Ubaid Jafri

DIGITAL FORENSIC PROJECT

DISCLAIMER

This document does not promote or encourage any Illegal activities, all content provided in this document is meant for education, research purposes. The document is not transformative in nature, it is used for teaching purpose.

Copyright Disclaimer Under Section 107 of the Copyright Act 1976, allowance is made for "fair use" for purposes such as criticism, commenting, news reporting, teaching, scholarship, and research. Fair use is a use permitted by copyright statute that might otherwise be infringing. Non-profit, educational or personal use tips the balance in favor of fair use.

The document is created with the intention of educating others in a motivational/inspirational form. Do not try to use the scripts/code/methods if it is not legal in your country.

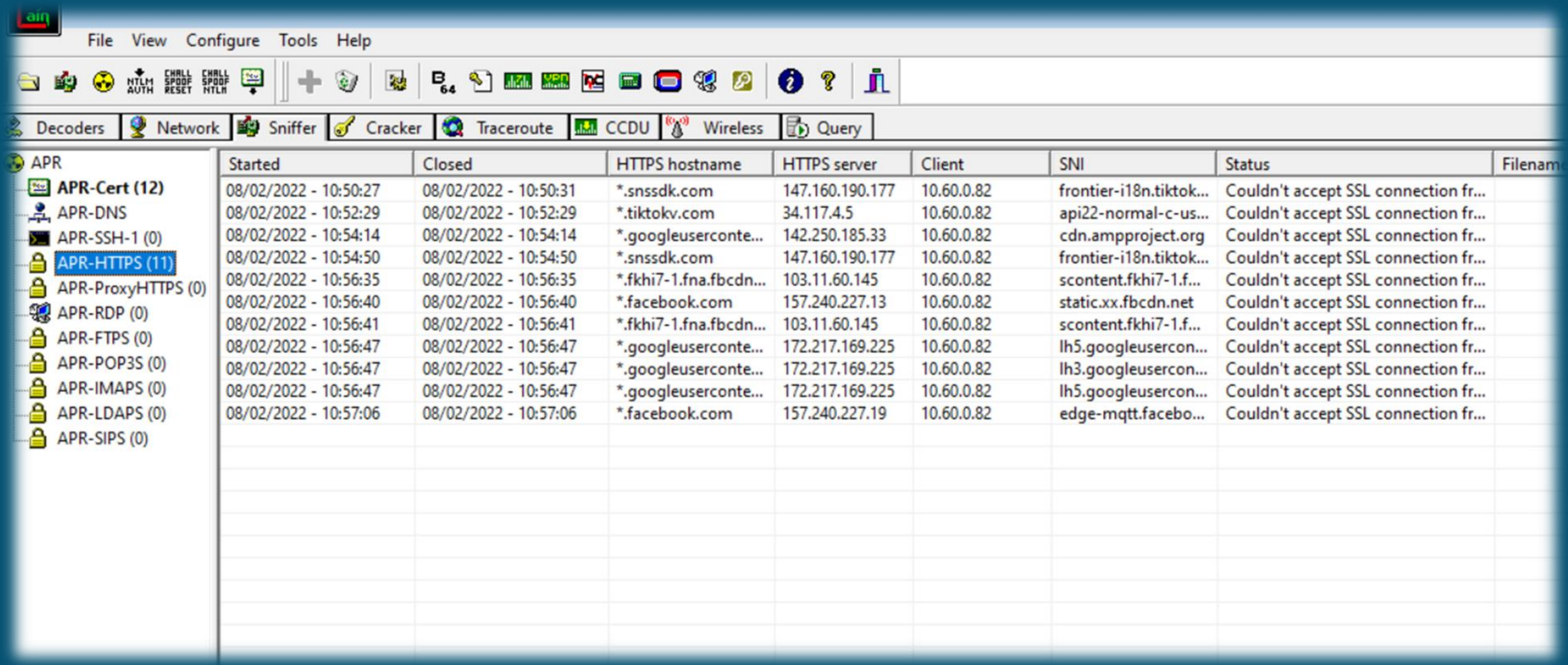
I Do not take any responsibility for anything you do using this document, Use at your own risk.

NETWORK FORENSIC OF CELL PHONE

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

NETWORK FORENSIC OF CELL PHONE

Project Name: Network Forensic of Cell Phone
Tool Used: Wire shark, Network Miner, Cain & Able
Platform: Windows



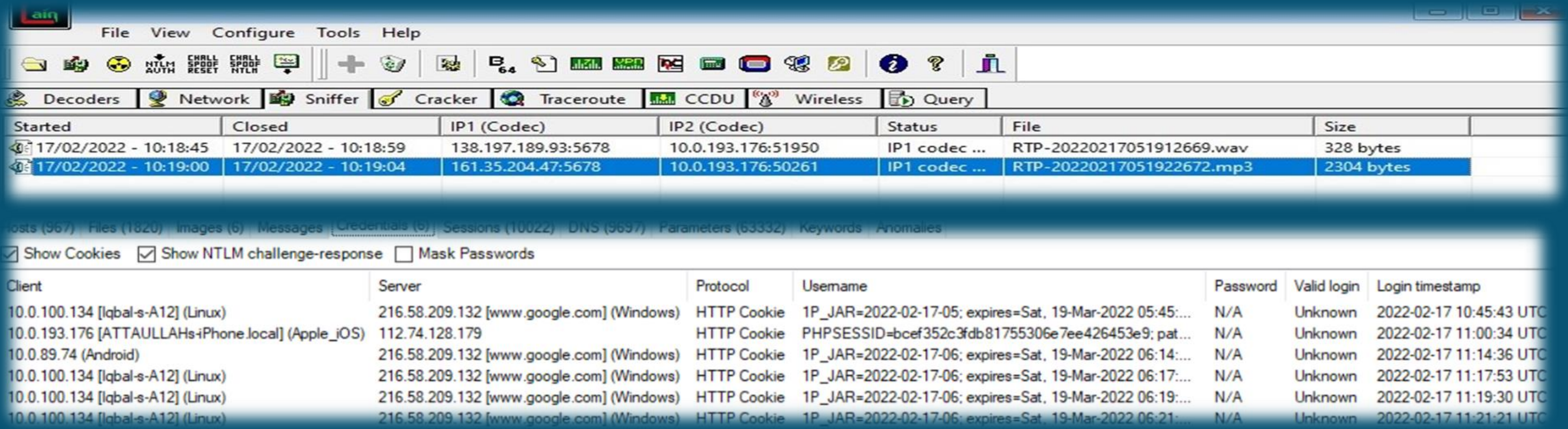
Started	Closed	HTTPS hostname	HTTPS server	Client	SNI	Status	Filename
08/02/2022 - 10:50:27	08/02/2022 - 10:50:31	*.snssdk.com	147.160.190.177	10.60.0.82	frontier-i18n.tiktok...	Couldn't accept SSL connection fr...	
08/02/2022 - 10:52:29	08/02/2022 - 10:52:29	*.tiktokv.com	34.117.4.5	10.60.0.82	api22-normal-c-us...	Couldn't accept SSL connection fr...	
08/02/2022 - 10:54:14	08/02/2022 - 10:54:14	*.googleuserconte...	142.250.185.33	10.60.0.82	cdn.ampproject.org	Couldn't accept SSL connection fr...	
08/02/2022 - 10:54:50	08/02/2022 - 10:54:50	*.snssdk.com	147.160.190.177	10.60.0.82	frontier-i18n.tiktok...	Couldn't accept SSL connection fr...	
08/02/2022 - 10:56:35	08/02/2022 - 10:56:35	*.fkhi7-1.fna.fbcdn...	103.11.60.145	10.60.0.82	scontent.fkhi7-1.f...	Couldn't accept SSL connection fr...	
08/02/2022 - 10:56:40	08/02/2022 - 10:56:40	*.facebook.com	157.240.227.13	10.60.0.82	static.xx.fbcdn.net	Couldn't accept SSL connection fr...	
08/02/2022 - 10:56:41	08/02/2022 - 10:56:41	*.fkhi7-1.fna.fbcdn...	103.11.60.145	10.60.0.82	scontent.fkhi7-1.f...	Couldn't accept SSL connection fr...	
08/02/2022 - 10:56:47	08/02/2022 - 10:56:47	*.googleuserconte...	172.217.169.225	10.60.0.82	lh5.googleusercon...	Couldn't accept SSL connection fr...	
08/02/2022 - 10:56:47	08/02/2022 - 10:56:47	*.googleuserconte...	172.217.169.225	10.60.0.82	lh3.googleusercon...	Couldn't accept SSL connection fr...	
08/02/2022 - 10:56:47	08/02/2022 - 10:56:47	*.googleuserconte...	172.217.169.225	10.60.0.82	lh5.googleusercon...	Couldn't accept SSL connection fr...	
08/02/2022 - 10:57:06	08/02/2022 - 10:57:06	*.facebook.com	157.240.227.19	10.60.0.82	edge-mqtt.facebo...	Couldn't accept SSL connection fr...	

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

NETWORK FORENSIC OF CELL PHONE

DESCRIPTION :

In this work we perform an experimental forensic study on multiple applications for the Android mobile phone operating system. We investigated Android applications through network traffic analysis and server/device storage analysis. This was performed in order to examine the digital evidence that could be of value to forensic examiners and also to evaluate application security in sending/receiving data and application privacy in storing data .



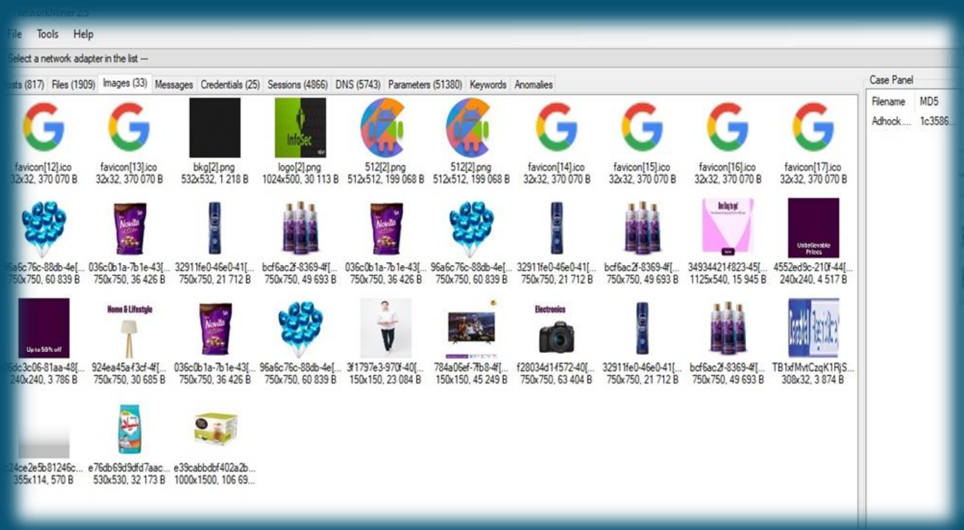
Started	Closed	IP1 (Codec)	IP2 (Codec)	Status	File	Size
17/02/2022 - 10:18:45	17/02/2022 - 10:18:59	138.197.189.93:5678	10.0.193.176:51950	IP1 codec ...	RTP-20220217051912669.wav	328 bytes
17/02/2022 - 10:19:00	17/02/2022 - 10:19:04	161.35.204.47:5678	10.0.193.176:50261	IP1 codec ...	RTP-20220217051922672.mp3	2304 bytes

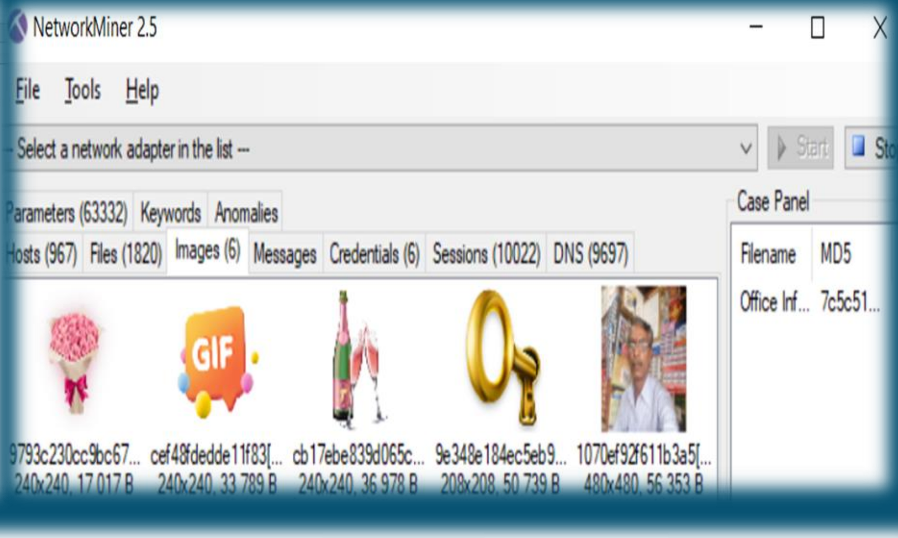
☑ Show Cookies ☑ Show NTLM challenge-response □ Mask Passwords

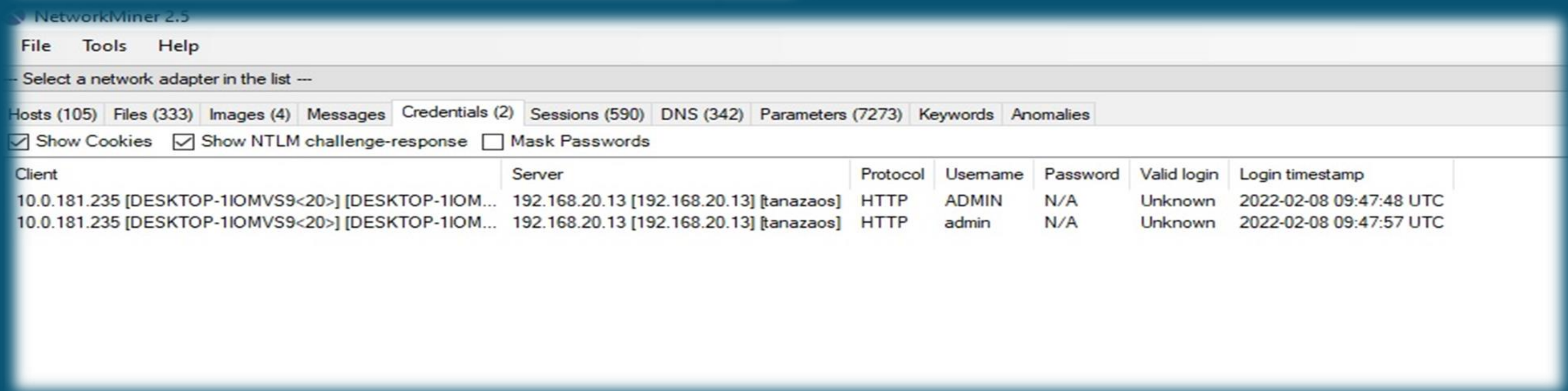
Client	Server	Protocol	Username	Password	Valid login	Login timestamp
10.0.100.134 [Iqbal-s-A12] (Linux)	216.58.209.132 [www.google.com] (Windows)	HTTP Cookie	1P_JAR=2022-02-17-05; expires=Sat, 19-Mar-2022 05:45:...	N/A	Unknown	2022-02-17 10:45:43 UTC
10.0.193.176 [ATTAULLAHs-iPhone.local] (Apple_iOS)	112.74.128.179	HTTP Cookie	PHPSESSID=bcef352c3fdb81755306e7ee426453e9; pat...	N/A	Unknown	2022-02-17 11:00:34 UTC
10.0.89.74 (Android)	216.58.209.132 [www.google.com] (Windows)	HTTP Cookie	1P_JAR=2022-02-17-06; expires=Sat, 19-Mar-2022 06:14:...	N/A	Unknown	2022-02-17 11:14:36 UTC
10.0.100.134 [Iqbal-s-A12] (Linux)	216.58.209.132 [www.google.com] (Windows)	HTTP Cookie	1P_JAR=2022-02-17-06; expires=Sat, 19-Mar-2022 06:17:...	N/A	Unknown	2022-02-17 11:17:53 UTC
10.0.100.134 [Iqbal-s-A12] (Linux)	216.58.209.132 [www.google.com] (Windows)	HTTP Cookie	1P_JAR=2022-02-17-06; expires=Sat, 19-Mar-2022 06:19:...	N/A	Unknown	2022-02-17 11:19:30 UTC
10.0.100.134 [Iqbal-s-A12] (Linux)	216.58.209.132 [www.google.com] (Windows)	HTTP Cookie	1P_JAR=2022-02-17-06; expires=Sat, 19-Mar-2022 06:21:...	N/A	Unknown	2022-02-17 11:21:21 UTC

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

NETWORK FORENSIC OF CELL PHONE


NetworkMiner 2.5
File
Tools
Help
Select a network adapter in the list --
osts (817)
Files (1909)
Images (33)
Messages
Credentials (25)
Sessions (4866)
DNS (5743)
Parameters (51380)
Keywords
Anomalies
Case Panel
Filename
MD5
Adhock....
1c3586...
favicon[12].ico 32x32, 370 070 B
favicon[13].ico 32x32, 370 070 B
bkg[2].png 532x532, 1 218 B
logo[2].png 1024x500, 30 113 B
512[2].png 512x512, 199 068 B
512[2].png 512x512, 199 068 B
favicon[14].ico 32x32, 370 070 B
favicon[15].ico 32x32, 370 070 B
favicon[16].ico 32x32, 370 070 B
favicon[17].ico 32x32, 370 070 B
6a6c76c-88db-4e[... 750x750, 60 839 B
036c0b1a-7b1e-43[... 750x750, 36 426 B
32911fe0-46e0-41[... 750x750, 21 712 B
bcf6ac2f-8369-4f[... 750x750, 49 693 B
036c0b1a-7b1e-43[... 750x750, 36 426 B
96a6c76c-88db-4e[... 750x750, 60 839 B
32911fe0-46e0-41[... 750x750, 21 712 B
bcf6ac2f-8369-4f[... 750x750, 49 693 B
34934421f823-45[... 1125x540, 15 945 B
4552ed9c-210f-44[... 240x240, 4 517 B
6dc3c06-81aa-48[... 240x240, 3 786 B
924ea45af3cf-4f[... 750x750, 30 685 B
036c0b1a-7b1e-43[... 750x750, 36 426 B
96a6c76c-88db-4e[... 750x750, 60 839 B
3f1797e3-970f-40[... 150x150, 23 084 B
784a06ef-7fb8-4f[... 150x150, 45 249 B
f28034d1f572-40[... 750x750, 63 404 B
32911fe0-46e0-41[... 750x750, 21 712 B
bcf6ac2f-8369-4f[... 750x750, 49 693 B
TB1xfMvtCzqK1RjS... 308x32, 3 874 B
24ce2e5b81246c... 355x114, 570 B
e76db69d9dfd7aac... 530x530, 32 173 B
e39cabbdbf402a2b... 1000x1500, 106 69...


NetworkMiner 2.5
File
Tools
Help
Select a network adapter in the list --
Start
Sto
Parameters (63332)
Keywords
Anomalies
Hosts (967)
Files (1820)
Images (6)
Messages
Credentials (6)
Sessions (10022)
DNS (9697)
GIF
9793c230cc9bc67... 240x240, 17 017 B
cef48fdedde11f83[... 240x240, 33 789 B
cb17ebe839d065c... 240x240, 36 978 B
9e348e184ec5eb9... 208x208, 50 739 B
1070ef92f611b3a5[... 480x480, 56 353 B
Case Panel
Filename
MD5
Office Inf...
7c5c51...



☑ Show Cookies ☑ Show NTLM challenge-response □ Mask Passwords

Client	Server	Protocol	Username	Password	Valid login	Login timestamp
10.0.181.235 [DESKTOP-1IOMVS9<20>] [DESKTOP-1IOM...	192.168.20.13 [192.168.20.13] [tanazaos]	HTTP	ADMIN	N/A	Unknown	2022-02-08 09:47:48 UTC
10.0.181.235 [DESKTOP-1IOMVS9<20>] [DESKTOP-1IOM...	192.168.20.13 [192.168.20.13] [tanazaos]	HTTP	admin	N/A	Unknown	2022-02-08 09:47:57 UTC

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.