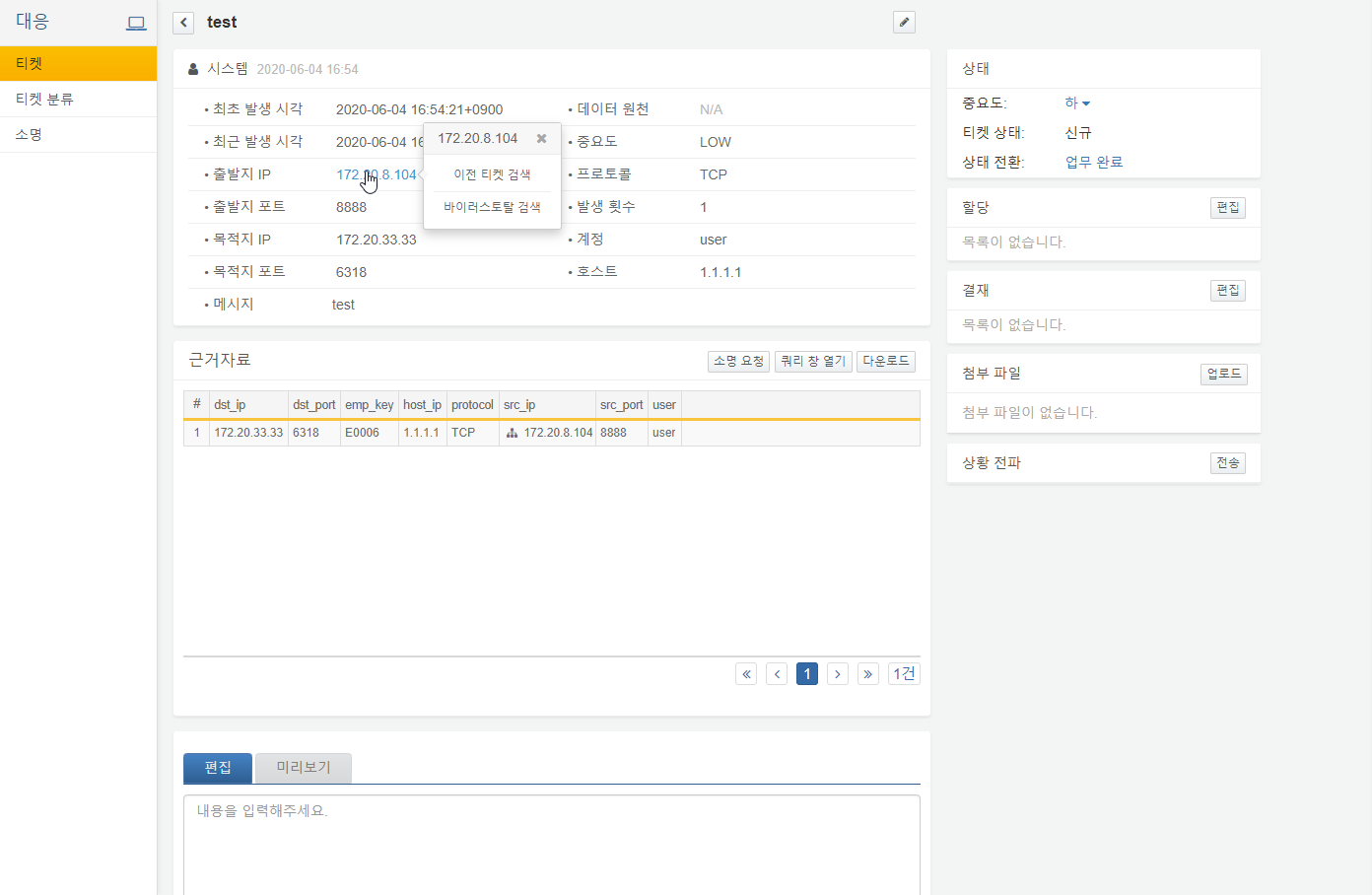
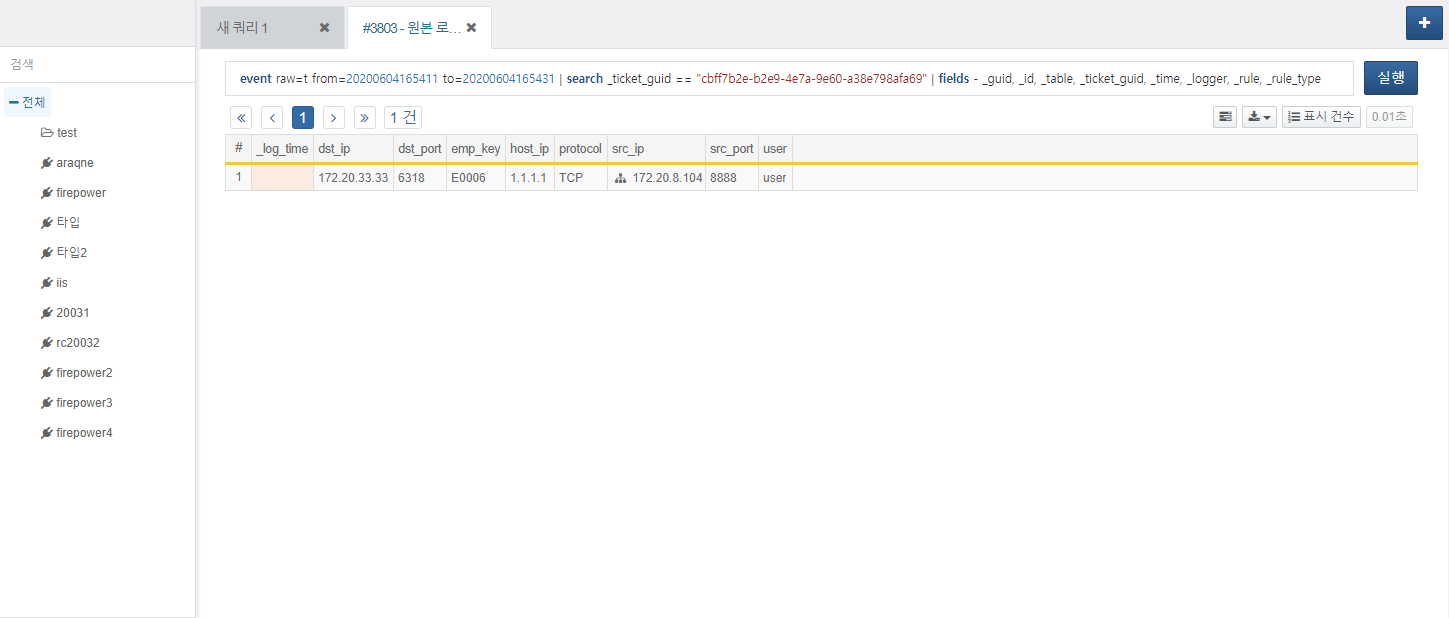
#### 티켓 조회

티켓 목록에서 티켓 제목을 클릭하면 해당 티켓의 내용과 할당 상태를 조회합니다.



티켓이 탐지 시나리오에 의해 자동으로 생성된 경우, 티켓 본문은 위와 같이 이벤트 내용을 표시합니다. 하단의 근거자료에는 이벤트를 발생시킨 원본 로그나 티켓과 관련된 데이터가 표시됩니다. 예를 들어, 호스트 스캔을 탐지한 경우, 아래 화면 예시처럼 스캔을 시도한 목적지 IP와 포트 등의 정보를 근거자료로 표시할 수 있습니다. 근거자료 공간이 좁아서 보기 힘든 경우, 쿼리 창 열기 버튼을 클릭하면 쿼리 화면에서 데이터를 검토할 수 있습니다.

또한, 출발지 IP, 도착지 IP, 호스트에 대하여 이전 발생했던 티켓 내역을 검색하거나 바이러스 토탈에서 악성 여부를 조회할 수 있습니다.



분석가는 티켓의 근거자료부터 시작하여 실질적인 위협이나 이상징후가 있는지 확인하고 대응 내역을 기록한 다음, 티켓 진행상태를 바꿔서 완료합니다.