Window 8 Style UI 기반의 페이스북 앱에 대한 디지털 포렌식 분석

이 찬 진*, 정 목 동**

*부경대학교 컴퓨터공학과
{leecj011,mdchung}@pknu.ac.kr

Digital Forensic Analysis of the Window 8 Style UI based Facebook App

ChanJin Lee and Mokdong Chungⓒ
Dept. Of Computer Engineering, Pukyong National University, Republic of Korea
{leecj011,mdchung}@pknu.ac.kr

요 약

기존 window8 Style 에 대한 디지털 포렌식 연구는 윈도우 기본 애플리케이션에 대해서만 진행되어 있는 상황이고, 다른 3rd party Style App 들에 대해서만 진행되어있는 상황이다. 본 논문에서는 Window8 Style UI 의 Instant Messengers 에 대해 디지털 포렌식 분석하고 이를 통해 범인의 행동 흐름 파악 및 증거확보 매커니즘을 제시하고자 한다. 본 논문은 기존의 Window8 의 접근방법을 토대로 하여, Style App 의 사용흔적이나 내용에 대해 확인하며, 시간정보, 이미지 등 각종 애플리케이션들을 다각적으로 분석한다. 본 논문에서 제안한 접근법은 개별 App 들에 대한 정보를 효율적이고 빠르게 분석하고 사건에 대한 정보를 제공함으로써 범죄수사과정에 도움이 될 것으로 기대된다.

키워드 : 컴퓨터 보안, 디지털 포렌식, 윈도우 8 스타일 UI, 페이스북.

1. 서론

최근 컴퓨터에서 만들어지고 저장, 기록되어 있는 데이터가 법정에서 다루어지는 경우가 많은데, 이런 전자적 데이터로 이루어지는 범죄에 대한 법정 증거 자료 확보를 위해 컴퓨터 저장매체와 네트워크로부터 자료를 수집, 분석 및 보존하여 법적 증거물로서 제출 할 [1]수 있도록 하는 일련의 절차와 방법을 디지털 포렌식으로 정의할 수 있다[1]. 지금까지 윈도우는 인텔이나 AMD 가 만드는 x86 기반 프로세서를 지원했다. 하지만, 윈도우 8 로 들어서면서 ARM 기반 SoC(System on chip)까지 지원하는 PC 와 모바일을 동시 지원하는 운영체제를 내어 놓았다. 이로인해, 현재 급격하게 성장하고 있는 스마트폰과 태블릿 PC 기기와의 연동이 가능하게 됐으며, 일반 PC 에서도 별도의 앱 플레이어 없이, 앱을 상용화할 수 있게 되었다. 앱에는 스마트폰의 각종 센서와 통신 기능을 탑재하고 있어, PC 에서 앱을 사용하기 위해 앱계정을 입력시 앱 실행을 위한, 최소한의 데이터들이 스마트폰이나 태블릿 PC 를 통해 동기화 되어 넘어오거나 그 흔적들이 남는다. 특히, 이런 흔적들은 앱의 종류나 실행횟수, 시간정보들을 남기기 때문에 디지털 포렌식 측면에서 범죄자의 사용 패턴이나 행위 등을 파악 할 수 있는 중요한 단서 또는 증거가 될 수 있다[2]. 특히, 수사 초기 단계에서는 범인의 대인관계나 가까운 사람들을 단번에 알아내기는 어렵다. 본 논문에서 언급하는 연락처 리스트는 증거수집 방법이 수사 초기 단계에서 범인의 주변지인을 얼마나 빠르게 파악할 수 있는지를 보여주는 중요한 증거 수집 방법이다.

따라서, 본 논문은 Window 8 Style UI 에서 수집할 수 있는 파일정보 기법에 대해 확인하고, 이에 대한 분석 및 조사 절차를 제안한다. 본 논문 2 절에서 관련연구에 대해 살펴보고, 3 절에서 Style UI 에 등록된 앱들에 대해서 디지털 포렌식 관점에서 접근한다. 그리고 마지막으로 4 절에서 결론 및 향후 연구방향을 제시한다.

2. 관련연구

2.1 윈도우 8 Style UI 관련 아티팩트 접근 관련 연구

먼저, Style UI 는 우리가 잘 알고 있는 기존 Metro UI 와 같은 표현 방법이다. 아티팩트란, 디지털 포렌식에서 운영체제나 애플리케이션을 사용하면서 자동으로 생성되는 흔적을 말한다. 어떤 프로세서건, 설치

* 본 논문은 중소기업청에서 지원하는 2013 년도 산학연 첫걸음기술개발사업(No.C0146737)의 연구수행으로 인한 결과물임을 밝힙니다.

된 운영체제나 설치된 앱이 남기는 흔적을 분석하는 것은 디지털 포렌식 분석 대상으로 분류할 수 있다. 윈도우 8 의 Style UI 를 분석하면, 사용자의 사용습관이나 선호도를 알 수 있다. 또, 메일이나 SNS 서비스 앱을 통하여 다양한 사용자의 개인정보 등을 가져올 수 있다.

표 1. Window 8 Style UI 아티팩트[3,4]

Style App 흔적	경 로
앱 실행파일	%SystemDrive%\Program Files\WindowsApps
앱 바로가기	%UserProfile%\AppData\Local\Microsoft\Windows \Application Shortcuts
앱 패키지 목록과 설정 상태	%UserProfile%\AppData\Local\Packages
시작 화면 고정 목록	%UserProfile%\AppData\Local\Microsoft\Windows\Roaming Tiles
시작 화면 타일 배열	%UserProfile%\AppData\Local\Microsoft\Windows \appsFolder.itemdata-ms
앱 인터넷 사용흔적	%UserProfile%\AppData\Local\Packages\[AppName]\AC \[Sub folders]
앱 저장소	%SystemDrive%\ProgramData\Microsft\Windows\AppRepository
빠른 접근 메뉴 설정	%UserProfile%\AppData\Local\Microsoft\Windows\WinX
앱 알림 설정	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion \PushNotifications\Applications

2.2 안드로이드 App 관련 파일시스템 접근 관련 연구

모바일 수집장치 “Cellebrite UFED”을 사용하여 증거를 수집할 수 있다. 수집 작업을 하기 전에 휴대폰 설정에서 USB 디버깅 활성화를 한다. 휴대폰 내부 메모리에서 추출할 수 있는 내용들은 데이터베이스 파일, 시스템 구성 파일 등을 확인할 수 있다. 아래 표 2 를 통해서 파일경로와 아티팩트들을 확인해 볼 수 있다.

표 2. 애플리케이션과 아티팩트 위치 정보[5]

애플리케이션	폴더 위치	폴더 이름
WhatsApp	/data/data/com.whatsapp/	/databases
Viber	/data/data/com.viber.voip	/databases

또한, DB 파일의 위치한 곳을 알 수 있으며, WhatsApp 과 Viber 의 메시지, 연락처 등을 알 수 있다.

2.3 스마트폰 메신져 포렌식 관련 연구

스마트폰이 널리 보급됨에 따라 SMS 보다 메신저 애플리케이션을 사용하는 사용자들이 급격히 증가하였다. 또한 메신저는 메시지 전송 뿐만 아니라 멀티미디어, 파일 공유 등 다양한 기능을 탑재하고 있으므로, 메신저를 분석하면 범죄 수사시 유용한 정보를 획득할 가능성이 높다. 아이폰과 안드로이드 기반에서 페이스북 메신저, 위챗, 카카오톡 등 12 가지의 메신저 애플리케이션에 대해 얻을 수 있는 정보와 그 경로에 대해 분석한 연구가 있고, 안드로이드에서 Viber 와 whatsapp 애플리케이션에 대해 사용흔적, 분석방법 등 상세하게 조사한 연구가 있고, Style UI 의 기본 앱인 People 에 대해서 분석한 연구가 있다 [5, 6, 7]. 기존의 연구에서는 다양한 메신저에 대해서 분석하였지만, 윈도우 8 기반 Style UI 애플리케이션에 대한 연구가 부족한 실정이다. 사용자가 남기는 흔적들 중 친구정보, 메시지정보, 송수신 정보 등 수사에 필요한 중요한 정보를 획득할 수 있다. 그러므로 본 논문에서는 Style UI 페이스북에 대해서 분석한다.

3. Style UI 환경에서 페이스북 분석

디지털 포렌식은 많은 자료를 남길만한 곳을 찾아야 한다. 메시지, 사진을 보내거나 정보교환 등을 할 수 있는 SNS 애플리케이션으로 전세계적으로 많이 쓰는 Facebook 을 선택하여 분석하였다. 설치된 애플리케이션의 계정과 연동하여 PC 에 동기화가 진행된다. 이를 통해 PC 에는 많은 흔적들이 남는데, 연락처, 시간, 대화 내용, 친구리스트 등 여러 가지 정보를 확인할 수 있다. Facebook 의 경우, SQLite 를 이용한 DB 열람을 통해서 많은 정보를 수집할 수 있다. 아래의 경로를 통하여 접근이 가능하며, 표 3 부터 표 7 까지 테이블의 속성들을 정리해 놓았다.

DB-File Address : \%SystemDirve%\Users\<username>\AppData\Local\Packages\Facebook.Facebook_8xx8rvfyw5nnt\LocalState\100000343378744\DB\FriendRequests

표 3. FriendRequests – DB 정보

	Events
Uid_from	발생된 이벤트의 ID
Time	이벤트 발생 시간
Unread	0 : 이벤트 읽음 1 : 이벤트 읽지않음
Name	친구 신청자 이름
Affiliations_name	단체, 기업, 상호 등의 이름

페이스북 내에서는 친구신청이 빈번하게 일어나는데 이 경로를 통해서 사용자의 친구신청 목록들을 확인할 수 있다.

DB-File Address : \%SystemDirve%\Users\<username>\AppData\Local\Packages\Facebook.Facebook_8xx8rvfyw5nnt\LocalState\100000343378744\DB\FriendRequests

표 4. Friends – DB 정보

	Events
Uid	사용자ID – 난수형
Name	사용자이름
First_name	이름
Middle_name	중간이름 (일부 외국인의 경우 해당)
Last_name	성씨
Contact_email	사용자메일
Phones	폰번호 및 등록된 번호
Profile_url	사용자 url 경로 (단, 로그인 되어 있을 경우만 접근 가능)
Is_pushable	0 : push수신 불가능 1 : push수신 가능

Has_messenger	0 : 메신저 설치 않됨 1 :메신저 설치 되어 있음
Communication_ Rank	커뮤니티 랭크(1에 가까울수록 횟수가 높은 것임)
Birthday_date	생년월일

표 4 는 사용자 주변 사람들의 정보를 수록하고 있는 정보이다. Has_messenger 에서 확인할 수 있듯이, 모바일 폰의 메신저 설치 유/무를 확인할 수 있다. 이것을 가지고 IS_pushable 의 상태와 대조할 수 있다. 예를 들어, Is_pushable 은 1 인데 Has_messenger 가 0 인 경우가 있다. 이 경우는 메신저를 설치를 하여 push 메시지는 수신을 할 수 있으나, 장기간 메신저를 사용하지 않은 사용자임을 추측할 수 있다.

is_pushable	has_messenger	communication_rank
1	1	0,022415161132812
1	0	0,012252807617188
1	0	0,012187480926514
1	0	0,007972717285156 2

(그림 1) Friends 안의 정보들

Communication_rank 의 경우 1 에 가까울수록 사용자와의 커뮤니케이션 빈도수가 높다. 디지털 포렌식 관점에서 볼 때 수사시에 이런 빈도수를 조회하여 사용자간의 친밀도 등에 활용하면 수사에 큰 도움이 될 것으로 예상된다.

DB-File Address : \%SystemDirve%\Users\<username>\AppData\Local\Packages\Facebook.Facebook_8xx8rvfyw5nt\LocalState\100000343378744\DB\Messages

페이스북 자체 채팅기능도 증거 수집을 할 많은 흔적들을 남긴다.

last_action_id	refetch_action_id	last_seen_time
1411192437715000000	1335397842959000000	1411192437655

(그림 2) Messages 안의 시간정보

그림 2 에서 볼 수 있듯이, 메시지에 대해 마지막 이벤트시간 등 여러 시간 정보를 얻을 수 있다. 위 그림을 예로 설명하면, 각 항목의 숫자 중 시간의 경우 앞의 10 자리가 Unix Timestamp 로 되어 있다.

Last_action_id 의 1411192437 을 GMT+9 로 변환
2014 년 9 월 20 일 토요일 오후 2:53:57

위의 같은 결과값을 얻을 수 있다.

표 5. Messages – threads 정보

	Events
Action_id	발생된 이벤트의 시간정보
Refetch_action_id	재접속 이벤트의 시간정보
Last_visible_action_id	마지막 방문 이벤트의 시간정보

folder	폴더 이름
Snippet	마지막 메시지 대화 내용
Snippet_sender_id	메시지 보낸이 ID
Senders	대화방 채팅했던 사용자들 아이디
Unread	0 : 이벤트 읽음 1 : 이벤트 읽지않음
Num_messages	메시지 주고 받은 횟수
Can_reply	0 : 메시지 수신 불가 1 : 메시지 수신 가능
Is_subscribed	0 : 채팅 참여 불가능 1 : 채팅 참여 가능

표 5 의 Messages 정보들은 각 이벤트 발생 시간 정보들과 상호간 메시지 주고 받은 상태와 대상이 누군지를 알 수 있게 한다.

email	name	first_name
1000018[redacted]88552@	J[redacted]Herrera	JH[redacted]lle
1124652[redacted]@face	P[redacted]Aca-Yang	Pr[redacted]ed
1000025[redacted]17985@	J[redacted]Sim	Ji[redacted]ng
1000015[redacted]36453@	A[redacted]hen	Ad[redacted]Xi
1000013[redacted]84181@	Y[redacted]im	Ye[redacted]Ji
1000028[redacted]81787@	김[redacted]	지[redacted]

body	sender
anyeong haseyo ^^	{"user_id":"100001884988552","name":"[redacted]era","email":
huu	{"user_id":"100001884988552","name":"[redacted]era","email":
에고... 넘 고생이 많(	{"user_id":"100000343378744","name":"[redacted]","e[redacted]l":"10000034
나는 오늘 집에서 잔:	{"user_id":"100001383784181","name":"[redacted]Ji K[redacted]"email":"100
ㅋㅋㅋ	{"user_id":"100001383784181","name":"[redacted]Ji K[redacted]"email":"100
일은 할만해?	{"user_id":"100001383784181","name":"[redacted]Ji K[redacted]"email":"100

(그림 3) Messages 안의 대화상대 정보

앱이나 폰 PC 등을 이용하여 상대방과 채팅기능을 통해 대화를 하면 그림 3 과 같이 상대의 기록들이 남아 있음을 확인 할 수가 있다.

표 6. Messages – messages 정보

	Events
ID	사용자 ID
Thread_id	쓰레드 ID
Body	대화 내용
Senders	Uesr ID : 메시지 보낸이 ID Name : 사용자 이름 Email : Facebook에 등록된 E-mail
Tags	폴더이름 : inbox Read : 메시지를 수신 후 읽음 Send : 메시지를 보냄 Messenger : 메시지를 메신저에서 보냄 Source-chat : 페이스북 메신저에서 보냄 Source-web : 웹사이트에서 보냄 Source-mobile : 스마트폰에서 보냄
Timestamp	메시지 수신 시간정보
Action_id	이벤트 발생 시간정보 및 이벤트 ID
Offline_id	오프라인 ID
Attachments	첨부파일정보
Shares	그림 또는 사진 첨부파일
Server_timestamp	서버 메시지 수신 시간정보

여기서 주목할 수 있는 정보는 메시지를 수신시 시간정보를 PC 측과 서버 측의 시간정보가 동시에 DB 에

입력이 된다.

timestamp	server_timestam
1411442665904	1411442665904
1411442662289	1411442662289
1411442655096	1411442655096
1411442637020	1411442637020
1411442625192	1411442625192
1411442784044	1411442784044
1411442900259	1411442900259

(그림 4) Messages 안의 메시지수신 시간 정보

디지털 포렌식 관점에서 볼 때, 수사자료로 제출시 무결성 증명의 어려움을 겪을 수 있다. 하지만 이와 같이 수신 시간을 서버와 PC 에 동시에 표기함으로써 무결성을 증명할 유용한 정보로 쓰일 수 있다.

표 7. Notifications 정보

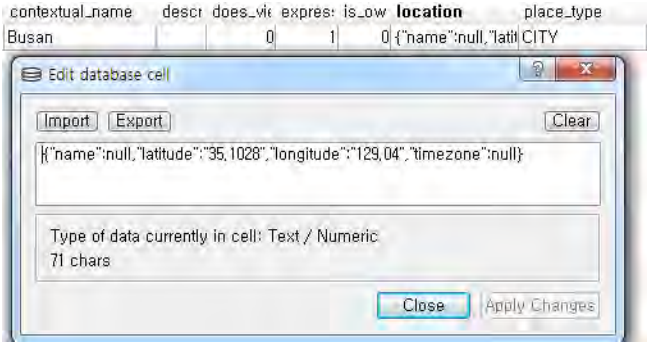
	Events
Notification_id	알림 ID
Object_id	오프젝트 ID
Object_type	Group : 그룹 Album : 앨범 User : 사용자 Stream : 동영상 Friend : 친구
Sender_id	보낸이 ID
Title_text	내용
Title_html	보낸이 경로
Icon_url	아이콘 경로
Href	알림 경로
Unread	0 : 이벤트 읽음 1 : 이벤트 읽지않음
Undated_time	알림 업데이트 시간
Created_time	알림 생성시간

표 7 의 Notifications 정보들은 Facebook 의 지인들이나 사용자의 활동 글에 대한 답변, 소속해 있는 그룹 알림 등 모든 활동에 관한 알림을 순차적으로 표시해주는 영역으로 최근 주변인 활동들에 대해서 알 수 있다.

name	type	icon_image	approx_count
Busan, South Korea Area	FRIEND_LIST	{"height":32,"widt	4
Pukyong National University	FRIEND_LIST	{"height":32,"widt	0
Dong-eui University	FRIEND_LIST	{"height":32,"widt	0
동의대학교	FRIEND_LIST	{"height":32,"widt	0
Dong-eui University	FRIEND_LIST	{"height":32,"widt	0
한국생산기술연구원(KITECH)	FRIEND_LIST	{"height":32,"widt	0
동의대학교	FRIEND_LIST	{"height":32,"widt	0
한국생산기술연구원(KITECH)	FRIEND_LIST	{"height":32,"widt	0
Busan Area	FRIEND_LIST	{"height":32,"widt	4
동의대학교	FRIEND_LIST	{"height":32,"widt	0
Acquaintances	FRIEND_LIST	{"height":32,"widt	0
Family	FRIEND_LIST	{"height":32,"widt	0
동의대학교	FRIEND_LIST	{"height":32,"widt	0
Close Friends	FRIEND_LIST	{"height":32,"widt	0

(그림 5) Stories – feed_sections 정보

그림 5 의 경우, 사용자의 프로필 등록된 전 학교, 전 직장 등 입력한 정보들을 확인할 수 있다. Stories 는 많은 정보를 가지고 있었으나, 많은 정보만큼이나 대부분의 정보가 암호화 되어 있어 열람할 수 있는 정보는 제한적이였다.



(그림 6) Stories – places 정보

다만, 사용자의 프로필 입력정보를 토대로 places 에서 특정 시에서 거주중임을 확인할 수 있으며, 대략적인 GPS 정보 또한 확인할 수 있었다.

4. 결론 및 향후 연구방향

본 논문에서는 Window8 의 Style UI 의 SNS 애플리케이션인 Facebook 에 대해서 분석하였다. 우리는 사용자의 대화내용, 시간정보 및 친구리스트 등 다양한 개인정보와 사용흔적을 발견 할 수 있었다. 본 논문은 대부분의 사용자에게는 친숙한 운영체제이나 대중성이 낮아 잘 알려지지 않은 애플리케이션 부문인 Window8 의 Style UI 앱에 대해 선행적으로 분석하였다. 이를 통해 윈도우기반 디바이스를 조사하는 경우에 도움이 될 것으로 기대된다. 향후, 암호화로 인해 열람하지 못한 정보를 가지고 DB 암호화 해석을 통해 더 많은 양의 정보를 얻을 수 있도록 연구를 진행할 계획이다.

참고문헌

[1] 이형우, 이상진, 임종인 "컴퓨터 포렌식스 기술", 정보보호학회지. 10 월 (2002)

[2] Youngjun Son, Mokdong Chung, "Digital Forensics for Android Location Information using Hierarchical Clustering", Journal of The Institute of Electronics and Information Engineers, Volume51-No.6, June (2014)

[3] AhnLab, Window8 Forensic(1) Metro UI and Artifacts,May (2012)

[4] Forensic-Proof, (http://forensic-proof.com)

[5] Aditya Mahajan, M. S. Dahiya, H. P. Sanghvi, "Forensic Analysis of Instant Messenger Applications on Android Devices", International Journal of Computer Applications(0975-8887), Volume68-No.8, April (2013)

[6] Darren Quick, "Forensic Analysis of Cloud Storage Client Data", University of South Australia, October (2012)

[7] Asif Iqba, Andrew Marrington, Ibrahim Baggili, "Forensic artifacts of the ChatON Instant Messaging application", 8th International Workshop on Systematic Approaches to Digital Forensics Engineering , November (2013)