이 대회는 포렌식 위주를 대회였는데 나름 포렌식에 대해 많이 배운 대회라고 생각한다. 별 기대 없이 시작했지만 최종 스코어는 2800, 6등으로 대회를 마쳤다. 6 문제를 못 풀었지만 하나하나 풀이를 해보도록 하겠다.

우선 메모장을 열면 이런 값이 주어진다.



이 값들을 HXD에 옴기면



이렇게 나오는데 IHDR이라는 값이 보인다. png라는 것을 짐작할 수 있었고 FLAG부분을 png 헤더로 바꿔준다.

플래그가 보인다. 여기서 조금 당황한 것은 1과 l이다 둘다 1을 입력해서 틀렸었다.

{F0r3ns1c\_Probl3m\_St4rt}

이 문제는 HWP파일을 주는데 열면



아무것도 안보이는데 색을 바꾸게 되면



플래그가 나온다.

문제를 압축 풀면 메타몽 사진이 보이는데



속성에 들어가서 자세히 보면 플래그가 나온다.

백지 사진이 있는데 HXD로 열어보면 맨 밑에



이렇게 나오는데 저 부분이 키 값일 줄은 몰랐다. 처음에 인증을 했었는데 !때문에 실패를 해서

나중에 다시 풀어 보니깐 정답 이였다.

Rtf 파일이 주어지게 된다.



열어보았는데 예전에 봤던 브레인 퍽이라는 언어가 있었다.



이걸 온라인에서 돌리면 HELLO로 앞으로 채우고있는, 이런 플래그가 나온다.

Hidden.png가 주어진다. 이 문제는 5.2 구버전의 오픈스테가노를 써서 돌리면 된다.



이렇게 LSB로 맞추고 돌리면 key.txt가 나온다.

FLAG IS {0P3N\_ST3G0\_!S\_FL4G}

괄호를 채우면 되는데 답은 {디지털수사통합업무관리시스템\_무결성\_진정성\_원본성}

이문제의 답은 {csrf}였는데 처음에 인증이 안돼서 어이없었지만 나중에 다시 하니깐 인증이 됬다.

이 문제는 웹 문제다.

이 사이트가 나오는데 지문에 flag를 이미 알고있다고 나온다. 그래서 봤더니

진짜 flag를 이미 알고있다 저 값 md5를 복호화 했더니

e1RoaXNfaXNfRGVjb2RlX1Byb2I0ZW19 해당 값이 나온다 이걸 base64로 디코딩하면

{This\_is\_Decode\_Prob4em}가 나오게 된다.

이 파일은 역시 헤더가 바뀌였다



맨 밑에 이런게 있는데 jpge로 바꿔 주도록 하자

바꾸면 You Rock이라는 이미지가 나오는데 더 있는 줄 알았더니 이게 그냥 답이다

{You Rock}

볼라티리티를 사용해 cmdscan 명령을 사용하면 층로 입력했던 것들을 볼 수 있다.

|  |
| --- |
| FLAG IS {CMD\_Log\_IS\_FL49~!!} |
|  |

이 문제는 못 풀었다. Png 파일이 두개가 보이는데 하나를 복구하면 이미지가 반밖에 안보인다.

위에 보다 보면 나머지 반이 보이는데 넣었지만 내가 잘못했는지 확인 할 수 가 없었다.

이 문제의 압축을 풀면 파일 3개가 나온다.



이번에도 역시 헤더를 맞춰 주면 되는데 FLAG IS {Y0u\_607\_7h15}

Ascii 와 Rot 13 말고는 뭘 뜻하는지 몰라서 그냥 포기한 문제다.

의심스러운 실행 파일은 secret.exe가 두개 나오는데 이거 말고는 잘 모르겠다 그래서 못 풀었다.

흐릿한 이미지가 나오는데 포토샵을 이용하면 조금이나마 선명하게 보인다.

FLAG IS {Welcome\_t0\_B3verly\_ill$} 처음에 이렇게 인증 했었는데 분명 아니라 해놓고 몇시간 뒤에 하니깐 됐다.

음 깨진 이미지를 보여주는데 못 풀겠다.

이것도 게싱으로 풀었다. 이지 이미지 보다 조금 더 흐린데 선명하게 하고 이미지를 작게 보면

앞에 4g3이 보이고 가운데는 forensic이라는 것을 알 수 있다 그리고 D3blur이렇게 보이는데

게싱을 하다 보니 image\_forensic\_deblurring라는 것을 알 수 있었다.

FLAG IS {Im4g3\_for3nsic\_D3blurring}

스케줄러 관련 프로세스를 세부적으로 보면 플래그를 구 할 수 있다.

Tasking.exe에서 확인 할 수 있는데 FLAG IS {G0d\_F0r3ns1c\_J0b}

휴지통을 뒤져보면 될 것 같은데 휴지통은 $Recycle.Bin으로 검색하면 된다.

FLAG IS {G00D\_R3cycl3\_FLAG~!!}

E01 파일을 주는데 ftk로 열어서 보면 1섹터 부분이 이상한 값으로 되어있다. Fat32인데

이러면 6섹터에 망가졌을 때를 대비해서 백업해 두는데 이 부분을 복사해 붙여놓고 다시 열면

중요한 문서.hwp가 나온다. 그러나 두 번째 헤더 I가 다른 걸로 바뀌었다. 그래서 변경해주면

FLAG IS {USB\_R3c0v3ry\_Succ3ss}



NEW 이런 문자열이 보인다. 완전 신기하다. 아스키 아트다. 이걸 디코딩하면 hwp 파일이 나온다.

FLAG IS {$SK11\_4RT\_IS\_FL4G}

이 문제는 열어보지도 않았다………

마지막 문젠데 볼라티리티를 사용해 index.dat를 검색해서 다운받고 index.dat 분석하는 프로그램으로 열어보면 아래의 주소가 나온다.

<https://drive.google.com/file/d/0BxHFww6YnFnrN2w2SUlvZnNrWjA/view?usp=sharing>

Spy Project.zip을 다운받는데 비밀번호를 모른다 4글자로 브루트포싱을 하면 금방 비밀번호를 얻을 수 있는데 FL49라는 것을 알 수 있다. 압축을 풀고 hwp를 열면 맨 밑에 아주 작은 글씨로 플래그가 나온다. FLAG IS {WoW\_GOD\_H4CK3R!!}