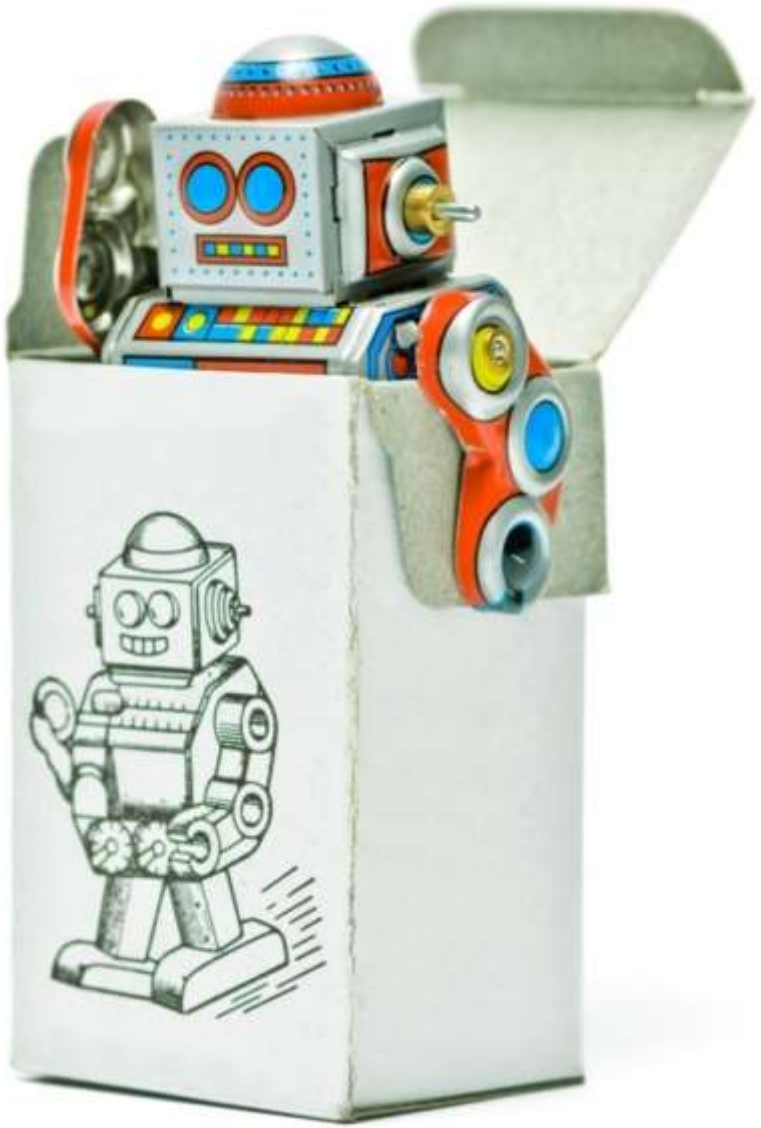
數位鑑識競賽
CTF of Digital Forensic

Jimmy Hsu
winterthink@gmail.com



競賽規則

- 限時150分鐘
  - 10mins：分工及需求解讀
  - 140mins：執行分析

- 分析標的：hd.e01

- 請找出數位證據，並使用下列任一工具或任何雜湊值計算工具算出其HASH值：
  - hashmyfile
  - Md5sum (SIFT內建指令)

競賽規則(續)

- 16:00前各組須繳交
  - 分工說明
  - 需求解讀
    - 以哪些鑑識分析功能(不可只寫工具名稱)完成各項分析需求
  - 分析過程截圖
  - 數位證據HASH
    - 格式：[證據種類名稱]-HASH前5碼
    - 範例：[證明有上網行為]-xxxxx

- 各分析項目前三名完成的組別有額外加分
- 數位鑑識報告於7/3 16:00前以組為單位繳交至 winterthink@gmail.com

案件情況說明

- 在一起涉嫌侵犯商業秘密案件中，A公司聲稱離職技術人員趙能嘉洩露了公司機密項目的技術資料。
- 現辦案機關委託鑑定機構對其工作電腦進行鑑定，以查找相關的證據。
- 現查明A公司的機密項目資料以“JMXM”加三位數字形式命名，存放在名為“JSZL”的文件服務器上，僅限公司內部局域網訪問。
- 公司要求員工的工作電腦不得訪問互聯網或私自外接存儲設備。
- 趙能嘉於2016年4月28日上午辦理了離職手續，4月29日交還了工作電腦。辦案機關於4月30日對趙能嘉的工作電腦進行了保全，製作了硬盤鏡像文件

鑑定需求

- 在辦理了離職手續後，趙能嘉是否使用其工作電腦訪問、複製、外傳了公司機密項目的技術資料。如存在上述情況，提取相關數據並分析相關行為。

分析需求

- 證明有上網行為
- 證明有瀏覽網路磁碟機
- 非法資料存在本機
- 非法資料存在外接裝置
- 證明有外傳資料

評分方式

需求解讀

1. 分工方式
2. 需求解讀能力

技術能力

1. 答案(數位證據HASH)是否正確
2. 工具或功能操作是否正確

分析邏輯

1. 需求解讀後如何決定分析方向、判讀結果或推斷等
2. 鑑識報告撰寫

離職後非法行為 (答案)

❖ 網路行為 – 離職後

證據種類	HASH
證明有上網行為	
證明有瀏覽網路磁碟機	4079c
	bbb14
	4ac09
證明有外傳檔案	b2015
	cca7e
	ffb4e

❖ 非法儲存行為

種類	HASH
存在本機	1317c
	f7f54
	7573a
	62778
	3a6f9
	ce006
	ebbd7
	e25bd
	7529d
	cc71d
	cad1f

種類	HASH
存在外接裝置	89cd8
	5c0c1
	bb584

問題與討論