Korea University School of Cybersecurity

DFRC Korea University Digital Forensic Research Center

FACT: Forensic Acquisition & Criminal investigation Tool

Byeongchan Jeong[a], Jieon Kim[a], Junho Kim[a], Geunyeong Choi[a], Jewan Bang[b], Jungheum Park[a*], Sangjin Lee[a]

School of Cybersecurity, Korea University[a]

Investigation Bureau, National Office of Investigation, Korean National Police Agency[b]

Introduction

Widespread adoption of anti-forensic technologies and the emergence of new online services such as secure messengers, cloud storage services, and anonymous networks, are changing investigation methods for forensic experts to analyze digital evidence. These services aim to safeguard user privacy by utilizing encryption techniques and preventing data from being stored in non-volatile areas. As a result, digital forensics professionals are shifting their methods to gather evidence from volatile areas and cloud-based storages rather than non-volatile areas.

Credential Acquisition in Volatile Data

Credential data & Volatile data

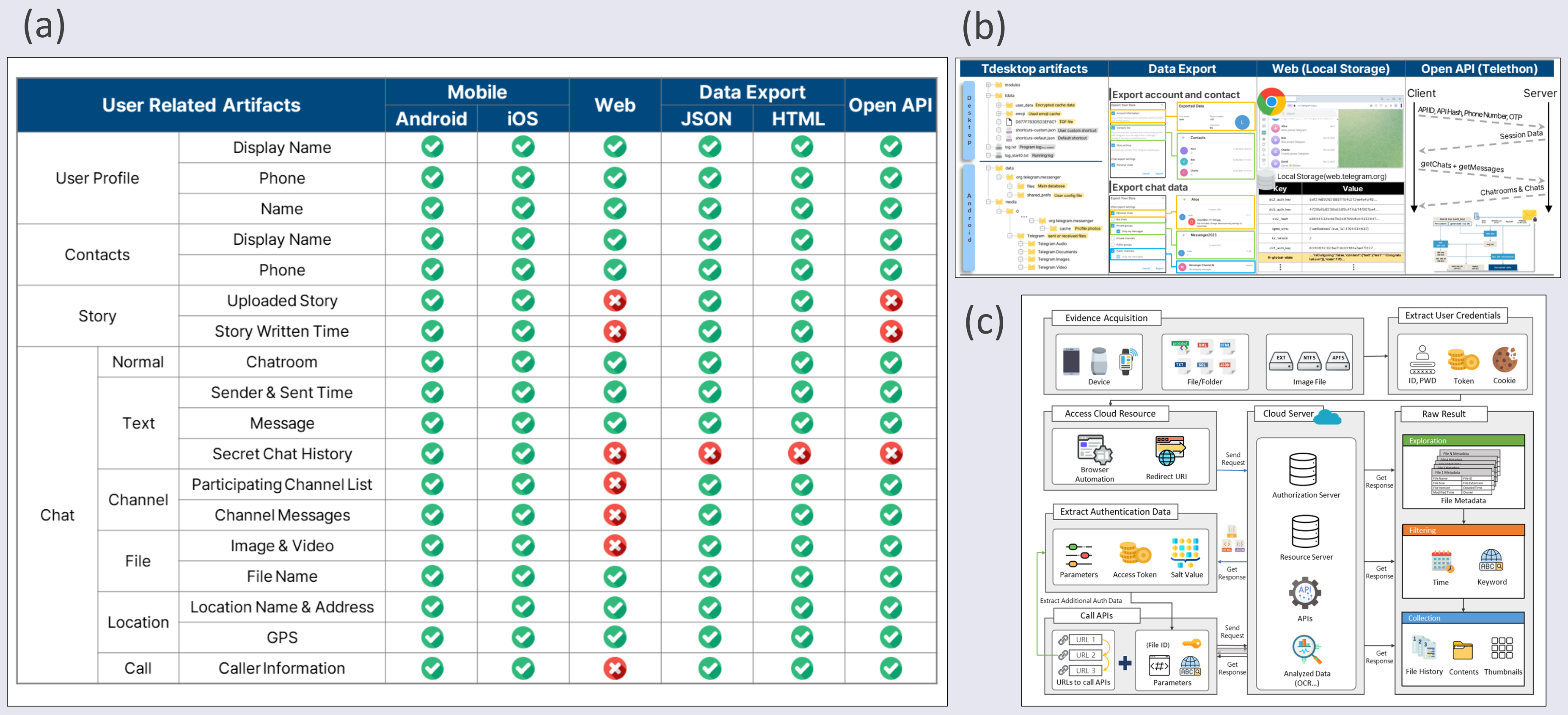
Running software programs might affect how user data (e.g., user credentials, processes, cryptographical keys) are stored in volatile areas.

These volatile areas include **physical memory, physical memory of virtual machines** (such as VMWare or VirtualBox), **hibernation file** (hiberfil.sys), **crash dumps**, **page file** (pagefile.sys), and **swap file** (swapfile.sys).

Methodology

Cloud-based Services (Messenger & Cloud)

To ensure a thorough forensic investigation, forensic experts should obtain relevant information from both local storage and cloud servers. The experts also need to consider that instant messaging (IM) services utilize one account while synchronizing data across multiple devices. Additionally, the investigation should address the analysis of specific functions supported by cloud-based services, such as personal vaults, file encryption, or file history.


(a)

User Related Artifacts			Mobile		Web	Data Export		Open API
			Android	iOS		JSON	HTML	
User Profile		Display Name	✓	✓	✓	✓	✓	✓
		Phone	✓	✓	✓	✓	✓	✓
		Name	✓	✓	✓	✓	✓	✓
Contacts		Display Name	✓	✓	✓	✓	✓	✓
		Phone	✓	✓	✓	✓	✓	✓
Story		Uploaded Story	✓	✓	☒	✓	✓	☒
		Story Written Time	✓	✓	☒	✓	✓	☒
Chat	Normal	Chatroom	✓	✓	✓	✓	✓	✓
	Text	Sender & Sent Time	✓	✓	✓	✓	✓	✓
		Message	✓	✓	✓	✓	✓	✓
		Secret Chat History	✓	✓	☒	☒	☒	☒
	Channel	Participating Channel List	✓	✓	☒	✓	✓	✓
		Channel Messages	✓	✓	☒	✓	✓	✓
	File	Image & Video	✓	✓	☒	✓	✓	✓
		File Name	✓	✓	✓	✓	✓	✓
	Location	Location Name & Address	✓	✓	✓	✓	✓	✓
		GPS	✓	✓	✓	✓	✓	✓
	Call	Caller Information	✓	✓	☒	✓	✓	✓

(b)

(c)

Figure 1. Data acquisition techniques for server-based services
(a) shows the range of data depending on the collection method
(b) illustrates collection techniques for Telegram service
(c) demonstrates data collection steps for cloud-based services

[Supported Services]

- Messenger: Instagram, Facebook Messenger, Naver BAND
- Cloud: OneDrive, Dropbox, Box
- Anonymous Network: Tor, Brave, Lokinet

Anonymous Network

While users utilize anonymous network services to conceal their history, analysts can acquire data and reconstruct user activities within the system by examining physical memory and the file system. Additionally, crawling dark web URLs extracted from memory can reveal activities on the dark web.

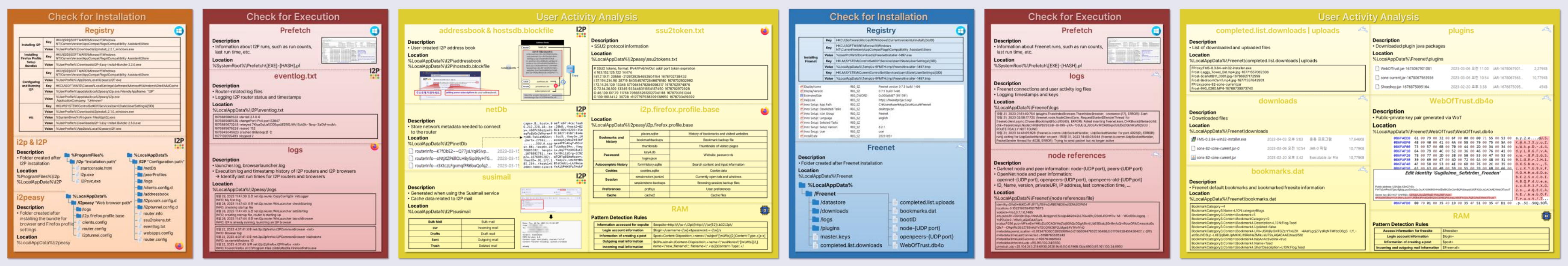
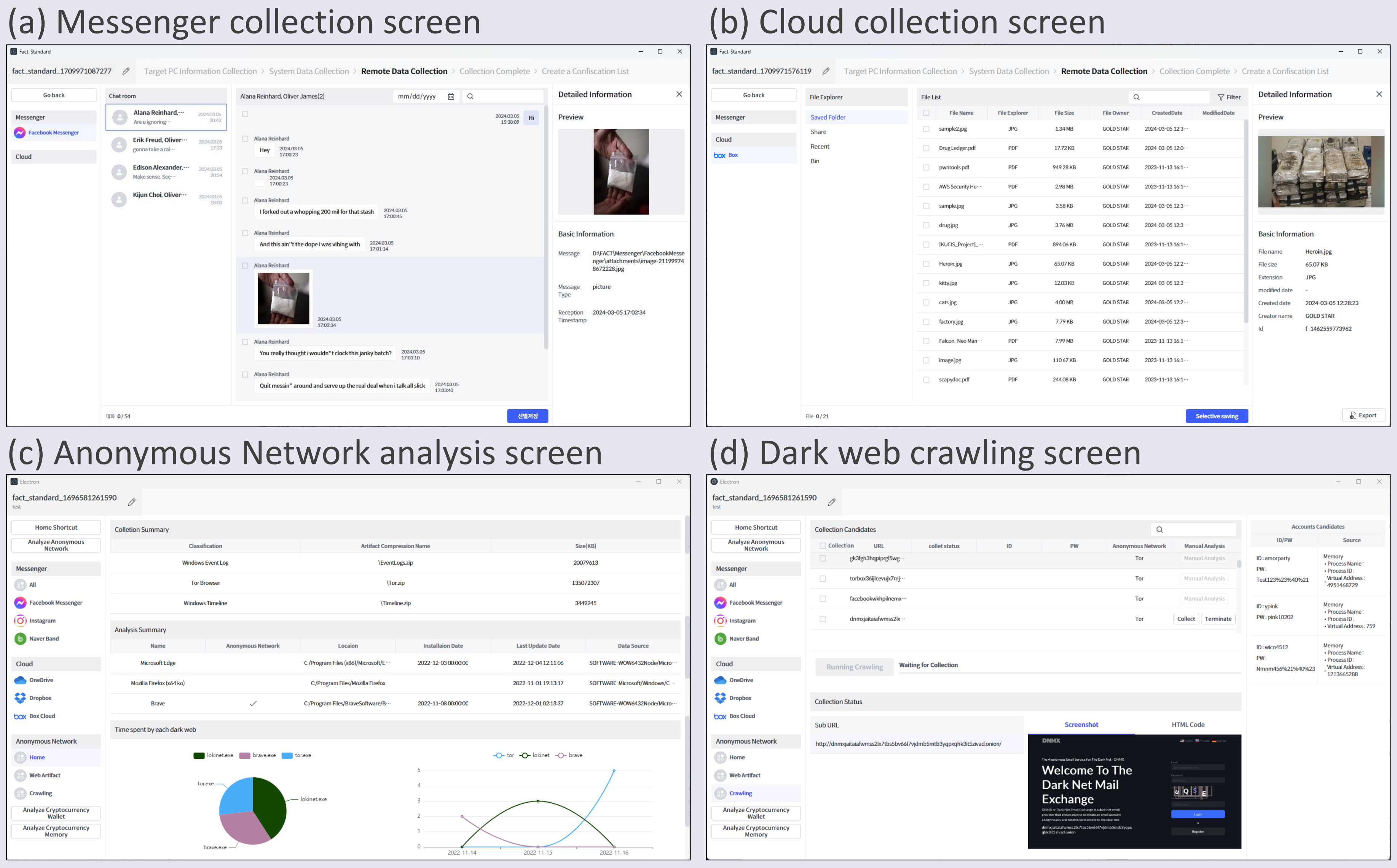


Figure 2. Overview of I2P and Freenet artifacts

Results & Implementation

FACT supports on-site digital evidence collection through **FACT-Standard** and analysis through **FACT-Expert**. FACT-Standard dumps physical memory and extracts credentials such as IDs and passwords from it. It then utilizes the recovered credentials to log in to messaging, cloud storage, and dark web services.

FACT-Expert analyzes seized data obtained from FACT-Standard. This tool offers visualizing data collected from messenger/cloud data and system artifacts related to anonymous networks. Additionally, its crawling function captures and downloads the dark web pages that users accessed through the Tor network.


(a) Messenger collection screen

(b) Cloud collection screen

(c) Anonymous Network analysis screen

(d) Dark web crawling screen

Figure 3. FACT tool main screen

Conclusion

Many applications employ anti-forensic techniques to prevent reverse engineering and protect user privacy. For a prompt response, the tool FACT examines chat data that are synchronized even when accessed from one user account across different devices. Additionally, the tool provides corresponding collection functions for each feature that cloud-based services support, such as personal vault and file history.

The FACT-Standard collects user credentials from physical memory and cloud-based data. The tool also captures system and web browser artifacts to reconstruct user behavior on dark web browsers. FACT-Expert shows analysis results of data collected by FACT-Standard. FACT will assist forensic investigators to collect and analyze digital evidence in efficient ways.

Acknowledgments

This work was supported by Police-Lab 2.0 Program funded by the Ministry of Science and ICT(MSIT, Korea) & Korean National Police Agency [Project Number: 210121M07].