다크웹에서의 개인정보 불법거래 추적 및 차단 기술

- 다크웹 접속 및 개인정보 검색 기술
- 다크웹 개인정보 불법거래 추적 기술

#기술 세부내용

- 다크웹을 통한 개인정보 거래를 추적하고 차단하기 위한 웹 탐지기술 개발 (비정형 데이터의 개인정보 탐지 기술과 연계)
- 다크웹 기반의 기존 불법거래 사례 분석을 통해 다크웹 내 개인정보 불법거래 추적기술 개발

▼ 필요시 인터넷진흥원 침해대응센터, 방송통신심의위원회, 경찰청 사이버수사국 등과 협업을 통해 적용 가능성 검증

#제도 개선 사항

- 효과적인 개인정보 불법거래 차단을 위하여 ISP 사업자, 방송통신심의위원회 등 유관기관과의 협업체계 구축 및 법적 근거 정비 추진

3. 다크웹에서의 개인정보 불법거래 추적 및 차단 기술

구분	2022	2023	2024	2025	2026
다크웹 개인정보 불법거래 추적 및 차단 기술		다크웹 접속 및 개인정보 검색 기술			
			다크웹 개인정보 불법거래 추적 기술(5년)		

⬡ 기술 세부내용

- 다크웹을 통한 개인정보 거래를 추적하고 차단하기 위한 웹 탐지기술 개발 (비정형 데이터의 개인정보 탐지 기술과 연계)
- 다크웹 기반의 기존 불법거래 사례 분석을 통해 다크웹 내 개인정보 불법거래 추적기술 개발
  - 필요시 인터넷진흥원 침해대응센터, 방송통신심의위원회, 경찰청 사이버수사국 등과 협업을 통해 적용 가능성 검증

⬡ 제도 개선 사항

- 효과적인 개인정보 불법거래 차단을 위하여 ISP 사업자, 방송통신심의위원회 등 유관기관과의 협업체계 구축 및 법적 근거 정비 추진

ㅁ 다크웹을 통한 개인정보 거래를 추적하고 차단하기 위한 웹 탐지기술 개발

ㅁ 다크웹 기반의 기존 불법거래 사례 분석을 통해 다크웹 내 개인정보 불법거래 추적기술 개발

- 포렌식 수사를 위한 다크웹 데이터 수집 및 분석 방안 연구

RISS 검색 - 학위논문 상세보기 (swu.ac.kr)

1. **다크웹에서 데이터를 지속적이고 안정적으로 수집하도록 설계된 크롤링 시스템 구현**
2. **수집된 정보를 분석하여 다크웹의 현재 상황 분석(Ex. 사용 언어 분포, 많이 사용되는 암호 화폐 종류 등)**
3. 다크웹 수사 과정에서 발생할 수 있는 외상 후 스트레스 장애(PTSD)를 방지하기 위한 수사 기법 도출: 선정적인 내용을 가릴 수 있는 기계학습 방안
4. **다크웹과 표면웹을 연결할 수 있는 흔적을 기반으로 다크 웹 사이트 운영자를 추적하는 방법 제안** – Tracking code, Status mode (33쪽 내용 참고)
5. 사례 연구 : 아동 음란물, 온라인 카지노, 암시장 - tracking code확보, 웹사이트에 대한 군집화 진행(40쪽 내용 참고)

: 본 논문에서는 다크웹 생태계를 고려하여 데이터를 수집하는 크롤러를 제시하며, 조사자의 정신 건강을 보호하기 위해 선정적인 콘텐츠를 감지하는 기계학습 모델을 구현한다. 추가로, 이전까지의 연구에서 제안했던 암호 화폐 거래를 추적하는 방법과 함께 운영자의 익명성을 제거할 수 있는 중추적 단서인 Tracking code와 Status mode를 소개한다. 이후, 크롤러가 수집한 14,993개의 다크웹 사이트를 분석하여 다크웹의 현재 상태를 소개하고, 세 가지 사례 연구를 제시함으로써 제안한 데이터 분석 방법론이 다크웹과 표면웹 사이트를 연결하여 불법 행위가 이뤄지는 다크웹 사이트의 운영자를 식별할 수 있음을 입증한다.

- 메모리 포렌식 기반 키워드 매칭을 통한 다크 웹 사용자 행위 분석

https://s3-us-west-2.amazonaws.com/secure.notion-static.com/3eeaab52-eb0f-4cf2-896c-9c26ca02fc2f/%EB%A9%94%EB%AA%A8%EB%A6%AC_%ED%8F%AC%EB%A0%8C%EC%8B%9D_%EA%B8%B0%EB%B0%98_%ED%82%A4%EC%9B%8C%EB%93%9C_%EB%A7%A4%EC%B9%AD%EC%9D%84_%ED%86%B5%ED%95%9C_%EB%8B%A4%ED%81%AC_%EC%9B%B9_%EC%82%AC%EC%9A%A9%EC%9E%90_%ED%96%89%EC%9C%84_%EB%B6%84%EC%84%9D.pdf

:> 논문을 응용해 개인정보 거래 내역을 추적하는 데에 사용하면 좋을 듯

: 최근 토어 네트워크가 보장하는 익명성을 기반으로 한 다크 웹을 통해 불법적인 거래가 다수 발생함에 따라, 다크 웹 내의 범죄 행위 추적을 위한 디지털 포렌식 수사의 중요성이 강조되고 있다. 토어 브라우저의 경우 범용 웹 브라우저와 달리 웹 아티팩트 흔적을 남기지 않아 분석이 제한적이다. 그러나 메모리 덤프 기반 포렌식을 수행할 경우 사용자의 행위에 관한 평문이 그대로 저장되어 포렌식 아티팩트를 획득할 수 있다. 이에 본 논문에서는 메모리 포렌식을 통해 토어 브라우저를 통한 다크 웹 내 사용자 행위를 분석하는 프레임워크를 제안한다.

: 본 논문에서는 입력으로 주어진 메모리 덤프 형태의 활성 데이터로부터 효율적인 메모리 포렌식을 통해 다크웹 사용자 행위를 자동으로 분석하는 프레임워크를 제안한다. 먼저 호스트 내 토어 설치 여부 및 접속 여부 와 같은 포렌식 수사 과정에서 필요한 정보를 수집한 뒤, 평문 형태로 저장되는 사용자의 다크 웹 검색 내역을 메모리 덤프로부터 추출한다. 이 과정에서, 사용자 행위 분석의 효율성 향상을 위해 실제 토어 네트워크상에서 운용되고 있는 토어 히든 서비스로부터 웹 크롤링을 통해 키워드를 수집한다. 이렇게 자동으로 수집한 키워드들을 바탕으로 활성 데이터에 대해 패턴 매칭을 수행함으로써 수사의 효율성을 보장한다. 키워드에는 범죄와 관련된 직접적인 단어뿐만 아니라 불법 거래 시 은밀하게 사용되는 은어도 수집되는 실질적 포렌식 아티팩트 탐지가 가능하며, 실제 다크 웹상의 Onion 도메인에서 수집된 키워드를 선정하기 때문에 범죄 행 위 패턴 매칭 수사의 효율성을 올릴 수 있음을 보여준다.

+ 추가:

다크웹에서 제공하는 시각자료 검색, 수집 기술(비정형 데이터의 개인정보 탐지 기술과 연계)

https://s3-us-west-2.amazonaws.com/secure.notion-static.com/cc0a4861-8de8-4660-b2be-30f5956c4c13/%EC%9B%B9_%EB%B8%8C%EB%9D%BC%EC%9A%B0%EC%A0%80_%EB%A0%8C%EB%8D%94%EB%A7%81%EC%9D%84_%ED%99%9C%EC%9A%A9%ED%95%9C.pdf

- 웹 브라우저 렌더링을 활용한 컨테이너 기반 다크웹 스캐너 설계

: 다크 웹 불법 서비스에서 제공하는 시각 정보를 다크 웹 접속 없이 일반 웹 브라우저를 통해 확인 및 수집할 수 있는 기술 제시

: 다크 웹 내에서 발생하는 범죄의 이해를 높이려면 해당 서비스에서 제공하는 콘텐츠(이미지, 비디오 등)에 대한 포괄적인 정보 수집 및 보관이 필요하다. 또, 이를 일반 브라우저에서 확인할 수 있게 한다면 다크 웹의 실상에 다수가 보다 쉽게 접근할 수 있다. 이를 위해 본 연

구에서는 다크 웹 불법 서비스의 당시 페이지를 일반 브라우저에서 렌더링 할 수 있는 형태로 저장하는 컨테이너 기반 다크 웹 스캐너를 제안한다.

+ 추가:

- 개인정보 거래 시 이용되는 암호화폐 추적 기술

: 암호화폐의 흐름을 추적하고 취급업소를 식별하여 범죄자를 추적할 수 있는 기반 기술

https://s3-us-west-2.amazonaws.com/secure.notion-static.com/231d371f-71b0-44ae-baa5-d4161cb49e79/%EC%82%AC%EC%9D%B4%EB%B2%84_%EB%B2%94%EC%A3%84%EC%97%90_%EC%95%85%EC%9A%A9%EB%90%98%EB%8A%94_%EC%95%94%ED%98%B8%ED%99%94%ED%8F%90_%EB%B6%88%EB%B2%95%EA%B1%B0%EB%9E%98_%EC%B6%94%EC%A0%81.pdf