Advanced JPG Forensic Analysis Playbook

Environment: Linux Forensic OS (REMnux, SIFT, Tsurugi, Kali)

Purpose

This playbook provides a structured, forensic-grade methodology to analyze JPEG files suspected of malicious content. It is designed for SOC analysts, DFIR investigators, and malware researchers.

Phase 0 – Operational Security

- Perform analysis only in an isolated virtual machine.
- Disable clipboard, drag-and-drop, and shared folders.
- Never open the image with a GUI viewer.
- Take a VM snapshot before analysis.

Phase 1 – File Identification

Identify the real file type using magic bytes.

```
file suspicious.jpg
```

```
xxd -l 16 suspicious.jpg
```

Phase 2 – Hashing & Integrity

Generate cryptographic hashes for evidence handling.

```
sha256sum suspicious.jpg
```

```
md5sum suspicious.jpg
```

Phase 3 – Metadata Analysis

Inspect EXIF metadata for anomalies or embedded data.

```
exiftool -a -u -g1 suspicious.jpg
```

Phase 4 – Embedded Payload Detection

Detect appended or embedded payloads.

```
binwalk suspicious.jpg
```

```
binwalk -e suspicious.jpg
```

Phase 5 – Strings & Entropy Analysis

Look for suspicious strings or high entropy.

```
strings -a suspicious.jpg | less
```

```
ent suspicious.jpg
```

Phase 6 – Steganography Checks

Detect hidden data using steganography tools.

```
steghide info suspicious.jpg
```

```
zsteg suspicious.jpg
```

Phase 7 – Exploit & YARA Analysis

Scan for known exploit patterns.

```
yara rules.yar suspicious.jpg
```

Phase 8 – Reputation & Threat Intelligence

Correlate file hashes with threat intelligence platforms such as VirusTotal, FortiGuard, and abuse.ch.

Phase 9 – Conclusion & Reporting

Determine whether the file is malicious, a false positive, or weaponized. Document findings, IOCs, and recommended mitigations.

Analyst Notes

Image-based malware is rare but high impact. Treat all flagged images as suspicious until proven otherwise. Never rely solely on file extensions.