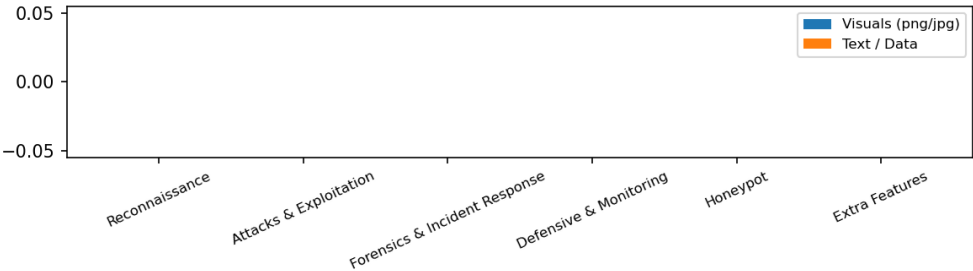# raja

Client:	alan
Creator:	davis
Session folder:	/home/kali/Rajasploit/results/recon
Generated:	2025-10-08 01:16:35 UTC

Executive Summary

This report captures results collected in the session folder **recon**. The following analysis summarizes the modules executed, key files captured, and visualizations produced. Use the module sections to review raw outputs and charts for technical details and evidence.

Module	Files	Visuals	Logs/Text	JSON/CSV	Other
Reconnaissance	0	0	0	0	0
Attacks & Exploitation	0	0	0	0	0
Forensics & Incident Response	0	0	0	0	0
Defensive & Monitoring	0	0	0	0	0
Honeypot	0	0	0	0	0
Extra Features	0	0	0	0	0

Visual Summary (Visuals vs Text/Data)

Reconnaissance

Folder: Auto-detected or mixed (see files below)
Total files: 0
Counts:

Attacks & Exploitation

Folder: Auto-detected or mixed (see files below)
Total files: 0
Counts:

Forensics & Incident Response

Folder: Auto-detected or mixed (see files below)
Total files: 0
Counts:

Folder: Auto-detected or mixed (see files below)
Total files: 0
Counts:

Defensive & Monitoring

Folder: Auto-detected or mixed (see files below)
Total files: 0
Counts:

Folder: Auto-detected or mixed (see files below)
Total files: 0
Counts:

Honeypot

Folder: Auto-detected or mixed (see files below)
Total files: 0
Counts:

Honeypot

Folder: Auto-detected or mixed (see files below)
Total files: 0
Counts:

Extra Features

Folder: Auto-detected or mixed (see files below)
Total files: 0
Counts:

Notes & Recommendations

This report aggregates results recorded during the session. Files larger than a certain threshold are truncated for in-report display — use the archived session folder to access complete logs and artifacts.
Recommendations: - Validate any suspicious IPs found in Recon. - Review the AutoVuln Nmap & Nikto logs for actionable vulnerabilities. - Preserve disk images and memory extracts securely for forensic analysis.