





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

- <u>https://wiki.wireshark.org/samplecaptures</u>
- 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

파일(F) 편집(B) 부기(V) 이동(G) 철책(C) 분석(A) 올게(S) 전희(Y) 우선(W) 도구(T) 도용할(H

🖌 = ८ 8 📒 🗅 🕱 🖻 ९ + + 🕾 T 🛓 🚍 ९ ९ ९ ९ 🗉 🖂 표시 딸린 작용 ... <001-/> Time Destination Protocol Lenot Info 10.1.1.101 10.1.1.1 62 3177 - 80 [SWN] Seq=0 Win+0 Len=0 NSS=1460 SACK PERM 10.1.1.1 10.1.1.1 TCP 10.1.1.101 54 3177 - 80 [ACK] Seg=1 Ack+1 Min+65535 Len+0 4 0.013660 10.1.1.1 10.1.1.101 📕 Wireshark - 접치 파일 열기 10.1.1.1 10.1.1.1 10.1.1.101 다음에서 찾기: 🦲 C.#Users#user#Downloads#http_with_jpegs.cap 10.1.1.1 10.1.1.101 10.1.1.101 10.1.1.1 🥦 내 컴퓨터 이름 표기 형식 수정찬 날짜 289.225.11.2 10.1.1.101 http_witp_jpegs.cap 319.358 네..저 2004-1_천 7:40 10.1.1.101 10.1.1.1 2 user 10.1.1.101 10.1.1.1 12 0.364255 209.225.11.237 18.1.1.101 18.1.1.281 289.225.11 289.225.11. 18.1.1.181 209.225.11.237 18.1.1.101 289.225.11. 289.225.11.237 18.1.1.101 289.225.11.237 18,1,1,101 19.0.554540 209.225.11.223 10-1-1-101 289,225,11 23 1.198834 18.1.1.181 289.225.11. 26 1.199417 19.1.1.101 289.225.0.6 > Frame 1: 62 bytes on wire (496 bits), 62 bytes captur 8 .. 15 * Ethernet II, Src: SWCNetworks_22:5a:05 (00:04:e2:22:5 > Destination: KYE_20:0c:df (00:c0:df:20:0c:df) > Source: SHCNetworks_22:5a:83 (80:84:e2:22:5a:83) Type: 1Pv4 (0x8808) 9271(D) (Stream index: 8) Reg Olector http://tp.jpegs.cap > Internet Protocol Version 4, Src: 18.1.1.181, Dst: 1 취소 Transmission Control Protocol, Src Port: 3177, Ost Po 파일 형식: 모든 참처 파일 ~ 588 파일 형식을 자동으로 감지 v \$4: Wireshark/tcpdump/__ - pcap 319 KB, 데이터 레코트 483개 시원/경2는 2004-11-20 07:29:14 / 00:00:11 第7 월타: 87 월터 적용

0



HTTP 패킷 필터링

□ 필터: http 입력

□ 이미지 포함 HTTP 응답 확인

□ 크기 큰 패킷, 응답 본문에 이미

지 포함 가능성 높음

A http witp ipegs.cap 편집(E) 보기(V) 이용(G) 접자(C) 분석(A) 통계(S) 전좌(Y) 무선(W) 도구(T) 도용말(H

| No. | Time | Source | Destination | Protocol | Lengt Info |
|-----|---------------|----------------|----------------|----------|--|
| | 4 0.013569 | 10.1.1.101 | 10.1.1.1 | HTTP | 530 GET / HTTP/1.1 |
| | 6 8.032289 | 10.1.1.1 | 18.1.1.181 | HTTP | 489 HTTP/1.1 200 OK (text/html) |
| | 16 8,649949 | 10.1.1.101 | 209.225.11.237 | HTTP | 487 POST /scripts/cms/wcms.asp HTTP/1.1 (application |
| | 19 8,354648 | 289,225,11,237 | 18.1.1.181 | HTTP | 60 [TCP Previous segment not captured] Continuation |
| | 31 1.283985 | 10.1.1.101 | 18.1.1.1 | HTTP | 628 GET /Websidar/index.html HTTP/1.1 |
| | 38 1.292367 | 10.1.1.1 | 18.1.1.101 | HTTP | 275 HTTP/1.1 200 OK (text/html) |
| | 48 1.483683 | 10.1.1.101 | 28.1.1.1 | HTTP | 651 GET /Websidan/images/bg2.jpg HTTP/1.1 |
| | 50 1.404958 | 10.1.1.101 | 18.1.1.1 | HTTP | 654 GET /Websidan/images/sydney.jpg HTTP/1.1 |
| | 61 1.416360 | 10.1.1.1 | 10.1.1.101 | HTTP | 1520 HTTP/1.1 208 OK (3P25 3F1F image) |
| | 72 1.424518 | 10.1.1.1 | 10.1.1.101 | HTTP | 624 HTTP/1.1 200 OK (JPES JFIF image) |
| | 82 1.501785 | 10.1.1.101 | 209.225.0.6 | HTTP | 1211 GET /site=126585/brum=operal/bins=1/opid=10050285 |
| | 64 1.502133 | 10.1.1.101 | 209.225.0.6 | HTTP | 1211 GET /site=126585/bnum=opera2/bins=1/opid=10030367 |
| | 86 1.502407 | 10.1.1.101 | 209.225.0.6 | HTTP | 1211 GET /site=126885/bnum=opera3/bins=1/opid=10032112 |
| | 90 1.509970 | 10.1.1.101 | 209.225.0.6 | HTTP | 1211 GET /site=126885/bnum=opera4/bins=1/opid=10003005 |
| | 100 11 994517 | 289:225.0.6 | 10.1.1.101 | ITTE | 1301 [TCP Previous segment not captured] Continuation |
| | | | | | 1381 [TCP Previous segment not captured] Continuation |
| | | | | | 1301 [TCP Previous segment not captured] Continuation |
| | 128 2.588536 | 10.1.1.101 | 209.225.0.6 | HTTP | 1267 GET /site=0000127709/mnum=0000162763/genr=1/logs= |
| | 133 2.584153 | 10.1.1.101 | 209.225.0.6 | HTTP | 1267 GET /site=0000127709/mnum=0000162763/genr=1/logs= |
| | 137 2.882516 | 289,225,9.6 | 10,1,1,101 | HTTP | 1301 [TCP Previous segment not captured] Continuation |
| | 145 2.845244 | 10.1.1.101 | 209.225.0.6 | HTTP | 1267 GET /site=0000127789/anus=0000162766/genr=1/logs= |
| | 157 3.263072 | 10.1.1.101 | 18.1.1.1 | HTTP | 655 GET /Websidarv/dagbok/dagbok.html HTTP/1.1 |
| | 159 3.266188 | 10.1.1.1 | 28.1.1.101 | HTTP | 746 HTTP/1.1 208 OK (text/html) |
| | | | | 10000 | the set of the second second barries and the second s |



□ 하단에 이미지 관련된 패킷 존재



HTTP 스트림 저장

□ 대상 패킷 우클릭 → 따라가기 → HTTP 스트림 - 0 ×

A http://ipeqs.cap

파월(F) 편집(E) 보기(V) 이름(G) 캡쳐(C) 분석(A) 통계(S) 전화(Y) 우선(W) 도구(T) 도움말(H)

🖌 📰 🖉 😂 🖄 🖄 🔍 + + 🛎 Ŧ 🛨 🔜 🔍 Q. Q. U 🖽

| tcp. | stream eq 7 | | | | | | | | | | | | |
|--|------------------------------|------------|-------------|----------|--------|--|---------------------------------------|--------------------------|--|------------------------|---------------|---------------------------|--|
| No. | Time | Source | Destination | Protocol | Lengtl | Info | | | | | | | |
| | 49 1.379484 | 10.1.1.101 | 10.1.1.1 | TCP | 62 | 3189 | + 50 | (SYN) | Sequil W | inu0 Lenu0 MSS=1460 Sa | ACK PERM | | |
| | 41 1.379927 | 10.1.1.1 | 10.1.1.101 | TCP | 62 | 80 + | 3189 | (SYN, | ACK] Se | q=0 Ack=1 Min=5840 Lee | 1+0 MSS=1460 | SACK_PERM | |
| | 42 1.379978 | 10.1.1.101 | 10.1.1.1 | TCP | 54 | 3189 | 80 | ACK] | Seg=1 A | ck=1 Win=65535 Len=0 | | | |
| | 48 1.403683 | 10.1.1.101 | 10.1.1.1 | HTTP | 651 | GET / | Nebsie | dan/i | mages/bg | 2.jpg HTTP/1.1 | | | |
| | 49 1,404885 | 10.1.1.1 | 10.1.1.101 | TCP | 68 | 80 + | 3189 | TACK1 | Seg=1 A | ck=598 Win=6567 Len=0 | | | |
| 1 | 52 1.408298 | 10.1.1.1 | 10.1.1.101 | TCP | 1514 | 88 + | 3189 | [ACK] | Seg=1 A | ck=598 Win+6567 Len=1+ | 160 [TCP PDU | reassembled in 61] | |
| | 53 1.409540 | 10.1.1.1 | 10.1.1.101 | TCP | 1514 | 80 - | 3189 | (ACK) | Seg=146 | 1 Ack=598 Min:6567 Let | 1=1460 [TCP P | OU reassembled in 61] | |
| | 54 1.409607 | 10.1.1.101 | 10.1.1.1 | TCP | 54 | 3189 | + 60 | (ACK) | Seg=598 | Ack=2921 Min=65535 L | ense | | |
| | 56 1.412710 | 10.1.1.1 | 10.1.1.101 | TCP | 1514 | 88 + | 3189 | [ACK] | Seq=292 | 1 Ack=598 Win+6567 Ler | -1460 [TCP P | OU reassembled in 61] | |
| | 57 1.412812 | 10.1.1.101 | 10.1.1.1 | TCP | 54 | 3189 | 80 | ACK] | Seq=598 | Ack+4381 Min+65535 L | 9rns | | |
| | 58 1,413969 | 10,1,1,1 | 10.1.1.101 | TCP | 1514 | 80 ÷ | 3189 | TACK1 | Seg=438 | 1 Ack-598 Min-6567 Lee | -1460 [TCP P | DU reassembled in 611 | |
| | 59 1,415274 | 10.1.1.1 | 10.1.1.101 | TCP | 1514 | 80 + | 3189 | FACK1 | Seg=584 | 1 Ack-598 Win-6567 Let | -1460 FTCP P | DU reassembled in 611 | |
| | 60 1.415334 | 10.1.1.101 | 10.1.1.1 | TCP | 54 | 3189 | - 30 | (ACK) | Seq:598 | Ack:7301 Min:65535 L | enzē | | |
| | 61 1.416360 | 10.1.1.1 | 10.1.1.101 | HTTP | 1320 | MITTP/ | 1.1 20 | 90 OK | (JPI- | | | 1 | |
| | 62 1.416444 | 10.1.1.101 | 10.1.1.1 | TCP | 54 | 3189 | + 80 J | [ACK] | Seq=1 | 신덕 항복 마크/해제(M) | Ctrl+M | | |
| | 91 1.543378 | 10.1.1.101 | 18.1.1.1 | TCP | 54 | 3189 | · 88 | FIN, | ACK] | 전택 항묵 루시/해제(0 | Ctrl+D | | |
| > Frame G1: 1320 bytes on wire (1056b bits), 1320 bytes captured (10566 bits) > Etherwart II, Src: KYE_28:6c:df (00:c8:df:28:6c:df), Dat: SKCBatwarts 22:5a:03 (00:04:e2 > Internet Protocol Version #, Src: 10:1.1.4, Dat: 10:1.1.10! | | | | | | 0000 시간 철조 설 0010 타입시프트. 0020 제깃 주석 | 시간 참조 설정/해제 타입시프트 제짓 주석 | 제 Ctrl+T Ctrl+Shift+T | 88 80 45 60 Z. 1 E 81 81 80 8 3 Z. 1 E 58 60 58 19 e P.u7z 4 P.P 1b 23 a3 5b | | | | |
|) Pransmission control Protocol, Srt Port: do, Dit Port: 3189, Seq: 7301, Ack: 598, Len: . | | | | | | | NAME OF BRIDE | | 24 8b 1a 43 8p-5; ^4 \$ C | | | | |
| > [0 Newsymbolic for Anglesis (one sytes): est(sub); est(sub); est(sub); est(sub); e. w Humantart Transfar Protocol | | | | | | | 1110 118 0.8 | | a5 e8 a8 e4 c5 d H | | | | |
| | HTTP/1 1 288 OK\+ | -in | | | | | | | 6678 | 필터로 적용 | | b1 b6 78 3b nE% '. I(. p; | |
| Date: Sat. 28 New 2004 18-21-07 (MT\r)n | | | | | | 0000 | 필터로 준비 | | 4c 3b 43 23 8 G = 1x p+ ,L;C# | | | | |
| Server: Anache/2.8.48 (Red Hat Linux))r\n | | | | | | 0095 | rani atra | | 68 e0 81 8d ···· 4# G···h··· | | | | |
| Last-Modified: Fei, 12 Jan 2001 05:00:00 GMT\r\n | | | | | | | 14 61 | | 02 30 14 01 VN 60 2 | | | | |
| FTag: "46a4f-2852-5a467488"\r\n | | | | | | | 대회 색상화 | • | F1 ac 61 51 | | | | |
| Accent.Bandas: hytesinin | | | | | 1 | 0000 | SCTP | | 86 83 81 3e Yc-=-@-> -cM&> | | | | |
| Content I math: \$291) ele | | | | | | 00+00 | 따라가기 | | HTTP 스트립 Ctrl+Alt+Shift+H | 1 | | | |
| Connection: closelrin | | | | | | 00f0 | TCP A E BI Ctrile Alter Shifter T | | | | | | |
| | Content-Type: image/ineg\r\n | | | | | | · · · · · · · · · · · · · · · · · · · | | 00 8f 42 44 | 1 | | | |

프로토클 성정

다른 형식으로 디코드...

새 창에 패킷 표시(W)

Frame

77 99 7c 13 N p I\$ w]

三王号: Default

17(3.5%)

🔵 🝸 http_witp_jpegs.cap

X-Pad: avoid browser bug\r\n

R



RAW 파일 저장

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

474554202f576562736964616e2f696d616765732f6267322e6a706720485454502f312e310d8a557365722d4167656e743a204d6f7a696c6c612f 342e38202863676d70617469626r653b204d53494520362e303b2057696e646f7773204e5428352e3829204f7065726128372e313128205b656e5d 8d8ad86f737d43a2831382e312e312e312e312e31648ad1636365787d3a286178786c69636174696f6e2f782d73686f636b776176652d666c6173682c746578 742f786d6c2c6178706c69636174696f6e2f786d6c2c6170706c69636174696f6e2f7868746d6c2b786d6c2c746578742f68746d6c3b713d302e39 2c746578742f786c61696e3b713d382e382c766964656f2f782d6d6e672c696d6167652f786e672c696d6167652f6a7865672c696d6167652f6769 663b713d302e322c746578742f6373732c2a2f2a3b713d302e310d0a4163636570742d4c616e67756167055a20655e0d0a4163636570742d436861 727365743a2877696e646177732d3132353227387574662d382r287574662d31362r286973612d383835392d313b713d382e362r282a4b713d382e 31040a41636353787424656a63666666675a20665566665170652+20677a60782+207824677a60782+206566760762+2078460782+20245677a60782+20245677a60782+20245677a60782+20245677a60782+20245677a60782+20245677a60782+2024573+20865766760782+208577a60782 8a526566657265723a28687474703a2f2f31302e312e312e312f576562736964616e2f696a6465782e68746d6c8d0a436f6a6e656374696f6e3a28 4b5555782d416c6976652c7854458d8854453x286465666c6174652c28677#69782c786358756+6b65642c286964656+746974792c28747261696c 485454582f312e312e312e31293e3903e284f4bedea446174653a285361742c283230284e6f762832303842831303a32313a303728474d546d8a5365727665 723a284170616368652f322a382a343828283656420486174284c696a757829848a4c6173742d4d6f6469666965643a284672692c283132204a61 6e20123038312038353a38303a3030204545454545454545455451623a202234366134662d123835392d3565343637343830228d8a4163636520742d526 be6765733a2062797465730d8a436f6e74655e742d4c655e6774683a20383238310d0a436f6e6e656374696f6e3a20636c6f73650d8a436f6e7465 6e742d547970653a20696d6167652f6a7065670d8a582d5061643a2861766f69642062726f77736572206275678d8a0d8a ffd8ffe000104#464946000101010048004800080fffe0017437265617465642077697468205468652847494d50ffdbc04300140#0f120f0d141210 12171514181e32211e1r1r1e3d2r2e243249484r4b47484545585a7362585564564564564865556d777b8182814e688/978r7496737e817rffdx8843 7588a3137131759a5r8har/0h36895688828h358928h358928h3582r1584a1288a25941482r48148a28018a8281ar/0298a5259658ab228r35924/44r6432a1 554050b285812c22894090d20a9458000202d942c110b2c2504a054945582d9405161022acccd422892926a5528801420b288b04b092ac58974828 802802594b822892c22840b65250505828942842a1004b84d42594a82a522c28082a04b8410550140059400020a8804524d4337512c55a8290d250 89428289484284948173444a18884692c945345594888882a8b882d82cb814968588896c2a5168582cb866c2a8b816522c2a859466828a888928 cacb2drd96d944b858082a52c882d94841412c8524b1349554888812c2021526a558885cd3482254585a84b645228582c482c4b881622dcd2a175 0084a455cd2c5150d10582c444b1572b2d894104aa595288b05cdb210d334d2204ab65859a5ccb108aaa964b2c80b08a2ad8956548b15449650154 2cb00128ca922d32b4cb45cac1400022c24b4cd002a5b025b60b9b1014b0108b6ccaa05a52559a24a100525a12c00000288b025008a210590d2001 14465851229582z4b349658128z401488z5225558822z2z949b/288b/bb8449554842z808892zz2288828z81548488848z4z433443341334155825844 16560b012c0b0582820da85a942508282a52011480024b0582d0ab0148b092d3134b52b2296aa59452282525b00042812c12c2c2c016596a010b14 5940000040092c4516d9a10255008b092c493515ace901565102594d4b02c2c09642905949359b2a5945082c0a010b60a0000484128a945524d64b 603524b899de5285bac68a82c524d4141652cb8ca8cd42cb4c88528b8282a6a25a84b882a52a8b824b859d58a85c8b68bacd12a119d2b8b2c5cea2 ac52814b10b60024a2148d648b88102adcd16252c17352ca59350016022c581658294002a0bac68d42584b33379494a6b165b6509420b60590b02a 5128935092c26b36cb14894b8956a2a12c02c8a22896a228a852c084a16a52dc8148a32b01493433688a0000142c1288893500b2c0165002235155 82cb81a494502542ca2022c168a522802a51288a004a2582cb88b0028840094212ca88a82a5a1658020a96cb49560025045100094173450a9402c0 8994b856a9414935925885a2824ab281622a2adc8a64b4cd9d25945282284b88d12416a1145a52594588b898b84848481acd35822c88b812c29b22 89289414165940806b1536rd5#60960b7200rdb2c#22d855942c102#0b005332c4#85b65160582#0#092c22c2824#b28142894684b2836dcd3482 전체 대화(9163 bytes) 다른 형식으로 표시 Raw(무면집) 형식 ~ 멸타 시간 없음 ~ 스트림 7 □ 대소문자 구분 다음 찾기면 다루 이름으로 저장 5.88





Hex Editor 설치 및 사용

□ HxD 다운로드

 <u>https://mh-</u> nexus.de/en/downloads.php?pr oduct=HxD20

□ 파일 열기 또는 새 창 생성

❑ Wireshark에서 저장한 Raw 파일 열기

| FbD - (C3)Jsen//secc//Download/(pegcap) | |
|--|-------------------------------------|
| 화율(F) 관립)지 찾기(S) 보기(N) 분석(A) 도구(T) 항 설정(N) 도용율(H) | |
|) 👌 = 🗐 🔳 💷 🖬 🐨 🐨 Windows (ANS) 🔗 16정수 🖓 | |
| #개1 및 help gif 및 tester.gif 및 longcap | 목수 편합기 |
| Offsesin) 00 01 02 03 04 05 04 07 08 09 0A 08 0C 0D 0E OF Decoded text | . 데이터 변환기 |
| 00000000 47 45 54 20 27 57 65 62 73 69 64 61 62 27 69 60 GET /Nebsidan/im | 14.4 M 1 |
| 00000010 61 67 65 73 2F 62 67 32 2E 63 70 67 20 63 54 54 spes/bo2.too HTT | |
| 00000020 50 2F 31 2E 31 00 0A 55 73 65 72 2D 41 67 65 6E F/1.1. User-Apen | 2전수 (5세 年) 01100001 |
| 02000030 74 3A 20 4D 4F 7A 65 6C 6C 61 2F 34 2E 30 20 20 54 Mozilla/4.0 (| 1008 QLB: 97 |
| 02000040 63 62 6D 70 61 74 65 62 6C 65 38 20 4D 53 45 45 compatible; MSIE | 11058 0.4 97 |
| 00000050 20 36 22 30 38 20 57 69 62 69 67 77 73 20 42 54 6.0; Windows NT | 14716 01E 8380 |
| 03000060 20 35 2E 30 29 20 4F 70 65 72 61 20 37 2E 31 31 5.0) Opera 7.11 | 10414 0.5 0100 |
| 00000000 20 20 50 65 62 50 00 00 40 67 73 74 30 20 31 50 [48]0365 10 | 1001 015 011750 |
| | 1020 2012109 |
| 02000010 6F 63 6B 77 61 76 65 70 66 6C 61 73 68 7C 74 65 octowere-flash.te | 01824 018 3912709 |
| 01000080 78 74 2F 78 4D 4C 2C 51 70 70 6C 59 63 51 74 59 st/ssl.aveligati | W152 018 775394705 |
| 03000000 &F 6E 2F 78 4D 6C 2C 61 70 70 6C 69 63 61 74 69 on/aml,applicati | UM32 018 775364705 |
| 01000000 6F 6E 2F 78 68 74 6D 6C 2B 78 6D 6C 2C 74 65 78 on/shtml+xml,tex | 1004 0.5 2314904295766958177 |
| 000000E0 74 27 68 74 6D 6C 38 71 3D 30 2E 39 2C 74 65 78 t/html;q=0.9,tex | Uint64 0.8 2314934295766958177 |
| 000000F0 74 2F 70 6C 61 69 6E 35 71 30 30 2E 38 2C 76 69 %/plainig=0.8,91 | LE0120 9.8: -31 |
| 03000100 64 65 6F 2F 75 2D 6D 6E 67 2C 65 6D 61 67 65 2F deo/x-mmp,imape/ | ULE8128 018 97 |
| 01000110 70 68 67 20 69 60 61 67 68 27 64 70 68 67 20 69 png,image/jpep,i | AnsiChar / charit a |
| 00000120 &D 61 67 65 28 67 65 66 38 71 3D 30 28 33 20 74 mage/gif/g=0.2,6 | WideChar / char16 t |
| 00000140 01 00 03 41 43 43 45 20 74 10 40 41 47 43 47 41 1 Accest Janua | LITE-8 code point a 81x00611 |
| 00000150 67 65 3A 20 65 6E 0D 0A 41 63 63 65 70 74 2D 43 de: en. Accept-C | Gavia (Engli2) 4 161814065180626.11 |
| 00000160 60 61 72 73 65 74 3% 20 77 69 6E 64 6F 77 73 2D harset: windows- | Country Country A CONTRACTORY INC. |
| 03000170 31 32 35 32 20 20 75 74 66 2D 35 20 20 75 74 66 1252, unf-5, unf | CUTTAIT 1000 13 30 |
| 00000180 2D 31 36 20 20 69 73 6F 2D 38 38 35 39 2D 31 38 -16, 180-8859-12 | Guarriera 11899-12-30 |
| 03000150 71 3D 30 2E 36 2C 20 2A 38 71 3D 30 2E 31 0D 0A g=0.6, */g=0.1 | 바이트 순서 (Ryte Order) |
| 030301A0 41 63 63 65 70 74 2D 45 6E 63 6F 64 69 6E 67 3A Accept-Encoding: | 008909 09980 |
| 01000180 20 64 65 66 6C 61 74 65 2C 20 67 73 69 70 2C 20 deflate, gsip, | |
| 000001C0 78 2D 67 7% 69 70 2C 20 69 64 65 62 74 69 74 79 x-gzip, identity | 14친수 형식으로 변환 (영수) |





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)





- 악성코드 은닉 탐지 (확장자 위장이 아닌 시그니처 확인)
- 메모리/디스크 덤프에서 유효 파일 추출
- 데이터 손상 복구

□ 시그니처 사용 목적

- ASCII: %PDF → PDF 시작
- Hex: FF D8 FF → JPEG 시작

□ Hex에서의 표현 방식 예시

파일 시그니처 개념과 구조





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)
- □ 파일시작시그니처
 - FF D8 FF
 - FF D8 → SOI
 - 뒤따르는 FF는 JFIF, EXIF 등 메타 정보 시작 마커 (FF EO, FF E1 등)
- □ 파일종료시그니처
 - 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 검 색 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







□ 힌트 : JPG 말고 다른 이미지 형식입니다.

□ 해당 사이트 하단에 있는 ybo.pcapng 파일에서 융보공과 관 련된 포스터를 추출해보세요. 가운데 있는 사람이 누군지 맞춰보세요!

미션

https://creamerburger.tistory.com/72

