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.

DATA COMPROMISE ASSESSMENT

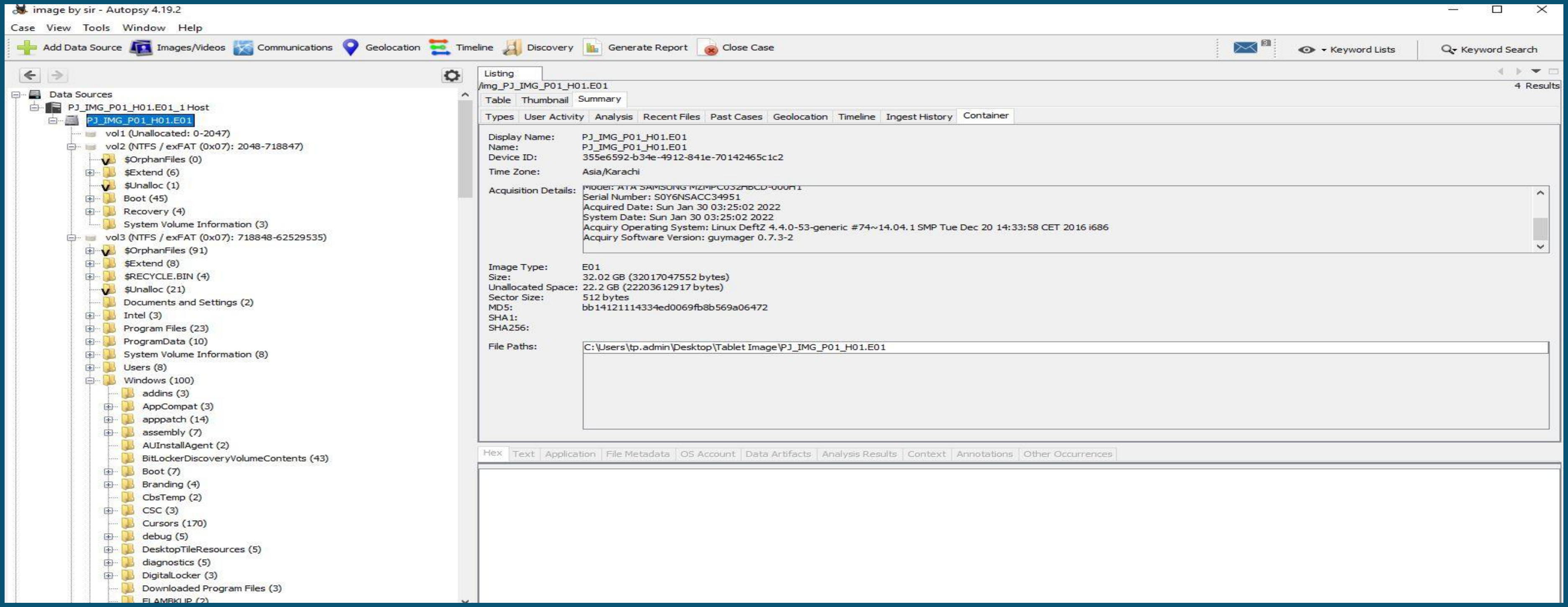
Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

DATA COMPROMISE ASSESSMENT

Project Name: Data Compromise Assessment

Tool Used: Crowd Strike

Platform: Windows



```
Data Sources
  PJ_IMG_P01_H01.E01_1 Host
    PJ_IMG_P01_H01.E01
      vol1 (Unallocated: 0-2047)
      vol2 (NTFS / exFAT (0x07): 2048-718847)
        $OrphanFiles (0)
        $Extend (6)
        $Unalloc (1)
        Boot (45)
        Recovery (4)
        System Volume Information (3)
      vol3 (NTFS / exFAT (0x07): 718848-62529535)
        $OrphanFiles (91)
        $Extend (8)
        $RECYCLE.BIN (4)
        $Unalloc (21)
        Documents and Settings (2)
        Intel (3)
        Program Files (23)
        ProgramData (10)
        System Volume Information (8)
        Users (8)
        Windows (100)
          addins (3)
          AppCompat (3)
          apppatch (14)
          assembly (7)
          AUInstallAgent (2)
          BitLockerDiscoveryVolumeContents (43)
          Boot (7)
          Branding (4)
          CbsTemp (2)
          CSC (3)
          Cursors (170)
          debug (5)
          DesktopTileResources (5)
          diagnostics (5)
          DigitalLocker (3)
          Downloaded Program Files (3)
          FLAMBKUP (2)
```

/img_PJ_IMG_P01_H01.E01

```
Display Name:        PJ_IMG_P01_H01.E01
Name:                PJ_IMG_P01_H01.E01
Device ID:           355e6592-b34e-4912-841e-70142465c1c2

Time Zone:           Asia/Karachi

Acquisition Details: Model: ATA SAMSUNG MZMPC032HBCD-000H1
                     Serial Number: S0Y6NSACC34951
                     Acquired Date: Sun Jan 30 03:25:02 2022
                     System Date: Sun Jan 30 03:25:02 2022
                     Acquiry Operating System: Linux DeftZ 4.4.0-53-generic #74~14.04.1 SMP Tue Dec 20 14:33:58 CET 2016 i686
                     Acquiry Software Version: guymager 0.7.3-2

Image Type:          E01
Size:                32.02 GB (32017047552 bytes)
Unallocated Space:   22.2 GB (22203612917 bytes)
Sector Size:         512 bytes
MD5:                 bb14121114334ed0069fb8b569a06472
SHA1:
SHA256:

File Paths:          C:\Users\tp.admin\Desktop\Tablet Image\PJ_IMG_P01_H01.E01
```

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.

DATA COMPROMISE ASSESSMENT

DESCRIPTION :

Compromise assessments are high-level investigations where skilled teams utilize advanced tools to dig more deeply into their environment to identify ongoing or past attacker activity in addition to identifying existing weaknesses in controls and practices. We used crown strike tool for data compromise assessment and after performing actions we are able to gather information and vulnerabilities.

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.