Guidance on Non-routine Offsite Forensic Examination of Digital/Multimedia Evidence

Prepared by
OSAC Digital and Multimedia Scientific Area Committee

Published July 1, 2020

EXECUTIVE SUMMARY

The emergence of the COVID-19 has led to the implementation of social distancing, travel restrictions, and closure of non-essential facilities. To address these constraints, many organizations have implemented teleworking strategies. Individual organizations have varying abilities and resources to support remote operation and must carefully assess the associated risks. Remote processing is not appropriate for many forensic disciplines but can be feasible for the examination of digital/multimedia evidence. The forensic duplication of digital evidence helps to maintain evidence integrity while permitting remote analysis of working copies.. Encryption, virtual private networks (VPN), Remote Desktop Services (RDS), cloud computing, and secure file transfers can support a secure remote examination environment.

This document provides information on the background, risk mitigation tactics, nonroutine offsite options, and additional considerations for the forensic examination of unclassified forensic digital/multimedia evidence.

BACKGROUND

On March 11, 2020, the World Health Organization (WHO) characterized the COVID-19 outbreak as a pandemic. With the unprecedented impact of COVID-19 on day-to-day interactions, there is a need to address how to maintain a continuity of forensic examination services under such circumstances. Restrictions, such as stay-at-home or shelter-in-place orders, may require a change in how forensic analyses are conducted. To ensure the health and well-being of examiners, as well as the community as a whole, forensic organizations must be aware of strategies and options that reduce the risk of exposure to personnel on-site and for work to be conducted remotely in a secure manner.

In any teleworking situation, supervisors must balance productivity with management decisions such as the mental and physical health of their employees, work prioritization, security requirements, and resource allocation. These considerations are magnified in forensic exams where sensitive data, government regulations, and legal implications significantly impact the work being performed. Additionally, the extraordinary circumstances surrounding the COVID-19 pandemic require a thoughtful review of standard laboratory policies and procedures.

Unique Nature of Digital/Multimedia Evidence

In general, forensic sciences do not allow for working remotely. However, the ability to forensically duplicate[1] digital/multimedia evidence, in accordance with best practices, makes remote examinations possible. Because the integrity and confidentiality of the evidence are paramount, a number of factors must be taken into consideration prior to engaging in case-related work outside a typical forensic setting. Standard practice generally requires original digital/multimedia evidence be re-created as a working copy to maintain the integrity of the original evidence. This working copy is substantively identical to the original and allows the ability to conduct the work in a forensically sound manner. This practice provides digital and multimedia forensics with a unique opportunity over other disciplines that require analysis of the original evidence. The ability for an examiner to conduct an examination without physical proximity to the original evidence, as well as the availability of encryption and Remote Desktop Services, facilitate the secure remote processing of digital/multimedia evidence. While this guidance is focused on Digital/Multimedia Forensics, other disciplines may consider the tactics and workflow presented here. It is imperative that practitioners consider the issues outlined in this document as well as factors that may be unique to their disciplines.

Every organization will have varying abilities and resources to support the remote examination of digital/multimedia evidence. As adjustments to existing processes are made to accommodate telework, organizations must assess the logistics of remote examinations of digital/multimedia evidence including the costs, benefits, legal considerations, health and safety requirements, security requirements, and stakeholders' issues. Leadership within each organization must evaluate their requirements for any types of examinations that are conducted. Policies and procedures should continue to be followed. These documents must also be evaluated to determine if modifications would be beneficial for the support of remote examinations. The budget and technology of an organization will also impact the feasibility or the implementation of any type of remote examination of evidence.

RISK MITIGATION

Contingency plans can introduce potential risks to confidentiality, integrity and fidelity to digital/multimedia forensic examinations. These risks can be mitigated by actions already implemented in an existing management system. The ISO/IEC 17025:2017 General Requirements for the Competence of Testing and Calibration Laboratories international

[1] A **Forensic Duplicate** is a file that contains every bit of information from the source, in a raw bitstream format. (http://www.cse.scu.edu/~tschwarz/coen152_05/Lectures/HDDuplication.html)

standard provides general criteria that are applied to the development of these systems. While the entirety of this standard should be considered as practices transition to accommodate telework, key sections of interest include those that provide direction on confidentiality, facilities and environmental conditions, equipment, test item handling, and actions to address risks and opportunities[2]. Likewise, following best practices and standards published by organizations such as the Scientific Working Group on Digital Evidence (SWGDE), Facial Identification Scientific Working Group (FISWG), and ASTM International, provides an additional layer of risk mitigation[3]. For example, using a working copy during an examination ensures the evidence remains unchanged and available for review.

The examples herein do not address all potential risks or the only approaches available to mitigate these issues but offer possible considerations. Additionally, the details below are not intended to promote a specific course of action for the sub-disciplines listed, as mitigation tactics are dependent on many unique variables.

Risk Mitigation: Security

Baseline information security parameters must be determined before forensic examinations can occur in a telework environment. These considerations include physical access controls for the remote location, network security, and determination of what devices are allowed to access the information. NIST’s Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security provides direction for mitigating risks to support confidentiality, integrity, and the availability of enterprise information and resources[4]. Organizational policies and procedures should ensure these objectives are met and should outline which forms of remote access are permitted, the access levels granted to various users, and account provisioning. However, it is strongly recommended that personal devices never be used for forensic examinations due to the difficulties involved in maintaining an approved forensic workstation configuration outside of the enterprise environment. Examination data must never pass unprotected through unsecured networks. To the extent possible, organizations should leverage existing telework policies to determine specific technical requirements for secure remote examinations. The use of enterprise supplied devices and equipment via a secure connection is promoted throughout this Organization of Scientific Area Committees for Forensic Science (OSAC) guidance document.

[2] See Sections 4.2.4, 6.3.5, 6.4.1, 7.4.1 and 8.5.1 of ISO/IEC 17025:2017(E) for additional information.

[3] There are many best practices and standards that outline the use of a working copy. For example, see ASTM’s Standard Guide for Forensic Digital Image Processing and Standard Practice for Examining Magnetic Card Readers.

[4] NIST’s Guide to Enterprise Telework, Remote Access and BYOD Security defines the objective of confidentiality as ensuring data cannot be read by unauthorized parties; integrity as detecting any changes to communications that occur in transit; and availability as ensuring authorized users can access resources.

Risk Mitigation: Testing Tools and Techniques

Knowing potential limitations related to any tools or equipment introduced in the selected strategy is crucial. SWGDE's Minimum Requirements for Testing Tools used in Digital and Multimedia Forensics states, "Testing…can establish confidence that a tool or procedure performs correctly to reduce the risk of errors." Digital/Multimedia practitioners must determine if the implementation of the techniques (for example, software or hardware tools) are correct and appropriate for the environment where they are used[5].

While testing can help identify potential limitations introduced by a contingency plan, practitioners should also consider if additional function tests (controls) are necessary during the course of telework. These function tests can be modeled similarly to the initial limitations test[6].

Risk Mitigation: Environmental Conditions

Because of the sensitivity and confidentiality of the data, forensic examinations must not be conducted in public or open areas where incidental observation is possible. Examiners must conduct their work in a private space under their constant control. In multi-person households, teleworkers should avoid shared or common space that may be accessible by other residents. At a minimum, the space must have reasonable controls (e.g. privacy locks, doors, window shades or curtains, etc.) to mitigate the possibility of incidental exposure and maintain confidentiality of case-related data. Data protection requirements also may require the use of secure storage (e.g. lockers, safes, etc.) for protecting working copies of data and work products.

When specific equipment and environmental conditions are required for proper video, image, and audio analysis, these requirements must be maintained when conducting telework. In order to maintain a consistent examination environment between the organization and a remote location, several factors should be considered to obtain results consistent with those observed at the host agency:

- Standard workstation configurations utilized by a host organization should be considered when configuring remote workstations. Specific requirements may include the following:
    - Compatibility of applications and software versions for remote examinations
    - Interfaces for importing and exporting work products (e.g. USB thumb drives for forensic copies of evidence, optical drives, etc.)
    - Approved anti-virus (AV) software, if appropriate. For example, digital forensic examinations may involve activities incompatible with the presence of AV software
    - Timely updates to software delivered via offline methods

[5] See ASTM E3016-18 Standard Guide for Establishing Confidence in Digital and Multimedia Evidence Forensic Results by Error Mitigation Analysis.

[6] SWGDE's Minimum Requirements for Testing Tools used in Digital and Multimedia Forensics provides a framework that can be applied to testing tools or equipment not listed within that document.

    - Software for digital evidence preservation, such as hashing and validation utilities
- Audio workstations may require additional equipment or software to support remote examinations:
    - Sufficient quality audio reproduction equipment such as high-fidelity sound cards, speakers, and headphones
    - Video monitor suitable for viewing waveforms, spectrographs, etc.
    - Software tools for tasks such as audio enhancement, speaker recognition, etc.
- Video and image analysis workstations may require additional equipment or software to support remote examinations
    - High quality video cards and cabling
    - Appropriate video monitor size and quality
    - Software tools for tasks such as image enhancement, facial recognition, etc.
- Work environments should be configured appropriately for examination activities:
    - Audio examinations require a quiet environment with acoustic isolation from nearby activities.
    - Video and image analysis may require controlled lighting conditions such as illumination levels, color balance, and light-diffusing (i.e. non-glare) surfaces. External light sources (e.g. sunlight, adjacent areas, etc.) which vary the operational environment lighting should be eliminated so that lighting is consistent during the course of the work period.

Options for Non-routine Offsite Forensic Examinations

Organizations that perform examinations on digital/multimedia evidence have several options to consider when developing contingency plans for telework. The chosen course of action should be based on applicable variables such as the types of examinations performed, available equipment or technology, and established policies and procedures. Finalized contingency plans may vastly differ across federal, state, local, and private entities. For example, while one organization may approve of examinations performed through remote desktop connections, another may opt for the transport of an encrypted data copy.

Accessing Remote Workstations

Given today's technology options, teleworkers can access remote workstations through a secure connection using organization provided equipment. Remote connections provide access to approved resources residing within the physical confines of the laboratory. Teleworkers (practitioners) must continue to ensure their space is secure and computers are locked when not in use.

Supervisors should look to their organizations' policies regarding the issuance, configuration and maintenance of equipment. At a minimum, computers and storage media used to remotely access the network and conduct analysis should require authentication and data at rest must be protected in accordance with organizational standards.

Internet access speeds may significantly impact the efficacy of a digital/multimedia forensic exam when using secure remote connections. For example, multimedia playback quality can be greatly impacted through a slow remote desktop connection. It is important to test both the reliability and the capacity of available bandwidth across different processes to establish minimum standards prior to conducting casework and assess how limitations can be mitigated.

Forensic audio examiners must be able to sufficiently evaluate the signal characteristics of a recording both aurally and through measurement. It is important to distinguish distortions in the source audio from those occurring due to transmission or audio playback at the remote computer. Additional considerations may apply if the initial evaluation meets these standards:

- Forensic audio examiners should characterize remote signal quality in case notes when remote listening is used as part of the analysis process to ensure decisions are documented and traceable.
- If the remote connection causes too much distortion to reliably review audio material, the file should be copied to the local computer for reviewing purposes.
- Any filtering must be performed on the source audio.

Forensic video and image examiners must be able to sufficiently evaluate the video/image content without suffering reduced quality due to poor playback of video, possible delays while processing images, and the potential risk of erroneous opinions if the details necessary for content analysis or comparisons are not observable. Testing the processing techniques used through remote connections prior to casework will help examiners to evaluate possible impacts to the examination. The examiner must also be aware of inconsistent network conditions that can affect the forensic examination. Tactics such as reviewing a file on a local device, advancing the video frame by frame, or batch processing could be applied if not in conflict with existing policy and procedure.

More rigorous testing is necessary to assess the impact of using a remote desktop connection to view the fine detail present in evidentiary imagery and should include performance under various remote connection settings. If an examiner is able to detect a difference between an image viewed on a local computer and an image viewed remotely that will impact the examination, then remediation will be necessary prior to continuing. Additional considerations, such as those listed below, may apply if the initial evaluation meets these standards.

- Visually examine a sample of images individually on a local device and RDS to determine if details required to perform the examination are affected by viewing remotely.
- If the remote viewing has a negative effect, discontinue the examination, and notify appropriate management. If no negative effect is observed, document this function test and the results in the case notes, and proceed with the examination.
- Examiners performing work through remote desktop connection must be cognizant of the remote desktop settings as well as aware that connection speed can affect the speed at which the full resolution image is displayed in the remote desktop interface.

Offline Examinations Conducted at a Telework Location

Organizations that do not have the technical infrastructure or policy framework in place for remote desktop access can implement an off-line solution to ensure continuity of operations. In this instance, a standalone forensic workstation should be issued to examiners and corresponding case information should be loaded separately onto portable drives and verified according to procedures. Organizations should look to their existing information security policies for remote work (e.g. encryption schemes, encryption at rest, account authentication, etc.).

Additionally, organizations should consider the following:

- To avoid the possibility of commingling evidence between cases, associated or derived data, case notes, reports, and exhibits created should be copied directly to the portable drive. Upon case completion, the drive must be transported back to the laboratory as soon as practicable.
- Staff required to be onsite for other reasons can be designated to receive the drive, copy the contents to the examination network, and sanitize the portable drive.
- A wiping protocol must be in place to sanitize residual from the drive prior to reuse. Onsite employees can also load new cases waiting to be analyzed on portable drives for pickup by teleworking examiners.
- Protective policies should be implemented to physically disinfect items distributed or received from the laboratory.
- Organizations should consider using courier pouches for transporting drives between the laboratory and the telework location.
- Organizations must comply with their own policies for handling transportable media and documenting the transit of derivative case data. Original evidence should not be transported to the telework location.

Cloud Computing

Cloud computing models approved for use by the organization may offer additional advantages for the teleworker over traditional methods. The use of cloud solutions can prevent the loss or damage of physical storage devices, working copies, and work products during transport or home storage. The use of this technology provides both the organization and the teleworker with assurances in tracking digital evidence through audit logs, transparency on access of information, ability to restrict access to others, immediate synchronization of information, and access of information without the need of physical storage. Depending on the vendor, the technology may allow for video and audio processing services, examination tools, and provide additional computing power through cloud service models (e.g., Software as a Service, Platform as a Service, Infrastructure as a Service models). Cloud technology may offer the teleworker the ability to collect digital evidence, receive submissions, and share work products more efficiently during stay-at-home or shelter in place restrictions. Cloud computing models provide many advantages over traditional computing and storage models. Nevertheless, it is important for teleworkers to use cloud solutions that meet organizational information security requirements that are in compliance with Federal, State, and local ordinances.

Considerations for cloud computing go beyond the scope of this document. Further information can be found in NIST Special Publication 800-144 Guidelines on Security and Privacy in Public Cloud Computing and NIST Special Publication 500-299 Cloud Computing Security Reference Architecture.

Secure File Transfer

A type of secure file transfer system that an organization may use is the Secure File Transfer Protocol (SFTP). This type of file transfer system relies on a Secure Shell (SSH), which provides a secure channel over an unsecured network. A file transfer system like this is helpful when the sender or the receiver has unstable connections. The system is set up to verify that the sender and the receiver are both authenticated and secured. It then sends the file(s) in an encrypted message allowing for both unclassified and sensitive information to be transferred securely. Other secure file transfer options exist, and should be evaluated to ensure the files are properly encrypted.

ADDITIONAL CONSIDERATIONS

In addition to the aspects above, the following issues should also be considered.

Health and Wellbeing of Onsite Personnel

Submitted physical evidence requires that some staff remain onsite. For scenarios where remote processing of evidence is not feasible, enhanced hygiene and cleaning practices, establishing a quarantine period for packages, and providing personal protective equipment (e.g. masks, gloves, etc.) can mitigate risk. Additionally, organizations should maximize alternate or compressed work schedules with staggered shifts to facilitate social distancing of onsite personnel while balancing productivity.[7]

Forensic Examination Contents

Laboratories that regularly process criminal casework must address the possibility of contraband outside the work environment when forensic examiners telework. Organizations should develop their own policies on handling this situation and to the extent possible, address legal considerations with their legal counsel's office. Depending on state and federal regulations and organizational policies, the content of some digital/multimedia examinations may not be suitable for telework activities.

[7] Additional considerations are outlined in NWC3's guidance titled Coronavirus and Law Enforcement.

Software Licensing

Digital/Multimedia Forensics is reliant on commercial software. Over the past decade, many organizations have transitioned from single-user to network-based licensing, which may present problems when examiners work offline. Managers should identify contingency plans when licenses can be issued. Several forensic software providers have licensing schemes that support telework and other virtual evidence processing arrangements.

Policies and Procedures

Quality manuals may need to be updated, as appropriate, to encompass conducting examinations from an offsite location. References to specific physical locations currently written into a laboratory manual should be revised to allow for the location of a teleworker.

In addition, revised guidance should be provided to both supervisors and examiners with respect to how cases should be assigned, how often updates are to be provided, and the manner in which the work should be monitored. For example, supervisors can ask that examiners provide their examination notes on a periodic basis.

REFERENCES

ASTM Standard E2916-13, “Standard Terminology for Digital and Multimedia Evidence Examination,” ASTM International West Conshohocken, PA 2018, https://www.astm.org/Standards/E2916.htm.

ASTM Standard E3016-18, “Standard Guide for Establishing Confidence in Digital and Multimedia Evidence Forensic Results by Error Mitigation Analysis,” ASTM International West Conshohocken, PA 2018, https://www.astm.org/Standards/E3016.htm.

ASTM Standard E3017-19, “Standard Practice for Examining Magnetic Card Readers,” ASTM International West Conshohocken, PA 2018, https://www.astm.org/Standards/E3017.htm.

ASTM Standard E2825-19, “Standard Guide for Forensic Digital Image Processing,” ASTM International West Conshohocken, PA 2018, https://www.astm.org/Standards/E2825.htm.

International Organization for Standardization. (2017). “General Requirements for the Competence of Testing and Calibration Laboratories,” (ISO/IEC 17025), www.iso.org.

National Institute of Standards and Technology, Special Publication (2016). Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security 800-46rv (Department of Commerce, Washington, D.C.). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf

National Institute of Standards and Technology, Special Publication (2011). Guidelines on Security and Privacy in Public Cloud Computing 800-144 (Department of Commerce, Washington, D.C.). https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

National Institute of Standards and Technology, Special Publication (DRAFT). Cloud Computing Reference Architecture 500-299 (Department of Commerce, Washington D.C.). https://bigdatawg.nist.gov/_uploadfiles/M0007_v1_3376532289.pdf

National White Collar Crime Center. (2020). “Coronavirus and Law Enforcement,” nw3c.org.

Scientific Working Group on Digital Evidence. (2018). “Minimum Requirements for Testing Tools used in Digital and Multimedia Forensics,” www.swgde.org.