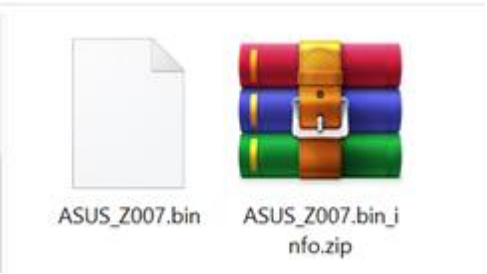
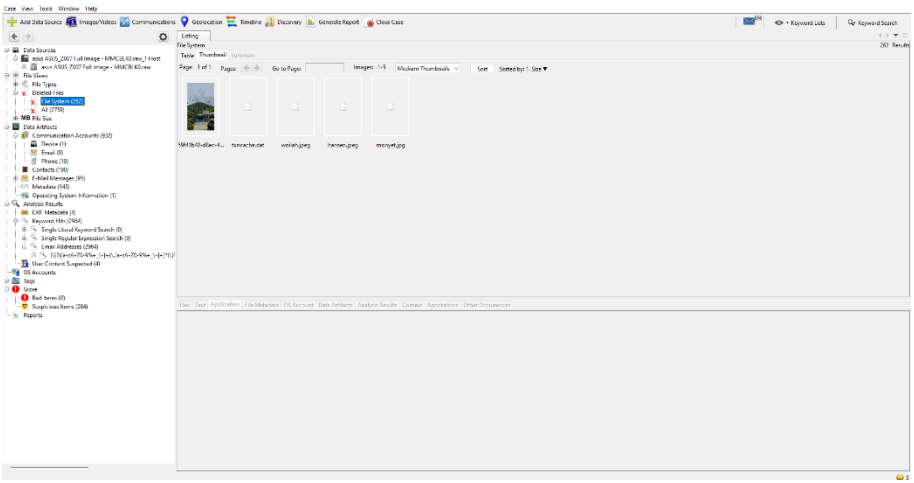
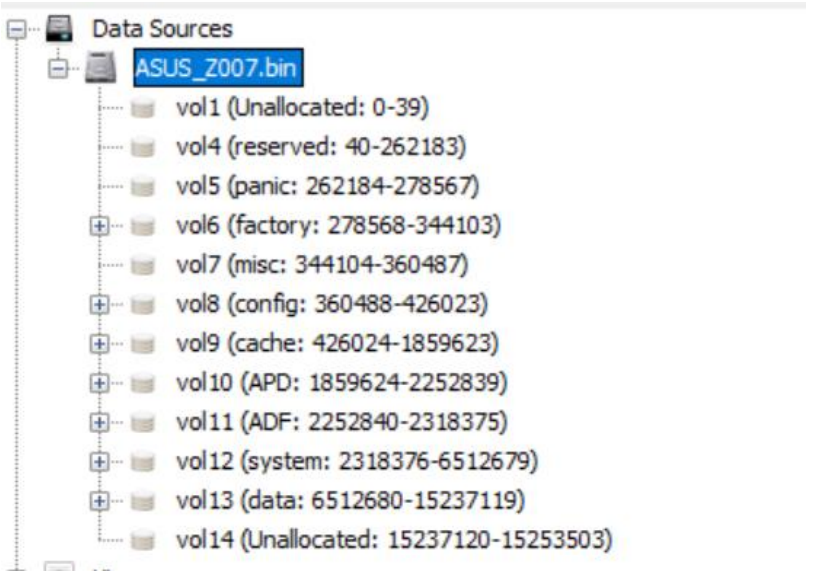
Pada bagian mobile forensics saya membantu dalam pengambilan image pada device Asus Z007 beserta analisisnya. Pengambilan Image menggunakan Magnet Axiom yang selanjutnya dianalisis menggunakan Autopsy dan andriller. Berikut beberapa dokumentasi dari proses analisis image:



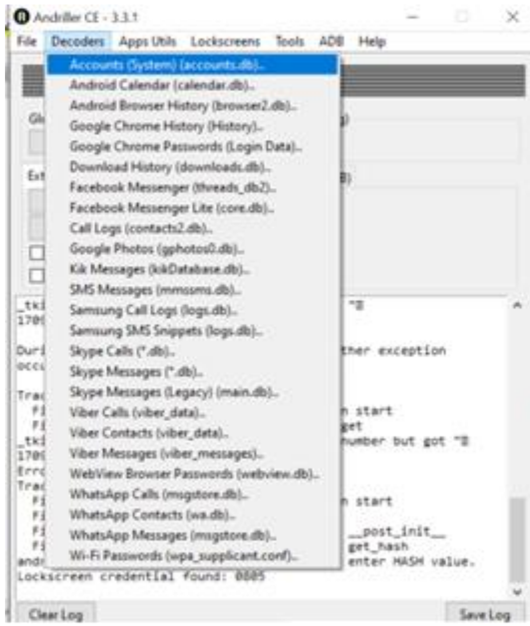
File image perangkat Z007



Tampilan data pada autopsy



Partisi pada android



Aplikasi Andriller

Accounts (System)

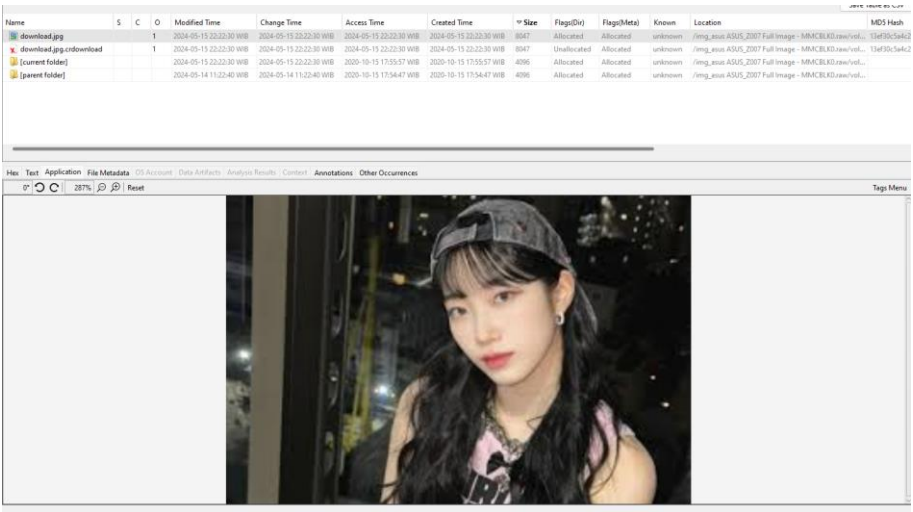
Total: 1

Index	Account type	Username	Password
1	com.google	kenascamnjir@gmail.com	aas_et/AKppINbtQb7WQfYbZ0a9JQtOLHwnYM8BfEAuQmSK1Vbc7yv--b5pBjs4dun8RpOZrEUUFmIRdaZ8t1gm8znuIL-GLKzGPXDyGc1Izndra46xKwHxLIQ5iMtHyE4Cn85O2E8_9GqnuoM74_lafPcps3-I8Xv_Q0v_xt466ul0_8jnY5VTW8-fhDMIuIUAOvIHDPUz0G-Hr9XLMmg79Ph6N4=

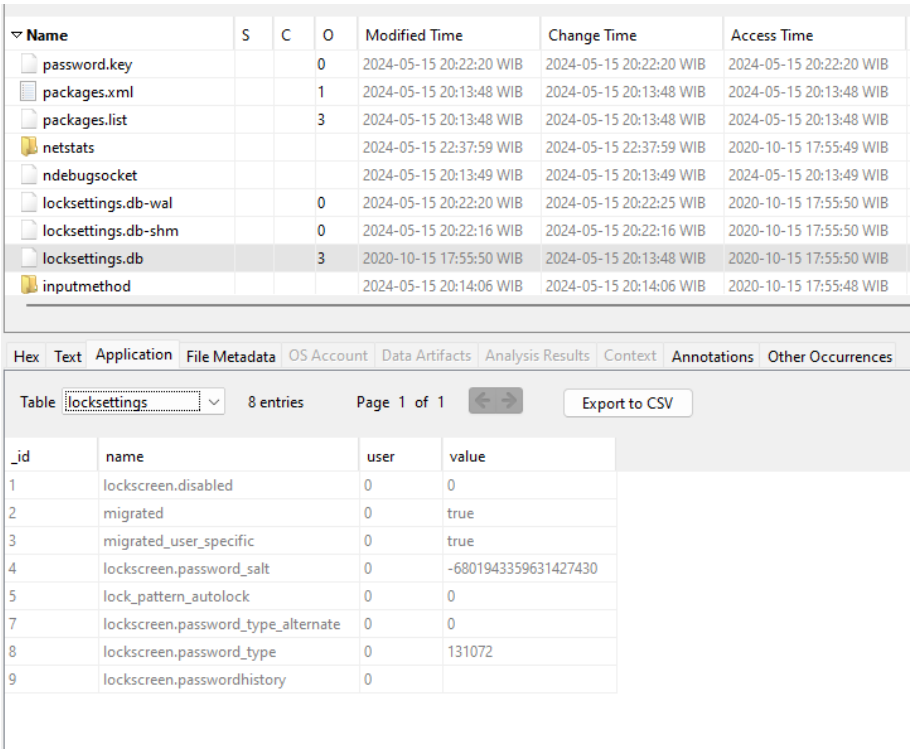
Hasil Andriller untuk pemeriksaan accounts.db

```
network={
        ssid="Turu"
        psk="chawnima"
        key_mgmt=WPA-PSK
        priority=5
}

network={
        ssid="KOST PUTRA"
        psk="123putra"
        key_mgmt=WPA-PSK
        priority=7
}
ctrl_interface=wlan0^ctrl_interface=wlan0^

------------------------------METADATA------------------------------
```

Isi file wpa_supplicant



File unduhan dari android



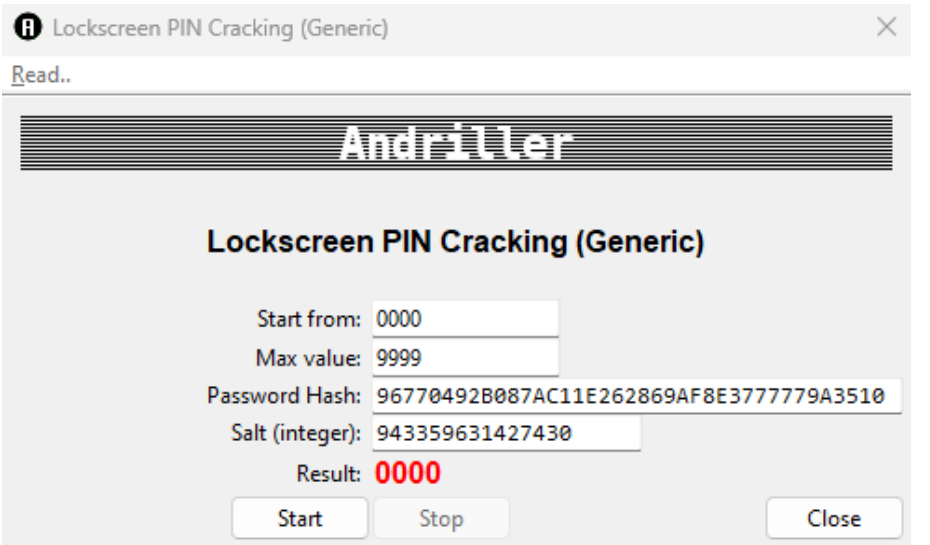
Name	S	C	O	Modified Time	Change Time	Access Time
password.key			0	2024-05-15 20:22:20 WIB	2024-05-15 20:22:20 WIB	2024-05-15 20:22:20 WIB
packages.xml			1	2024-05-15 20:13:48 WIB	2024-05-15 20:13:48 WIB	2024-05-15 20:13:48 WIB
packages.list			3	2024-05-15 20:13:48 WIB	2024-05-15 20:13:48 WIB	2024-05-15 20:13:48 WIB
netstats				2024-05-15 22:37:59 WIB	2024-05-15 22:37:59 WIB	2020-10-15 17:55:49 WIB
ndebugsocket				2024-05-15 20:13:49 WIB	2024-05-15 20:13:49 WIB	2024-05-15 20:13:49 WIB
locksettings.db-wal			0	2024-05-15 20:22:20 WIB	2024-05-15 20:22:25 WIB	2020-10-15 17:55:50 WIB
locksettings.db-shm			0	2024-05-15 20:22:16 WIB	2024-05-15 20:22:16 WIB	2020-10-15 17:55:50 WIB
locksettings.db			3	2020-10-15 17:55:50 WIB	2024-05-15 20:13:48 WIB	2020-10-15 17:55:50 WIB
inputmethod				2024-05-15 20:14:06 WIB	2024-05-15 20:14:06 WIB	2020-10-15 17:55:48 WIB

Hex | Text | Application | File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Table: locksettings | 8 entries | Page 1 of 1 | Export to CSV

_id	name	user	value
1	lockscreen.disabled	0	0
2	migrated	0	true
3	migrated_user_specific	0	true
4	lockscreen.password_salt	0	-6801943359631427430
5	lock_pattern_autolock	0	0
7	lockscreen.password_type_alternate	0	0
8	lockscreen.password_type	0	131072
9	lockscreen.passwordhistory	0	

Informasi dari file locksettings.db



Proses password cracking Andriller