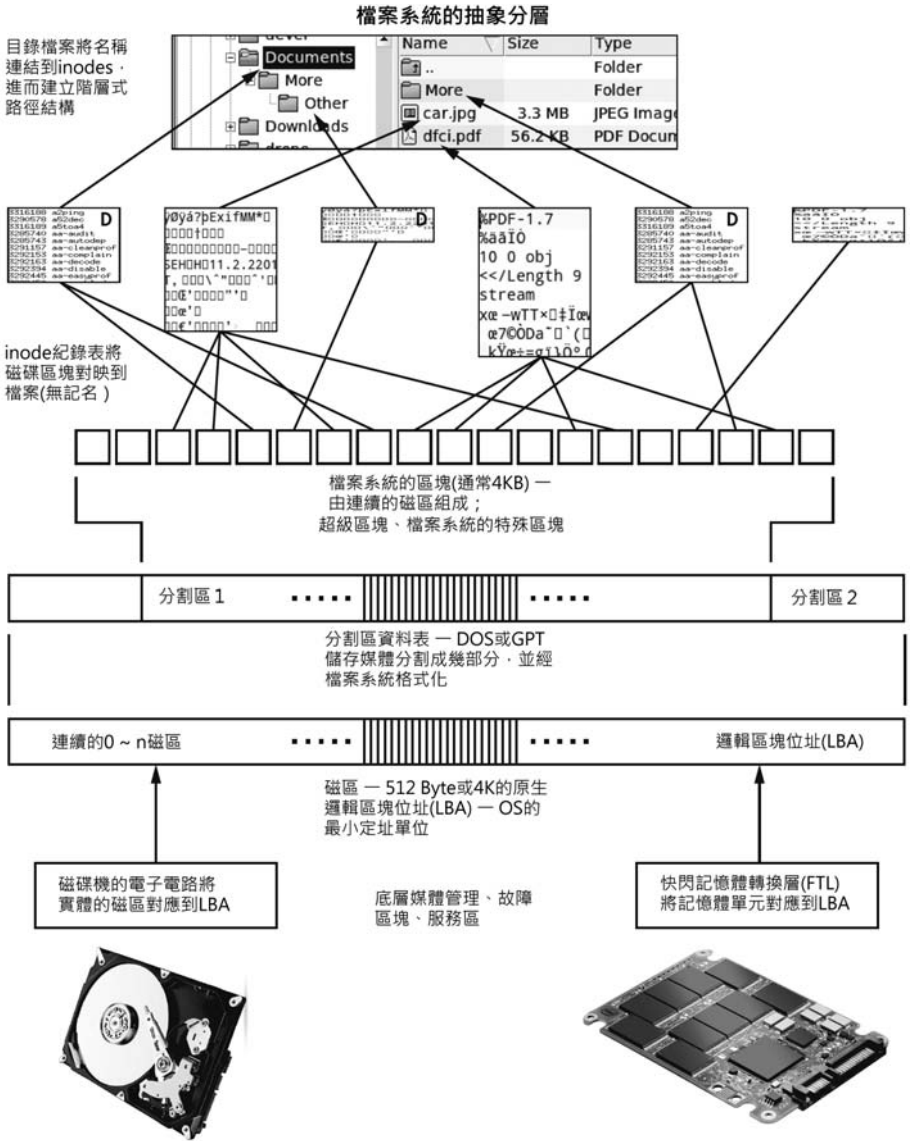


圖 3-2：檔案系統的抽象層次（此為簡化後的樣子，並不包括區塊群組、容錯、可伸縮性和其他特殊功能）



碁峰 www.gotop.com.tw

與上一節相同的復刻技術也可以用於休眠映像上，搜尋加密金鑰也可能對鑑識結果產生決定性影響。

研究顯示若將記憶體內容壓縮儲存於 swap 和休眠映像，要從檔案或分割區復刻內容，就不會那麼輕鬆得手，細節可參考 *http://old.dfrws.org/2014/proceedings/DFRWS2014-1.pdf*

## 分析檔案系統加密

對數位鑑識而言，加密一直是最大挑戰，加密的重點在於限制存取資料，而鑑識的重點則是要存取資料，兩者之間的矛盾，至今未解。

對儲存的資訊進行加密已成為普遍作法，而加密可在多個層次上進行：

- 應用程式的檔案：受保護的 PDF、辦公文件等
- 單一檔案容器：GPG、壓縮檔（zip）加密
- 目錄：eCryptfs、fscrypt
- 卷冊：TrueCrypt/Veracrypt
- 區塊裝置：Linux 的 LUKS、微軟的 Bitlocker、蘋果電腦的 FileVault
- 磁碟硬體：OPAL/SED（自加密磁碟機）

本節會介紹三種 Linux 上的加密技術：LUKS、eCryptfs 和 fscrypt（以前稱為 ext4 目錄加密），還有其他適用於 Linux 的檔案和檔案系統之加密機制，因為它們不是專為 Linux 設計，或者過於少用且晦澀難懂，本書就不予介紹。

要解密被保護的資料，就需要密碼或加密金鑰的複本（一組字串或金鑰檔），鑑識所面臨的挑戰就是要找到此解密金鑰，一些已知用於找出密碼／金鑰的方法（有些顯然沒有被鑑識社群採用）包括：

- 使用字典檔進行暴力破解以查找簡單的密碼
- 使用 GPU 叢集進行暴力破解，以實現快速窮盡可能的密碼搜尋
- 加密演算法分析（數學弱點，減少密鑰空間）
- 搜查被保存、寫下或被傳輸的密碼
- 跨多個帳號或裝置都使用的同一組密碼（密碼重用）
- 依法律規定，要求在法庭出示密碼
- 透過系統共同擁有者或共犯而取得密碼



碁峰 www.gotop.com.tw

- 企業環境中的密鑰備份／託管
- 設備弱點、漏洞或後門
- 使用鍵盤側錄器或監看使用者敲打的按鍵（利用高解析度攝影機或望遠鏡）
- 彩虹表：預先計算的密碼雜湊表
- 從記憶體萃取金鑰：透過 PCI 匯流排直接存取記憶體（PCI-bus DMA 攻擊）、休眠映像
- 對網路流量執行中間人攻擊
- 社交工程
- 強迫取得或暗中盜用生物識別
- 嚴刑、勒索、脅迫或其他惡意手段（見圖 3-3）

嘗試透過技術性取得密碼／金鑰的 Linux 工具有：John the Ripper、Hashcat 和 Bulk_Extractor。

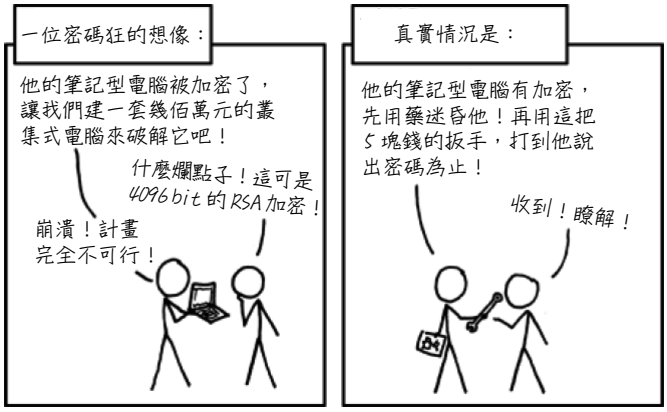


圖 3-3：XKCD 的密碼狂想法（譯自 *https://xkcd.com/538/*）

本節會說明加密的工作原理、如何判斷使用的加密方式，以及如何取得已加密的卷冊或目錄之詮釋資料，也會介紹解密方式，但這裡假設已取得解密金鑰。


碁峰 www.gotop.com.tw

## LUKS 全磁碟加密

LUKS[14] 是加密儲存裝置的標準格式，它的規格在 *https://gitlab.com/cryptsetup/cryptsetup/*，實作工具是 cryptsetup 軟體套件，詳細資訊可請參考 cryptsetup(8) 手冊頁。如果商業鑑識軟體不支援 LUKS 卷冊的分析和解密，可以試試在 Linux 機器上檢查鑑識映像。

磁碟上可以建立帶有或不帶分割區資料表的 LUKS 卷冊，DOS 分割區的 0xE8 類型[15] 和 GPT GUID 分割區的 CA7D7CCB-63ED-4C53-861C-1742536059CC 類型[16] 是指定給 LUKS 卷冊，如果使用分割區，前述分割區類型可能代表存在 LUKS 卷冊，請注意，並非所有工具都能識別這些分割區類型（例如 fdisk 會標示「unknown」〔未知〕），有時，LUKS 分割區也會以標準（通用）的 Linux 分割區類型來建立。

在開機時，Linux 系統會讀取 */etc/crypttab* 檔來設置加密檔案系統，此檔案對分析作業很有用，可以提示加密對象、密碼在哪裡及其他選項。*crypttab* 檔有四個欄位：

**name**：出現在 */dev/mapper/* 裡的區塊裝置名稱

**device**：一組 UUID 或加密卷冊的裝置檔

**password**：密碼來源，可能是金鑰檔或手動輸入（"none" 或 "-" 表示手動輸入密碼）

**options**：有關加密演算法、組態和其他行為的資訊

下列是 */etc/crypttab* 裡有關根目錄和交換分割區加密的一些範例：

```
#   <name>    <device>    <password>    <options>
root-crypt UUID=2505567a-9e27-4efe-a4d5-15ad146c258b none luks,discard
swap-crypt /dev/sda7 /dev/urandom swap
```

swap-crypt 和 root-crypt 是 */dev/mapper/* 裡的被解密裝置，root-crypt 的密碼需要人工輸入（none），而 swap-crypt 的密碼則隨機產生。*crypttab* 檔案也可能存在 initramfs 裡。有些管理員在重新啟動伺服器時懶得輸入密碼，可能將密鑰檔隱藏在某處，這份密鑰檔可能也會有備份檔。

14. 本書的 LUKS 範例使用 LUKS2 版本。

15. *https://www.win.tue.nl/~aeb/partitions/partition_types1.html*

16. *https://en.wikipedia.org/wiki/GUID_Partition_Table*



碁峰 www.gotop.com.tw

和低端運算環境（樹莓派和 IoT 嵌入式系統）所使用的 CPU 可能大不相同，下列是在樹莓派環境執行 file 命令的輸出：

```
$ file /usr/bin/mplayer
/usr/bin/mplayer: ELF 32-bit LSB executable, ARM, EABI5 version 1 (SYSV),
dynamically linked, interpreter /lib/ld-linux-armhf.so.3, for GNU/Linux 3.2.0,
BuildID[sha1]=bef918434bc5966b5bd7002c028773d3fc7d3c67, stripped
```

Linux 的架構可以是 32-bit 或 64-bit、大端序或小端序，並支援各種 CPU 指令集（x86、ARM、PPC、Sparc 等），使用鑑識工具時，必須確認系統架構，除非工具能夠自動檢測這些架構特徵，不然就要告訴它們如何產生合理及夠準確的結果。

## 當機和轉存重要資訊

電腦當機！軟體當機！這是多麼令人心傷的事，尤其是在資料還未存檔前！但對於鑑識人員來說，這又何嘗不是一件好事，因為揮發性記憶體裡的資料可能在當機時被保留下來，系統核心當機、執行程序當機或其他應用程式當機，它們的資料會記錄到本機磁碟上，這些是很有價值的鑑識對象。

當電腦或程式當機時，可能會將當機資料保存在本機磁碟上，以供開發人員進行分析、除錯，有時甚至會上傳到開發人員的伺服器進行分析，保有當機資料的檔案也可能存有決定性影響的鑑識證物。

系統核心當機、執行程序當機及高階的應用程式和特定發行版當機，可能各有不同的處理機制，對於每一種狀況，與鑑識調查有關的資料都可能被保存下來。

分析記憶體轉存資料是指從記憶體轉存檔（memory dump file）裡找出資訊內容的痕跡，或瞭解程式碼的行為和造成內容轉存的原因。解析程式碼行為，常用來尋找惡意軟體和技術性漏洞利用（堆疊和緩衝區溢位等），分析此類攻擊行為，將涉及程式碼的靜態和動態分析、逆向工程、反編譯和反組譯等技巧，必須深度瞭解 C、組合語言和 Linux 的記憶體管理，這一部分的知識都已超出本書預期範圍（事實上，這個主題足以寫成一本專書），這裡只會粗略介紹記憶體轉存和基本的字串資訊提取手法。



碁峰 www.gotop.com.tw

包含 systemd-pstore 服務，該服務會將 pstore 的資料複製到磁碟，然後清除韌體儲存體，以便讓它可以再被使用，複製的資料會儲存在 */var/lib/systemd/pstore/* 裡，執行鑑識作業時記得要檢查這個目錄裡的內容，如果可疑機器的主機板是正常的，也可以單獨讀取 EFI 變數和資料。

kdump 則會在開機時期載入第二系統核心，發生當機時，第二系統核心會嘗試取得第一系統核心的記憶體，透過 kexec（kexec-tools 軟體套件的一部分）將執行權移交給作用中的第二系統核心，該核心以獨立的 initrd 啟動，能夠將完整的記憶體映像儲存到預定的位置，圖 4-3 以流程圖說明這個過程 [9]。

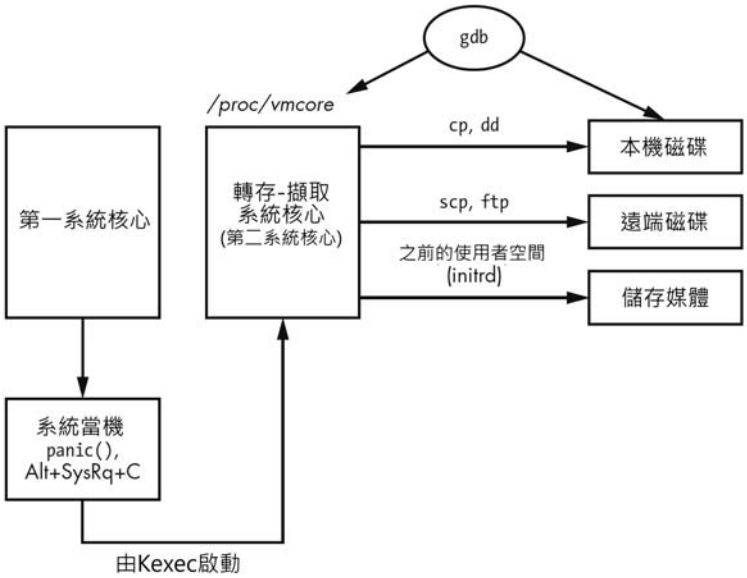


圖 4-3：使用 kdump 儲存系統核心映像

kdump 儲存系統核心記憶體映像和其他資訊的常見位置是 */var/crash/*，例如 Ubuntu 系統的 kdump 當機目錄會以時間戳記建立一個子目錄，如下所示：

```
# ls -lh /var/crash/202011150957/
total 612M
-rw------- 1 root whoopsie 69K Nov 15 09:59 dmesg.202011150957
-rw------- 1 root whoopsie 612M Nov 15 09:59 dump.202011150957
```

9. *https://commons.wikimedia.org/wiki/File:Kdump.svg*



碁峰 www.gotop.com.tw

日誌是儲存在本機之外的位置，對於無法持久記錄日誌的系統，這一項設定可能很重要。

圖 5-2 是 systemd 日誌網路功能的元件架構圖。

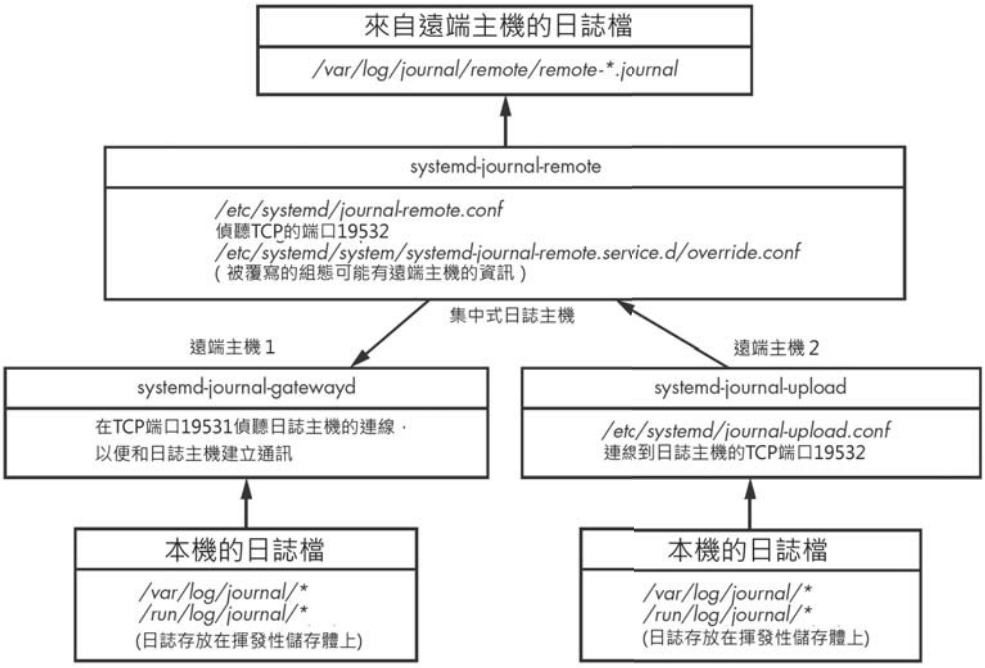


圖 5-2：Systemd 日誌的網路功能架構

有關 systemd 日誌的網路功能細節，請參 systemd-journal-remote(8)、systemd-journal-gatewayd(8) 和 systemd-journal-upload(8) 手冊頁，雖然這些創新大幅增進傳統日誌的功能，但屬 systemd 特有，與 Linux 以外的系統並不相容，知道這些功能的人可能也不多。

## Systemd 日誌的組態

瞭解 systemd 日誌的組態有助於從受鑑識的系統找出可能的證據，systemd 日誌是一支普通的 Linux 服務程序（見圖 5-3），稱為 systemd-journald，在 systemd-journald(8) 手冊頁有詳細說明。

檢查 systemd 單元檔（*systemd-journald.service*）可以得知 systemd 日誌在開機時是否被啟用（enable）。



碁峰 www.gotop.com.tw

本章將介紹有關 Linux 系統啟動和初始化過程的鑑識分析，會檢查 BIOS 或 UEFI 韌體將控制權傳遞給開機引導程序的初期引導階段、系統核心載入和執行，以及系統執行後的 systemd 初始化，還會分析睡眠和休眠等電源管理活動及最後的關機過程。

## 分析開機引導程序

傳統 PC 使用基本輸入輸出系統（BIOS）晶片執行開機磁碟的第一個磁區（磁區 0）之程式碼來啟動電腦，第一個磁區稱為主開機紀錄 (MBR)，負責將作業系統核心和其他元件載入記憶體裡執行，新式 PC 使用統一可延伸韌體介面 (UEFI) 從 EFI 系統分割區的 FAT 檔案系統執行 EFI 二進制程式檔，這些與 UEFI 相關的程式直接由韌體執行，並管理作業系統的載入和執行過程，本節將介紹 Linux 系統初期開機階段裡的鑑識證物（artifact），這些是鑑識人員應該要注意的。

PC 型 Linux 系統的開機過程，是由 BIOS 或 UEFI 使用所謂開機引導程序（bootloader）的軟體來啟動，開機引導程序負責將 Linux 系統核心和其他元件載入記憶體，選擇正確的核心參數，然後執行系統核心，非 PC 系統可能有全然不同的開機程序[1]，例如樹莓派（Raspberry Pi）不是使用 BIOS 或 UEFI，而是有自己的開機引導機制，本章也會酌加說明。

新式 Linux PC 絕大多數使用 GRUB 系統來開機，GRUB 取代老式、簡易的 LILO，本節主要關注 MBR 和 UEFI 如何搭配 GRUB 開機，後面會介紹樹莓派的開機過程，並簡要介紹其他開機引導程序。

以鑑識的觀點，在分析開機引導程序的過程中，可能會找到或萃取一些證物，例如：

- 安裝的開機引導程序
- 啟動多個作業系統的證據
- 先前安裝了多個 Linux 核心的證據
- 開機檔案的時間戳記
- 分割區和檔案系統的 UUID
- 開機時傳遞給系統核心的參數
- 根檔案系統的位置

1. 早期的 Apple Mac、Sun Microsystems 和其他舊型的硬體是使用 OpenBoot 韌體。



碁峰 www.gotop.com.tw

```
total 1096
-rw------- 1 root root   1529 Mar  5 11:22 casper.log
-rw------- 1 root root 577894 Mar  5 11:22 debug
-rw-r--r-- 1 root root 391427 Mar  5 11:22 initial-status.gz
-rw-r--r-- 1 root root     56 Mar  5 11:22 media-info
-rw------- 1 root root 137711 Mar  5 11:22 syslog
```

*casper.log* 和 *debug* 檔是安裝程式腳本的輸出，裡頭也包含錯誤訊息；*media-info* 檔案顯示安裝時的發行資訊；有些以 Ubuntu 為基礎的發行版（如 Mint）也可能還有版號檔；*initial-status.gz* 檔（已壓縮）包含初始安裝的套件清單。

## 樹莓派的 Raspian

樹莓派所用的 Linux 是以 Debian 為基礎的 Raspian，因為它是一套預安裝的映像檔，故不需要 Debian 安裝程式，這種預安裝映像有兩種格式：

**NOOBS**：適合初學者的安裝程序，使用者利用它格式化 SD 卡（FAT）及複製檔案，無需特殊工具。

**磁碟鏡像**：需要解壓縮再使用 dd 或類似工具傳輸到 SD 卡的原生映像。

由於沒有一般所說的「安裝」，因此，調查人員會想知道使用者第一次啟動樹莓派並保存初始設定的時間，然而，基於各種原因，要找到初始設定時間並不容易，一開始的檔案系統時間戳記是來自下載的 Raspian 映像，而非由本機安裝腳本所建立，樹莓派沒有電池供電的硬體時鐘[3]，每次開機時，時鐘都會重設為 Unix 紀元（1970 年 1 月 1 日 00:00），啟動作業系統過程會將時鐘設為最近一次斷電的時間，直到有網路可用時，再進行時間同步（有關系統時間的更多資訊請參見第 9 章）。檔案系統預設使用 noatime 選項掛載，因此不會更新最後存取時間，其他時間戳記可能已被更新，並在建立正確時間之前就寫入日誌條目，讓這些時間變得更不可靠。

首次使用樹莓派時，會配合 SD 卡調整檔案系統的大小，重新開機之後，會啟動 piwiz 應用程式[4]，讓使用者設定網路、重置密碼（預設為 raspberry），並指定國家、語系和時區等，piwiz 應用程式從 */etc/xdg/autostart/piwiz.desktop* 檔自動啟動，該檔案會在使用者完成初始偏好設定

3. 除非另外購買時鐘電池作為擴充的硬體模組。
4. 假設樹莓派已安裝圖形化界面（GUI）。



碁峰 www.gotop.com.tw