

# 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.



# LIVE FORENSIC ACQUISITION (WINDOWS)

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.

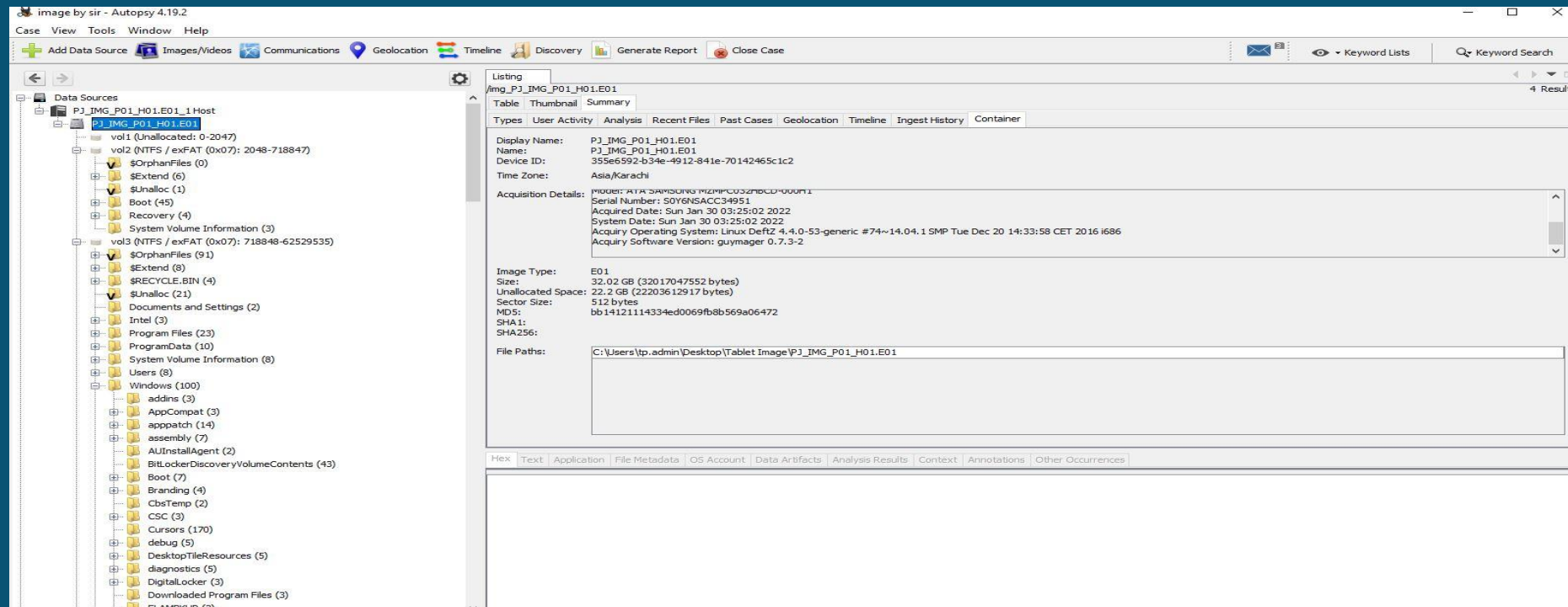


# LIVE FORENSIC ACQUISITION (WINDOWS)

**Project Name:** Live Forensic Acquisition (Windows)

**Tool Used:** Autopsy, Deft

**Platform:** Windows



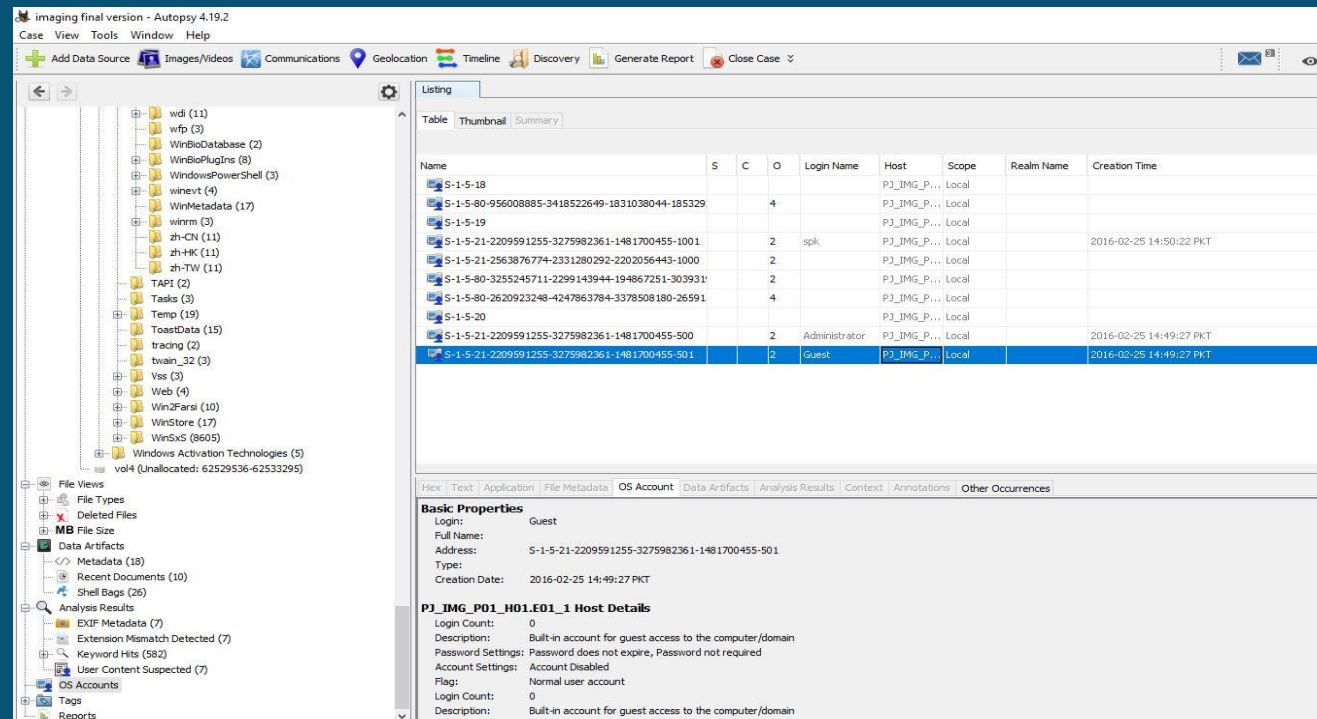
Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.



# LIVE FORENSIC ACQUISITION (WINDOWS)

## DESCRIPTION :

In this we used Autopsy tool and gather all the information of windows. We can find what are the activities done and on what time, also we can find the owner details and moreover many settings and what are the changes made , by whom , when , and on which destination.



The screenshot shows the Autopsy 4.19.2 interface. The left pane displays a tree view of the file system, including folders like 'wdi', 'wfp', 'WinBioDatabase', 'WinBioPlugins', 'WindowsPowerShell', 'winevt', 'WinMetadata', 'winrm', 'zh-CN', 'zh-HK', 'zh-TW', 'TAPI', 'Tasks', 'Temp', 'ToastsData', 'tracing', 'twain\_32', 'Vss', 'Web', 'Win2Farsi', 'WinStore', 'WinSxS', 'Windows Activation Technologies', and 'vols4 (Unallocated: 62529536-62533295)'. The right pane shows a table of OS accounts with columns for Name, S, C, O, Login Name, Host, Scope, Realm Name, and Creation Time. The selected row is for the 'Guest' account.

Name	S	C	O	Login Name	Host	Scope	Realm Name	Creation Time
S-1-5-18					PJ_IMG_P...	Local		
S-1-5-80-956008885-3418522649-1831038044-185329			4		PJ_IMG_P...	Local		
S-1-5-19					PJ_IMG_P...	Local		
S-1-5-21-2209591255-3275982361-1481700455-1001			2	spk	PJ_IMG_P...	Local		2016-02-25 14:50:22 PKT
S-1-5-21-2563876774-2331280292-2202056443-1000			2		PJ_IMG_P...	Local		
S-1-5-80-3255245711-2299143944-194867251-303931			2		PJ_IMG_P...	Local		
S-1-5-80-2620923248-4247863784-3378508180-26591			4		PJ_IMG_P...	Local		
S-1-5-20					PJ_IMG_P...	Local		
S-1-5-21-2209591255-3275982361-1481700455-500			2	Administrator	PJ_IMG_P...	Local		2016-02-25 14:49:27 PKT
S-1-5-21-2209591255-3275982361-1481700455-501			2	Guest	PJ_IMG_P...	Local		2016-02-25 14:49:27 PKT

The 'Basic Properties' section for the selected 'Guest' account shows:

- Login: Guest
- Full Name:
- Address: S-1-5-21-2209591255-3275982361-1481700455-501
- Type:
- Creation Date: 2016-02-25 14:49:27 PKT

The 'PJ\_IMG\_P01\_H01.E01\_1 Host Details' section shows:

- Login Count: 0
- Description: Built-in account for guest access to the computer/domain
- Password Settings: Password does not expire, Password not required
- Account Settings: Account Disabled
- Flag: Normal user account
- Login Count: 0
- Description: Built-in account for guest access to the computer/domain

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.

