CYBER GUIDELINE DOCUMENT

NCSP Digital Forensic Readiness

ABSTRACT:
This guideline provides information on how to preserve the integrity of digital evidence which supports the investigation cyber incidents.

APPENDIX A: If none, please delete

ISSUED	May 2025
PLANNED REVIEW DATE	May 2026
DISTRIBUTION	Community Security Policy Framework Members

POLICY VALIDITY STATEMENT
This guideline is due for review on the date shown above. After this date, this document may become invalid.

Cyber guideline users should ensure that they are consulting the currently valid version of the documentation.

Contents

Community Security Policy Commitment

National Policing and its community members recognise that threats to policing information assets present significant risk to policing operations. National Policing and its community members are committed to managing information security and risk and maintaining an appropriate response to current and emerging threats, as an enabling mechanism for policing to achieve its operational objectives whilst preserving life, property, and civil liberties.

This guidance in conjunction with the National Policing Community Security Policy Framework and associated documents sets out National Policing requirements for cyber incident management.

Summary

Digital forensics is a form of forensic science that can enable a thorough investigation to identify, acquire, analyse and report on electronically stored data.

Digital forensic readiness sets out the guidelines on how to carry out digital forensics in the event of a cyber incident and preserve integrity of digital evidence.

The ability to safely and reliably collect digital evidence in the early stages of an incident is vital to the success of any potential law enforcement investigation into the incident. Any data collected can then be handed over for a thorough investigation by specialist digital forensic experts and used in court alongside other provided evidence.

Even where no criminal charges are likely or possible, the learning that can be gained from a digital forensic examination, could greatly improve the resilience of the system post-incident.

The readiness aspect is to ensure that the collection and handling of digital evidence in the first instance is conducted correctly so that it provides value to a cybercrime investigation.

This document should be discussed with local specialist forensic investigators such as local digital crime units, Regional Organised Crime Units (ROCUs.)

Owner

National Chief Information Security Officer (NCISO).

Audience

The guidance is aimed at: -

- Information Security Officers (ISO)
- Senior Information Risk Owners (SIRO)
- Gold, Silver and Bronze Commanders who may be involved in cyber incident response
- Digital, Data & Technology or ICT managers
- Members of Cyber Incident Response teams
- Any role that requires an understanding of digital forensics and the processes required to collect digital evidence for any cyber incident, legal requirement and any ongoing investigation.

Purpose

Digital forensic readiness is essential in the effective response and management of cyber incidents. The purpose of the guidance is to describe measures to achieve forensic readiness. It outlines methods and processes to extract data from sources such as computers, smartphones, digital storage, data logs, and anything deemed pivotal to a digital forensic investigation which may be required to support a cyber incident response leading to a legal investigation and presentation at criminal court.

Having a tested digital forensic readiness policy in place, may act as a deterrent for potential computer crime as it increases the likelihood of a perpetrator being identified and prosecuted.

Cyber incidents have wide organisational impacts, it is important that forensics readiness is treated as a 'team effort' working with Information Security Officers, ICT (DDaT) teams, local or regional digital forensic units and Legal. These teams may already exist in the form of Cyber Incident Response or Computer Emergency Response Teams (CIRTs and CERTs).

During a major or critical cyber security incident, Forces will likely engage with external cyber incident response specialist teams, such as the National Crime Agency (NCA). The effective preservation of digital artefacts will be expected and will assist with any response, investigation and recovery.

Where appropriate and where possible, digital forensic artefacts will be crucial to any criminal proceedings that are undertaken. In the case of a cyber incident, live forensics, data captured as soon as possible after discovery of the incident, will be particularly valuable.

Scope

This guidance is applicable during the design, development, operation and decommissioning of any system that processes, accesses or holds policing information assets. This guideline and subsequent

operating procedures will form part of the Cyber Incident Response Plans and be utilised by local Cyber Incident Response Teams.

Digital Forensic Readiness Scenarios

Digital artefacts will be required to support intelligence and evidence gathering for events that lead to an actual or suspected cyber incident. It is also required for any investigation into employment, contractual legal disputes and criminal activity, which all potentially lead to a negative impact.

Listed below are examples of incidents that might require a digital forensics response: -

- Frauds perpetrated by employees or third parties
- Contractual disputes
- Allegations of breach of duty of care
- Email and Internet abuse
- Online defamation
- Employee disputes
- Sexual harassment
- Acquisition and storage any material that is a serious breach of professional standards
- Acquisition and storage of child abuse material or any other material that is illegal to possess
- Theft of confidential data, data theft and industrial espionage
- Theft of source code and software piracy
- Unauthorised access by employees
- Unauthorised access by outsiders (“hacking”) and unauthorised data modification (viruses, Trojan horses, etc.)
- Theft of corporate computer resources for private exploitation
- Abuse of communications devices
- Use of corporate computer resources to facilitate file-sharing which violates third-party intellectual property rights or are obscene or indecent
- Use of corporate computer resources as one stage in a complex criminal act and where a third party is the intended victim
- Failure of a computer system, causing damage to third parties and giving rise to legal claims for breach of contract or in negligence
- Failure of a computer system such that the Department wishes to sue suppliers for breach of contract
- Extortion attempts, whether based on physical threats or logical attacks such as distributed ransomware
- “Phishing”, where someone is induced to give away important confidential information to a fake website
- Denial of service attacks
- Ideologically motivated attacks intended to damage operational capability or policing systems

- Insurance claims arising out of the above

The table below shows categories of incident types: -

Activity	Incident
Cyber Security Incident	DoS (Denial of service), Malware attacks, Virus, Trojan, Worms, Tampering, Unauthorised access
Criminal Activity	Fraud, Blackmail, Harassment, Deception, Threats
Disciplinary Dispute	Grievance, Misconduct, Negligence, Performance Management
Privacy	Identity theft, Breach of data protection, Unauthorised sharing of personal data.
Intellectual Property Theft	Unauthorised use of media, Unauthorised use of software, Commercial disputes, Licensing disputes.

Preparing for Digital Forensic Activities

System owners should plan to conduct digital forensic activities as part of their response to a cyber incident. Some of the considerations that will inform this strategy are contained in the various sections of this document below.

Legal and Policy Considerations	• Standards for evidential collection will be higher where criminal proceedings are being brought. • Ensure compliance with policies/laws/regulations for data collected. • Authority to collect data from third-party owned systems.
Technical and Infrastructure Considerations	• Will there be a need to physically interact with devices that are offsite? • How will work be conducted if that link is down? • What mechanisms exist to preserve and collect Cloud logs if the connection is down? • Will there be domain administrators who can facilitate access (and required credentials) to enable data collections?
Logistical Considerations	• What out of hours coverage is there if an incident happens outside of core working hours? • Will anyone else be needed to gain physical access to servers, network devices etc? • What Service Level Agreements exist for systems where third parties will be required to collect data? • Responders will need basic tools ready to deploy. Is there somewhere to store these securely until required? • Is there somewhere to store items securely pending submission to digital forensic units?

Testing the digital forensic response is an important activity for any process which will be enacted in the event of a cyber incident.

Legal and Contractual Considerations

When collecting any type of evidence in the support of an incident it must be carried out with the correct legal authority to avoid any additional disputes.

Where arrests are made, police powers can form the authority for seizure and examination of certain devices. Internal user agreements may form the authority for examination of corporate devices that may also contain data belonging to users.

When conducting data collection from computers, servers and mobile devices, it is typical that all, or all accessible data will be captured. This is normal practice as it is not clear before reviewing any data, where material of relevance to the case will be found. User data that is later discovered to be of interest, may also be reliant on other data to provide provenance.

At the reviewing stage, it is normally possible to minimise the data that will be reviewed. Digital forensic units will have experience in doing this but will need direction concerning what data the examination should focus on. This is where a tasking form to the digital forensic unit will be important.

The impact of collecting any evidence might impact published and agreed Service Level Agreements, will require consideration when choosing a forensic strategy.

When investigating a cyber incident on a system that is not owned or managed by policing, there are concerns that the third-party will refuse to cooperate with policing. Contract managers should be consulted prior to the creation of any forensic strategy to establish any existing contractual agreements relating to cyber incidents.

Terms and conditions of the contract may stipulate actions that will take place in the event of a cyber incident on these systems. Cooperation with these third parties could determine the success of any digital forensic investigation.

In the event system owners do not envisage using local or regional digital forensic units, other than for advice, consideration needs to be given to who will conduct the forensic investigation in the event of a cyber incident.

Many private companies provide incident response and digital investigations on government systems and have SC and potentially even DV vetted staff. The strategy should consider how those parties will be engaged as the initial or whole provider of forensic services in the event of a cyber incident. Liaison with local Purchasing teams may be required to avoid any contractual disputes around the awarding of work to a company who may not be on an approved supplier list.

Engagement with Digital Forensic Units

Local and regional digital forensic units will have significant workloads, where waiting times of months are commonplace, before devices are examined for most crime types. Limited capacity will exist to accept urgent and critical cases in accordance with local and regional policies.

When engaging with the digital forensic unit, it will be important to determine their level of capacity to support an investigation into a cyber incident of police systems. Consideration should be given to their capacity and ability to support the live evidential collection phase, prior to submission of exhibits, and their capacity and ability to support investigations of a cyber nature.

It is strongly recommended that system owners discuss potential needs with their local or regional digital forensic unit to determine capacity and expertise availability.

Where local or regional digital forensic units will undertake the examination work, they might prefer, or insist upon conducting the live forensics element, so that it complies with their internal processes and ensures they have obtained the data they would require during the examination stage.

In some situations, for example where the system compromise was carried out by an inside threat actor, the constabulary may request assistance from a neighbouring constabulary. This could be for reasons of conflicts of interest that might exist.

This approach may also be needed if the complexity of the investigation might exceed the resources and expertise available locally. Engagement and the creation of a Memorandum of Understanding is recommended for these situations.

To understand some of the processes that exist in digital forensics units, a 'Level' of Digital Forensic Capture table has been created (shown on the following page): -

Examination Level	Definition	Specifics
Level 1	Logical capture of data from a device	Kiosk downloads of a mobile devices Logical images of storage drives including groups of files/folders Includes live forensics
Level 2	Capture of a device using mainstream tools	Capture of mobile devices using mainstream tools Forensic images of whole storage device(s)
Level 3	Advanced capture tools	Specialist mobile device tools requiring additional costings/licences Advanced recovery techniques from storage devices Includes 'chip off' examinations

The availability of resource and tooling to capture data from devices/sources of interest may vary from one digital forensic unit to another. A general rule of thumb will be that captures at Level 1 will be available more quickly than at level 2 and Level 3. Specialist tools might not be available at all within the Digital Forensic Units of some smaller constabularies.

As we move towards more advanced capture methods, the cost of capture generally becomes higher, with specialist licencing or equipment required. In addition, more advanced captures typically capture more data, meaning more data to analyse, which may increase the analysis and reporting costs.

Consideration should be given to the severity of the incident when considering proportionate costs of capture and analysis.

As part of requirements set by the Forensic Science Regulator (FSR), Digital Forensic Units are required to work to ISO 17025 standards and comply with a Code of Practice, created by the FSR. Any work where data will be used for criminal prosecution will be conducted in accordance with approved processes.

Discovery and Verification of the Incident

Discovery might come via several different potential sources, including from the National Management Centre (NMC).

Upon discovery of an incident, the first step will be to verify the incident and establish the severity. The severity will inform the recovery strategy required and may influence the extent to which capturing data for digital forensic analysis will be incorporated.

The source of the attack might also impact the extent to which digital forensics is deployed. Evidence that an attack originated from abroad, versus an inside threat actor, will determine the prospect of criminal proceedings being a potential outcome.

Where the discovery was made internally, (for example suspicious activity was reported directly by a user), this should be reported to the NMC.

Sources of Potential Evidence

The table on the following page shows a list of systems, devices and data types, which might form part of the collection strategy in the event of an incident. This is not an exhaustive list, and neither is the list of 'Forensic Opportunities', i.e. what the collection of data from a given source might contain in terms of value to the investigation: -

Source Type	Reason for Examination	Forensic Opportunities	Source Ownership/Location
Industrial Control Systems (For example an AC system at a police data centre)	Often rely on older software and can be an easier target for attackers than the actual IT systems. In some cases, there may be very little other evidence if this was the target of the attack.	Can be limited in terms of data stored and may require assistance from the manufacturer or the other specialists. Many systems rely on older versions of common operating systems and will therefore include access logs, configuration settings and so forth.	System may not be owned by police. May not be held in police buildings even if owned. Engagement with third parties may be required to obtain data.
Servers	A good source of evidence in cases of unauthorised use by insider threats. Potential evidence of changed state of devices following attack. May be attempting to talk back to the attacker. Different server types will collectively store large quantity of artefacts of system use.	File access histories. Logs, including system and application. User account status and histories. Network activity/settings. Configuration settings. May contain email/MS Teams. May contain user internet histories. Databases -including access/change logs	May be at offsite or third-party data centres but are police owned. Might be offsite and not police owned. Might be Cloud based servers with differing levels of data that can be obtained for examination. In the case of Cloud servers, the management or control of the server might sit with the cloud provider.

Removable storage	May have been used as the method of payload. May contain recoverable 'other' data showing owner/user of storage device.	Potential means to match the removable storage to one or more computers (to which it had been attached). May contain copies of malware.	Potentially unknown if found in the workplace. Examination could determine ownership/usage. If seized from the suspect post arrest, would have been under PACE powers.
Corporate computers	May contain local evidence of unauthorised use by inside threat actors. Potential evidence of changed state of devices following attack. May be attempting to talk back to the attacker.	Logs, including system and file access, and application logs. Some 'Thin' client systems may store very little data locally.	May be owned by a third-party IT provider. May be owned/controlled by police.
Standalone or non-corporate computers	Devices not connecting to official systems may have been easier targets for attack. Inside threat actors may have used non-corporate systems to compromise corporate ones.	Being less 'locked down' than corporate systems, may contain a much broader range of artefacts including: - Internet histories. Email/Chat. File/folder access. Installed tools.	Potentially corporate devices but are not connected to networks. May be owned by third parties. Ownership might not be known.

Corporate mobile devices	If synchronised with corporate systems, may contain similar data to the computers.	May contain everything the corporate computer does might also contain records of calls, SMS etc. Likely to additionally contain location data.	May be owned/managed by a third-party IT provider. May be owned/controlled by police.
Standalone or non-corporate mobile devices	Devices not connecting to official systems may have been easy targets for attack.	Internet histories. Location data Chat/Calls/Messaging May contain emails May contain other apps with data of interest.	Potentially corporate devices but are provided for custom uses. May be owned by third parties. Ownership might not be known.
Firewalls	Will contain significant artefacts of interest in cases of system compromise. May contain logs showing individual user attempts to access blocked resources.	Connection logs. Blocked traffic. VPN connection logs. Configuration settings, including rules and changes made. Policy violations such as unusual hours, site accesses etc.	Will be corporately owned or supported. Administrative access to obtain data might require cooperation of third-party providers. Could include Cloud based firewalls.
Routers and Managed switches	Likely to contain some beneficial artefacts	Port status (on/off etc) Routing tables	Will be corporately owned or supported. Administrative access to obtain data might require cooperation of third-party providers

Intrusion protection and detection devices	Will contain significant logs showing discovery and blocking of suspicious activity.	Detection logs Logs of blocked ports or other activity.	Will be corporately owned or supported. Administrative access to obtain data might require cooperation of third-party providers
Printers and fax machines	Larger printers will have internal storage.	There is potential to recover data from internal memory Potentially there will be logs of access and use	Will be corporately owned or supported. Administrative access to obtain data might require cooperation of third-party providers
Backups	The system may have been compromised for some time. The evidence of compromised might be amongst offline backups. Evidence of wrongdoing in the case of inside threat actors, may be in offline backups. The last 'good' state of the system might be in offline backups only.	Backups may be of systems in a good state, which could be restored and used for comparison to the current compromised state. Older data may contain evidence of wrongdoing by an inside threat actor. Evidence of original compromise may be in offline backups. Any static malware analysis may require restoration of backups.	Backups will be run and owned by the unit who run this system, this may or may not be policing, depending on the system. For restoration of data from the Cloud, there will likely be some charges based on quantity requiring restoration.
Suspect owned mobile devices	Evidence of planning including potential hostile reconnaissance.	Location history. Significant messaging and email artefacts. Internet histories.	Belongs to suspect and will typically be seized under PACE powers.

Suspect owned computers/servers	Suspect may have used own computers to develop or deploy malware. Evidence planning and execution of criminality. Evidence of researching alibi or implicating third party.	Presence of malware to be deployed. Evidence of researching attack process. Information about motivations, causes for conducting attack. Evidence of association with removable storage used in the compromise.	Belongs to suspect and will typically be seized under PACE powers.
SIEM events and logs from secondary logging servers	Reports may show first detection of suspicious activity and provide a timeline to map forensic artefacts against. Secondary logging servers might show discrepancy between these and primary network and server logs (which hackers edited).	IP addresses and ports showing unauthorised connection attempts. IP addresses and ports showing unauthorised exfiltration of data.	National Monitoring Centre (NMC). Locally managed logs and SOC/SIEM events. Third-party managed provider logs and SOC/SIEM. Cloud based logs and security events.
Open online resources	Suspect may have used openly available resources to conduct attacks. Suspect may have been ideologically motivated and posted comments online.	Online social media platforms may show ideologies. Websites may include downloadable malware and user guides.	May still require authority to collect despite being publicly available. May be appropriate to use OSINT trained staff on miss-attributable systems.

Private online resources	Suspect may have used online virtual machines to conduct criminality.	Collection of private data such as Google Takeout process would contain; internet searches, histories, location data, device association and usage and so forth.	May require additional legal authority to capture. May require evidential capture approach.
Other items – This could include anything that may be relevant to the case.	May have been used to leverage the attack, for example keylogging devices. May have been used to conduct hostile reconnaissance.	Very much depends on the item. May contain internal storage which can be captured and examined. May contain model numbers, serial numbers etc.	Items may belong to the suspect and would normally be seized under PACE powers. Items found may require examination to determine ownership/usage.

Live Forensics

Collection of data from the live system, or devices on that system can greatly improve the quantity and quality of data available to conduct later post-mortem analysis. The most critical data in the investigation of a cyber incident is often the live data.

The trade-off risk associated with collecting live forensics is that it may require leaving compromised systems up and running when a 'contain and eradicate' strategy is urgently applied. Options to collect live forensics and mitigate some of the risk could include blocking all traffic at the perimeter of the network, but permitting unauthorised activity to remain within the network until the required live data collection has completed.

The risk of losing valuable data from key devices by isolating them or 'pulling the plug' must be weighed against the risk of losing data elsewhere by allowing unauthorised activity to continue.

More robust and well tested Business Continuity and Disaster Recovery plans might allow greater flexibility in terms of collecting live data from key devices.

The capacity within digital forensic units will vary from one constabulary to another but it is very likely, expertise will exist in all of them to conduct live forensics, but there may be greater capacity and experience in larger constabularies, when conducting this work on corporate networks.

Dead-box Forensics

This guidance will not go into the details of the analysis and reporting of data but will mention two aspects of analysis specifically related to the investigation of cyber incidents. These are; Static and Dynamic malware analysis. These two different methods are characterised in the following way: -

Static Analysis	This relates to examination of malware without executing it. It is focussed on what the malware was written to do based upon code that is available to review.
Dynamic Analysis	This relates to running the malware in a controlled environment and observing what the malware does to that environment. This can provide much greater information than a static analysis. A forensic image of that environment can also be obtained and analysed.

It should be noted that the expertise to conduct these examination techniques may not exist in all digital forensic units. Expertise in Dynamic analysis is less prevalent than Static analysis.

Where the attack came from a state-sponsored group, it is likely the required expertise to examine such malware does not exist in mainstream policing, assuming it was detected in the first place!

Depending on the complexity and nature of the examination required, it might be necessary to provide the investigating digital forensic unit with system design documents, or other documentation, which will enable them to understand how the data they have relates to the activities on the system.

Forensic Activities Timeline

A potential timeline of data collection, alongside the containment, eradication and recovery phases has been mapped to illustrate how these might be done in conjunction with one another.

This is very high level and is intended to show how forensic collections can be included.

Verification of the Incident	Determine forensic strategy to be used. Begin documentation of actions/decisions. Record alerts and triggers. Establish timeline. Begin continuity of data/devices.
Containment Phase	RAM capture of relevant computers/servers. Capture screenshots, system times, system information. Collect other volatile data from relevant systems. Export logs from SIEM/log server. Manually collect logs from relevant systems. Logical imaging of relevant computers/servers including exporting copies of virtual servers. Preserve configurations of network devices.
Eradication Phase	Use collected data to validate scope of compromise. Link activity across devices. Continue logical acquisitions if appropriate. Analysis of data may help with eradication phase.
Recovery Phase	Analysis of data may help with recovery phase. Dead-box imaging of systems taken out of service. Consider inclusion of backups for examination. Create scope of forensic strategy for full examination. Create verified copy of all material for forensic examination.

Initial Response Activities

Some system owners may have the resources to conduct the initial digital forensics response in the event of a cyber incident. It is assumed that there will be sufficient understanding of the implications of conducting this work before it is undertaken. Where this is the case, this section outlines considerations and recommendations for that initial digital forensic response.

Where system owners do not have the necessary expertise, or capacity to conduct any initial digital forensics response, there will be a greater reliance on local or regional digital forensic units to provide this support. Digital forensic units are likely to recommend data collections, but this document could be used to agree on a strategy.

Where a third-party will conduct this work, discussions over the strategy to be used should be agreed.

Vital to all evidential collection, from any device where you are making changes (by interacting with it), is that contemporaneous notes of examination are maintained throughout. It is essential to ensure items can be identified, (perhaps by serial number), and include the time of all actions taken on that device. This will enable a digital forensic examiner to understand which changes were caused by the initial responder when conducting the later analysis.

Where artefacts are being collected via a 'harvest' USB storage drive, this should be a new or wiped drive with any tools that may be used already installed on it. Most collection tools run from the USB drive and do not require installation onto the computer from which you are collecting information.

USB storage devices, when connected to a computer, will create artefacts, including the manufacturer's Vendor ID (VID) and Product ID (PID). Mainstream branded USB drives will also have a unique serial number. This information could be collected from the harvest USB drive to be used in advance and recorded as part of the contemporaneous notes of examination. This ensures the digital forensic examination will identify which device(s) were used by the incident responders.

The contemporaneous notes of examination for network devices, will likely be different, but recording times of actions are still a critical element. Any logs/configurations collected might be transferred to a laptop, which would connect to the management interface of the network device.

In situations where one or more devices are to be removed from the system and retained for full forensic imaging, it should be clearly labelled and retained securely.

Consideration must also be given to protect any items retained from damage.

Any contemporaneous notes of examination should be retained and provided with any tasking form for examination for that/those devices.

The table on the following page lists several recommended and optional actions which might be appropriate for a range of device types. Not all actions might be appropriate in all circumstances and other actions not listed here might be appropriate in certain circumstances.

Device Type	Recommended Actions	Optional Actions
Computers/Workstations (epicentre of compromise or suspects' computer(s)	• Photograph accurate time source against screen showing clock. • RAM capture (onto USB storage) • Any open unsaved files saved onto USB storage)	• Collect running processes • Capture connected ports • Disconnect from network(s) • User activity logs • Browser history • Credential use (password dumping) • Endpoint detection logs • Registries (using dumping tool)
Corporate Servers	• Photograph accurate time source against screen showing clock. • Make contemporaneous notes of actions • System and Application logs • Collect running processes • Capture connected ports	• RAM capture (servers may contain very large amounts of RAM, so this may not be practicable) • File access histories • User account histories/activities (including use of user credential dumping commands)
Perimeter Firewalls	• Connection logs • Threat detection logs • VPN logs • Blocked traffic	• Rules list • NAT translations • Policy violations (out of normal hours activity etc) • Traffic metrics

Intrusion Detection/Prevention Systems	• Alert logs • Signature matches (known exploits) •	• Response action (blocked or not) • Protocol analysis (traffic types)
Managed Switches	• VLAN configurations • MAC address tables	• Port statistics

The choice of actions to be taken will depend on the circumstances being investigated and what devices might be relevant to investigate further.

When running data collection tools, it is very likely that local administrative privileges will be required. Where computers/workstations are logged into accounts with User level access, administrative credentials will be needed to run them.

In relation to servers, the table suggests initial actions that should or could be undertaken at the initial response stage. It might be that further collection will take place beyond that point, but it is important to consider that data collected much later, might be of limited use in terms of their forensic value.

When dealing with virtual servers, it might be possible checkpoint and export a copy of the server, which could be retained for later analysis. In such situations, this could offset the need for a larger amount of data collection at the initial response stage.

Servers often fulfil different functions, for example, authentication, internet proxy, email and so on. As such the types of data that might be important will differ from one to another. The table provides some general recommendations, but consideration should be given to incorporating a digital forensic strategy into the organisation's incident response playbook.

Regarding network devices, these are much more likely to have their logs and activities, continually replicated to a separate logging server, or even a staffed SOC/SIEM. Where there is confidence that collection processes have continued to operate as expected, this might offset the need to collect some of the data suggested in the previous table.

Understanding the Digital Forensic Lifecycle

The digital forensic process may differ from case to case, but the table on the following page describes activities that may take place from identification of devices of interest and live forensics, through to final reporting. Because this policy relates specifically to the examination of compromised systems, malware analysis as examination steps has been added.

Examination Stage	Practices/Functions	Practical Actions
Stage 1 – Control of devices and initial data collection	Identify devices in scope for examination	Determine items of interest and ensure continuity.
	Prevent changes to devices	Prevent changes could include placing phones into Flight Mode or attaching mouse jigglers to prevent computers going into hibernate
	Collect initial evidence	Collecting evidence may include RAM capture, collection of limited data from computer systems, collection of active network traffic or running processes. For network devices this could mean extraction of live logs, routing tables etc. Accuracy of device time should be established. Use of tools like Wireshark may be used to collect data from the network. Where devices cannot be removed from service, live acquisitions will be performed.
	Seize items safely	Seizing safely means recording locations of devices and ensuring seized items are protected from damage, recorded and secured for later analysis. In practice this is likely to be end user devices in most cases, and more so where the attack may have been an insider threat.

Stage 2 – Main data collection	Full forensic acquisitions Standard and enhanced mobile device acquisitions Collection of data from other sources	For seized computers, this will mean dead-box forensic imaging. For mobile devices this will mean download using kiosks or specialist tools. Extractions might include, logical, file system or physical downloads. Includes 'chip off' extractions. This may include the addition of logs from the NMC or other sources, collection of open online sources or from a wide range of other data sources that may be relevant.
Stage 3 – Ingestion and discovery	Data ingested into tools to allow data recovery, searching, file identification and classification. Creation of initial material for review. Ingestion of logs will allow reviewing of that material.	Forensic tooling will verify file types and determine known files (via hashing) that can be flagged as relevant or excluded from review. Artefacts will be decoded using tools that will enable assessment for relevance, potentially by non-technical persons but who understand the remit of the investigation. Logs are likely to be reviewed by specialist experts but could be overlaid to data from devices of interest.
Stage 4 – Detailed analysis	Detailed analysis of artefacts to determine provenance of items found to be of interest Analysis could include static analysis of malware Examination may establish what changes were made and how.	Detailed analysis of artefacts using forensic tools, including manually decoding and verifying data from discovery stage. Deconstruction of code to determine intended actions.

Stage 5 – Testing	This may not happen in all cases. Test devices may be seeded to create artefacts that can be matched to those in the case. This stage would also cover dynamic malware analysis. These tests might enhance the capacity to explain how changes were made to the system.	Sandbox environments created and test scenarios run to monitor changes made. This is followed by forensic analysis with test artefacts compared to data from the compromise. Monitoring of artificially infected sandbox systems can show outcomes of compromise.
Stage 6 - Reporting	Reports detailing findings of analysis. Statements and reports for charging to be produced.	Reports may be technical only, with the intention being learning around compromise. Statements and reports might include details of material which could be used to enable criminal charges.
Stage 7 – Additional analysis, reporting and disclosure	Where criminal charges are being brought, additional work will usually take place post interview. Disclosure work should happen throughout the lifecycle of the investigation once criminal charges are being considered.	Further statements and reports might be created following interview of defendants. Prior to the case going to trial, final reviewing of data for scheduling of unused material is completed.

Communication of Outcomes

There is potential for learning based upon the findings of the forensic examinations conducted. Where possible, reports, or at least executive summaries of reports should be shared with the National Management Centre (NMC). These results could inform future monitoring decisions.

Depending on the nature of the breach, the Information Commissioner's Office (ICO) may also be interested in the outcome of the investigation.

Communication Approach

This document will be communicated as follows:

- Internal peer review by the members of the National Cyber Policy & Standards Working Group (NCPSWG), which includes PDS and representatives from participating forces.
- Formal publication and external distribution to PDS community, police forces and associated bodies.

Measurables generated by adopting this guideline can also form part of regular cyber management reporting.

This guideline and associated local supporting policies and procedures should be communicated to all members of the cyber incident response team and any person who is likely to support investigations into cyber incidents.

It should also be shared with those responsible for bringing in new digital / ICT systems so that forensic readiness requirements can built into non-functional requirements.

Review Cycle

This guideline will be reviewed at least annually (from the date of publication) and following any major change to Information Assurance (IA) strategy, membership of the community, or an identified major change to the cyber threat landscape. This ensures IA requirements are reviewed and that the guideline continues to meet the objectives and strategies of the police service.

Document Compliance Requirements

(Adapt according to Force or PDS Policy needs.)

Equality Impact Assessment

(Adapt according to Force or PDS Policy needs.)

Document Information

Document Location

https://knowledgehub.group/web/national-standards/policing-standards

Revision History

Version	Author	Description	Date
0.1	PDS Cyber	Cyber Security Specialist	29/01/25
0.2	PDS Cyber	Cyber Specialist	09/04/25

Approvals

Version	Name	Role	Date
1.0	NCPSWG	National Cyber Policy & Standards Working Group	07/05/25

Document References

Document Name	Version	Date
ISF - Standard of Good Practice (for Information Security)	v2024	03/2024
ISO 27002:2022 - Information security, Cybersecurity and privacy protection – Information security controls	v2022	02/2022
CIS Controls	v8	05/2021
NIST Cyber Security Framework	v1.1	04/2018
CSA Cloud Controls Matrix	v4	01/2021
10 Steps to Cyber Security - NCSC.GOV.UK	Web Page	05/2021
Home Office Forensic readiness Policy	V 1.0	11/2024