네트워크 포렌식 스터디

CERT-IS

양윤지

19.11.17.일요일

17장 무선 패킷 분석

무선랜: 와이파이 등 🡪보안: 파이어월, VPN // 백도어

1. 무선랜 개요

1) 무선 네트워크 유형

-WPAN: 단거리 Ac Hoc 방식 or Peer to Peer 방식

🡪노트북간의 데이터 전송이나 핸드폰과 헤드셋과 같이 한 쌍을 이루는 무선 단말기에 사용

🡪블루투스는 마우스와 키보드에서 유선 라인을 대신해 사용

-WLAN: 유선랜의 확장개념 또는 유선랜의 설치가 어려운 지역으로의 네트워크 제공

🡪WLAN은 임시 사무실과 같은 환경에서 유선랜 구축으로 인해 발생되는 불픽요한 비용소모 줄임

-WMAN: 대도시와 같은 넓은 지역을 대상으로는 높은 전송속도를 제공

🡪대학 캠퍼스와 같은 넓ㅅ은 지역에서 건물간의 무선 연결 기능을 제공

2) 무선랜 표준

-802.11: (1997) 2.4GHz 2Mbps 20~100M

-802.11a: (1999) 5GHz 54Mbps 35~120M

-802.11b: (1999) 2.4GHz 11Mbps 38~140M

-802.11g: (2003) 2.4GHz 54Mbps 38~140M

-802.11n (2009?) 2.4~5GHz 300Mbps 70~250M

3) 무선랜 구성요소

-무선 단말기: SSID(Service Set Identifier), 인증, 암호화 설정 충족

-무선 AP: 단말기의 무선랜 접속 관여.

4) 주요 취약점

-도청: 무선 AP 존재여부, 데이터 수신

-서비스 거부: 클라이언트와의 통신 시 SSID + ‘Probe Request’ 브로드캐스트 🡪 ‘Probe Response’

다량의 request 무선 AP로 전송하면 response 동작 반복으로 다른 단말기 접속 불가

-불법 AP: 불법 AP 설치, 전송 데이터 수집,, 위치 파악 어려움

+WEP 인증 취약점: 클라이언트-AP 공유키로 암호 인증. 공유키의 KEY ID, IV 값 평문으로 전달.

-짧은 길이의 초기벡터(IV)값의 사용으로 IV 값의 재사용 가능성 높음

-불완전한 RC4 암호 알고리즘 사용으로 인한 암호키 노출 가능성

-짧은 길이의 암호키 사용으로 인한 공격 가능성

-암호키 노출로 인한 무선 전송데이터의 노출 위험성

+WPA/WPA2: 초기 무선랜 접속 인증 시 Presharde 키 값(PSK) 패킷 수집으로 일반적인 단어, 짧은 자리수 암호 유추 가능. 고정된값이 아니라 암호화 키 값 유추x.

2. 무선 패킷 분석

-802.11 패킷 복호화: 키 값 알아야 됨

\*\*와이어샤크 무선패킷 복호화(WEP, WPA/WPA2):

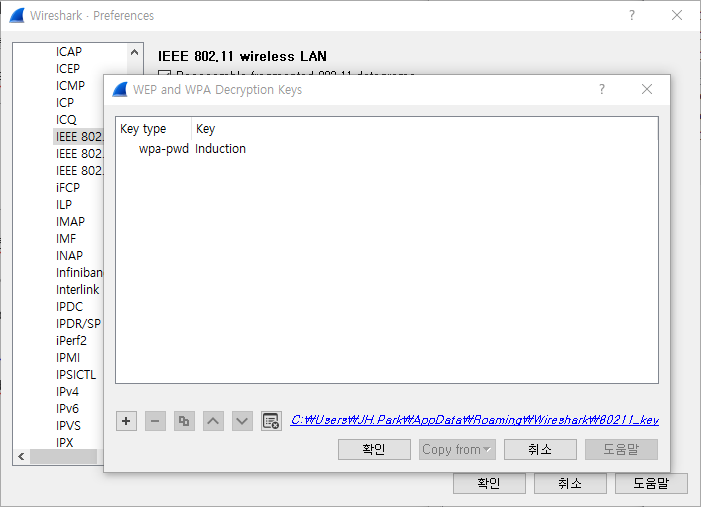
[Edit]-[Preference]-[User Interface]-[Protocol]-[IEEE 802.11]

01:02:03:04:05 (40/64비트 WEP 방식)

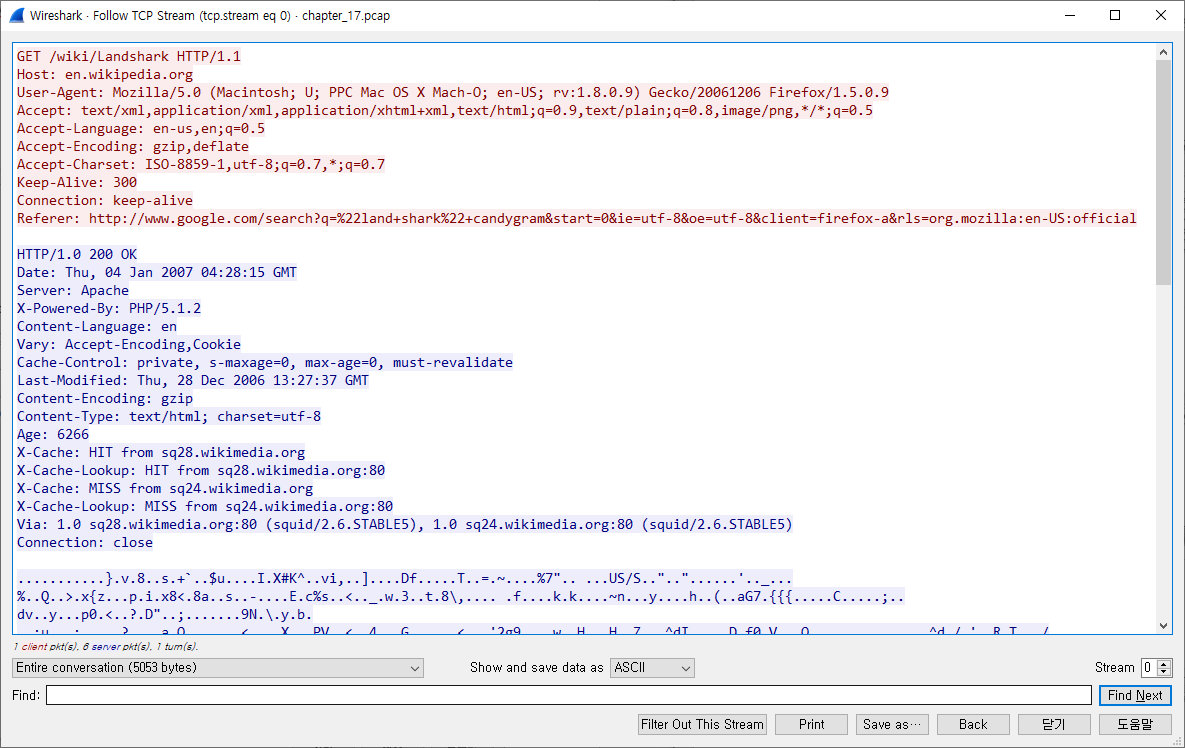
wpa-psk:0102030405060708091011…6061626364 (104/128비트 WEP 방식)

wpa-pwd:Induction:Coherer (WPA + 암호 값 + SSID)

1) chapter\_17.pcap 파일 복호화



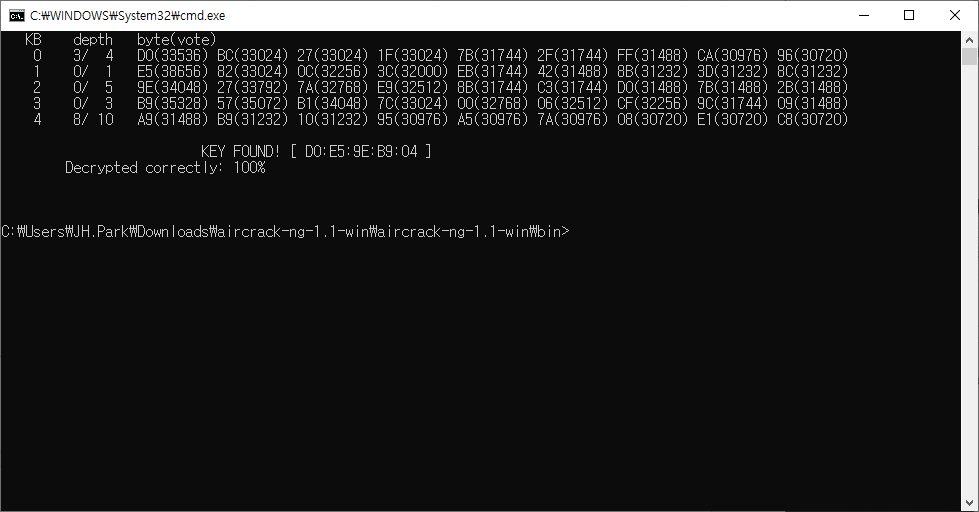
wpa-pwd:Introduction



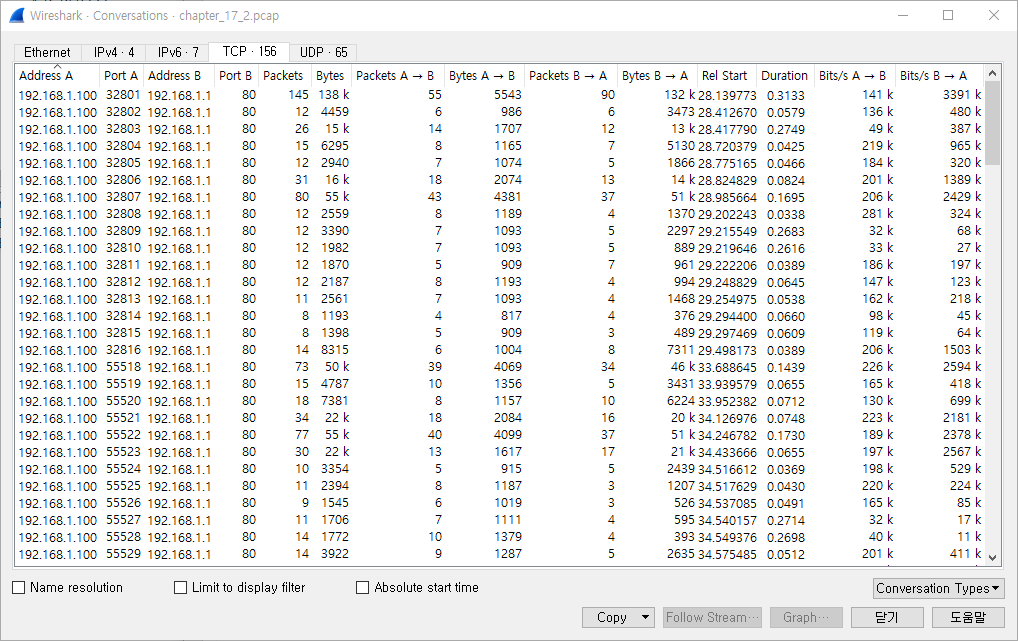
🡪 복호화 완료

\*[View]-[Wireless Toolbar] 이게 없네

2) chapter\_17\_2.pcap 파일 복호화



\*\*Aircrack-ng GUI.exe로 키 값 크랙: D0:E5:9E:B9:04



TCP 패킷들이 복호화되어 보인다.

3) 무선 AP 접속 계정과 암호 및 WAP 변경 암호

(연구실 컴퓨터가 무선랜을 사용하지 않아서 실습은 x)

[Analyze]-[Expert Info Composite]: 접속한 HTTP 페이지 정보

[Chat] or [경고] 탭: 어떤 HTTP 페이지 요청했는지 확인

-GET: 요청한 페이지

-Host: 접속한 서버

-User-Agent: 접속에 사용한 웹 브라우저

-Accept: 수신에 사용되는 미디어 타입

-Accept-Language: 수신에 사용되는 언어 타입

-Accept-Encoding: 수신에 사용되는 인코딩 타입

-Accept-Charset: 수신에 사용되는 언어 타입

-Keep-Alice: 클라이언트와 서버간 connection 일정시간 지속

-Reference: 경유지

-Authorization: 인증정보: AP 페이지에 접근여부 결정

4) WEP 인증 변경 암호

HTTP를 알아야 몬가 보일 것 같다

어제 양종헌 선배님의 웹해킹 강의에서 GET 방식과 무슨 방식이 있었는데 이건 GET 방식같다.