[논문 리뷰 보고서]

[포렌식 관점에서의 Element 인스턴트 메신저 아티팩트 분석]

작성일	2025.05.26
작성자	김신아
검토자	김예은

목차

Ⅰ. 개요

항목	내용
논문 제목	포렌식 관점에서의 Element 인스턴트 메신저 아티팩트 분석
저자 및 연도	조재민(고려대), 변현수, 윤희서, 서승희, 이창훈(과기대)
출처	정보보호학회논문지 제32권 제 6호 (p.1,113-1,120)
분석 대상 프로그램	Element
관련 아티팩트 유형	메신저, 네트워크,메모리, 사용자 행위

[표1. 논문 개요]

Ⅱ. 논문 요약

1. 논문 요약

이 논문에서는 사이버 범죄, 특히 피싱 범죄의 증가 문제를 해결하고자 디지털 포렌식 관점에서 보안 메신저와 관련된 데이터 분석을 통해 사이버 범죄의 예방 및 대응 방안을 모색하는 연구 목적을 제시하였습니다.

실험 결과, 보안 메신저 앱인 Signal, Wickr, Threema의 암호화 메커니즘을 역공학을 통해 분석하였으며, 이를 통해 암호화된 정보의 복호화 방법을 제시하였습니다. 또한, Element와 같은 matrix 프로토콜을 사용하는 애플리케이션에 대한 포렌식 분석이 이루어졌으나, 암호화된 채팅 기록에 대한 평문 복구 방안은 제시되지 않았습니다.

이를 통해 사이버 범죄의 증가에 대한 경각심을 일깨우고, 보안 메신저의 암호화 메커니즘에 대한 이해를 높이며, 향후 연구 방향을 제시하는 데 기여하고 있습니다.

연구는 특정 보안 메신저 앱에 대한 분석에 국한되어 있으며, 다양한 플랫폼에 대한 포괄적인 분석이 부족하다는 한계를 가지고 있습니다.

또한, 암호화된 채팅 기록의 평문 복구 방안이 제시되지 않은 점은 연구의 한계로 지적될 수 있습니다.

후속 연구로는 다양한 보안 메신저 플랫폼에 대한 포괄적인 분석을 수행하고, 암호화된 데이터의 복호화 방법에 대한 연구를 심화시켜야 할 필요가 있으며, 사이버 범죄 예방을 위한 정책적 제안도 함께 고려해야 할 것입니다.

2. 논문 상세 경로
    1) Element 보안 채팅은 메시지 내용, 전송자, 전송 시각, 채팅방 ID 등이 C:\Users\user\AppData\Roaming\Element\EventStore 하위에 Events.db 파일에 저장되어있어, Events.db 파일의 암호화 프로세스를 분석하고 복호화 키를 찾는 방안을 연구함

Ⅲ. 방향성

1. 메타데이터, 비암호화 메타 정보중심 분석
2. 보안 기능 우회를 고려한 키 추출 및 메시지 해석 자동화 도구 개발

Ⅳ. 참고 문헌

[1] 조재민, 변현수, 윤희서, 서승희, 이창훈「포렌식 관점에서의 Element 인스턴트 메신저 아티팩트 분석」정보보호학회논문지, 32(6), 2022, 1113-1120.