Incident Response Interview & Analysis Workbook

This structured guide provides:

- An **incident response interview question sheet** (professional spreadsheet-ready table),
- Tailored **field notes**,
- A mapped process for **log and alert analysis**,
- Comprehensive procedures for **malware analysis and investigation** steps—ready for operational site work and forensic planning.

1. Incident Response Field Interview Questions

No.	Interview Question	Field Notes / Data to Capture	Purpose
1	Who discovered/reported the incident?	Name, contact info, time/date reported	Attribution, response contact
2	What suspicious activity or alert triggered the response?	Description, alert system/source, time	Scope, system classification
3	What were the first actions taken after the incident/alert?	Timeline, users involved, containment steps	Chain of custody, impact
4	What systems/hosts appeared affected?	Hostname(s), IPs, user accounts	Asset inventory
5	Has this issue been reported before?	Past tickets, incident ID, previous measures	Detect recurring threats
6	Are there business processes/data at risk?	Data type, applications, sensitivity level	Risk assessment
7	What logs or devices generated alerts?	Proxy, firewall, EPP/AV, SIEM, IDS/IPS	Forensic trail, log sources
8	Any	Usernames,	Lateral

	unauthorized account activity or privilege escalation?	**timeframes, detected/anomalous**	**movement detection**
9	**Were there unusual network connections?**	**Source/dest IPs, protocols, geolocations**	**Exfiltration, C2 check**
10	**Did anyone download/open suspicious files, links, emails?**	**File/email name, sender, hashes, time**	**Infection vector mapping**
11	**Have any remediation steps been performed?**	**AV malware cleaning, blocklists, isolations**	**Prevent evidence loss**
12	**Any other notable user/system actions noted?**	**Manual changes, config alterations, logins**	**Insider threat review**

These questions create clear documentation and investigative workflow, ensuring all relevant information is gathered for a thorough response.

2. Field Notes Spreadsheet Example

Field	Captured Data
Incident Reporter	**(Name, Role, Contact)**
Date/Time	
System Affected	**Hostname, IP, User**
Nature of Incident	**Malware, Phishing, etc.**
Initial Alert	**Source, Description**
Immediate Action	**Isolated? Cleaned?**
Log Sources	**Firewall, SIEM, Proxy**
Open Questions	
Analyst Name	
Status/Resolution	**Ongoing, Closed, etc.**

3. Alert & Log Analysis Workflow

Primary sources for isolating alert origin:

- User complaints about suspicious activities on endpoints
- Proxy logs (web access, app control)
- Firewall alerts
- SIEM systems, IDS/IPS logs
- Endpoint security/protection (e.g., McAfee, Sophos, Symantec) alerts

Source Type	What To Look For	Example Tools
User Reports	Unusual behavior, pop-ups, slowdowns	Manual, field interview
Proxy/Firewall Logs	Blocked connections, malicious URLs	Proxy/Firewall consoles
SIEM, IDS/IPS	Signature/heuristic alerts, anomalies	SIEM dashboards
Endpoint Alerts	Malware detection, process blocks	EPP/EDR product logs

4. Malware Analysis: Areas and Methods

Area/Tool	Process
User Profile	Review for unknown files and recent changes
Registry Run Keys	HKCU/HKLM\Software\Microsoft\Windows\CurrentVersion\Run for strange autostarts
Prefetch Folders	Inspect for suspicious new/executed binaries
Browser History & Cache	Analyze for drive-by, forced downloads, exploit pages

5. Technical Forensic & Diagnostic Procedures

Log & Traffic Analysis

- Analyze suspicious activity using Wireshark:
  - Check info field for suspicious activity/unknown services
  - Use filters (e.g., tcp.port==443) for port-specific traffic
  - Follow TCP streams for data exfiltration or hidden communications
  - Review HTTP POST requests for covert file/screenshot uploads

Malware Traces and System Artifacts

- Inspect Prefetch folder for newly created/abnormal executables.
- Use attrib -s -h -r -a * in C: and the C:/RECYCLER folder for hidden malware.
- Manual inspection or search for lingering malicious files; remove manually or with AV tools.

Registry Inspection

- Check:
  - HKCU\Software\Microsoft\Windows\CurrentVersion\Run
  - HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- Identify and clear malicious autoruns.

Memory and Signature Analysis

- **WinHex:** Detect malware fingerprints and unique patterns in memory dumps.
- **MD5sum:** Generate hashes for suspicious binaries; compare with reference software.
- **VirusTotal:** Submit suspect files and URLs for threat intelligence and signature matching.

Network, DNS, and Connection Review

- Use wireshark to find malicious DNS requests/responses, analyze via dns filter.
- Use nslookup and whois for IP reputation and ownership tracing.
- Map 3-way TCP handshakes and review anomalous sessions.

Executable and Process Diagnostics

- Engage tools: Process Explorer, Tcpview, Autoruns, and tasklist for running process review.
- Map open ports using nmap and netstat.

Advanced Malware Analysis

- Use **Volatility Framework**:
  - plist for process list
  - netscan/connscan for connections
  - psxview to reveal hidden processes
  - malfind for malicious process characteristics
- Review exported DLLs with DLLExport Viewer
- Inspect previous DOS command history (doskey/history)

- Check shared folders (net share)
- Examine browser download folders, cookies, and installed addons.

Binary & Firmware Analysis

- **Hex Editor Neo**, **PEiD**, **Binwalk**: Identify packers/compilers, firmware anomalies, malware signatures, company or individual coding traces.

Automated Tools

- Use TDSSKiller (Kaspersky), Malwarebytes to scan systems, quarantine, and maintain logs.
- Safely analyze suspicious files in sandboxes (malwr.com, anubis.iseclab.org) for:
  - String/behavioral/network analysis
  - Registry/file artifacts

Backdoors & Payloads

- Create/encrypt payloads with **Empyre/Veil Frameworks** (for red team; do NOT submit to public scanners).
- Review for C2 server details, exfiltration attempts, command signatures, and campaign fingerprints.

6. Investigation Planning Checklist

- Prepare a detailed interview and collection sheet based on the template above.
- Document every finding with timestamps, tools, hashes, and screenshots.
- Correlate user, log, and artifact data for chain of custody.
- Use all above tools and methods as per incident context—always in a forensically sound manner.
- Maintain clear notes for handover or future audit/investigation.

🌐 General Search Engines

1. **Bing**
2. **Brave**
3. **DuckDuckGo**
4. **Goodsearch**
5. **Google Search**
6. **Instya**
7. **Impersonal.me**
8. **Lycos**
9. **Mojeek**