Introduction to Kindle Forensics

baadc0de

http://baadc0de.blogspot.com

개요

1. Introduction
2. Research
3. Method
4. Results
5. Conclusion

Introduction

Introduction

- **다목적 활용이 가능한 Kindle**
  - E-book 감상뿐만이 아닌 음악 감상, 게임, 웹브라우징, 데이터 저장 등
  - 다양한 포멧 지원
    - .doc, .docx, .txt, .rtf, .html, .htm, .jpeg, .jpg, .gif, .png, .bmp, and .zip
  - Kindle Development Kit (KDK)
    - 사용자 고유의 컨텐츠 생성
- **다양한 데이터를 저장 가능하기 때문에...**
  - 사건과 연관된 증거의 존재 가능성
  - 사용자의 성향을 파악하는데 도움 (책, 음악...)

Research

- 최신 기종의 Kindle(당시 Kindle 3세대)을 FTK Imager를 이용하여 이미징

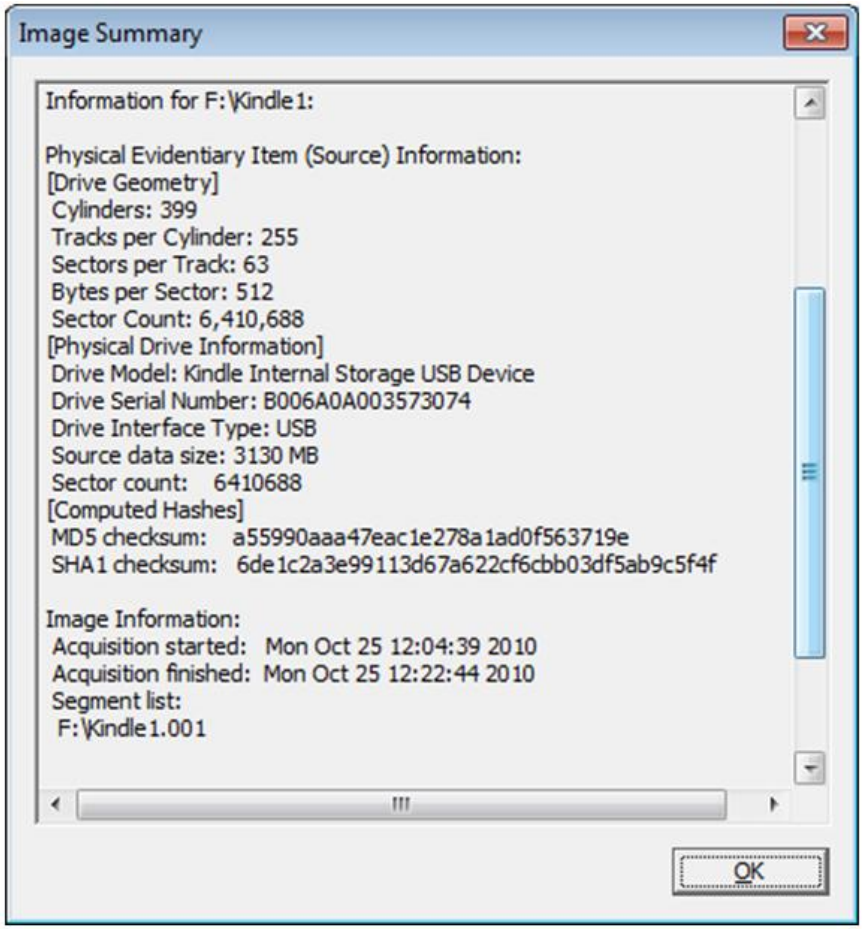


Figure 1: Kindle Image Summary

- **기본 정보**
  - File System : FAT32
  - Operating System : Linux
  - Image Size : 3130MB

- **의문사항**
  - Kindle의 용량은 4GB ←→ 수집한 이미지의 용량은 3130MB
  - 나머지 용량의 행방은??

- **Kindle 디스크 파티션 구성**
  - User Accessible Partition : mmcblk0p4 (3130MB)
  - System Partition : mmcblk0p1 (650MB), mmcblk0p2 (24MB), mmcblk0p3 (8MB)

- **System Area로의 접근**
  - 권한 상승을 통해 접근 가능 a.k.a. Jail-Break (향후 설명)
  - 저자는 mmcblk0p1의 전체 이미지를 수집할 수 없었음
    - dd를 이용하여 system partition의 이미지를 user accessible partition으로 복사 수행
    - Telnet session이 끊기면서 이미징 진행 불가
    - 부분적인 이미지로 분석 수행

    → *Netcat으로 해결 가능 by baadc0de*

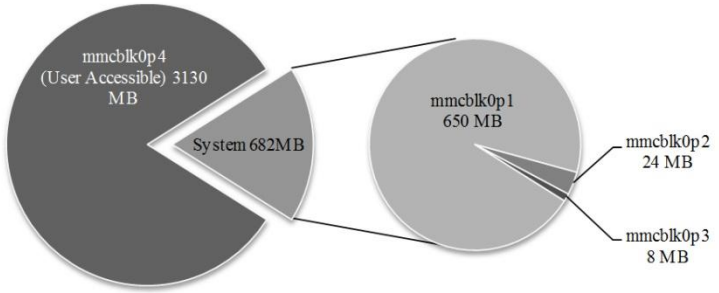
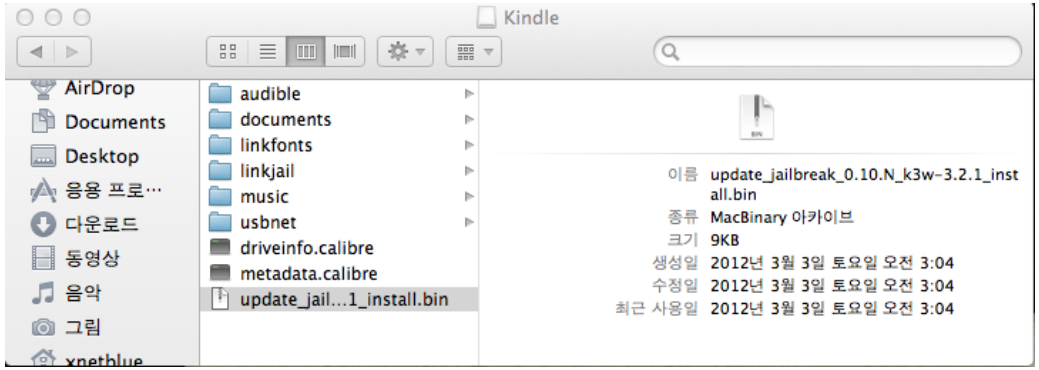


Figure 2: Kindle Disk Partitions

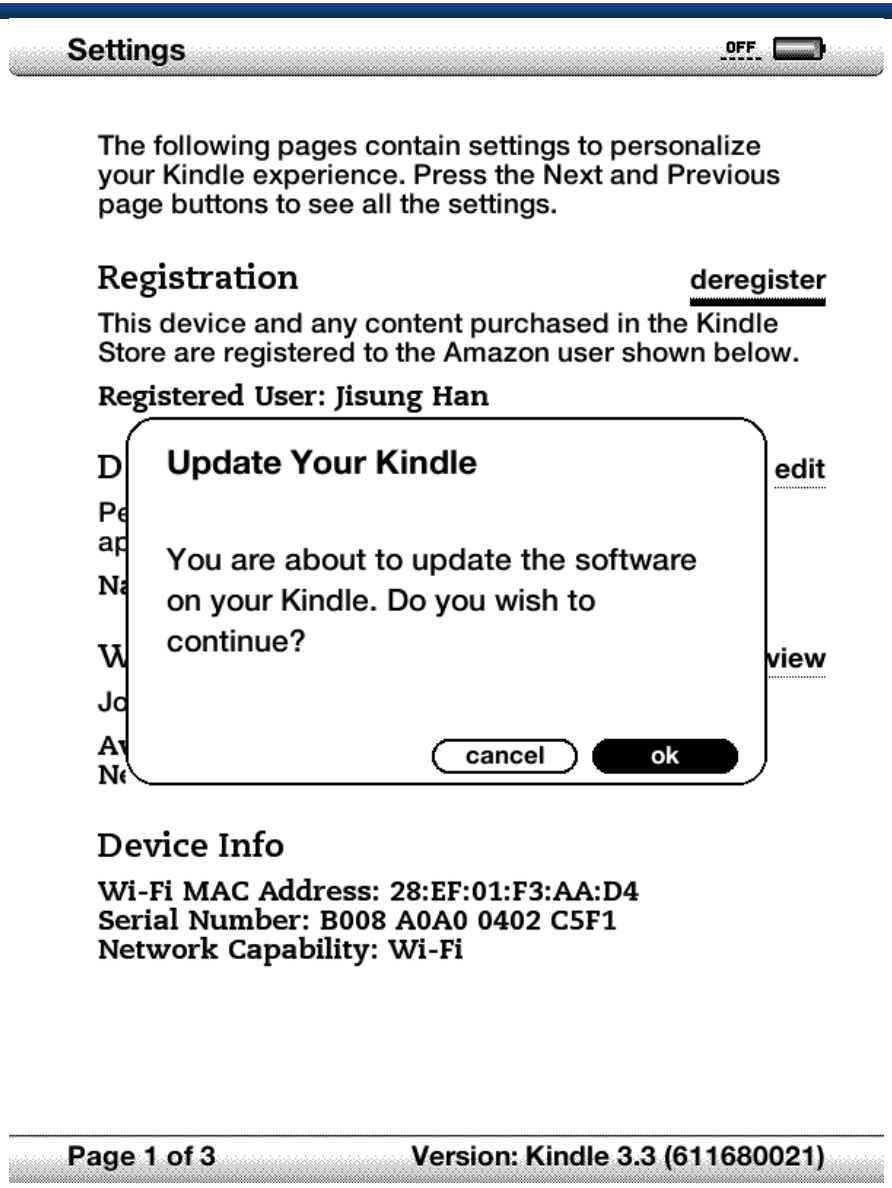
Method

Method

- kindle-jailbreak-.4.N.zip 다운로드 받고, PC에 연결
- update_jailbreak_0.4.N_0.4.N_k3g_install.bin 파일을 Kindle의 루트 디렉토리에 복사

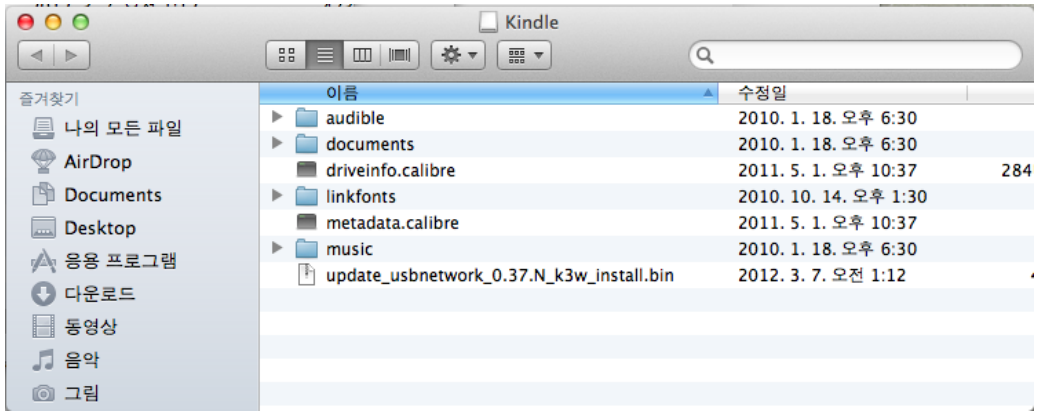


- PC에서 Kindle 연결 제거
- 킨들에서
  - *Menu | Settings | Menu | Update Your Kindle*
  - *OK*


Settings
OFF
The following pages contain settings to personalize your Kindle experience. Press the Next and Previous page buttons to see all the settings.
Registration
deregister
This device and any content purchased in the Kindle Store are registered to the Amazon user shown below.
Registered User: Jisung Han
Update Your Kindle
You are about to update the software on your Kindle. Do you wish to continue?
cancel
ok
edit
view
Device Info
Wi-Fi MAC Address: 28:EF:01:F3:AA:D4
Serial Number: B008 A0A0 0402 C5F1
Network Capability: Wi-Fi
Page 1 of 3
Version: Kindle 3.3 (611680021)

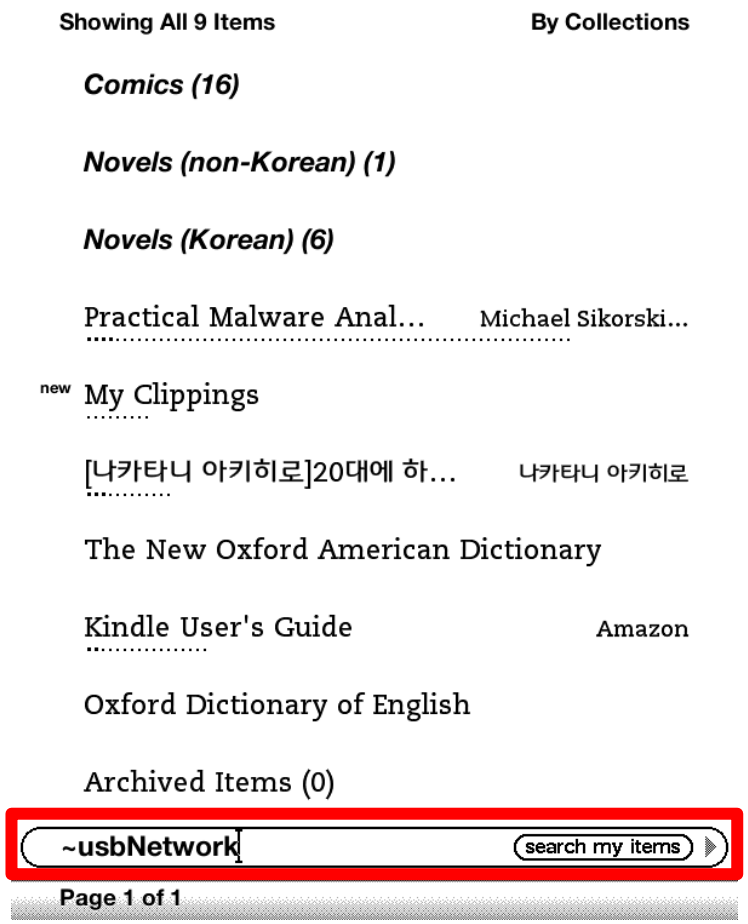
Method

- kindle-usbnetwork-0.30.N.zip 다운로드
- update_usbnetwork_0.30.N_k3g_install.bin 파일을 Kindle의 루트 디렉토리에 복사



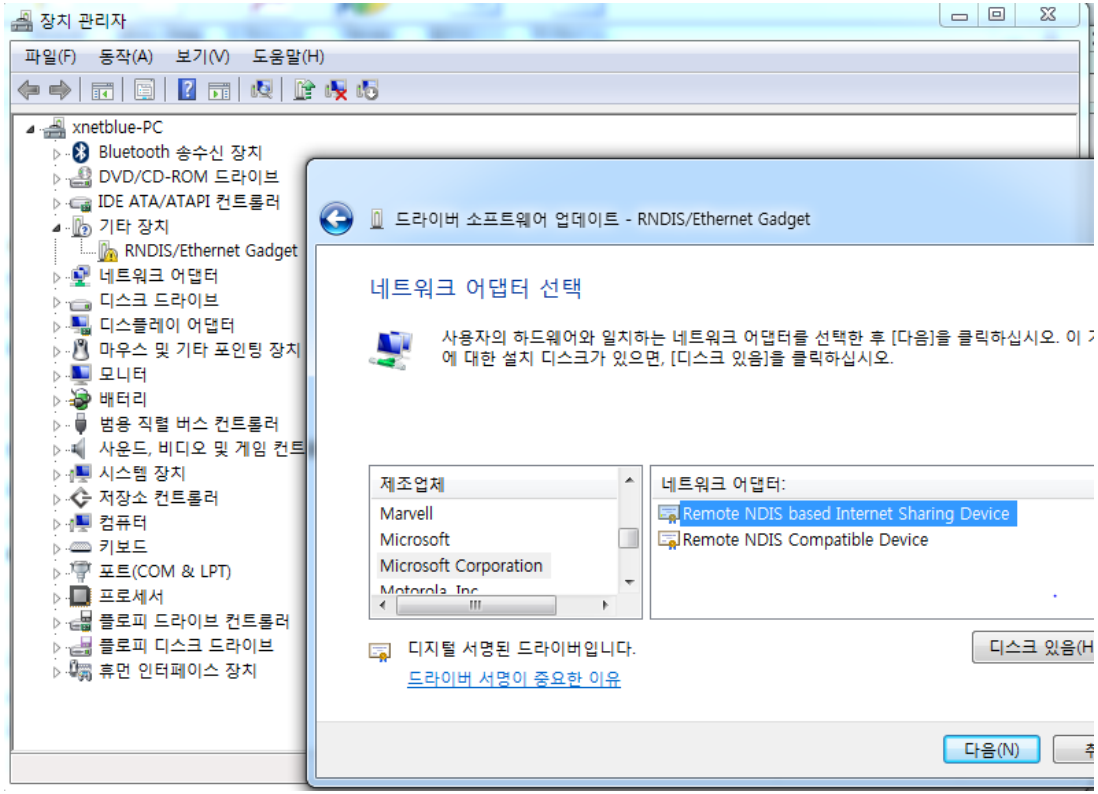
- PC에서 Kindle 연결 제거
- 킨들에서
  - *Menu | Settings | Menu | Update Your Kindle*
  - *OK*

- Kindle에서 다음을 입력

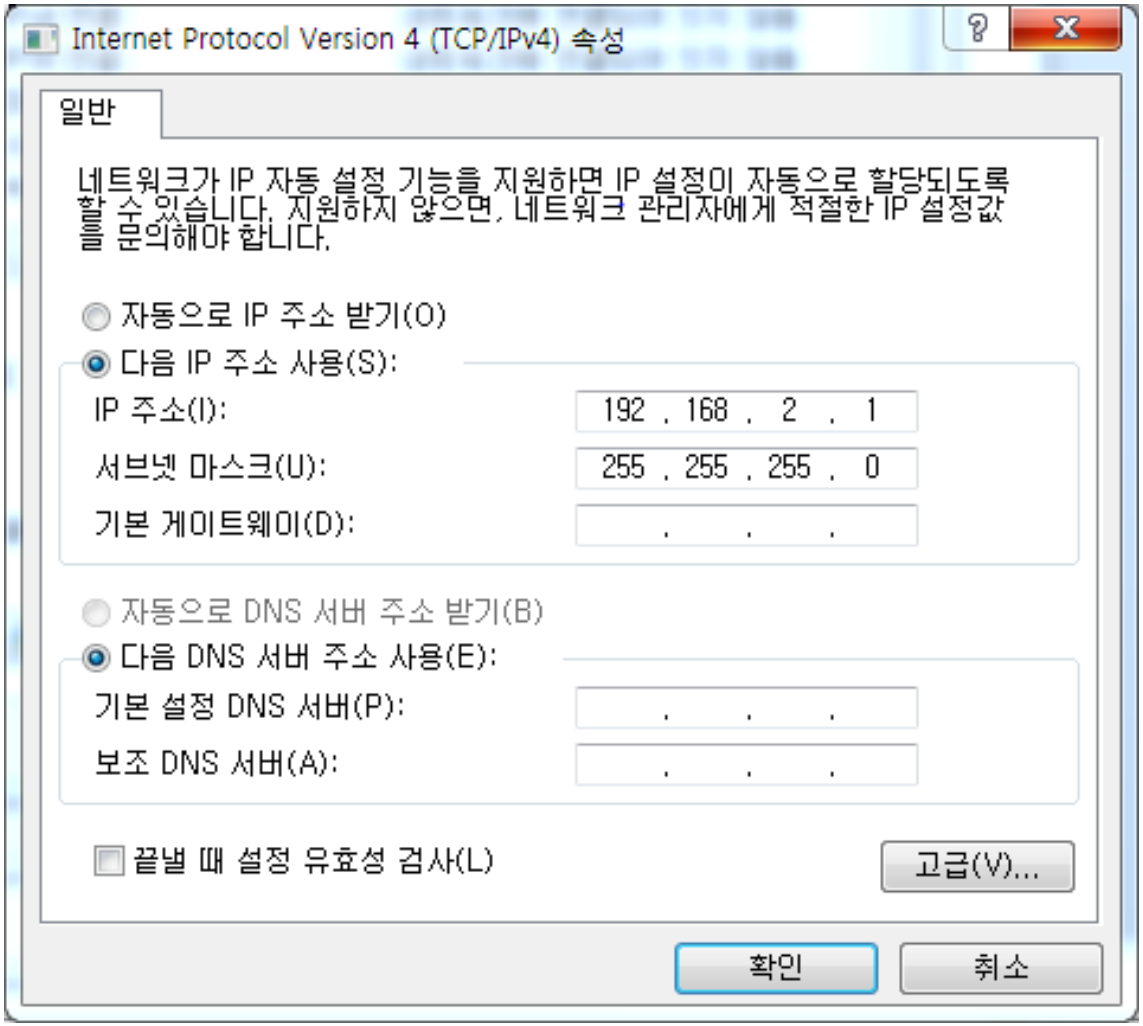


Method

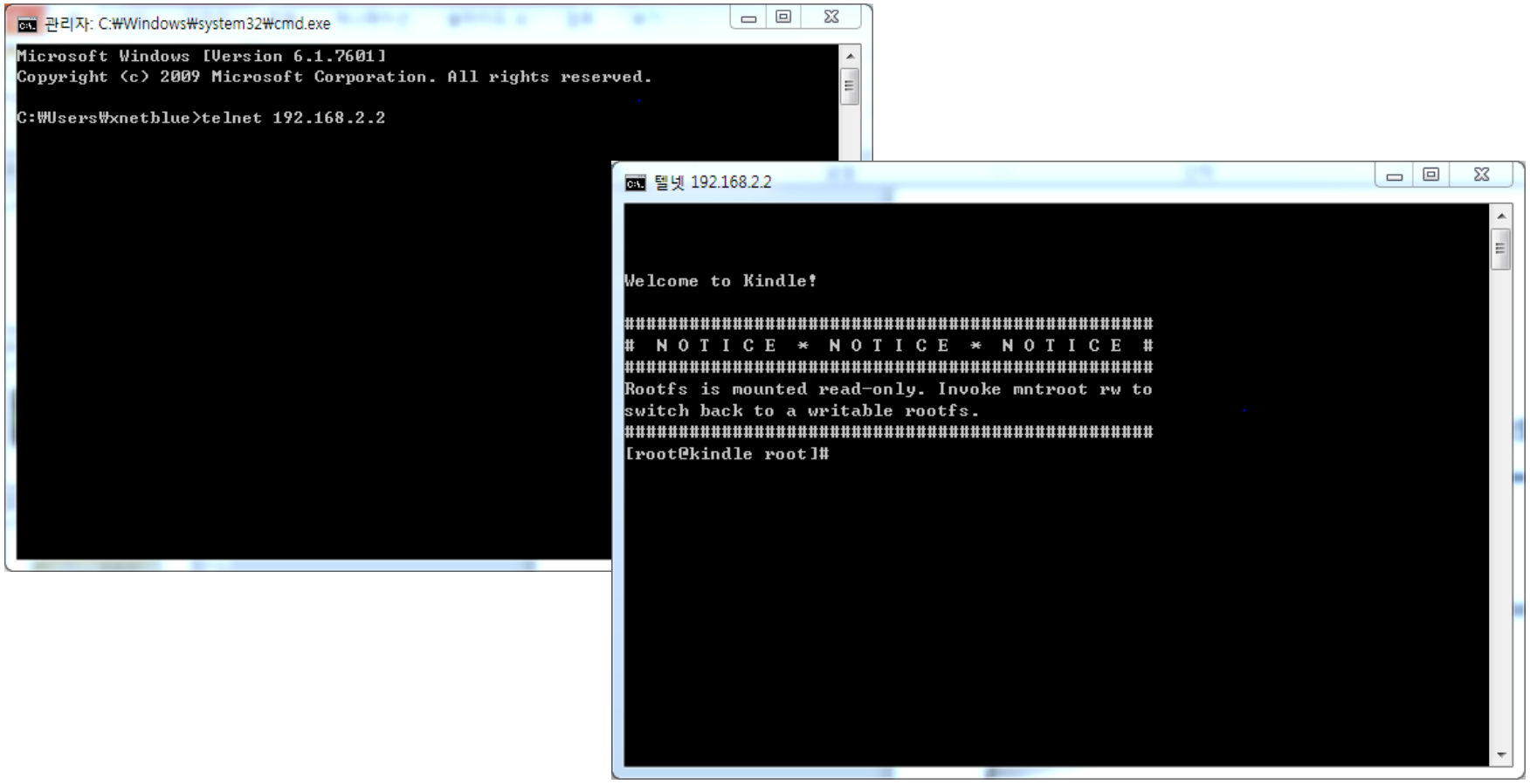
- Kindle을 PC에 연결
- *제어판 | 장치 관리자 | 네트워크 어댑터*
- RNDIS/Ethernet Gadget → 드라이버 소프트웨어 업데이트
- Microsoft Corporation – Remote NDIS based Internet Sharing Device



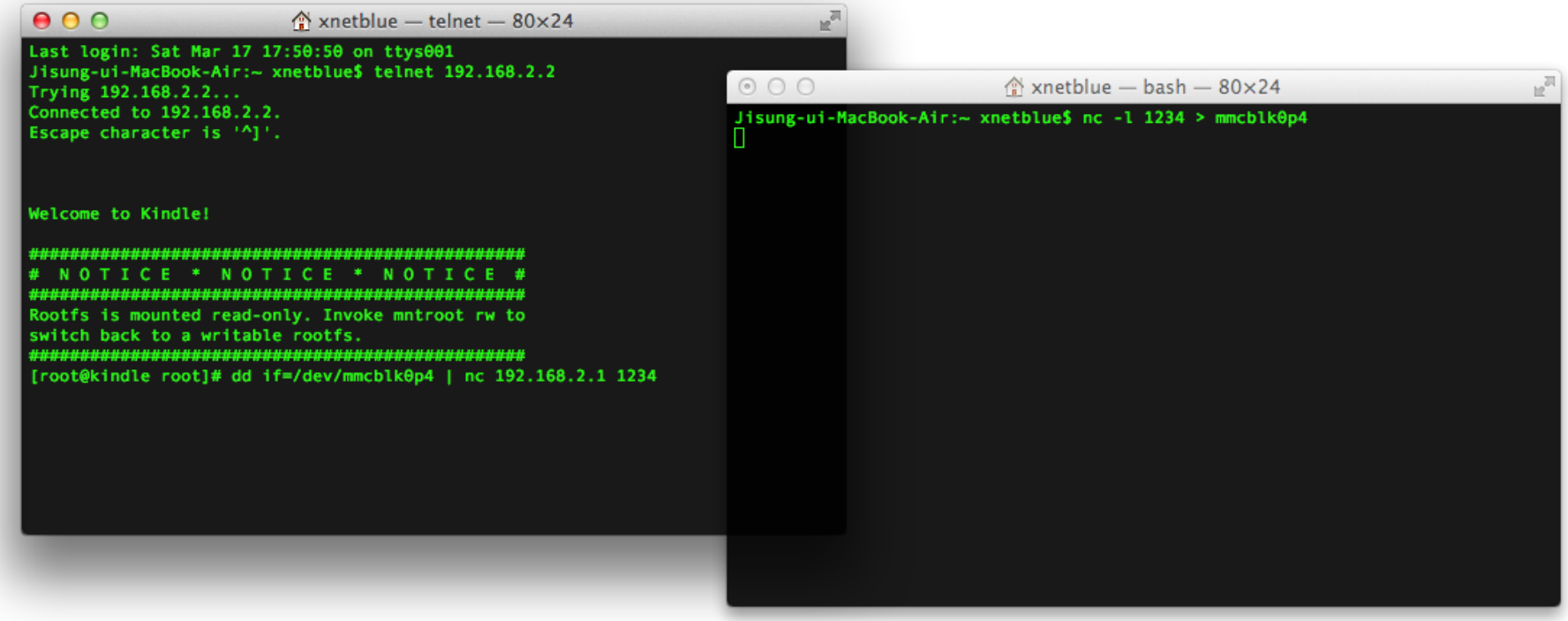
- 해당 네트워크 어댑터 IP 주소 설정



- Kindle로 Telnet 연결
  - telnet 192.168.2.2

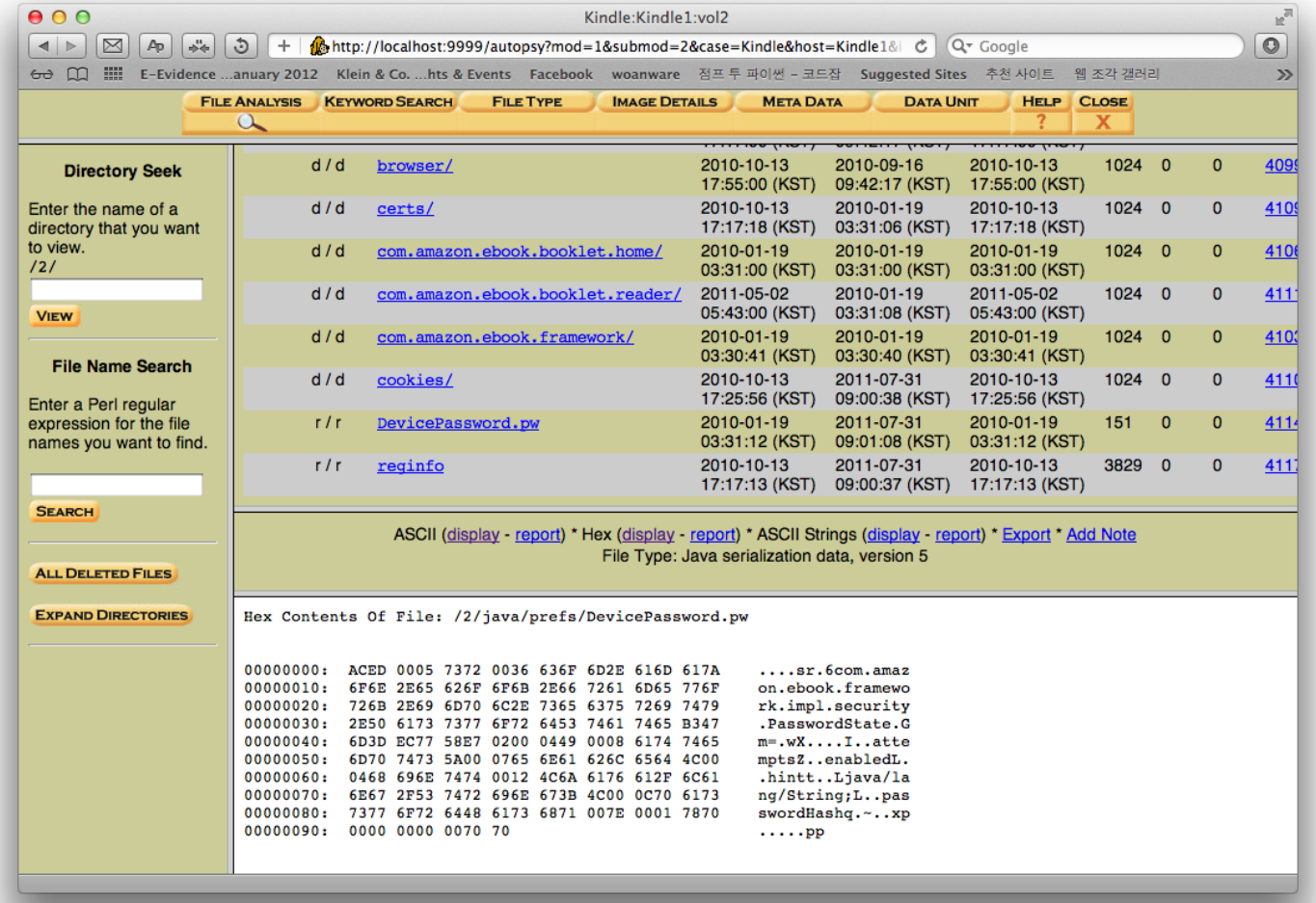


- dd를 이용해 이미징
  - Author : mmcblk0p4(user accessible partition)으로 이미징 후 복사
    - Telnet session 유실
  - Baadc0de : netcat(nc)를 통한 전송
    - 정상 전송 가능 (***추천***) – 그림 참조



Method

- Autopsy(or sleuth kit)를 이용해 분석



Results

- Kindle Files (1/2)

Content	Location	Content	Location
Active Content	Kindle-FAT32\.active-content-data\<SHA-1>	Personal Documents	Kindle-FAT32\documents\<title>-asin_<SHA-1>-<0-8>-converted-azw-type_PDOC-v_0.mbp
Audio	Kindle-FAT32\audible\<title>-asin__<Amazon Standard Identification Number>-type_AUDI-v_0.aax_<number>		Kindle-FAT32\documents\<title> azw-asin_<SHA-1>-<0-8>-azw-type_PDOC-v_0.azw
	Kindle-FAT32\audible\<title>-asin__<Amazon Standard Identification Number>-type_AUDI-v_0.pos		Kindle-FAT32\documents\<title> azw-asin_<SHA-1>-<0-8>-azw-type_PDOC-v_0.mbp
Books Downloaded	Kindle-FAT32\documents\<title>-asin_<Amazon Standard Identification Number>-type_EBOK-v_0.azw	Notice	Kindle-FAT32\documents\<title> W-asin_<SHA-1>-<number>-<number>-DEVICE_WIFI-wifi-type_PDOC-v_0.azw
	Kindle-FAT32\documents\<title>-asin_<Amazon Standard Identification Number>-type_EBOK-v_0.phl	Non-converted PDF	Kindle-FAT32\documents\<file name>.pdf
Blogs	Kindle-FAT32\documents\<title>-asin_<Amazon Standard Identification Number>-type_FEED-v_65746.azw	Sample Books Downloaded	Kindle-FAT32\documents\<title>-asin_<Amazon Standard Identification Number>-type_EBSP-v_0.azw
Magazines	Kindle-FAT32\documents\<Magazine Title><Date>-asin_<Amazon Standard Identification Number>-type_MAGZ-v_2.azw		Kindle-FAT32\documents\<title>-asin_<Amazon Standard Identification Number>-type_EBSP-v_0.tan

- Kindle Files (2/2)

Newspapers	Kindle-FAT32\documents\<Newspaper Title><Date>-asin_<Amazon Standard Identification Number>-type_NWPR-v_6.azw	Screen Saver Pictures	mmblk0p1\NONAME-ext3\opt\screen_saver
	Kindle-FAT32\documents\<Newspaper Title><Date>-asin_<Amazon Standard Identification Number>-type_NWPR-v_6.mbp	Screenshots	Kindle-FAT32\documents\screen_shot-<number>.gif
Personal Documents	Kindle-FAT32\documents\<title>-asin_<SHA-1>-<0-8>-azw-type_PDOC-v_0.azw	Thank You Letter	Kindle-FAT32\documents\Thank You Letter-asin_ThankYouLetter_ATVPDKIKX0DER_A1VC38T7YXB528-type_PSNL-v_0.azw
	Kindle-FAT32\documents\<title>-asin_<SHA-1>-<0-8>-azw-type_PDOC-v_0.mbp		Kindle-FAT32\documents\Thank You Letter-asin_ThankYouLetter_ATVPDKIKX0DER_A1VC38T7YXB528-type_PSNL-v_0.mbp
	Kindle-FAT32\documents\<title>-asin_<SHA-1>-<0-8>-converted-azw-type_PDOC-v_0.azw	User Highlights and Notes	Kindle-FAT32\documents\My Clippings.txt

- Kindle Statistics (1/2)

Statistic	Location
3G/WIFI	Kindle-FAT32\system\Audible Activation.sys B006xxxxxxxxxxx = 3G, B008xxxxxxxxxxx = WIFI only, B00Axxxxxxxxxxx = 3G Europe[3]
	mmblk0p2\LocalVars-ext3\java\prefs\com.amazon.ebook.framework\Features
	mmblk0p2\LocalVars-ext3\wan\info
Book Collections	Kindle-FAT32\system\collections.json
Bookmarks	mmblk0p2\LocalVars-ext3\java\prefs\browser\bookmarks_wv
Browser Cookies	mmblk0p2\LocalVars-ext3\browser\cookies
Browser Settings	mmblk0p2\LocalVars-ext3\java\prefs\browser\settings_wv
Current Location in Last Book Read	Kindle-FAT32\system\userannotlog
Device Email Address	mmblk0p2\LocalVars-ext3\java\prefs\com.amazon.ebook.reader\social-clipping\social-prefs
	mmblk0p2\LocalVars-ext3\java\prefs\reginfo
Device Name	mmblk0p2\LocalVars-ext3\java\prefs\reginfo
Device Password/Hint	mmblk0p2\LocalVars-ext3\java\prefs\DevicePasswork.pw
Device Settings	mmblk0p2\LocalVars-ext3\java\prefs\com.amazon.ebook.framework\prefs
Firmware Version	Kindle-FAT32\Update_<previous version>-<current version>.bin

- Kindle Statistics (2/2)

Keywords searched by user	Kindle-FAT32\system\Searched Indexes (didn't find meaningful info in here, but should look into this more)
Kindle Time	Kindle-FAT32\system\com.amazon.ebook.booklet.reader\reader.pref
Last Book Read	Kindle-FAT32\system\com.amazon.ebook.booklet.reader\reader.pref
Personal Info	mmblk0p2\LocalVars-ext3\java\prefs\com.amazon.ebook.booklet.home\com.amazon.ebook.booklet.home.prefs
Registered User	mmblk0p2\LocalVars-ext3\java\prefs\reginfo
Serial Number	Kindle-FAT32\system\AudibleActivation.sys
Time last listened to Audio Book	mmblk0p2\LocalVars-ext3\java\prefs\audiofilecache
APs Accessed	Unknown location
IMEI	Unknown location
IP Address	Unknown location
MAC Address	Unknown location
Social Networks	Unknown location
Web Browsing History	Unknown location

Conclusions

Conclusions

- **향후 과제**
  - 분석 결과 중 Unknown Locations
  - 이 문서가 제시한 방법이 아닌 다른 방법
    - User Accessible Partition에 이미지 쓰기? (하지만 netcat으로 극복 가능)
    - 반드시 root 권한이 필요한가?
      - 저자는 증거 획득에 유용하다고 판단함
  - Kindle Development Kit
    - 검증되지 않은 악성앱
  - Wireless
    - Kindle e-mail address를 통한 무선 데이터 송신 가능
      - Disk full → data 덮어쓰기를 통한 포렌식 분석 방해
      - 악성앱 전송으로 데이터 삭제

Q&A