Artifact pom Michutda

Locality 기반 윈도우 아티팩트 및 파일 관계성 시각화 도구 개발

Windows Artifact

Relationship Visualizer

지도교수 : 손태식 (사이버보안학과 교수)

팀장 : 성민규 (사이버보안학과)

팀원 : 윤문경(사이버보안학과), 방재훈(사이버보안학과)

목차

PC 보급

Personal Computer의 시작
사업의 전산화 (직장생활)

Mobile 보급

일상에 밀접한 Digital Device의 등장
개인 밀접 데이터 생성 (사생활)

IoT 보급

가구 및 서비스의 스마트화
빅데이터 시대의 시작

1

분석량 증가

분석 데이터 증가

2

수사자원 한정

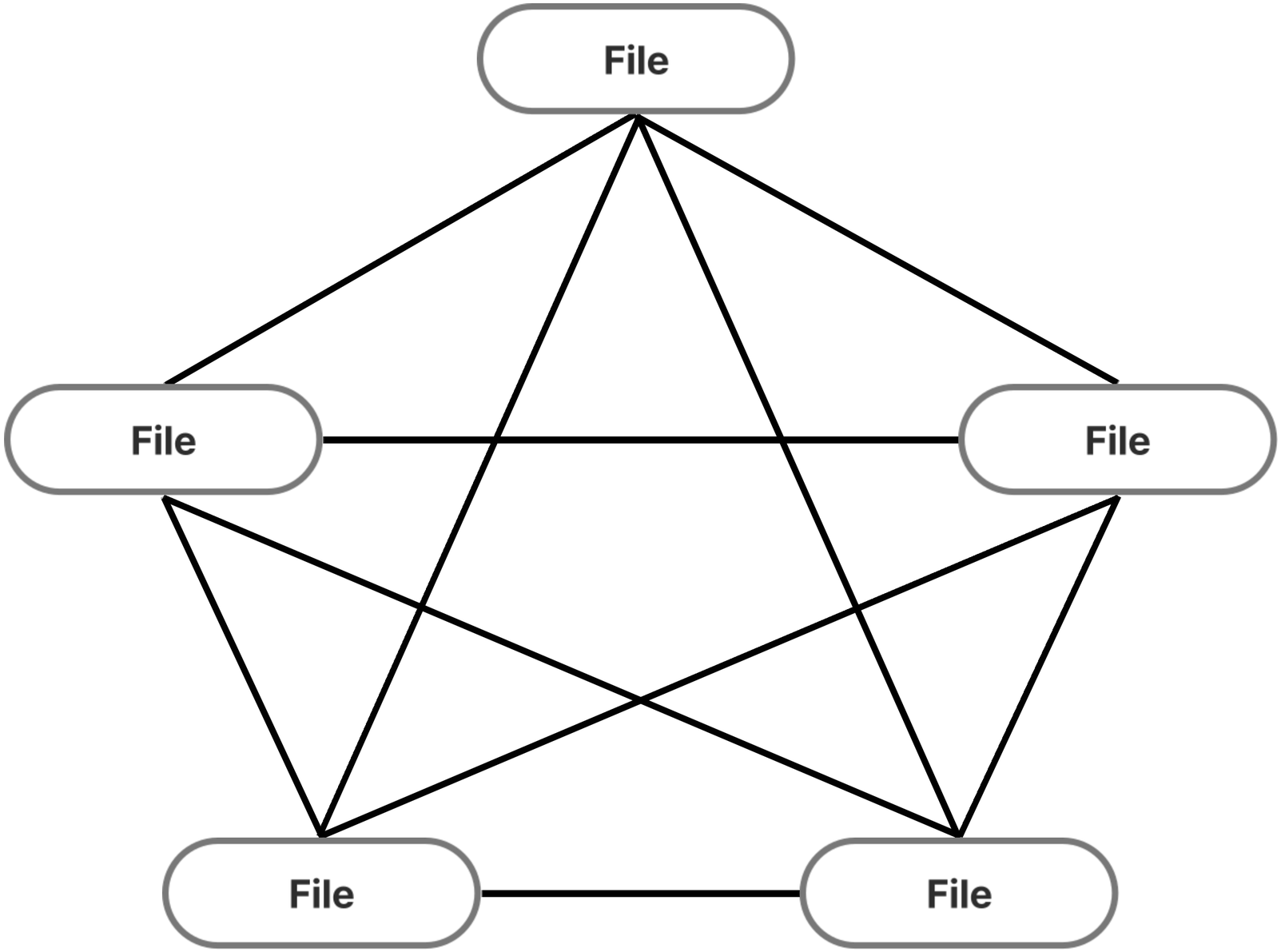
전문인력 및 자원 한정

3

수사효율 하락

수사 필요 자원 증가

프로젝트 목표



Locality

1

Time

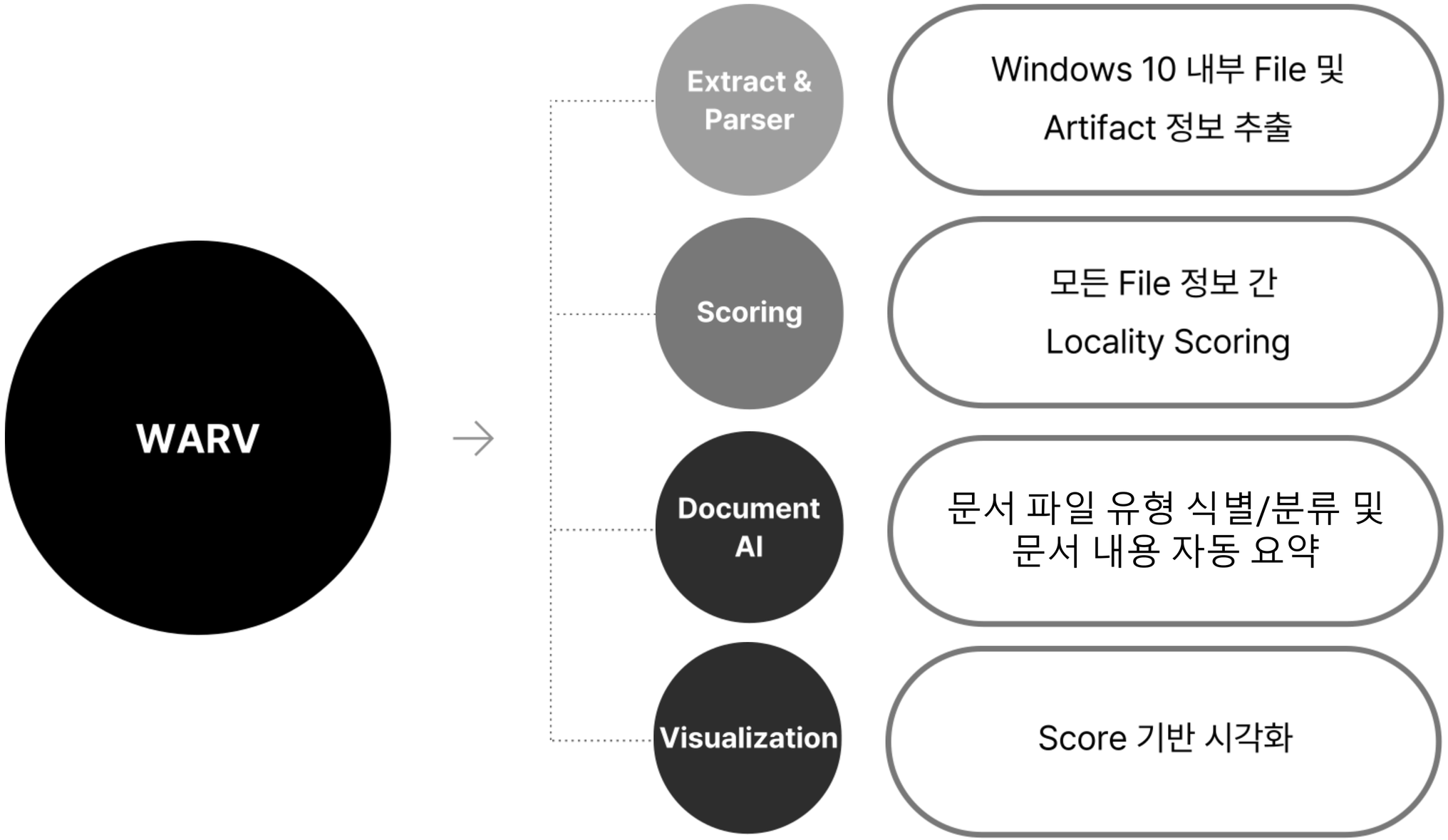
시간 차이

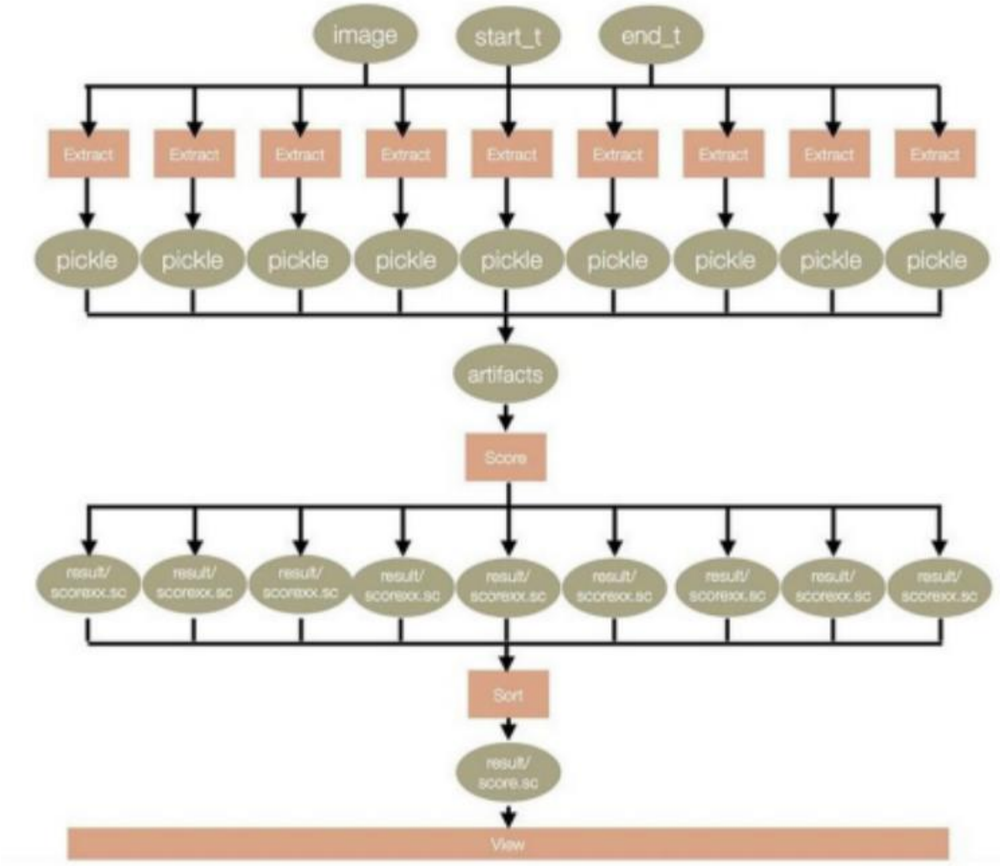
2

Distance

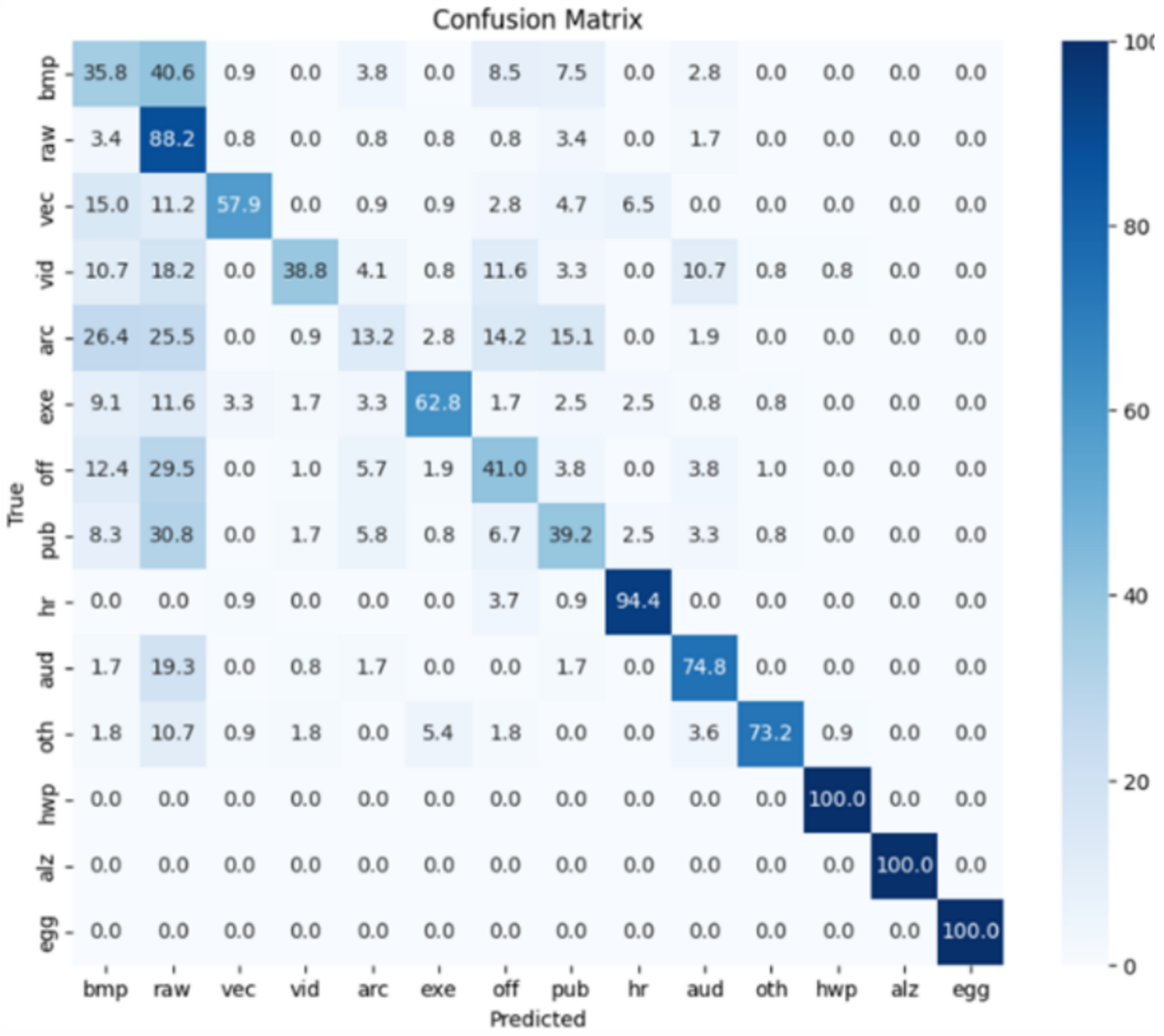
경로 차이

Develop Process

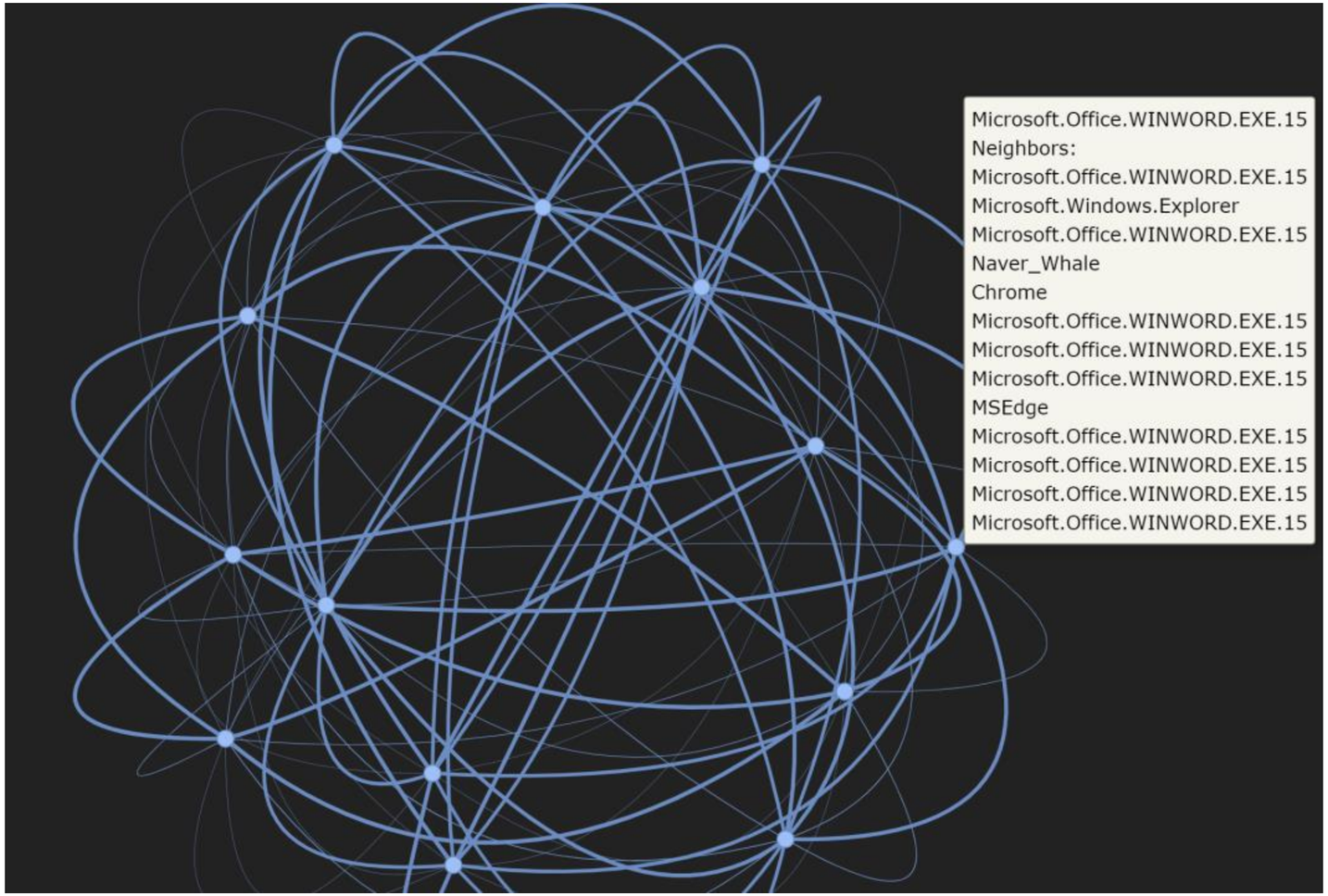




Program Process



Document AI EDA



Visualization

“Windows Artifact Relationship Visualizer”

Windows 운영체제에서 디스크에 존재하는 모든 파일/폴더 간의 연관성을 정량화하여 이를 그래픽으로 표현하는 분석 프로그램

시스템 파일과 중요 파일 식별:
- 자동으로 생성된 시스템 파일들을 식별하여 제외
- 중요한 파일들은 파일 내용이나 프로그램 이름을 분석
- 사용자가 필요한 정보에 쉽게 접근

저장된 결과물 관리:
- 프로그램이 계산한 관계성에 대한 결과물은 Python을 통해 파일로 저장
- 사용자는 저장된 결과물을 다양한 목적에 활용할 수 있도록 원하는 형식으로 결과를 관리

유연한 시각화:
- 파일 간의 관계성을 자유롭게 탐색
- Vertex-Edge 형식의 그래픽을 활용하여 사용자에게 직관적이고 명확한 정보 전달

사용 예시:
- 사용자는 프로그램을 실행한 후 Windows 파일 및 폴더 간의 관계를 시각화하여 확인할 수 있음
- 특정 파일 또는 폴더에 대한 상세 정보를 쉽게 찾을 수 있으며, 연결된 파일들의 중요성을 시각적으로 확인할 수 있음

확장성 및 개선 방향:
- 향후 Windows 업데이트나 새로운 파일 구조에 대한 대응을 위한 유연성 확보
- 사용자 피드백을 수용하여 프로그램의 기능을 개선하고, 새로운 요구 사항에 대응할 수 있는 업그레이드를 계획
- AI를 활용하여 파일 식별 및 내용 요약 수행

기술적인 측면:
- Python을 활용한 데이터 추출 및 처리는 효율적이며, 시각화는 널리 사용되는 라이브러리를 통해 구현
- 프로그램은 사용자 친화적인 인터페이스를 제공하여 비전문가들도 쉽게 사용할 수 있도록 고려

추후 목표

1. **시인성 개선**
   각 File에 대한 정보 표현
   Edge 개선

2. **다중 Drive 분석**
   다중 Drive 연관 분석
   서로 다른 사용자 간의 관계 분석

3. **가중치 최적화**
   Locality Scoring Weight Optimization

감사합니다

발표자 **방재훈**이었습니다

Special

Thank You!