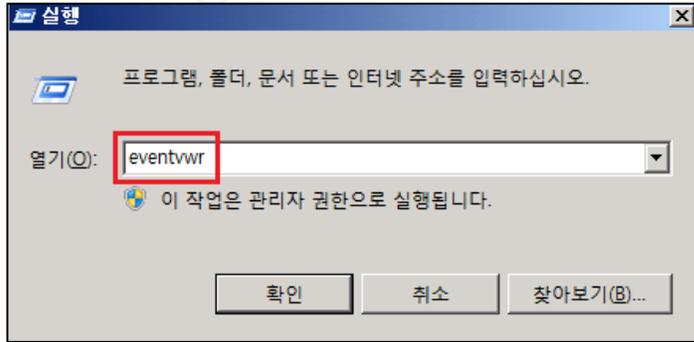
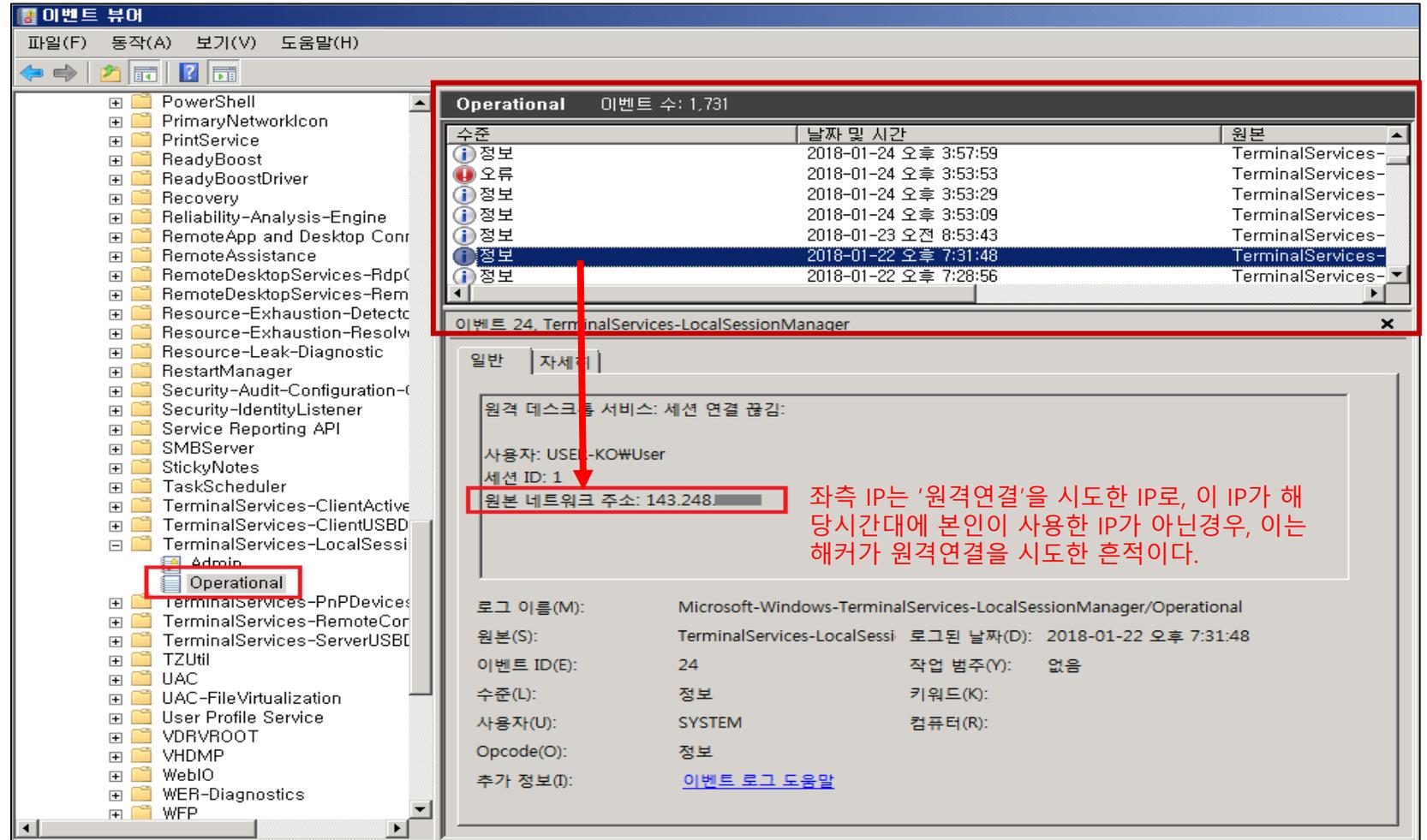


# ※ 윈도우 원격데스크톱 접속로그 확인

1. 윈도우키(  )+R → "eventvwr" 입력 후 엔터



2. "응용 프로그램 및 서비스 로그" -> "Microsoft" -> "Windows" -> "TerminalServices-LocalSessionManager" -> "Operational"에서 접속 로그 확인



| 수준 | 날짜 및 시간               | 원본                |
|----|-----------------------|-------------------|
| 정보 | 2018-01-24 오후 3:57:59 | TerminalServices- |
| 오류 | 2018-01-24 오후 3:53:53 | TerminalServices- |
| 정보 | 2018-01-24 오후 3:53:29 | TerminalServices- |
| 정보 | 2018-01-24 오후 3:53:09 | TerminalServices- |
| 정보 | 2018-01-23 오전 8:53:43 | TerminalServices- |
| 정보 | 2018-01-22 오후 7:31:48 | TerminalServices- |
| 정보 | 2018-01-22 오후 7:28:56 | TerminalServices- |

이벤트 24, TerminalServices-LocalSessionManager

원격 데스크톱 서비스: 세션 연결 끊김:  
사용자: USER-KOWUser  
세션 ID: 1  
원본 네트워크 주소: 143.248...

좌측 IP는 '원격연결'을 시도한 IP로, 이 IP가 해당시간대에 본인이 사용한 IP가 아닌경우, 이는 해커가 원격연결을 시도한 흔적이다.

로그 이름(M): Microsoft-Windows-TerminalServices-LocalSessionManager/Operational  
원본(S): TerminalServices-LocalSessi 로그된 날짜(D): 2018-01-22 오후 7:31:48  
이벤트 ID(E): 24 작업 범주(V): 없음  
수준(L): 정보 키워드(K):  
사용자(U): SYSTEM 컴퓨터(R):  
Opcode(O): 정보  
추가 정보(I): [이벤트 로그 도움말](#)

▶ 위의 경우로 확인한 결과, 의심스런 흔적이 발견되는 경우, [kaistcert@kaist.ac.kr](mailto:kaistcert@kaist.ac.kr) 또는 T. 2413로 문의하시기 바랍니다.