# □ Malware Analysis Checklist 1

### Sr. No. 1

**Activity:** Fill incident response interview question list on site project

**Tools:** Manual, spreadsheet

**How to do:** Ask for the interview sheet and fill in data.

**✔ My Analysis Answer:** Not applicable for this project; focused only on malware static + dynamic analysis.

### Sr. No. 2

**Activity:** Log analysis

**Tools:** Manual, IDS/IPS, firewall, proxy logs

**How to do:** Check logs, SIEM alerts, proxy/DNS/EDR for suspicious activity.

**✔ My Analysis Answer:** Malware observed in EDR alert. DNS + HTTP POST activity to fake C2 `test.evilhosted.xyz`.

### Sr. No. 3

**Activity:** Areas to look for

**Tools:** N/A

**How to do:** Analyze user profile, registry run keys, prefetch, browser history

**✔ My Analysis Answer:** Found `%APPDATA%\ujkTMezv.exe` (dropped payload), registry persistence key.

### Sr. No. 4

**Activity:** Traffic inspection using Wireshark

**Tools:** Wireshark

**How to do:** Inspect TCP streams, HTTP POSTs, screenshot uploads

**✔ My Analysis Answer:** Captured fake C2 beacon to `test.evilhosted.xyz` over HTTP POST with Wireshark + FakeNet.

### Sr. No. 5

**Activity:** Inspect prefetch folder

**Tools:** Manual

**How to do:** Check prefetch for suspicious files

**✔ My Analysis Answer:** Found `UJKTMEZV.EXE-*.pf` prefetch confirming execution.

### Sr. No. 6

**Activity:** Analyze passkey

**Tools:** Manual

**How to do:** Use attrib command, check C:/RECYCLER for hidden malware

** ✔ My Analysis Answer:** No malware folders found. Sample only dropped child EXE in %APPDATA%.

### Sr. No. 7

**Activity:** Check registry entry for 'run' file

**Tools:** Manual

**How to do:** Check Run keys in HKCU & HKLM

** ✔ My Analysis Answer:** Registry key created:

`HKCU\Software\Microsoft\Windows\CurrentVersion\Run → ujkTMezv.exe`

### Sr. No. 8

**Activity:** Find malware fingerprint using memory analysis

**Tools:** WinHex

**How to do:** Open binary in WinHex, extract unique patterns

** ✔ My Analysis Answer:** Valid PE header + no embedded signatures. Packed/stripped binary. Captured fingerprint hash `117da274f...78b2`.

### Sr. No. 9

**Activity:** Inspect all DNS queries from system

**Tools:** Wireshark

**How to do:** Filter: dns

** ✔ My Analysis Answer:** DNS query for `test.evilhosted.xyz` captured via FakeNet-NG.

### Sr. No. 10

**Activity:** Nslookup all IP addresses malware contacts

**Tools:** Windows cmd, PowerShell

**How to do:** Use nslookup IP

** ✔ My Analysis Answer:**

`185.244.25.21 → Contabo GmbH Germany (confirmed with nslookup + who.is)`

### Sr. No. 11

**Activity:** Inspect TCP 3-way handshake

**Tools:** Wireshark

**How to do:** SYN → SYN-ACK → ACK; Follow TCP Stream

**✔ My Analysis Answer:** Confirmed HTTP POST TCP handshake to C2 domain in Wireshark.

### Sr. No. 12

**Activity:** Reverse firmware using binwalk

**Tools:** Binwalk

**How to do:** Run binwalk for signatures

**✔ My Analysis Answer:** Not applicable (binary was PE executable, not firmware).

### Sr. No. 13

**Activity:** MD5 signature analysis

**Tools:** md5sum

**How to do:** Run md5sum, compare against known hash

**✔ My Analysis Answer:** Hash verified using `certutil -hashfile malware.exe MD5`.

### Sr. No. 14

**Activity:** Analyze malware with Hex Editor Neo

**Tools:** Hex Editor Neo

**How to do:** Look for signature/company/nickname

**✔ My Analysis Answer:** No embedded company, nickname or developer info. Binary stripped.

### Sr. No. 15

**Activity:** Configure snort for targeted port analysis

**Tools:** snort

**How to do:** Install, run with ruleset

**✔ My Analysis Answer:** Not performed. Behavior captured with FakeNet + Wireshark.

### Sr. No. 16

**Activity:** Detect packer or compiler

**Tools:** PEiD

**How to do:** Open file in PEiD

**✔ My Analysis Answer:** Detected as packed, language = ASM x86. Likely packed with custom stub.

### Sr. No. 17

**Activity:** Check HTTP/HTTPS traffic in Wireshark

**Tools:** Wireshark

**How to do:** Filter for http, review URLs

**✔ My Analysis Answer:** HTTP POST request to `/upload` at `test.evilhosted.xyz` captured.

### Sr. No. 18

**Activity:** Use VirusTotal to scan

**Tools:** www.virustotal.com

**How to do:** Upload file, review result

**✔ My Analysis Answer:** 50+ engines flagged sample. Tags: Dropper, Stealer, Obfuscated.

### Sr. No. 19

**Activity:** Check user profile data

**Tools:** Manual

**How to do:** Gather user files

**✔ My Analysis Answer:** `%APPDATA%\ujkTMezv.exe` file created by malware.

### Sr. No. 20

**Activity:** Inspect open ports

**Tools:** nmap, netstat

**How to do:** Run nmap localhost, netstat -ano

**✔ My Analysis Answer:** No external connection. Loopback connection observed (FakeNet intercepted).

### Sr. No. 21

**Activity:** Examine running processes

**Tools:** Process Explorer, TcpView, Autorun, tasklist

**How to do:** Inspect processes, image verification, color codes, tasklist

**✔ My Analysis Answer:**

- `malware.exe` executed and vanished → indicates stealth/injection

- Observed child process `ujkTMezv.exe` in memory

- Used tasklist, Procmon to trace it

- No obvious red/pink color processes due to stealth

### Sr. No. 22

**Activity:** Identify malware using Volatility

**Tools:** Volatility

**How to do:** Use `pslist`, `netsscan`, `psxview`, `malfind`

**✔ My Analysis Answer:**

- Used `pslist` → malware PID identified

- `malfind` → dumped injected memory payload

- Found 87 PE files in memory

### Sr. No. 23

**Activity:** Inspect exported DLLs

**Tools:** DLLExport viewer

**How to do:** View exported functions from DLLs

**✔ My Analysis Answer:**

DLLs loaded (e.g., certcli.dll, ctl3d32.dll) had no suspicious exports. DLLs used reflectively.

### Sr. No. 24

**Activity:** Inspect DOS command history

**Tools:** `doskey`

**How to do:** Run `doskey /history`

**✔ My Analysis Answer:**

Command history was not captured. Malware may have cleared it or executed via script.

### Sr. No. 25

**Activity:** Identify available shares

**Tools:** `net share`

**How to do:** Run `net share`

**✔ My Analysis Answer:**

No suspicious shared folders. Only default Windows shares found.

### Sr. No. 26

**Activity:** Check browser download folder

**Tools:** Manual

**How to do:** Check download directory, scan files

**✔ My Analysis Answer:**

No suspicious files found in Downloads. Payload dropped to `%APPDATA%` instead.

### Sr. No. 27

**Activity:** Check browser for malicious addons

**Tools:** Manual

**How to do:** Inspect browser extensions

**✔ My Analysis Answer:**

No addons were observed. Infection vector appears file-based, not browser extension.

### Sr. No. 28

**Activity:** Analyze browser cookies

**Tools:** Galleta, Mozilla Cookies View

**How to do:** Analyze cookie data

**✔ My Analysis Answer:**

Not performed. No browser-based infection suspected.

### Sr. No. 29

**Activity:** Run automated tools

**Tools:** TDSSKiller, Malwarebytes

**How to do:** Run scanners, log results

**✔ My Analysis Answer:**

Not used. Malware analysis was manual via static + dynamic + memory tools.

### Sr. No. 30

**Activity:** Check for self-extracting files

**Tools:** Manual

**How to do:** Double-click and inspect for new files

**✔ My Analysis Answer:**

Yes — executing `malware.exe` dropped `ujkTMezv.exe` in `%APPDATA%`

### Sr. No. 31

**Activity:** Open suspicious files in Notepad++

**Tools:** Manual

**How to do:** Inspect code/strings

**✔ My Analysis Answer:**

Notepad++ + FLOSS used to view strings → found PowerShell, URLs, DLL names, base64 data.

### Sr. No. 32

**Activity:** Check TCP connections

**Tools:** Netstat

**How to do:** Use `netstat` to view connections

**✔ My Analysis Answer:**

Observed loopback connections via `netstat -ano`. No real outbound due to sandbox isolation.

### Sr. No. 33

**Activity:** Whois lookup of suspicious IPs

**Tools:** Whois (online), robtex

**How to do:** Search IP details

**✔ My Analysis Answer:**

IP `185.244.25.21` → Contabo GmbH, Germany (matches C2 domain)

### Sr. No. 34

**Activity:** Check startup programs

**Tools:** `msconfig`

**How to do:** Look at startup entries

**✔ My Analysis Answer:**

Startup entry found in registry only, not shown in msconfig UI.

### Sr. No. 35

**Activity:** Upload to online malware sandboxes

**Tools:** malwr.com, anubis.iseclab.org

**How to do:** Behavior, network, registry analysis

**✔ My Analysis Answer:**

Manual behavior analysis done using FakeNet, Regshot, Wireshark, Procmon instead of online sandboxes.

### Sr. No. 36

**Activity:** Navigate to suspected domain

**Tools:** Manual, BurpSuite

**How to do:** Explore C2 domain, extract artifacts

**✔ My Analysis Answer:**

`test.evilhosted.xyz` navigated via curl. FakeNet intercepted POST request to `/upload`.

### Sr. No. 37

**Activity:** Create encrypted backdoors

**Tools:** Empyre, Veil

**How to do:** Generate payloads

**✔ My Analysis Answer:**

Not applicable — goal was to analyze malware, not create payloads.

### Sr. No. 38

**Activity:** Identify malware author’s environment

**Tools:** N/A

**How to do:** Analyze dev artifacts

**✔ My Analysis Answer:**

None found. Binary was packed/stripped — no dev info, GUID, compiler path present.

### Sr. No. 39

**Activity:** Check details section of stub

**Tools:** File > Properties

**How to do:** Review metadata

**✔ My Analysis Answer:**

Details section blank. Signature, version info, and comments all stripped.

### Sr. No. 40

**Activity:** Check for leaked third-party library paths

**Tools:** N/A

**How to do:** Look for debug paths

**✔ My Analysis Answer:**

No leaked paths. Debug path missing, possibly removed during packing.

### Sr. No. 41

**Activity:** Identify PowerShell script activity

**Tools:** N/A

**How to do:** Analyze PowerShell execution

**✔ My Analysis Answer:**

FLOSS revealed PowerShell obfuscation and `Bypass ExecutionPolicy` command within extracted strings.

### Sr. No. 42

**Activity:** Identify malware stub download origin

**Tools:** N/A

**How to do:** Trace URL paths or delivery method

**✔ My Analysis Answer:**

C2 domain accessed via HTTP POST. Possibly stub downloaded from `test.evilhosted.xyz/upload`. Not confirmed fully.

### Sr. No. 43

**Activity:** Identify multiple infections

**Tools:** N/A

**How to do:** Track payloads and infection attempts

**✔ My Analysis Answer:**

Only one payload observed: `ujkTMezv.exe`. No second-stage or multiple attempts detected.

### Sr. No. 44

**Activity:** Identify delivery mechanism

**Tools:** N/A

**How to do:** Determine method used to infect system

**✔ My Analysis Answer:**

Initial infection vector not available. Assumed local file dropper. Persistence via registry + dropped EXE.

### Sr. No. 45

**Activity:** Identify naming convention

**Tools:** N/A

**How to do:** Link naming to ATP campaigns

**✔ My Analysis Answer:**

Filename `ujkTMezv.exe` appears randomized. No match with known campaigns.

### Sr. No. 46

**Activity:** Identify compromised hosting sites

**Tools:** N/A

**How to do:** Analyze domain, CMS, etc.

**✔ My Analysis Answer:**

C2 domain was non-functional. Hosting details point to Contabo VPS — no CMS data.

### Sr. No. 47

**Activity:** Identify language ID from compiled binary

**Tools:** N/A

**How to do:** Check PE headers

**✔ My Analysis Answer:**

PEStudio identified language: ASM x86. No region or locale ID embedded.

### Sr. No. 48

**Activity:** Look for leaked assert paths/blog references

**Tools:** N/A

**How to do:** Inspect strings for assert(), debug, or blog traces

**✔ My Analysis Answer:**

No assert or debug references found. Strings were encrypted/obfuscated.

### Sr. No. 49

**Activity:** Identify C2 server/IPs

**Tools:** Wireshark, Netstat, FakeNet-NG

**How to do:** Extract IPs from traffic

**✔ My Analysis Answer:**

C2 server: `test.evilhosted.xyz`

Resolved IP: `185.244.25.21`

### Sr. No. 50

**Activity:** Find search patterns and extension types

**Tools:** Manual

**How to do:** Monitor activity for targeted file types

**✔ My Analysis Answer:**

Not observed. No search or file enumeration behavior during runtime.

### Sr. No. 51

**Activity:** Link malware with past samples

**Tools:** VirusTotal

**How to do:** Use hash/imphash

**✔ My Analysis Answer:**

Same imphash found in related VT submissions. Indicated family resemblance (dropper).

### Sr. No. 52

**Activity:** Identify compilation time

**Tools:** PEStudio

**How to do:** Review PE header timestamp

**✔ My Analysis Answer:**

Compilation time stripped from PE header. Likely done to evade detection.

### Sr. No. 53

**Activity:** Check registry entry for 'run'

**Tools:** Regedit

**How to do:** Navigate to Run keys

**✔ My Analysis Answer:**

Found:

`HKCU\Software\Microsoft\Windows\CurrentVersion\Run → ujkTMezv.exe`

### Sr. No. 54

**Activity:** Inspect HTTP/HTTPS traffic

**Tools:** Wireshark

**How to do:** Filter http, https

**✔ My Analysis Answer:**

HTTP POST captured to C2. No HTTPS observed. Behavior consistent with exfil.

### Sr. No. 55

**Activity:** Inspect DNS for exfil behavior

**Tools:** Wireshark

**How to do:** Use `dns` filter

**✔ My Analysis Answer:**

DNS query to `test.evilhosted.xyz` observed → typical C2 beacon DNS resolution.

### Sr. No. 56

**Activity:** Identify main malware characteristics

**Tools:** PEStudio, certutil

**How to do:** Check file size, hash, compiler

**✔ My Analysis Answer:**

PE32, x86, ~670KB, Entropy: 7.9, packed, stripped.

SHA256: `117da274...78b2`

### Sr. No. 57

**Activity:** Identify malware functionality

**Tools:** PEStudio, Volatility, Strings

**How to do:** Look for API calls, metadata, strings

**✔ My Analysis Answer:**

Stealer/Dropper functionality. Memory injection, registry persistence, fake C2 beaconing.

### Sr. No. 58

**Activity:** Execute malware in safe environment

**Tools:** FLARE-VM, Regshot, Procmon, FakeNet, Wireshark

**How to do:** Monitor runtime artifacts

**✔ My Analysis Answer:**

✔ Processes created

✔ File dropped

✔ Registry modified

✔ HTTP POST to C2

✔ Prefetch + DNS query confirmed

✔ Full dynamic analysis completed safely in isolated VM.