2022년 한국디지털포렌식학회 동계학술대회

메타마스크(MetaMask) 암호화폐 지갑 아티팩트 분석

2022. 12. 05

손지훈, 박정흠

hunjison@korea.ac.kr

고려대학교 KOREA UNIVERSITY

Digital Forensic Research Center

Institute of Cyber Security & Privacy, Korea University.

목차

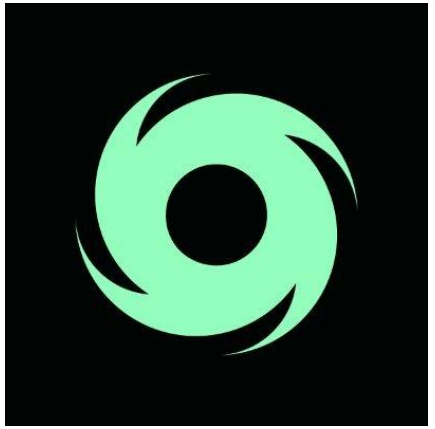
연구 배경

연구 배경

암호화폐와 이더리움

- **암호화폐를 이용하는 경우들이 점점 많아짐**
  - 개인 간 거래, NFT(Non Fungible Token), P2E(Play to Earn) 게임 등
- **이더리움 블록체인**
  - 이더리움은 '플랫폼 코인'으로 불리며 무한한 확장성을 지님
  - DApp(Decentralized App), Smart Contract, DeFi(Decentralized Finance) 등
- **범죄 및 자금세탁의 수단, 암호화폐**
  - 범죄에 따른 암호화폐 총 피해액은 2021년 140억 달러로, 작년대비 79% 증가
  - 러그풀(Rug Pull) 수법은 이더리움 블록체인 기반의 ERC-20 토큰을 이용함
  - 자금세탁 서비스(Uniswap, Tornado Cash) 역시 이더리움 블록체인 내에서 동작함

NFT



Tornado Cash

연구 배경

메타마스크(MetaMask)

- **메타마스크 지갑**
  - 이더리움 및 토큰들을 보관, 거래할 수 있는 암호화폐 지갑
  - DeFi, DAO, NFT 등 탈중앙화 서비스 이용을 위해 지갑 연동이 필요함
  - 브라우저 확장 형태로 설치되며 크롬·엣지·파이어폭스 등 브라우저 지원
- **연구의 필요성**
  - 메타마스크 사용자는 3000만 명을 돌파하였고, 2년 만에 38배 증가함
  - 이더리움 네트워크 내에서 메타마스크의 점유율은 약 85%로 추정
  - 주요 거래소들에서도 브라우저 확장 형태의 지갑을 새롭게 출시하였음
  - 브라우저 확장 형태의 지갑 분석 방법에 대해 국내외에 연구된 바 없음

메타마스크

바이낸스
브라우저 확장

코인베이스
브라우저 확장

연구 배경

선행 연구

- **암호화폐 트랜잭션과 지갑에 대한 디지털 포렌식 연구들**

분류	연도	연구 내용 요약
공개 트랜잭션 분석	2018	불법 거래로 의심되는 비트코인 거래의 추적 및 모니터링 방법
	2020	비트코인 트랜잭션 수사를 위한 extended safe Petri Net 기반의 분석 방법
	2021	비트코인 트랜잭션의 UTXO 데이터 분석을 통한 거래 추적 방법
비트코인 지갑 분석	2015	Base58 형식의 비트코인 지갑 주소, 개인키 검색도구 개발
	2018	범죄 시나리오를 기반으로 한 비트코인 지갑 수사 방법 제시
	2019	비트코인 아티팩트와 분석 방법의 제시 및 정규표현식 기반의 분석 도구 개발
	2022	비트코인 지갑 4종에 대한 아티팩트 분석 도구 개발
지갑 메모리 분석	2020	하드웨어 지갑의 메모리 아티팩트 분석 및 시각화 프레임워크 개발
	2022	하드웨어 지갑 Ledger, Trezor에 대한 아티팩트 분석 및 추출 도구 개발

- **기존 연구들의 한계**
  - 로컬 아티팩트 분석 결과가 공개 트랜잭션 데이터와 차별화되지 않음
  - 이더리움 지갑 및 브라우저 확장 형태의 지갑에 대해 고려하지 않음
  - 니모닉 코드 복호화 알고리즘에 대해 연구된 바 없음

메타마스크 아티팩트 식별 및 해석

연구 범위 및 실험 환경 구성

메타마스크 아티팩트 식별 및 해석

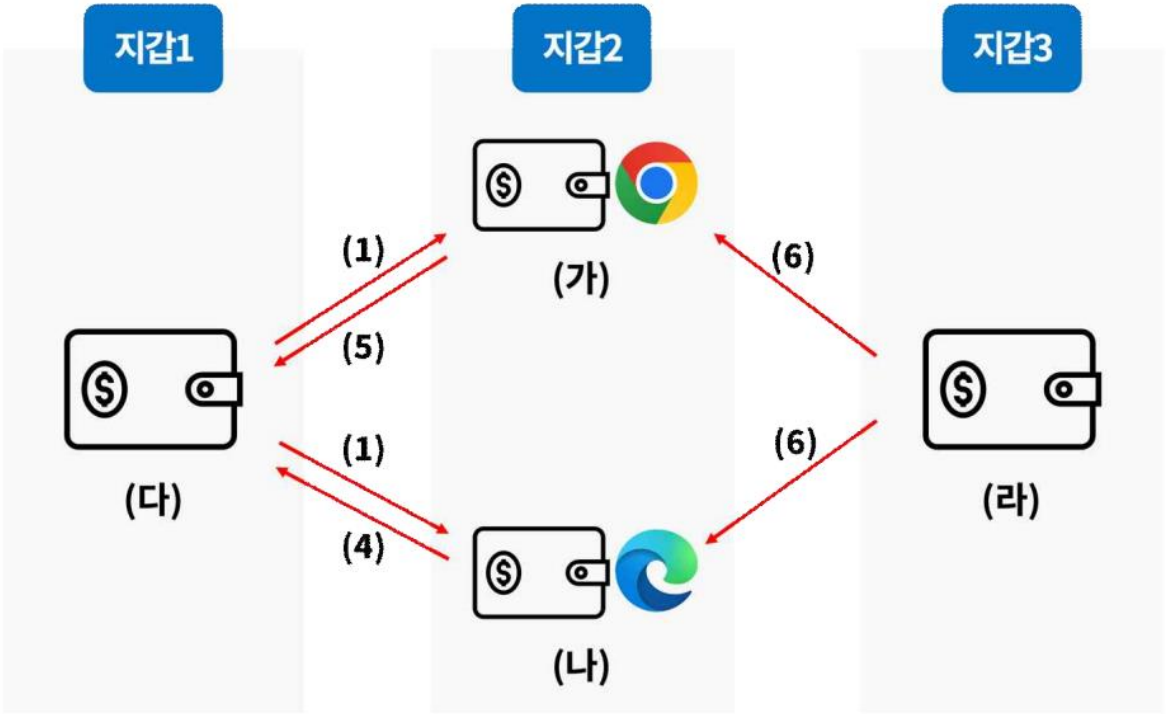
연구 범위

- **메타마스크 지갑 정보**
  - 지갑 주소, 지갑 잔액, 트랜잭션 로그 등
- **사용자 행위 추적**
  - 시나리오 기반 아티팩트의 생성 과정 분석
  - 공개된 트랜잭션 정보 이외의 사용자 행위 로그, 타임스탬프 등
- **사용자 지갑 확보(니모닉 코드 획득)**
  - 니모닉 코드 복호화
  - 니모닉 코드 검색

메타마스크 아티팩트 식별 및 해석

실험 환경 구성

- **서로 다른 브라우저에서의 아티팩트 분석**
  - 메타마스크는 여러 대의 PC, 모바일, 브라우저에서 동시에 로그인 가능
  - 같은 지갑 주소(지갑 2)에 대해 Chrome, Edge에서 각각 데이터 수집



순서	행위	연구 내용 요약
1	(다)	지갑 2에 이더리움 0.1 ETH 전송
2	(가)	브라우저 실행
3	(가)	메타마스크 로그인
4	(나)	(다)에 이더리움 0.01 ETH 전송
5	(가)	(다)에 이더리움 0.02 ETH 전송
6	(라)	지갑 2에 이더리움 0.03 ETH 전송
7	(가), (나)	브라우저 종료 후 다시 로그인

메타마스크 아티팩트 식별 및 해석

지갑 정보 분석

메타마스크 아티팩트 식별 및 해석

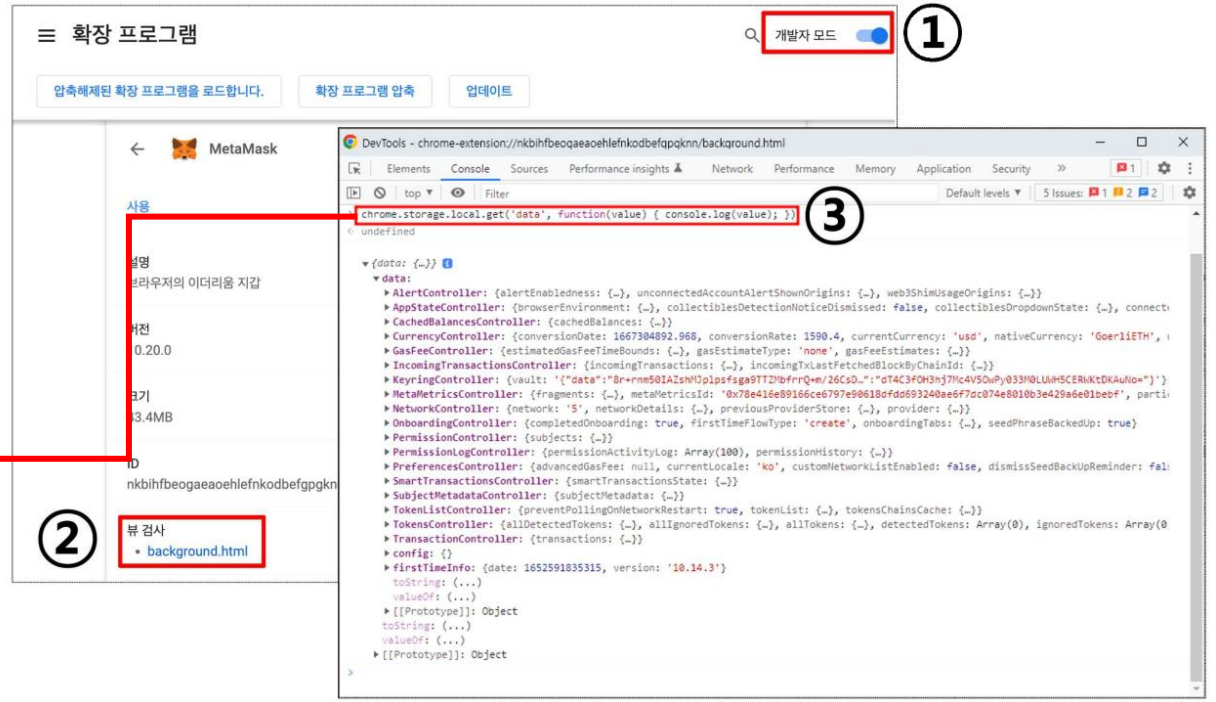
지갑 정보 분석

- **메타마스크 LevelDB 저장 경로**
  - Chrome: {Chrome Local Path}\User Data\{Profile}\Local Extension Settings\{ID}

    Edge: {Edge Local Path}\User Data\{Profile}\Local Extension Settings\{ID}
    - PROFILE: 유저 프로필(Default 등), ID: 브라우저 확장 웹스토어에서 검색 가능

- **브라우저 개발자 도구를 이용한 분석**
  - 확장 프로그램 개발자 도구가 별도로 존재
  - 스크립트 실행시 LevelDB 객체 반환됨

```
chrome.storage.local.get('data',
function(value){console.log(value)});
```



메타마스크 아티팩트 식별 및 해석

지갑 정보 분석

- **LevelDB 키에 대한 분석(일부 생략)**

키 이름	세부 항목	종류	설명
AddressBookController	addressBook	거래 기록	해당 지갑에서 **송신**했던 이더리움 **지갑 주소**
IncomingTransactionsController	incomingTransactions	거래 기록	이더리움 **수신** 트랜잭션 기록
MetaMetricsController	fragments	거래 기록	**송신** 트랜잭션 **실패 기록**(실패시간, 사유)
TransactionController	transactions	거래 기록	이더리움 **송신** 트랜잭션 기록
AppStateController	browserEnvironment	지갑 정보	브라우저 정보(Win, Mac)
CachedBalancesController	cachedBalances	지갑 정보	네트워크별 계좌의 이더리움 **잔액**
PreferencesController	identities	지갑 정보	해당 계정이 가지고 있는 **지갑 목록**
	selectedAddress	지갑 정보	사용자의 선택한 **지갑 주소**
TokensController	allTokens	지갑 정보	사용자의 토큰 목록
KeyringController	vault	니모닉 코드	니모닉 코드 복구에 사용되는 데이터
PermissionController	subjects	사용자 행위	메타마스크의 **외부 권한 허가** 기록
SubjectMetadataController	subjectMetadata	사용자 행위	사용자가 **최근에 방문했던 웹사이트**
CurrencyController	conversionDate	사용자 행위	환율 동기화 시각(**사용자 최종 접속 시간**)
firstTimeInfo	date	사용자 행위	사용자의 메타마스크 첫 설치 시각

메타마스크 아티팩트 식별 및 해석

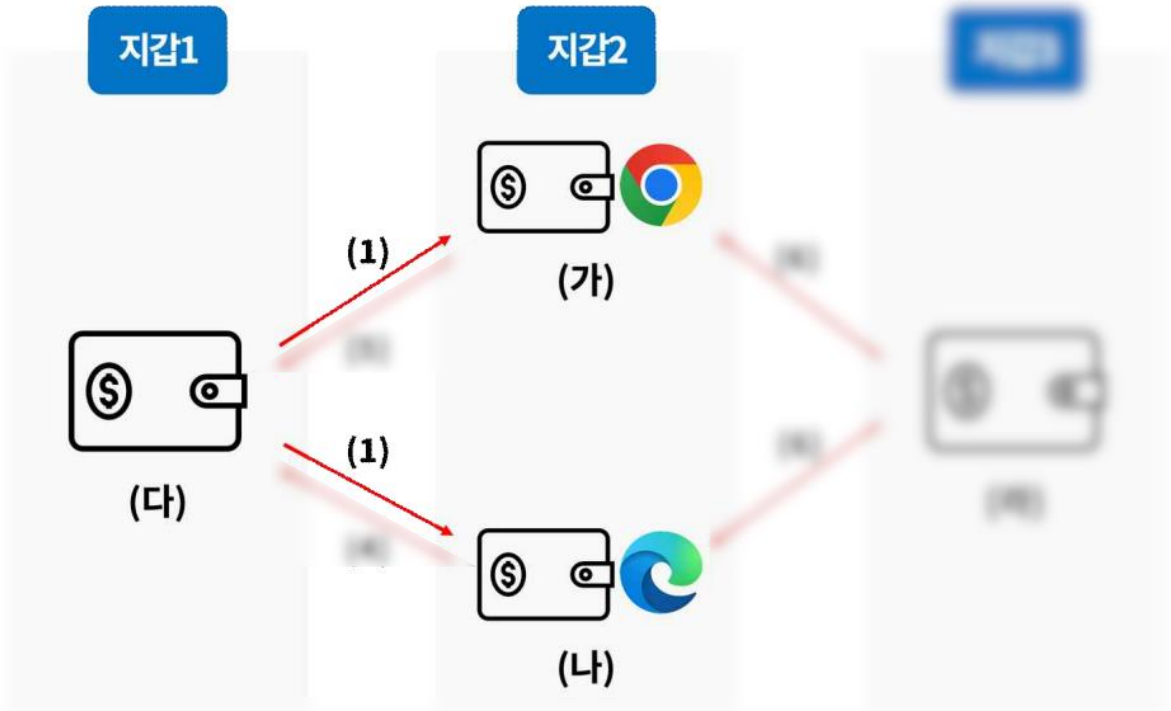
사용자 행위 분석

메타마스크 아티팩트 식별 및 해석

사용자 행위 분석

- **메타마스크 로그인 이전(순서 1, 순서 2)**
  - 로그인 이전에는 트랜잭션 정보가 갱신되지 않음
  - 사용자가 브라우저를 이용해도 아티팩트 변화 없음

- **메타마스크 로그인(순서 3)**
  - 트랜잭션이 잔액에 반영되며, 트랜잭션 로그 생성
  - 메타마스크 확장 프로그램을 실행하는 도중에는 주기적으로 지갑 계좌 정보가 동기화됨

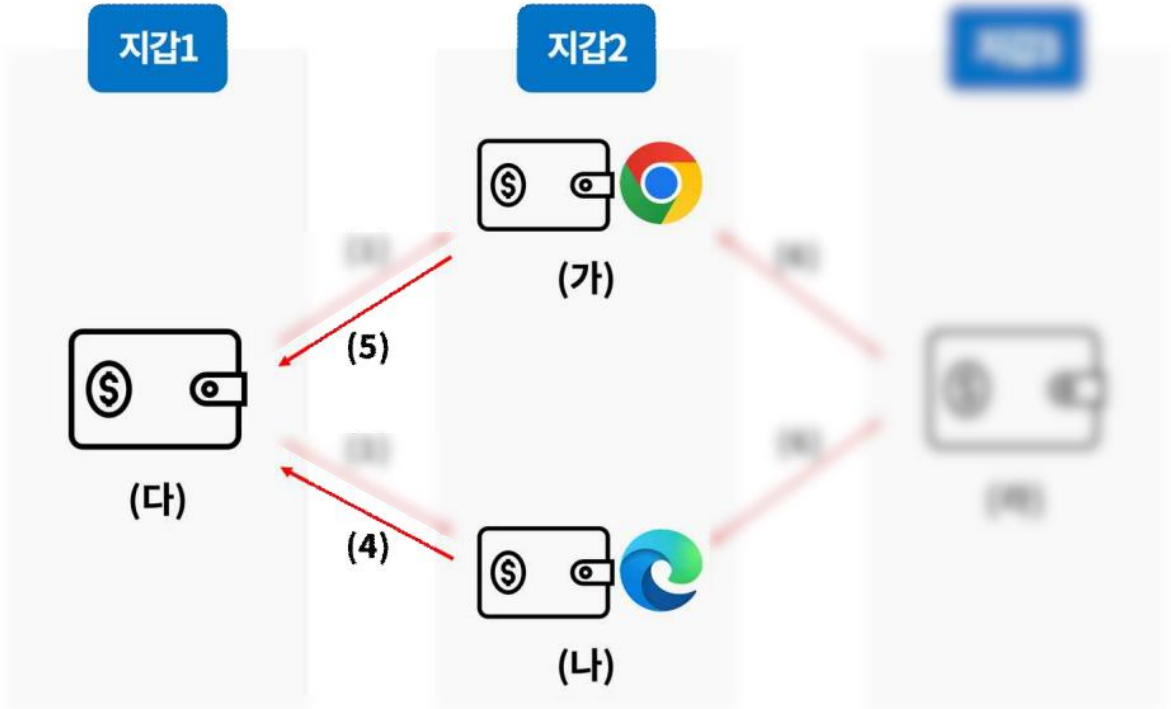


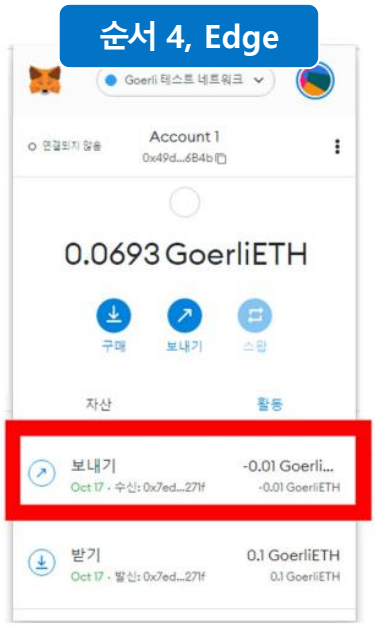
순서	행위	연구 내용 요약
1	(다)	지갑 2에 이더리움 0.1 ETH 전송
2	(가)	브라우저 실행
3	(가)	메타마스크 로그인
4	(나)	(다)에 이더리움 0.01 ETH 전송
5	(가)	(다)에 이더리움 0.02 ETH 전송
6	(라)	지갑 2에 이더리움 0.03 ETH 전송
7	(가), (나)	브라우저 종료 후 다시 로그인

메타마스크 아티팩트 식별 및 해석

사용자 행위 분석

- **이더리움 송신(순서 4, 순서 5)**
  - 송신 트랜잭션 로그는 송신한 지갑에 고유하게 남음
    → 해당 지갑에서의 이더리움 송신을 입증 가능함
  - 트랜잭션 실패, 취소 역시 송신한 지갑에만 생성



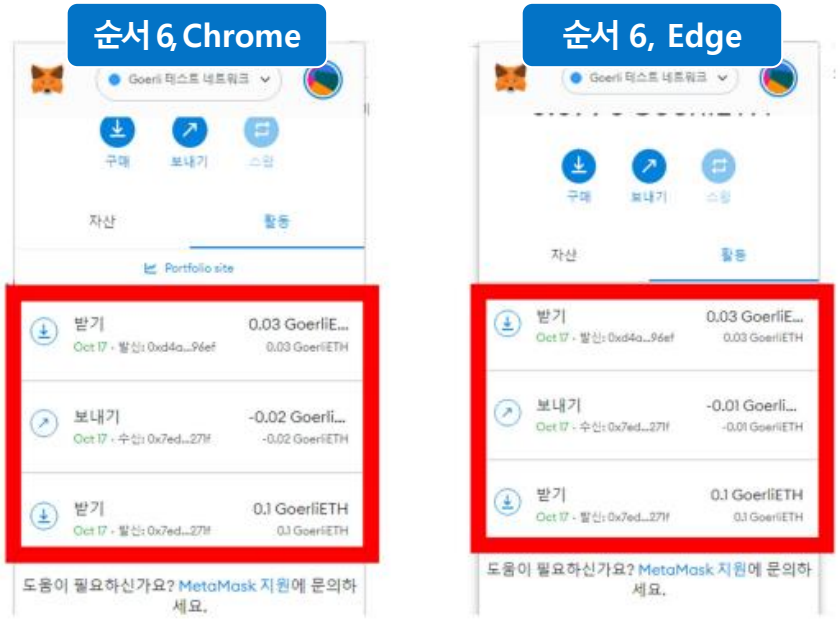


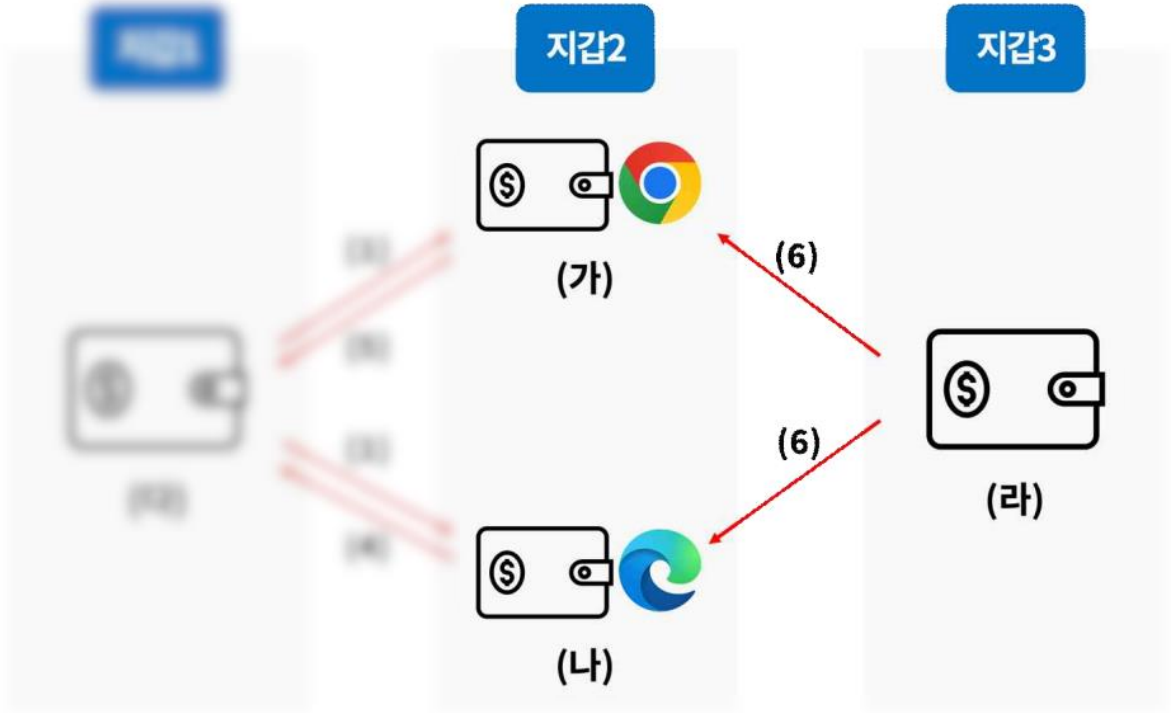
순서	행위	연구 내용 요약
1	(다)	지갑 2에 이더리움 0.1 ETH 전송
2	(가)	브라우저 실행
3	(가)	메타마스크 로그인
4	(나)	(다)에 이더리움 0.01 ETH 전송
5	(가)	(다)에 이더리움 0.02 ETH 전송
6	(라)	지갑 2에 이더리움 0.03 ETH 전송
7	(가), (나)	브라우저 종료 후 다시 로그인

메타마스크 아티팩트 식별 및 해석

사용자 행위 분석

- **이더리움 수신(순서 6)**
  - 수신 트랜잭션 로그는 모든 지갑에 생성됨
  - 송신 트랜잭션과 달리 양쪽 모두에 기록됨
    - 트랜잭션 횟수는 총 4회이지만 3회만 기록됨





순서	행위	연구 내용 요약
1	(다)	지갑 2에 이더리움 0.1 ETH 전송
2	(가)	브라우저 실행
3	(가)	메타마스크 로그인
4	(나)	(다)에 이더리움 0.01 ETH 전송
5	(가)	(다)에 이더리움 0.02 ETH 전송
6	(라)	지갑 2에 이더리움 0.03 ETH 전송
7	(가), (나)	브라우저 종료 후 다시 로그인

메타마스크 아티팩트 식별 및 해석

니모닉 코드 복호화 및 검색

메타마스크 아티팩트 식별 및 해석

니모닉 코드 복호화

- **니모닉 코드와 지갑 확보**
  - 사건을 조사할 때에 암호화폐 지갑과 지갑 속 잔액을 확보할 필요가 있음
  - 니모닉 코드를 이용하면 지갑 계정에 포함된 모든 지갑을 복구할 수 있음
- **기존의 공개된 자료**
  - 메타마스크에서는 브라우저를 이용한 복호화 방안을 제시
  - 따라서 활성 시스템에서만 니모닉 코드 복호화가 가능하다는 단점이 존재
- **복호화 알고리즘 연구**
  - 유저의 계정 패스워드 필요
  - LevelDB 내의 Vault 값 필요

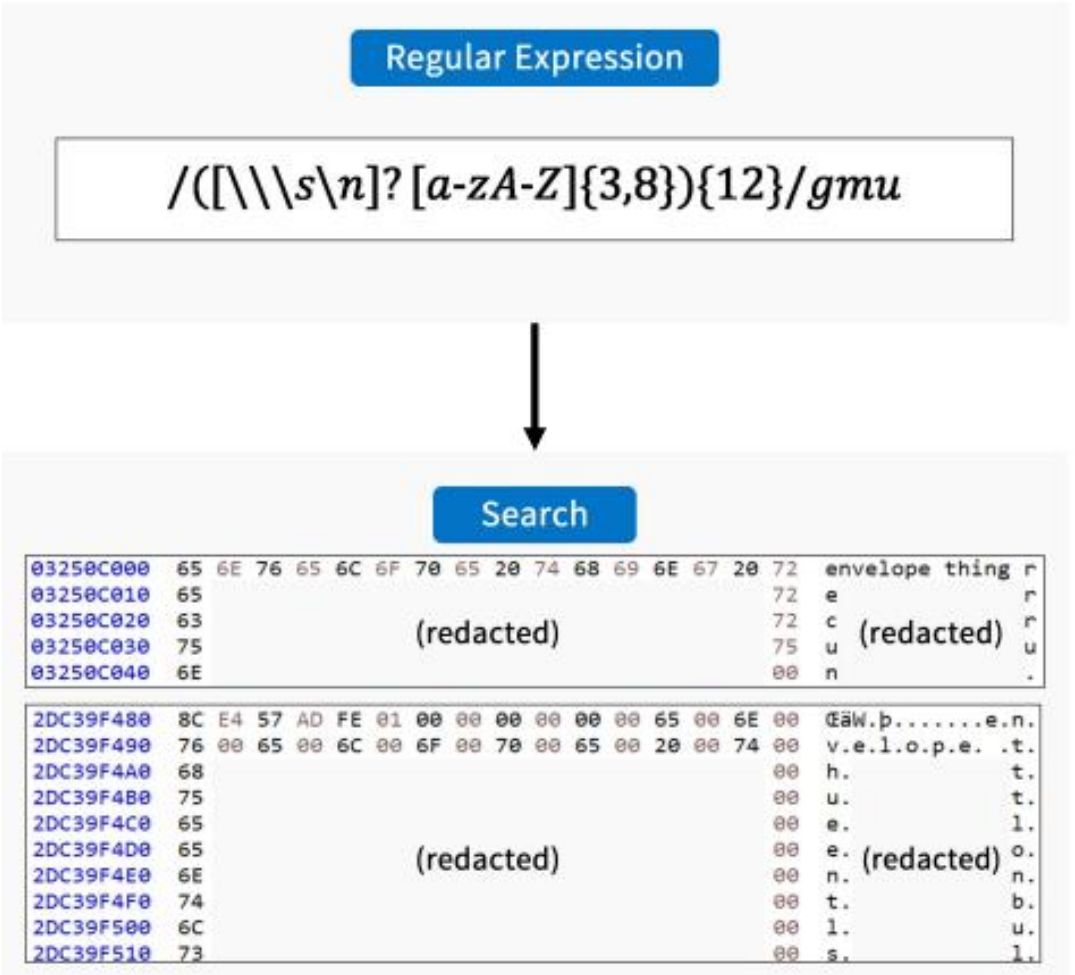
```
password        = "User's MetaMask password";
data            = GetValuesFromVault(ENCRYPTED_MNEMONIC_CODES);
salt, iv        = GetValuesFromVault(SALT_AND_IV);
iteration       = 1000;
length          = 256;

key             = PBKDF2-SHA256(password, salt, iteration, length);
mnemonics       = AES-256-GCM-DECRYPT(data, key, iv);
```

메타마스크 아티팩트 식별 및 해석

니모닉 코드 검색

- **니모닉 코드 복호화의 한계**
  - 복호화를 위해서는 유저의 패스워드가 필요함
- **니모닉 코드의 규칙성**
  - 길이가 3 이상 8 이하인 영단어
  - 영단어가 최소 12개에서 최대 24개 반복
  - 영단어 목록은 미리 정의됨(BIP-0039 표준)
- **검색 방법**
  - 디스크 및 메모리에서 검색 가능함
  - 정규 표현식 탐색 → 단어 목록 포함 여부 검증

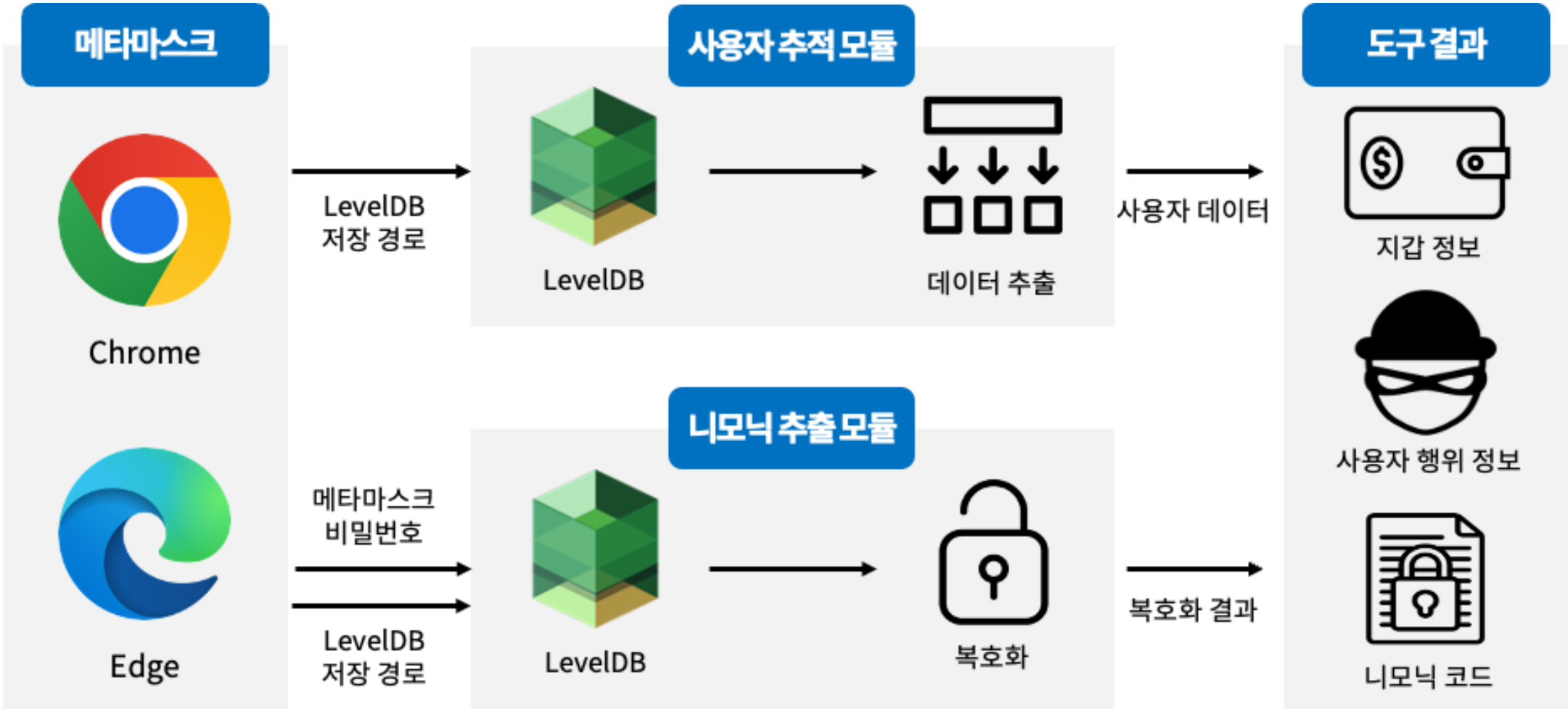


구현 및 평가

구현 및 평가

도구 구현

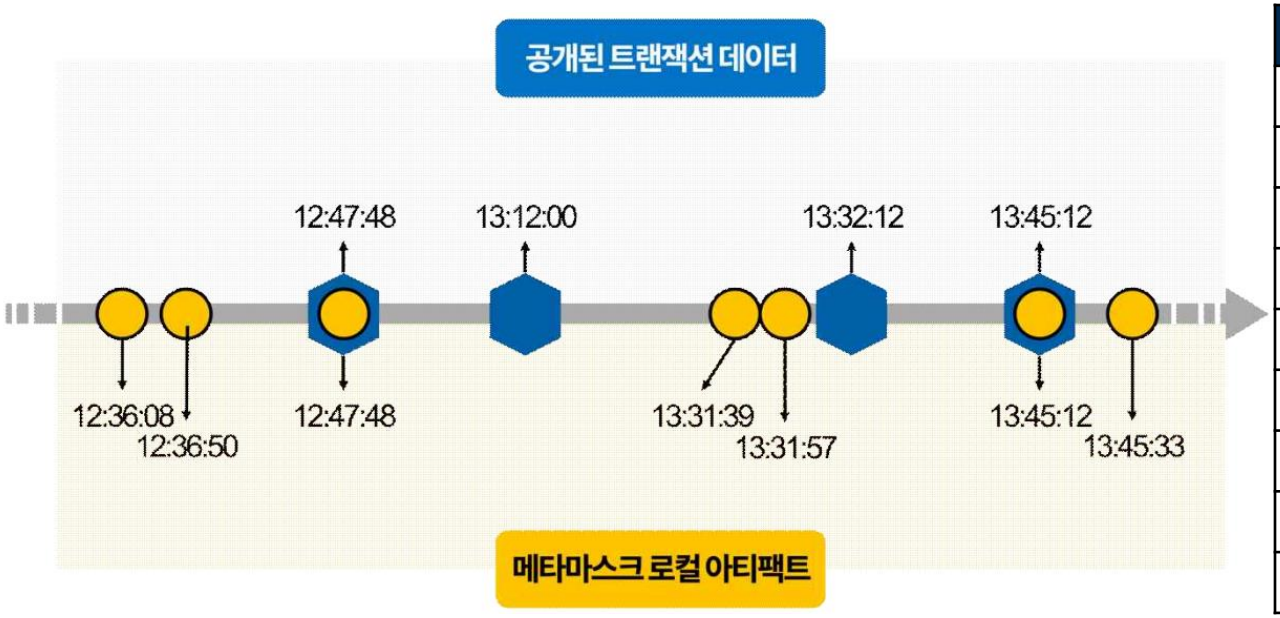
- 메타마스크 분석 도구의 동작 방식



구현 및 평가

도구 평가(공개 트랜잭션과의 비교)

- **타임라인 획득**
  - 더 자세한 사용자 행위 타임라인 구성 가능
    - 메타마스크 설치 시간, 사용자의 마지막 접근 시간, 이더리움 송신 요청/실패 시간 등



순서	시간	로컬 아티팩트	공개 트랜잭션
이전	12:36:08	메타마스크 프로그램 설치	
이전	12:36:50	"Account 1" 계정 선택	
1	12:47:48	이더리움 수신 트랜잭션 1(동일)	
4	13:12:00		이더리움 송신 트랜잭션 1
5	13:31:39	이더리움 송신 요청, dropped	
5	13:31:57	이더리움 송신 요청, confirmed	
5	13:32:12		이더리움 송신 트랜잭션 2
6	13:45:12	이더리움 수신 트랜잭션 2(동일)	
이후	13:45:33	사용자의 마지막 접속 시각	

구현 및 평가

도구 평가(공개 트랜잭션과의 비교)

- **사용자 행위 분석**

분류	내용	로컬 아티팩트	공개 트랜잭션	비고
거래 기록	이더리움 수신 트랜잭션	O	O	
거래 기록	이더리움 송신 트랜잭션	△	O	해당 지갑에서 송신한 경우 획득 가능
거래 기록	이더리움 송신 지갑 특정	O	X	
거래 기록	이더리움 송신 실패 기록(시간, 사유)	O	X	
지갑 정보	지갑 주소	O	X	
지갑 정보	이더리움 잔액	O	O	
지갑 정보	토큰 목록, 잔액	△	O	토큰 잔액은 획득 불가
지갑 정보	지갑 브라우저 정보	O	X	
지갑 정보	같은 계정에 포함된 지갑 목록	O	X	
사용자 행위	메타마스크 외부 권한 허가 기록	O	X	
사용자 행위	사용자가 최근 방문한 사이트	O	X	
사용자 행위	사용자의 마지막 접속 시간	O	X	
사용자 행위	메타마스크 첫 설치 시각	O	X	

THANK YOU
for Listening!

Digital Forensic Research Center

Institute of Cyber Security & Privacy, Korea Univ.

forensic.korea.ac.kr
hunjison(at)korea.ac.kr

Questions?