# "암호해독 v.s 안티포렌식" 특집호 발간에 즈음하여

디지털 사회가 가속화됨에 따라 우리는 일상생활에서 다양한 디지털 기기를 사용하고 있고 다양한 스마트한 디지털 기기들을 사용하면서 우리는 언제 어디서든지 우리가 원하는 정보를 습득하고 활용할 수 있게 되었다. 우리가 디지털 기기를 사용하며 스마트한 삶을 살아가고 있다고 느끼는 이유는 디지털 기기의 하드웨어 성능이 향상된 것뿐만 아니라 기기에 탑재된 운영체제와 애플리케이션들이 우리에게 다양한 서비스를 제공하고, 이로 인해 생성된 데이터를 분석하여 우리에게 필요한 정보도 제공하기 때문이다.

사이버 보안 관점에서 이 '데이터'는 관점에 따라 보호해야 할 대상이기도 하면서 동시에 보호를 해제하여 분석해야 하는 대상이기도 하다. 모든 디지털 기기에 탑재된 운영체제와 애플리케이션은 성능 개선과 사용자의 편의를 위해 사용자의 모든 행위를 시간 정보와 함께 로그로 저장한다. 이 과정에서 로그 데이터에는 우리의 민감한 개인정보가 포함된다. 따라서 정보 보호 관점에서는 이 데이터는 암호화하여 보호해야 할 대상이지만, 디지털 포렌식 관점에서는 이 데이터는 검색하고 추출하여 면밀하게 분석해야 할 대상이다.

본 특별호에서는 이러한 개인정보가 포함된 데이터를 보호하기 위한 다양한 안드로이드 애플리케이션들의 암호화 기법 동향, 복호화 가능성 및 취약점에 대한 연구를 소개한다. 첫 번째 논문은 사용자가 선택한 파일을 암호화하여 보호해주는 12개의 앱들에 대한 발표된 연구 결과를 정리하고 추가로 5개의 앱들을 분석한다. 두 번째 논문은 암호화 기능이 포함된 12개의 앱들의 암호화키 생성 방법을 분류하고 각 앱의 암호화 방법을 분석한다. 세 번째 논문은 암호화 기능이 적용된 메신저 앱들에 대한 안정성을 TMTO 및 GAN 모델을 활용하여 분석한다.

다음은 개인정보가 포함된 데이터를 활용한 디지털 포렌식을 방해하는 안티포렌식을 대응하기 위한 연구를 소개한다. 네 번째 논문은 보안 메신저 서비스, 클라우드 스토리지 서비스, 익명 네트워크 기반 서비스 사용으로 발생하는 안티포렌식의 기술 동향과 그 대응 방안을 소개한다. 다섯 번째 논문은 윈도우즈 운영체제에서 파일 완전 삭제를 위한 5개의 안티포렌식 도구의 사용 흔적을 분석하는 방안을 소개한다.

마지막으로는 안티포렌식 기능이 적용된 실행파일 분석을 위한 연구를 소개한다. 해커들을 일반적으로 PC기반 악성코드에 Themida, VMProtector와 같은 프로텍터를 사용하여 배포됨으로써 분석가의 분석을 방해한다. 안드로이드에도 이러한 프로텍터가 존재하며 악성앱에 프로텍터가 적용되어 있을 경우 이를 우회하여 분석해야 한다. 마지막인 여섯 번째 논문은 안드로이드 전용 프로텍터가 적용된 앱을 분석하기 위한 방법을 소개한다.

끝으로 바쁘신 중에도 소중한 시간을 내시어 원고를 집필해 주신 집필자분들과 편집에 수고해 주신 학회지 편집 위원회, 그리고 학회 사무국 관계자 여러분께 감사를 드립니다.

2022년 12월

부산가톨릭대학교 컴퓨터정보공학과 교수 김도현