네크워크 패킷에서 이미지 복원하기

WireShark 실습

목적 및 개요

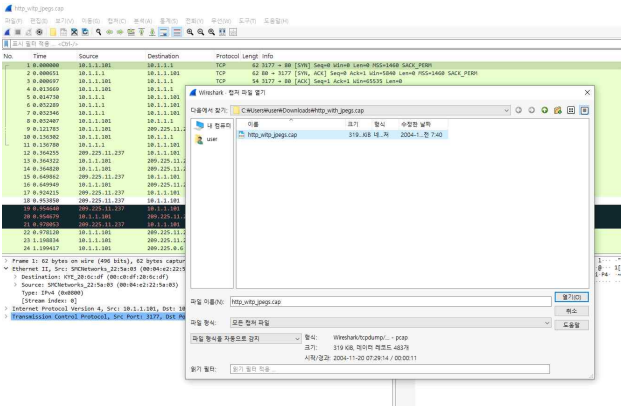
- Wireshark 캡처 파일에서 이미지 추출 절차 소개
- JPEG 시그니처 기반 수동 복원 실습 포함
- 디지털 포렌식, 분석 실무에 필요한 기본기 학습 목적

실습 파일 준비

- 샘플 캡처 파일 다운로드
  - https://wiki.wireshark.org/samplecaptures
  - https://creamerburger.tistory.com/72
    - 다운받고 압축풀기 귀찮으신 분들 제 티스토리에서 받아주세요
  - 예시: http_witp_jpegs.cap
- Wireshark에서 파일 열기

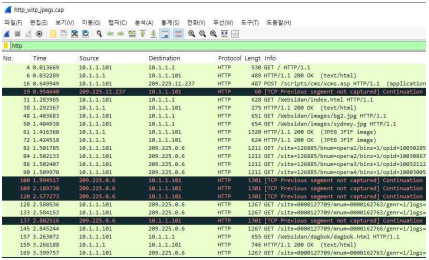
실습 파일 준비

- 파일 > 열기


http_witp_jpegs.cap
Wireshark · 캡처 파일 열기
C:₩Users₩user₩Downloads₩http_with_jpegs.cap
내 컴퓨터
user
이름
크기
항목
수정한 날짜
http_witp_jpegs.cap
319 KB
네...개
2004-1...전 7:40
파일 이름(N):
http_witp_jpegs.cap
열기(O)
취소
도움말
파일 형식:
모든 캡처 파일
파일 형식을 자동으로 감지
형식:
Wireshark/tcpdump/... - pcap
크기:
319 KB, 파이더 레코드 483개
시작/경과: 2004-11-20 07:29:14 / 00:00:11
읽기 필터:
읽기 필터 적용

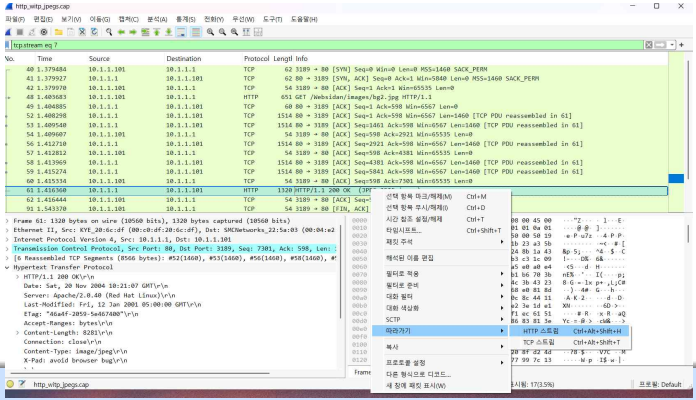
HTTP 패킷 필터링

- 필터: http 입력
- 이미지 포함 HTTP 응답 확인
- 크기 큰 패킷, 응답 본문에 이미지 포함 가능성 높음
- 하단에 이미지 관련된 패킷 존재



HTTP 스트림 저장

- 대상 패킷 우클릭 → 따라가기 → HTTP 스트림

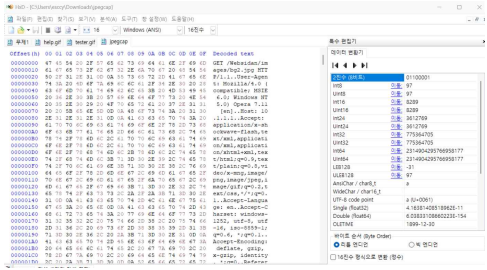


RAW 파일 저장

- 하단 옵션: Raw 선택
- 저장 후 확장자 없는 파일 생성됨 (실제 이미지 바이너리 포함)

Hex Editor 설치 및 사용

- HxD 다운로드
  - https://mh-nexus.de/en/downloads.php?product=HxD20
- 파일 열기 또는 새 창 생성
- Wireshark에서 저장한 Raw 파일 열기



파일 시그니처 개념과 구조

- 파일 시그니처(Signature)
  - 특정 파일 포맷이 가지는 고유한 바이트 패턴
  - 일반적으로 파일 시작(Header) 또는 파일 끝(Footer)에 존재
  - Hex 편집기나 포렌식 도구에서 파일 식별 및 복원 근거로 사용
- 구조 분류
  - 고정형 시그니처: 위치와 바이트값이 명확히 정의됨 (예: JPEG, PNG)
  - 가변형 시그니처: 일부 포맷은 끝 시그니처가 없음, 또는 CRC 등으로 결정됨 (예: ZIP, PNG)

파일 시그니처 개념과 구조

- Hex에서의 표현 방식 예시
  - Hex: FF D8 FF → JPEG 시작
  - ASCII: %PDF → PDF 시작
- 시그니처 사용 목적
  - 데이터 손상 복구
  - 메모리/디스크 덤프에서 유효 파일 추출
  - 악성코드 은닉 탐지 (확장자 위장이 아닌 시그니처 확인)

JPEG 포맷 분석 및 시그니처 탐색

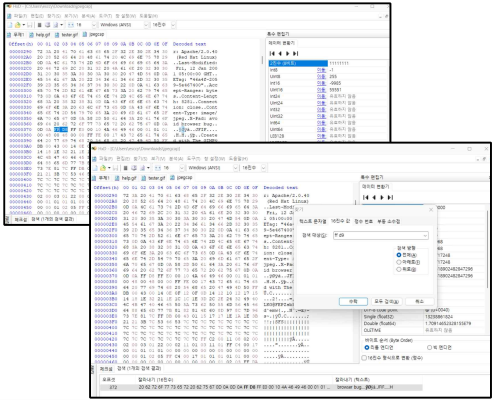
- JPEG 파일 구조
  - JPEG은 세그먼트 기반 포맷으로, 각 마커(marker)는 0xFF로 시작
  - 대표적인 마커:
  - FF D8 → Start Of Image (SOI)
  - FF D9 → End Of Image (EOI)
- 파일 시작 시그니처
  - FF D8 FF
  - FF D8 → SOI
  - 뒤따르는 FF는 JFIF, EXIF 등 메타 정보 시작 마커 (FF E0, FF E1 등)
- 파일 종료 시그니처
  - FF D9
  - 모든 JPEG은 이 바이트로 종료
  - 이후 데이터는 무시하거나 삭제 가능

기타 포맷 시그니처 비교

포맷	시작 시그니처 (Header)	종료 시그니처 (Footer)	설명
JPEG	FF D8 FF	FF D9	가장 흔한 이미지 포맷
PNG	89 50 4E 47 0D 0A 1A 0 A	CRC 끝	비손실 압축, 시그니처 고유
GIF87a	47 49 46 38 37 61	00 3B	구형 GIF
GIF89a	47 49 46 38 39 61	00 3B	애니메이션 지원
PDF	25 50 44 46	25 45 4F 46	텍스트 기반 문서 포맷
ZIP	50 4B 03 04	50 4B 05 06	압축 포맷, DOCX 계열 기반
EXE	4D 5A (MZ)	없음	윈도우 실행 파일

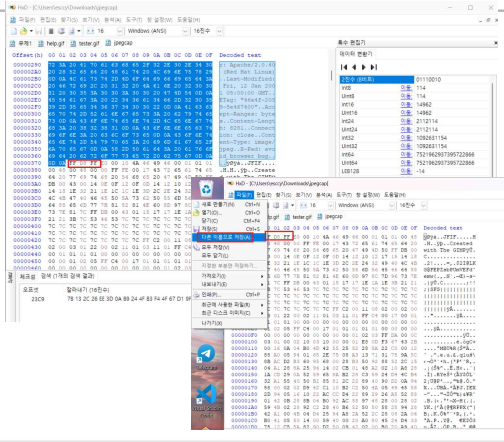
JPEG 시그니처 분석

- JPEG 시작 시그니처 (Header):
  FF D8 FF (Ctrl + F 버튼으로 검색 후, 16진수 탭 선택 > FF D8 검색)
- JPEG 종료 시그니처 (Footer):
  FF D9 (Ctrl + F 버튼으로 검색 후, 16진수 탭 선택 > FF D8 검색)



JPEG 시그니처 분석

- 시작 위치로 이동 후 그 앞 부분 삭제
- 다른 이름으로 저장 > 파일이름.jpg로 저장



해당 .jpg 파일 열어보기

- 잘 복원되었습니다

미션

- https://creamerburger.tistory.com/72
- 해당 사이트 하단에 있는 ybo.pcapng 파일에서 융보공과 관련된 포스터를 추출해보세요. 가운데 있는 사람이 누군지 맞춰보세요!
- 힌트 : JPG 말고 다른 이미지 형식입니다.