SmartPhone Rooting

데이터 네트워크 연구실
이현호
leeo75@cs-cnu.org

Previously

- 제출률 :
- 제발...pdf 제출 좀...압축...
- 스크린 캡쳐 찍는 법
- 모르면 물어보세요
- 프로필 사진

목표

- 루팅의 목적을 안다
- 루팅을 한다
- 잘 챙긴다

A5

삼성전자 갤럭시 A5 2016 16GB

삼성페이되는 보급형 스마트폰 출시! 갤럭시 A5

4G 스마트폰 / SKT / KT olleh / LG U+ / MVNO / 광대역 LTE-A / 13.22cm(5.2인치) / 1920x1080 / 풀HD / SAMOLED / 424ppi / 안드로이드5.1 롤리팝 / 엑시노스7 7580(64bit) / 옥타코어 / 1.6GHz / 램:2GB / 내장:16GB / MicroSD / 카메라:1,300만화소 / 500만화소 / 동영상:1080p(풀HD),30fps / 손떨림보정(OIS) / 터치 포커스 / HDR / 파노라마 / 버스트샷 / 지오태그 / WiFi 다이렉트 / NFC / GPS / 핫스팟 / WiFi / 블루투스4.1 / 지문인식 / 2,900mAh / 일체형 / 스마트로테이션 / 스마트화면유지 / S보이스 / 멀티윈도우 / 팝업플레이 / 갤럭시기어 / 삼성페이 / 세로:144.8mm / 가로:71mm / 두께:7.3mm / 무게:155g / 저성능

등록철 2016.01 | 관심상품

	공기계	528,800원	5몰
1위	가개통	409,800원	30몰
2위	국내중고	338,900원	12몰

A5

[판매완료] SKT GalaxyA5(SM-A500S) 펄화이트 팝니다. 초S급이에요. | SKT 2015.05.26. 18:49

호나우진요(seta****) ●성실회원● 1:1 http://cafe.naver.com/joonggonara/268038293 주소복사

신고하기

완료

[상품거래] SKT Galaxy A5 펄화이트

안전거래 미사용
구매자가 안전거래를 신청할 수 있습니다. ?

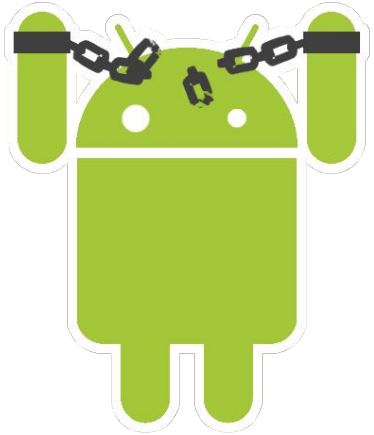
상품가격	~~33~~ 원
상품설명	150자 이내
거래방법	직접거래
배송방법	판매자와 직접 연락하세요.

네이버에 등록된 판매 물품과 내용은 개별 판매자가 등록한 것으로서,
네이버카페는 등록을 위한 시스템만 제공하며 내용에 대하여 일체의 책임을 지지 않습니다.

! 직접거래시 아래 사항에 유의해주세요.

불확실한 판매자(본인 미인증, 해외IP, 사기의심 전화번호)의 물건은 구매하지 말아주세요.
판매자와의 연락은 메신저보다는 전화, 메일 등을 이용하시고 개인정보 유출에 주의하세요.
계좌이체 시 선입금을 유도할 경우 안전한 거래인지 다시 한 번 확인해주세요.

루팅이란?



- 루팅은 폰의 최고 관리 권한을 얻는 것
  - 즉 폰의 모든 관리를 할수 있다는 것
- 쉽게 예를 들면 컴퓨터의 게스트모드와 관리자 모드!
  - 더쉽게 말하자면 집주인과 그집에 세들어 사는 사람 같은 것
    집주인은 가구나 벽지 같이 마음대로 바꾸거나 없앨수 있지만 세들어 사는 사람은 제약이 있습니다

- 루팅은 절대 불법이 아님!
- 루팅은 권한만 얻는 것 -> 루팅을 한다고해서 폰이 고장나거나 하는건 아님

출처: http://freeg159.tistory.com/7 [freeg]

루팅의 과정

- 정석은 아님 -> 찾아보고 실행
- 복구 모드에 TWRP 설치
  - 삼성은 ordin을 이용하여 설치 - *Downloads for rooting Galaxy A5 2016 SM-A510S* : (http://www.samsungsfour.com/tutorials/how-to-root-galaxy-a5-on-marshmallow-6-0-1-using-cf-auto-root-method.html)
  - twrp(https://drive.google.com/file/d/0B-vkU1R47CN0VFRibUR5U19ZcWM/view?usp=sharing)
- SuperSu 설치
- adb 로 접속 후 root권한 획득

휴대폰 설정

- 설정 -> 디바이스 정보 -> 소프트웨어 정보 -> 빌드번호 연타!
- 설정 -> 개발자 옵션 -> OEM 잠금해제, USB 디버깅 활성화

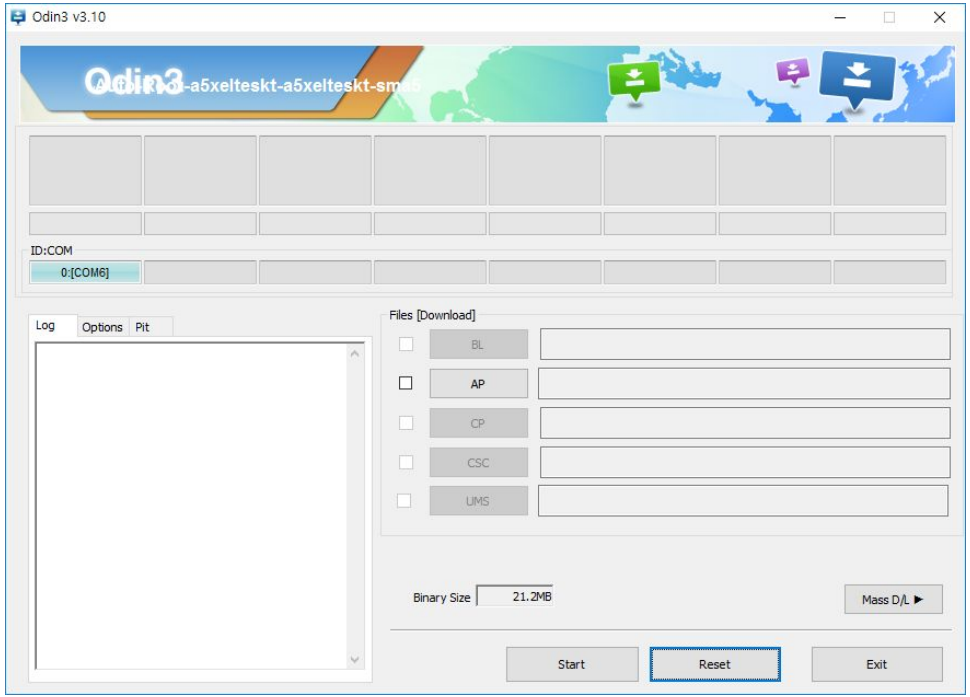
Rooting with WINDOWS

삼성은 ordin을 이용하여 설치

- 스마트폰
- Down load Mode
- 볼륨 아래키 + 전원 + 홈

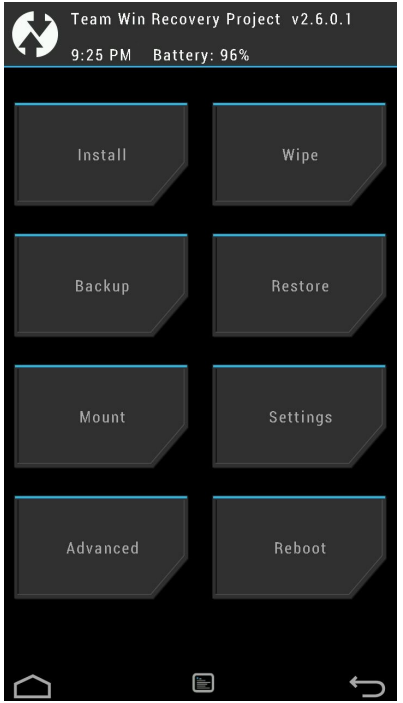
odin 실행

AP -> twrp 설치



복구모드

- 볼륨 상버튼 + 전원버튼+ 홈
- /sdcard/Download/ 에 SuperSu 이동 (pull)
- Install SuperSu
  - https://drive.google.com/file/d/0B-vkU1R47CN0UUt2dDdMQXRaTG8/view?usp=sharing
- ***ADB shell 이 필요!***
- Install /sdcard/Download/SuperSu
- Swipe to confirm Flash



ADB Shell
with
LINUX

ADB (Android Debug bridge)

- adb shell로 안드로이드 기기에 접속
- https://developer.android.com/studio/index.html?hl=ko#Other
- 참고 : http://wowan.tistory.com/118

명령줄 도구만 다운로드

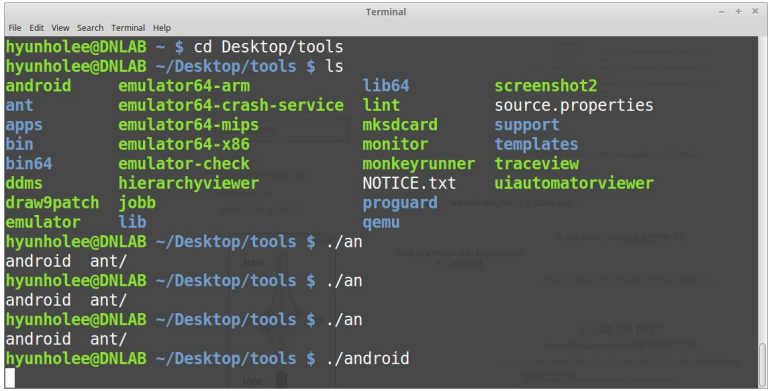
Android Studio가 필요 없으면 아래에서 기본 Android 명령줄 도구를 다운로드할 수 있습니다.

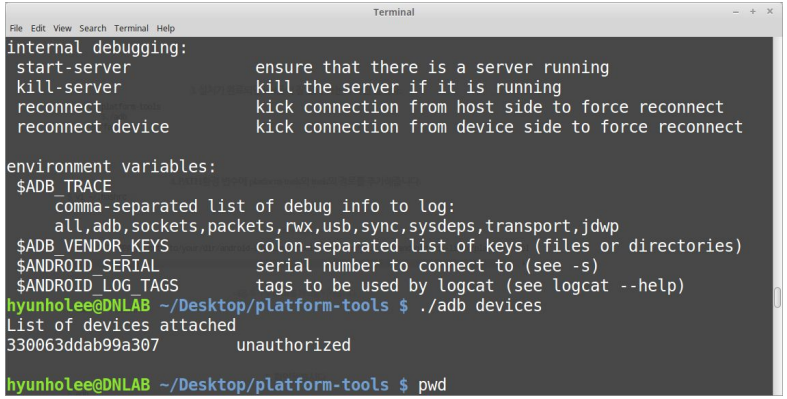
플랫폼	SDK 도구 패키지	크기	SHA-1 체크섬
Windows	tools_r25.2.3-windows.zip	292 MB (306,745,639 bytes)	23d5686ffe489e5a1af95253b153ce9d6f933e5dbabe14c494631234697a0e08
Mac	tools_r25.2.3-macosx.zip	191 MB (200,496,727 bytes)	593544d4ca7ab162705d0032fb0c0c88e75bd0f42412d09a1e8daa3394681dc6
Linux	tools_r25.2.3-linux.zip	264 MB (277,861,433 bytes)	1b35bcb94e9a686dff6460c8bca903aa0281c6696001067f34ec00093145b560

SDK 도구 릴리스 노트를 참조하세요.

ADB

- 압축 해제한 디렉토리에서 ./android로 SDK 매니져 실행





ADB push / pull

- adb push 파일이름 안드로이드 위치 : 안드로이드에 파일을 올림
- adb pull 안드로이드의 위치 파일 이름 : 안드로이드의 파일을 가져옴

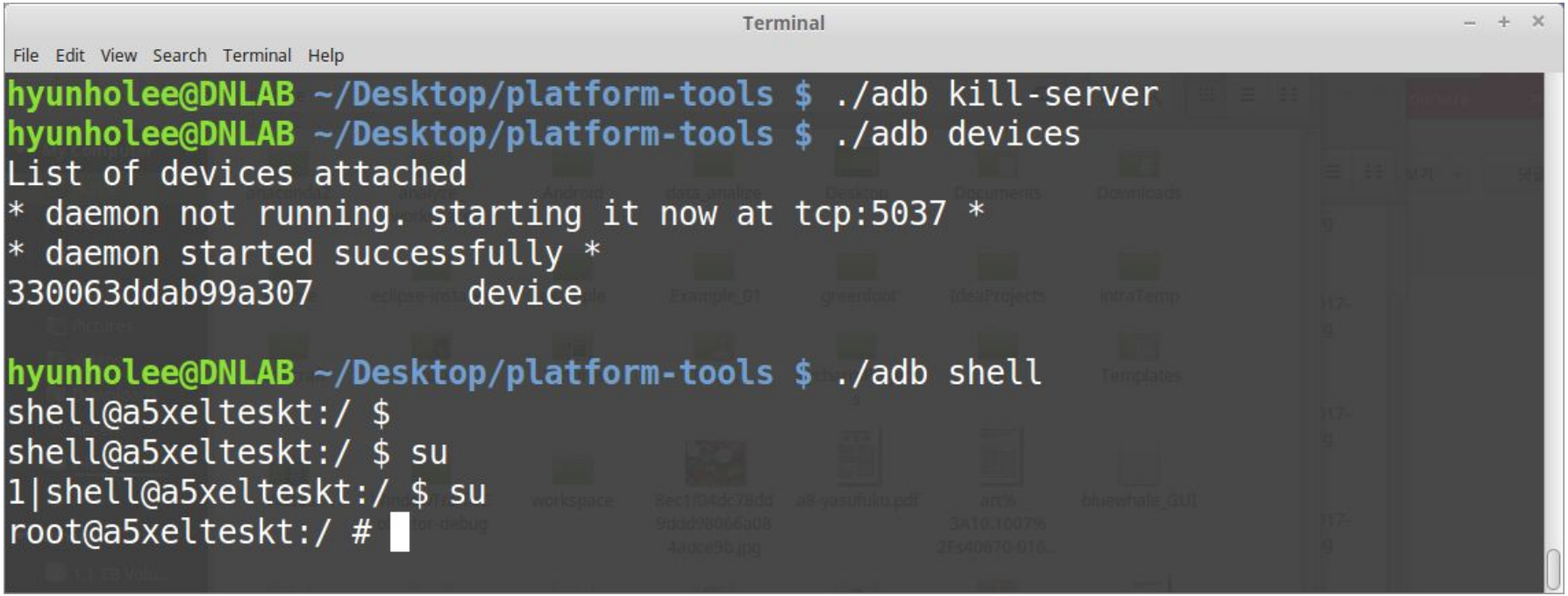
```
hyunholee@DNLAB ~/Desktop/platform-tools $ sudo ./adb push /home/hyunholee/Deskt
op/SR2-SuperSU-v2.79-SR2-20170103215521.zip /sdcard/Download
[sudo] password for hyunholee:
/home/hyunholee/Desktop/SR2-SuperSU-v2...ed. 5.0 MB/s (5941186 bytes in 1.140s)
```

```
hyunholee@DNLAB ~/Desktop/platform-tools $ sudo ./adb pull /data/local/test3.pca
p test.pcap
/data/local/test3.pcap: 1 file pulled. 5.9 MB/s (5582214 bytes in 0.895s)
```

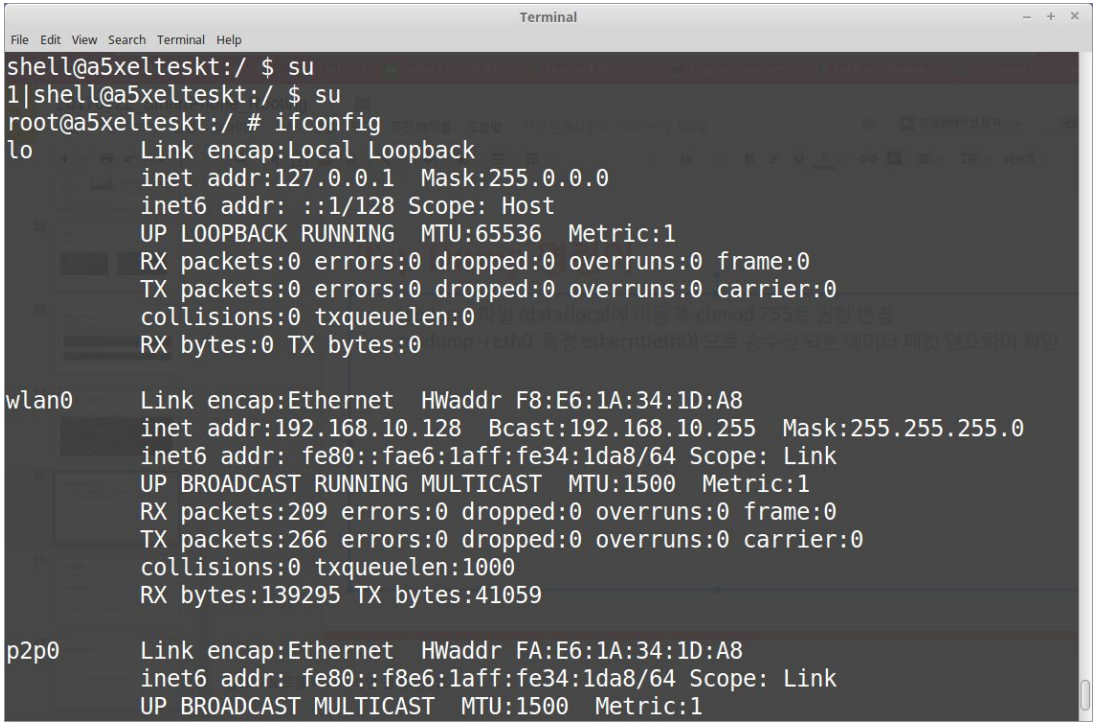
push tcpdump

- tcpdump를 실행권한이 낮은 /sdcard/Download 로 이동한다
- /sdcard/Download -> /data/local 로 이동한다
- 1 . adb push tcpdump /sdcard/Download
- 2. adb shell
- 3. su
- 4. mv /sdcard/Download/tcpdump /data/local

ADB shell 명령어



ifconfig


Terminal
File Edit View Search Terminal Help
shell@a5xelteskt:/ $ su
1|shell@a5xelteskt:/ $ su
root@a5xelteskt:/ # ifconfig
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope: Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:0 TX bytes:0
wlan0 Link encap:Ethernet HWaddr F8:E6:1A:34:1D:A8
inet addr:192.168.10.128 Bcast:192.168.10.255 Mask:255.255.255.0
inet6 addr: fe80::fae6:1aff:fe34:1da8/64 Scope: Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:209 errors:0 dropped:0 overruns:0 frame:0
TX packets:266 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:139295 TX bytes:41059
p2p0 Link encap:Ethernet HWaddr FA:E6:1A:34:1D:A8
inet6 addr: fe80::f8e6:1aff:fe34:1da8/64 Scope: Link
UP BROADCAST MULTICAST MTU:1500 Metric:1

Tcp Dump 명령어

- tcpdump 파일 /data/local에 이동 후 chmod 755로 권한 변경
- tcpdump -i eth0 특정 ethernt(eth0) 으로 송수신 되는 데이터 패킷 덤프하여 확인
- tcpdump -w output.pcap 캡쳐한 패킷들을 output.pcap 파일에 저장

Raspberry pi

Raspberry pi를 AP로 만들기

- 참고 : http://momoci99.blogspot.kr/2016/08/3-ap.html
- 라즈베리파이와 안드로이드 연결

Assignment

- Q1. 루팅 과정 및 안드로이드에서 ifconfig 실행화면
- Q2. 주어진 pcap파일에서 검색 키워드 찾기 (각 2 개씩)
- Q3. coupang, gmarket 앱실행 후 검색한 뒤 키워드 찾기
- Q4. coupang, gmarket의 키워드 패킷에 대한 아래 질문에 답하기

Question

1. Is the frame an outgoing or an incoming frame?
2. What is the source IP address of the network-layer header in the frame?
3. What is the destination IP address of the network-layer header in the frame?
4. What is the total number of bytes in the whole frame?
5. What is the number of bytes in the Ethernet (data-link layer) header?
6. What is the number of bytes in the IP header?
7. What is the number of bytes in the TCP header?
8. What is the total bytes in the message (at the application layer)?

Answer

Question	Answer
Outgoing or incoming	
Source IP address	
Destination IP address	
Total number of bytes	
Number of bytes in the Ethernet header	
Number of bytes in the IP header	
Number of bytes in the TCP header	
total bytes in the message	

과제 제출

- 과제 제출 기한:
  - 실습 하루 전 18시
- Google Classroom에 제출
  - E-mail이 아닌 Classroom
- 보고서 제목 : DC_학번_이름_실습번호.pdf
- 추가 첨부파일 : DC_학번_이름_실습번호.zip

제출 파일 내용

- DC_학번_이름_실습번호.zip
  - 각종 소스코드
  - 그 외 파일
  - 보고서는 .pdf (**DC_학번_이름_실습번호.pdf**)
  - .hwp/.doc 등 채점 안 함
- 파일 이름 준수!
  - 파일 이름이 다를 경우 채점 안 함

보고서

- 과제를 해결한 방법
  - 주요 소스코드 포함 및 주석
- 과제를 해결하기 위해 알아야 하는 것
- 결과 화면 캡쳐와 설명
- 기본적으로 보고서는 자신이 직접 과제를 해결했다는 것을 증명하기 위함