

FORENSIC INVESTIGATION: APPLE DEVICES ACQUISITION & ANALYSIS

Dr. Parag Shukla

Assistant Professor, School of Cyber Security and Digital Forensics, National Forensic Sciences University, Gandhinagar, Gujarat, India <u>parag.shukla@nfsu.ac.in</u>

Abstract— In the field of forensic investigation, Apple devices have always been of great interest. As a result of the device's security features, its architecture as well as its new hardware and software features, investigators have been unable to do much with it. There is limited exposure of Apple devices to investigators since they are more familiar with Android & Windows devices. As part of this research paper, we will present a brief overview of iOS and Mac devices. Understanding the Internal Filesystem, Application Data Storage, Boot Modes & what are the new Security features that even encrypt that data stored within the eMMC. We'll also look into what are the different acquisition and analysis methods available for Apple devices which can be performed via Open-Source tools.

Keywords— Apple Devices, Acquisition, Jailbreak, iOS, Mac, forensic investigation

INTRODUCTION

T

With increase in number of Cyber crimes, the need for forensic investigation comes into play to present the investigation in court of law. And in the recent years, with launch of new and cheap mobile phones as well as more usage of mobile phones for data storage and day to day tasks, have concern over investigating mobile devices.

In investigation of mobile devices, Apple iOS devices are a big concern due to increased security features of the device. When investigating iOS devices, sometimes it involves investigating other Apple device like Macbook.

A. AIM

The project discuss about acquisition and analysis methods to perform on Apple devices including iOS and MacOS with use of open-source tools.

Main objective of the project is to provide awareness about the internals of Apple devices and allow audience to perform the mentioned steps on their own device. The project discuss about the security features, application data, acquisition and analysis methods on devices like iPhone 6 Plus, iPhone 11 Pro Max, iPad 2 WiFi and Macbook Air (M1 Chip).

II. METHODOLOGY

A. IOS Architecture

- Core OS Layer
 - First layer on device hardware

Aditya Pratap

Student, M.Sc. Digital Forensics & Information Security, School of Cyber Security and Digital Forensics, National Forensic Sciences University, Gandhinagar, Gujarat, India <u>aditya.pratap9557@gmail.com</u>

- Provides low level services like networking, memory management
- Helps to create and manage certificates and called upon keychain services
- Core Services
 - Provides applications the fundamental services
 - Support for framework like Address, Cloud, Coredata, location etc
- Media Layer
 - Enables audio, video graphics of devices
 - Use frameworks running different libraries to enable the technology
- Cocoa Touch
 - Infrastructure to implement visual interface to apps
 - Support for touch and motion event
 - B. IOS Boot Process
- Boot ROM
 - Read-only block contains Root Certificate which verifies signature and decrypt Low Level Bootloader (LLB)
- Low Level Bootloader (LLB)
 - LLB contains code invoked by Boot ROM
 - Verifying authority of iBoot and executes it
- iBoot
 - Verify signature of kernel before execution
 - Failure to load iBoot results in DFU or Recovery mode
- Kernel
 - Verify device iOS version and required services and applications
- C. IOS Operating Modes
 - Normal Mode
 - By-default mode to allow user access apps and data from interface
 - Device Firmware Upgrade (DFU) Mode
 - Used for upgrading or downgrading iOS versions
 - Can be used to perform Physical acquisition
 - Recovery Mode
 - Bypass loading of OS by booting in Stage 2 bootloader
 - Can be used to perform activation of device as well as for Logical acquistion

D. IOS Jailbreaking



CYBER SECURITY & DIGITAL FORENSICS

Jailbreaking allows to remove the barriers set by manufacturer manually is Jailbreak; this unlocking process is possible with special software that modifies iOS

- Tethered Jailbreak
 - Temporarily pawns handset for single bootcycleAfter device turned off, it cannot complete a boot cycle without help of computer based jailbreak application and physical connection between device and computer
 - Example, redsn0w (for iOS devices with A4 chip)
- Semi-Tethered Jailbreak
 - Permits handset to complete boot-cycle after being pawned
 - But jailbreak extensions won't load until computer based application is deployed over physical cable connection between device and computer
 - Example, checkra1n (for iOS devices with A7-A11 chip)
- Semi-Untethered Jailbreak
 - Permits handset to complete boot cycle but jailbreak extensions won't load until side loaded jailbreak app on device is deployed
 - Example. Chimera, unc0ver
- Untethered Jailbreak
 - Permits handset to complete boot-cycle after being pawned without any interruptions to jailbreak oriented functionality
 - Example, Pangu, JailbreakMe

E. IOS Acquisition Parameters

- iDevice Model
 - Earlier iOS device models allows easy file system acquisition
- iOS Version
 - Acquisition is highly dependent on iOS version due to encryption and updated security features
- Passcode
 - User passcode required at time of acquisition
- Backup Passcode
 - Optional feature to create passcode while creating backup
- Jailbroken Device
 - Jailbreak allows easy acquisition and bypassing restrictions

F. IOS Lockdown Certificate

- Lockdown certificate created on system when device connected for first time with iTunes
- It stores the UDID data for iOS devices that are synced using iTunes
- Once this certificate is generated, no longer is required to unlock the device when connected to same device again
- This can be used to gain partial access to the device without knowing the passcode of the iOS device

- NFSU Journal of Cyber Security and Digital Forensics Volume – 1, Issue – 1, December 2022 E – ISSN – 2583-7559
 - III. IMPLEMENTATION

A. Environment Setup

- 3uTools
 - All in one tool for iOS Devices
 - Allows to take backup, jailbreak & manage apps, photos and other multimedia files
 - Full view of iOS device status including activation, battery and iCloud lock status as well as detailed iOS & iDevice information
 - Additional feature of flashing & downgrading firmware
- Checkra1n
 - Community project which provides semitethered jailbreak that are based on "checkm8" exploit
 - Exploitation supports A10 and A10X chipsets
- iLEAPP
 - Developed by Alexis Brignoni for analysis of physical image of iOS device
 - Provide detailed report after analysis process
- Belkasoft Evidence Center X
 - A creation of Belkasoft for the forensic analysis of computer, mobile and cloud platforms
 - Helps to acquire and analyse wide range of mobile devices and creating report as well
- Sumuri Recon Lab
 - Forensic suite developed by Sumuri specially for Apple devices
 - Allows to take Windows, Mac, iOS, Android and Google takeout automated analysis
 B. Jailbreaking iOS
- On Kali Linux terminal, install checkra1n by command sudo apt-get install checkra1n

Welcome to checkrain!	
Made by: argn axi0my dany1931 jaywalker	
kirb littlelailo nitoTV never released	
nullpivel pimekeke gwertvoruion	
abingnon sigura	
manage to be defende date the statement of the state	
Thanks to: hairisch, inackbanme, jhdok,	
jonseals, xerub, lilstevie, psychotea,	
sferrini, Cellebrite (ih8sn0w, cjori,	
With <3 from Kim Jong Cracks	
[] Quick Mode [Or	ptions j [Start] [Quit]

- Connect iDevice on system with lightning cable and run checkra1n with sudo privileges
- Select start and iDevice will be put in DFU mode before starting with checkm8 exploit
- After iDevice booted to normal mode, checkra1n app visible on springboard
- Open the checkraln app and select option "Install Cydia" to finish the jailbreak process







c. iOS Logical Acquisition with 3uTools On Windows, connect the iDevice and open 3uTools

3 3uTools	iDevice	Apps	RT & WP	Smart Flash	Toolbex	Tutorials			
iPhone									
🔛 Info	6			Phone 6 Plus	16G8 Silver		PC Ch	erging(2.4W) 🛉	19%
, Аррз (24)		•		iOS Version	12.5.5	(16H62) Ap	ple ID Lock	On Onlin	e Query
EA Photos				Jailbroken.	Ves Inst	AFC2 (C)	eud	On	Details
J] Mair		23:27		Activited		Ves Pro	d. Date	9	/13/2015
0.5		Saturday, Jun 1	4	Product Type	iPhone7,1	(A1524) Via	rranty Date	Onlin	e Query
Lui Kingtones		1	1000	Sales Model	MGA	92 LL/A Sal	es Region	United States	of Am
CP Videos				(ME)	35924706	R820465 CP	U	Apple A8 Dual	Details
Books		-		Serial No.	DX3QD5	GIGSQR Dis	k Type	MLC	Details
🖞 UDisk		- 20	Eng	ECID	001809522	1698C26 Ch	arge Times	3	14 Times
🗁 Deta			201	Verify UDID		Yes Bal	tery Life	99%	Details
Files		0		UDIO		TAE7DADDE30	M98E7A6D5	568C6388A4798	D856974
88 Common tools		0		E View	Verification Rep	ort	⊟ Va	w iDevice Detail	£
		iPhone 🛙	5	Hard Disk Capaci	ty	_	_	10.36 GB	/ 14.89 GB
	Re	beet Turn Off	Refresh	System 🔳 A	opps 📕 Pho	tos 📕 Media	UDis	c 🗖 Others	II Free
		G Backup/Re	store JuAirP	ayer Make Ringto	ne Stop iOS Up	date Transfer	Data	More	

Select "Backup/Restore" option at bottom

		-	iPhone				Las	t backup time	e Unknow
View all-data Backups	10	0:10	iDevice	Type i	Phone 6 Plus				
	6.51		Produc	t Type 🛛 🕯	Phone7,1 (A1524	E.			
Customized Backup			Enclos	ure Color S	ilver				
	1.		iOS Ver	sion 9	OS 12.5.5 (Backu	ps can't be	restored to lowe	r iOS versions	i)
Customized Restore		1	iDevice	Capacity 1	6 GB (Used:10.56	GB Free sp	oace:4.34 GB)		
		- alter	No bao	kup passwor	d has been set o	this Devic	e. no password	is required to	
		0	restore	backups.	Aanage Password	r -			
					Backup includes				
	App Data	Photos	Contacts	Messages	Call History	Notes	Bookmarks	Desktop	Setting
Tutorial list									
							1.		

- D. iOS File System Imaging with Linux Terminal
- On Linux, connect iDevice and within terminal; *iproxy* 4242 22



• Open second terminal and write command; ssh root@127.0.0.1 -p 4242





- Identify partition of iPhone using command; df H
- Within the system terminal, type the command to create tar image of the iPhone partition; *ssh* root@127.0.0.1 tar czf private/var > iPhone_var.tar
 - E. iOS Physical Acquisition with Belkasoft Evidence Center
- Open Belkasoft Evidence Centre X and connect iDevice to the system
- In "Add data source", select "Acquire > Mobile Image"
- After selecting model of iDevice, choose "Jailbroken device Image" and Belkasoft will display the detected device

		AFC	C Agent backup	Crash reports	
2	Add a data course Russian Austa dasiris	iTunes backup	Jailbroken device image	Screen capturer	
Det	Add a data source neview Apple device	propercies			^
	7ae7dadde3d498e7a6d5568c631 UDID: 7ae7dadde3d498e7a6d55 IOS version: 12.5.5 Device name: iPhone Device model: iPhone 6 Plus	8ba479bd856974 68c638ba479bd856974			Ć

• Enter the path to save the iDevice image and Belkasoft will start process

Jailbroken device image			
Acquir	red data target path:		
E:\iP	hone\iPhone 6 Jailbroken Image		
	Log: Beikasoft Evidence Center X v.1.13.10338		
	License explained rozenszoff LLC License explained rozsz1.229 License ecoder 7KaB6N-8SEAJG-2Uu5i4-IEfDBR-9rc1Az-CWE2D5-5s0UI5-53bBRI-TrOD38-tNAVBC Task "Creating the full file system copy for "IPhone" is started at 6/10/2022 11:13:51 PM		

• Open iBackup Viewer and browse the iOS backup and select "manifest.db" file



CYBER SECURITY & DIGITAL FORENSICS

- Home page will display the default applications installed within the device. For eg, view the whatsapp chats selecting the "WhatsApp" icon
- Select "App Store" icon to view all installed applications on the iDevice and view the respected application data stored within



Phone - 🙆			Expor	t~ ≣
Web.app	File Path	Created	Modified	Size
2 com.apple.webapp	Documents/blockedcontacts.dat	8/12/2021	8/12/2021	217 Bt
WebContentAnalysisUI.app	Documents/StatusMessages.plist	11/7/2021	11/7/2021	657 Bt
com.apple.WebContentFilter.remoteUI.WebContentAnaly	Documents/SyncHistory.plist	4/11/2022	4/11/2022	334 Bt
WebSheet.app	Library/Cookies/Cookies.binarycookies	8/12/2021	8/12/2021	203 Bt
com.apple.WebSheet	Library/network-usage.data	4/13/2022	4/13/2022	60 Bt
Webex.app	Library/optimistic-upload.state	4/13/2022	4/13/2022	1.30 KB
com.webex.meeting	Library/Preferences/com.apple.EmojiCache	1/28/2022	1/28/2022	50.50 KE
WhatsApp.app	Library/Preferences/net.whatsapp.WhatsAp	4/13/2022	4/13/2022	8.28 KB
net.whatsapp.WhatsApp	Library/Preferences/UITextInputContextIde	4/12/2022	4/12/2022	12.72 K
WhatsApp.app	Library/WebKit/WebsiteData/ResourceLoad	5/7/2021	4/9/2022	136.00 ₽
net.whatsapp.WhatsAppSMB	Library/WebKit/WebsiteData/ResourceLoad	12/29/2021	4/9/2022	28.00 K8
77 Wikipedia.app				
V org.wikimedia.wikipedia				
Xcode Previews.app				
com.apple.dt.XcodePreviews				
YouTube.app				
com.google.ios.youtube				
Zoom.app				
us.zoom.videomeetings				

- iBackup viewer allows to export any selected data and examine the files with applications like SQLite DB Browser, Notepad++, 3uTools, HexEditor
 - G. iOS Filesystem Image Analysis with iLEAPP
- Open GUI version of iLEAPP and select the filesystem image file path
- Select all the modules to analyze within the image and start the analysis process



- After the analysis process is completed, iLEAPP creates HTML report for the process
- Analysis provides different sections to view such as "Account data, Call History, WhatsApp messages, WiFi known networks etc."

H. Mac OS Triaging with Sumuri Recon Lab Sumuri Recon Lab is all in one tool for triaging, imaging,

Sevito Report Home	IOS Logs Events And Protobuf Parser (LEAPP is an open source project that arms to parse every known IOS artifact for the purpose of forensic analys
ACCOLARTS	
R. Account Data	Case Information
PP POBASSIONS	
of TCC - Permissions	Details Device details Script run log Processed files list
Cale Biothage	
Pi Identity	ProductBuildVersion: 16H62 Product: UPsone OS
C. Barris	IOS version: 12.5.5
	Latif Known ICCID: 89910484051536590823 Dependent Disease Newther: 010536374745
	IMEL 359247069820466
SALL HERTORY	MEID: 35924706982046
Call History	Keep with Howered Airpaine Mode. Thue
SELLULAR WRELESS	
Cellular Wireless	
LOUGHIT	The
< Note Sharing	A A
FALES APP	
The states is an ordered related in some	

acquiring and analyzing the apple devices. The tool also has additional support for imaging Mac devices including the M1 and M2 chipsets.

- Install Sumuri Recon Lab on Mac and run the application with proper privilege permissions
- Select "Logical Evidence" from Evidence Type that will display the logical volumes present inside



the Mac device

- Once the analysis procedure is completed, provides a list of artifacts including
 - Apple Installed Applications
 - Bash History
 - Escalate Privileges
 - Connected iOS devices

I. Mac OS Triaging via Mac Terminal





NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

÷	Airport WirelessNetwork		
	Apple Dock		
	Apple Installed Applications	RECON	
	Apple Mail Extractor	LAB	
	Bash History		
110	Calendar	Case Details Source1 Source2	
1	Connected iOS Devices		
_	·····	RECON Version	1.5.2
	Contacts	Report Scope	Full
C	Escalate Privileges	Case No.	02
_	Excelling	Case Name	Mac OS Sumuri Forensics
-	Pacettime	Location	
	Finder	Case Notes	Mac OS Monetery Forensics with Sumuri Recon Lab
1.0	HES+ Devices Loop	Examiner	Aditya Pratap
-	ing i dences cogs	Examiner Phone	
	KnowledgeC	Examiner Email	
9	Launchpad	Agency Name	
		Agency Address	
1000	Mail	User Selected Time Zone	Asia/Kolkata-IST-GMT+5:30
18 22	Maps	Report Generated Time	2022-Jun-10 23:53:21 +5:30
_		Report Generated Machine Time Zone	Asia/Kolkata-IST-GMT+5:30

Terminal allows to gather acquire the volatile information as well as files information stored within the Mac device.

For this purpose, script is developed for Mac OS Monterey version 12.3 to allow investigator to perform the most basic operations such as:

- Collect user info, process info, network information
- Determine disk usage, installed applications etc
- List out different office files, application files, pdf files, multimedia files etc
- All the output can be saved dynamically by the investigators



V. RESULTS & DISCUSSIONS

There are some limitations when analyzing with commercial tools like Sumuri Recon Lab and Belkasoft Evidence Center X. There are some features that commercial tools lack if the focus of analysis is application-based, namely extracting data from installed applications

It is quite useful to have open-source tools available for Apple devices with an understanding of iOS and Mac file systems

Jailbreaking iOS devices allow to obtain privileged access on the iDevice and allows to extract physical image via SSH. Free tool like 3uTools allow to take iOS backup (Logical Image) of the device and analyze the same with the tool.

From the analysis conducted on the different devices, common artifacts that can be found are as follows: *Common IOS Artifacts Location*

IOS ARTIFACTS LOCATION				
DESCRIPTION	PATH			
	NETWORK CONNECTIONS			
Network data usage per App	/private/var/networkd/netusage.sqlite			
Network Extension	/private/var/preferences/com.apple.networkextension.plist			
Network IP, Wi-Fi, Cellular	/private/var/preferences/SystemConfiguration/ com.apple.networkidentification.plist			
Wi-Fi	/private/var/preferences/SystemConfiguration/ com.apple.wifi.plist			
Wi-Fi Mac Addresses	/private/var/preferences/SystemConfiguration/ NetworkInterfaces.plist			
	MULTIMEDIA ARTIFACTS			
Photos	/private/var/mobile/Library/Preferences/ com.apple.mobileslideshow.plist			
MMS File	/private/var/mobile/Library/SMS/Attachments/			
User Created/Saved Photos	/private/var/mobile/Media/DCIM/1*APPLE			
iTunes Media Library	/private/var/mobile/Media/iTunes_Control/iTunes/ MediaLibrary.sqlitedb			
	BROWSER ACTIVITY			
Safari Cache files	private/var/mobile/Containers/Data/Application/ <apple Safari GUID/Library/Caches/com.apple.mobilesafari/</apple 			
Safari Cache database	/private/var/mobile/Containers/Data/Application/ <apple Safari GUID/Library/Caches/com.apple.mobilesafari/Cache.db</apple 			
Safari Website cache	/private/var/mobile/Containers/Data/Application/ <apple Safari GUID/Library/Caches/com.apple.WebAppCache/Applicati onCache.db</apple 			
Safari Cookies	/private/var/mobile/Containers/Data/Application/ <apple Safari GUID/Library/Cookies/Cookies.binarycookies</apple 			

iOS Physical image open-source analysis tool developed by Alexis Brignoni "iLEAPP", create detailed report for the iDevice with information like device details, call info, contacts info, messages info, applications info etc.

Commercial tool like Belkasoft Evidence Center & Sumuri Recon Lab provides the feature for Timeline analysis, Geo-location analysis, Link analysis are among some of the advanced features

Newly launched iOS applications may not be analyzed in detail by commercial tools

Common Mac OS Artifacts Location



CYBER SECURITY & DIGITAL FORENSICS

IOS ARTIFACTS LOCATION				
DESCRIPTION				
Operating System	/private/var/installd/Library/MobileInstallation/			
Last BootTime	LastBuildInfo.plist /private/var/mobile/Library/Preferences/			
IMSIs	com.apple.aggregated.plist /private/var/mobile/Library/Preferences/			
Device name	com.apple.mmcs.plist /private/var/mobile/Library/Preferences/			
	com.apple.mobilegestalt.plist			
Account information	/private/var/mobile/Library/Accounts/Accounts3.sqlite			
Phone number	/private/var/mobile/Library/Preferences/ com.apple.commcenter.shared.plist			
Mobile Applications	APPLICATION USAGE /private/var/installd/Library/Logs/MobileInstallation/			
Installation Logs Application traces	mobile_installation.log. /private/var/mobile/Library/AggregatedDictionary/			
Installed Apps and	ADDataStore.sqlitedb /private/var/mobile/Library/AppConduit/			
Apps Path	AvailableApps.plist			
Seen Bluetooth	/private/var/containers/Shared/SystemGroup/ <guid>/</guid>			
devices	Library/Database/ com.apple.MobileBluetooth.ledevices.other.db			
Apple Maps history	/private/var/mobile/Containers/Data/Application/ <apple_maps_guid>/Library/Maps/ GeoHistory.mapsdata</apple_maps_guid>			
Last latitude and longitude, map search history	/private/var/mobile/Containers/Data/Application/ <apple_maps_guid>/Library/Preferences/ com.apple.Maps.plist</apple_maps_guid>			
Apple Maps bookmarks	/private/var/mobile/Containers/Data/Application/ <apple_maps_guid>/Library/SyncedPreferences/</apple_maps_guid>			
	MAC OS ARTIFACTS LOCATION			
DESCRIPTION	PATH			
Recent Items	/Users/%user%/Library/Application			
	Support/com.apple.sharedfilelist/com.apple.LSSharedFil eList.ApplicationRecentDocuments/ com.apple.textedit.sfl2			
Recent Applications	Users/%user%/Library/Application Support/com.apple.sharedfilelist/com.apple.LSSharedFil eList.RecentApplications.sfl2			
Last Logout Session	/Users/%user%/Library/Preferences/ com.apple.loginwindow.plist			
Dock Items	/Users/%user%/Library/Preferences/ com.apple.dock.plist			
Installed Applications	/Applications			
Mail	/Users/%user%Library/Mail/			
Bash History	/Users/%user%/.zsh_history			
Connected Devices	/Users/%user%/Library/Preferences/ com.apple.iPod.plist			
Contacts	/Users/%user%/Library/Application Support/AddressBook/			
Escalate Privileges	/Users/%user%/.zsh history			
FaceTime Account	/Users/%user%/Library/Preferences/ com apple imservice ids FaceTime plist			
Finder	/Users/%user%/Library/Preferences/ com.apple.finder.plist			
Device Logs	/private/var/db/diagnostics/ /private/var/db/uuidtext/			
LaunchPad	/private/var/folders/kt/ _dtxp9y52l37k_nt5xkg0v_80000gn/0/ com.apple.dock.launchpad/db/db			
Maps	/Users/%user%/Library/Containers/com.apple.Maps/ Data/Library/Preferences/com.apple.Maps.plist			
Message Account	/Users/%user%/Library/Preferences/ByHost/ com.apple.imservice.SMS.<>.plist			

IV. FUTURE SCOPE OF WORK

While open-source tools and terminal applications can perform all acquisition and analysis steps, some enhancements can be made related to automating these processes.

Automating the acquisition tasks by identifying the iDevice version, jailbreak status, and if not jailbroken then allow to jailbreak the iDevice with appropriate jailbreak tool and perform suitable acquisition method will allow to cut the time taken for the acquisition purpose.

With the aid of Artificial Intelligence, develop new methods for identifying suitable and efficient data from a large database using keyword-based searching

With enhancement in security features, quite difficult to acquire physical image of Mac devices due to integration of storage device with the motherboard. Therefore, research new method to acquire physical image from Mac devices to recover deleted data from the device

Reversing and analyzing iOS applications to get detailed information that may also cater the need for malware analysis as well would be included in the future advancement.

ACKNOWLEDGMENT

I would like to express my sincere gratitude to my mentor Dr. Parag C. Shukla sir for his continuous support and motivation that enabled to diversify the road-map for the project and providing the golden opportunity to do this wonderful project on the topic Apple Devices Acquisition & Analysis, which also helped me in doing a lot of Research and I came to know about so many new things related to Apple hardware security, application security, jailbreaking etc.

Secondly, I would also like to thank my parents and friends who helped me a lot in finishing this project within the limited time.

REFERENCES

- [1] Jaron Bradley,OS X Incident Response, Syngress, 2016, ISBN 9780128044568
- [2] Gianluca Tiepolo, iOS Forensics for Investigators, Packt, 2022, ISBN 9781803234083
- [3] Jesse Varsalone, Mac OS X, iPod, and iPhone Forensic Analysis DVD Toolkit, Syngress, 2008, ISBN 9780080949185
- [4] Kunal Relan, iOS Penetration Testing, Apress Berkeley, 2016, ISBN 9781484223550
- [5] Naveen, 'iOS Architecture', August 30 2021, https://intellipaat.com/blog/tutorial/ios-tutorial/iosarchitecture/
- [6] Apple Inc., Apple Platform Security, May 17 2021, https://support.apple.com/enin/guide/security/sec59b0b31ff/web
- [7] File System Programming Guide, Apple Inc., https://developer.apple.com/library/archive/documentati on/FileManagement/Conceptual/FileSystemProgrammi ngGuide/FileSystemOverview/FileSystemOverview.ht ml#//apple_ref/doc/uid/TP40010672-CH2-SW13
- [8] Apple Developer Documentation, Keychain Services, https://developer.apple.com/documentation/security/key chain_services
- [9] TheTechPortal, Phoenix Jailbreak Tutorial for iOS 9, https://thetechportal.com/phoenix-jailbreak-tutorial-forios-9/
- [10] Jack Farley, Forensic Analysis of iTunes Backup, April 14 2019, https://farleyforensics.com/2019/04/14/forensicanalysis-of-itunes-backups/
- [11] SANS Institute, DFIR Advanced Smartphone Forensics, <u>https://www.sans.org/posters/dfir-advanced-</u> <u>smartphone-forensics/</u>
- [12] Sumuri, Sumuri Recon Lab, https://sumuri.com/software/recon-lab/
- [13] Belkasoft, Belkasoft Evidence Center X, https://belkasoft.com/x



NFSU – Journal of Cyber Security and Digital Forensics Volume – 1, Issue – 1, December 2022 E – ISSN – 2583-7559

[14] iBackupViewer, iMacTools, https://www.imactools.com/iphonebackupviewer/ [15] AlexisBrignoni,iLEAPP,https://github.com/abrignoni/iLEAPPiLEAPP,[16] 3uTools, 3uTools, https://www.3u.com/