cyber.encse

IR Evidence Collection Checklist

Forensic evidence collection checklist for incident responders — volatile memory, disk images, log sources, network captures and chain of custody.

Order of volatility (RFC 3227) — collect the most volatile evidence first: registers/cache, routing table/ARP cache/process table, memory, temporary filesystems, disk, remote logging/monitoring data, physical configuration/network topology, archival media.

Published by eNeoteric Consultancy Services · cyber.encse.com · v1.0, August 2026

1. Pre-Collection

	Action	Notes
	Confirm legal authority to collect evidence on this system	Employment agreement, data processing policy, or law enforcement warrant as applicable
	Identify Incident Commander and evidence custodian	One person owns chain of custody for each piece of evidence
	Prepare sterile/write-protected collection media	Freshly wiped or write-blocked drives; verify with hash before use
	Document system state before touching anything	Photograph screen, note running processes, logged-in users, time/date shown

2. Volatile Data (Collect First — Order of Volatility)

	Evidence Type	Collection Method
	System date/time (and offset from NTP/UTC)	date /t & time /t (Win) or date (Linux) — note any clock drift
	Logged-on users / active sessions	query user, net session (Win); who, w (Linux)
	Running processes and command lines	tasklist /v (Win); ps auxww (Linux); prefer EDR process tree if available
	Network connections (established + listening)	netstat -anob (Win); ss -tunap (Linux)
	ARP cache	arp -a
	DNS cache	ipconfig /displaydns (Win)
	Loaded DLLs / kernel modules	listdlls (Win Sysinternals); lsmod (Linux)
	Full memory (RAM) capture	WinPmem / Magnet RAM Capture (Win); LiME (Linux) — capture before any shutdown
	Clipboard contents	If forensically relevant and legally permitted

3. Disk & Filesystem Evidence

	Evidence Type	Collection Method
	Full disk image (bit-for-bit)	dd / dc3dd / FTK Imager — write-blocked source, verify with SHA-256 hash before and after
	Hash of acquired image logged	Record hash in chain-of-custody form immediately after acquisition
	Master File Table / journal (Windows)	$MFT, $LogFile, $UsnJrnl extracted for timeline analysis
	Prefetch / Amcache / Shimcache (Windows)	Evidence of program execution history
	Browser history and downloads	Chrome/Edge/Firefox history, download, and cache databases

	Registry hives (Windows)	SYSTEM, SOFTWARE, SAM, NTUSER.DAT, SECURITY
	Scheduled tasks / cron jobs	schtasks /query /v (Win); crontab -l, /etc/cron* (Linux)

4. Log Sources

	Log Source	Retention Priority
	Windows Security/System/Application Event Logs	Export as .evtx before rotation deletes relevant events
	Authentication logs (AD/Entra ID sign-in logs)	Especially 4624/4625/4648/4672/4768/4769 event IDs
	EDR/AV alert and telemetry history	Extend retention hold before automated purge
	Firewall and proxy logs	Include allow AND deny/block entries around the incident window
	DNS query logs	Reveals C2 domain resolution and beaconing patterns
	DHCP lease logs	Maps IP-to-host/MAC over time — critical if DHCP leases rotate
	VPN / remote access logs	Session start/end times, source IPs, MFA status
	Cloud provider audit logs (CloudTrail / Azure Activity / GCP Audit)	Export before default retention window expires
	Email gateway logs	Original phishing message headers, attachments, sender infrastructure

5. Network Evidence

	Evidence Type	Notes
	Full packet capture (PCAP) if available	From TAP/SPAN port or NDR/IDS sensor covering the incident window
	NetFlow/sFlow records	Useful when full PCAP isn't available — shows connection metadata at scale
	Proxy/web filtering logs	URLs, categories, and data volume for outbound connections
	Identified C2 IPs/domains documented	With first-seen/last-seen timestamps and source hosts

6. Chain of Custody

	Requirement	Confirmed
	Every item logged with: description, source system, collector name, date/time, hash value	
	Evidence transferred only with signed hand-off (from/to, date/time, reason)	
	Evidence storage is access-controlled and logged	
	Original media preserved unmodified; all analysis performed on verified copies	

	Hash values re-verified before any evidence is presented or shared externally	