A NATIONAL CYBER CENTER

DC3

Defense Cyber Crime Center
Air Force Office of Special Investigations

Data Tape, Log File, and Multimedia Submission Tips

Tips for submitting a Data Tape

Data tapes often contain valuable clues for your case. It is important the proper information is collected and documented at the time a tape is seized as evidence or created. Each tape submitted within a request should include the following information.

When the proper information is not recorded or provided, data tape recovery can become exceedingly demanding and impacts the ability to provide results. This outline will assist in completing DCFL Form 1, Section 48. Analysis of evidence will be conducted, even with missing information. However, increased time may be associated with these requests.

- Systems Administrator Information:
  - Identify the systems administrator responsible for the network (if possible). Include his/her name and phone number.

- Evidence Collector Information:
  - Identify the person who physically conducted the backup process or seized the evidence (if possible). Include his/her full name, phone number and agency mailing address.

- Physical Tape Information:
  - Is the Data Tape in storage? Retentioning may be required before the tape is handled.
  - Upon seizure, write protect each Data Tape.
  - 4mm tape: Tape tab must remain in OPEN position
  - 8mm tape: Tape tab must remain in CLOSED position
  - DLT/SDLT and LTO tape: Tape tab must show ORANGE
  - If a backup set has been created, ensure all tapes are labeled properly. Write the number of the tape out of the total number of tapes. Example: Tape 1 of 2, Tape 2 of 2.
  - Write any password used during the backup process on the tape's label.

- Hardware:

  - Does the system use a robotic tape arm? Seizure of the device is preferred. This may require seizure of the server since many robotic arms utilize a special card installed in the server the device is attached to.
  - What is the model number of the tape drive? Example: Exabyte 8585 SCSI-II 8mm tape.
  - What is the IP address of ALL network interfaces of the machine being backed up. Include the fully qualified domain name (This is crucial for Intrusions Cases). Example: IP=13X.1X.6X.X, Name=This.is.the.domain.

- Operating System:
  - What operating system was the tape created with? Include the exact version number and server type if possible. Examples: SunOS 5.1 (Solaris 2.5) running on a SunSparc 5; Windows 2000 with Service Pack 4; Netware 6 with Support Pack 3.

- Backup Information:
  - Does the backup process display the tape block size or density? If so, please include. Example: Block Size = 1024 bytes, Density Code 21.

- Data Backup Volume:
  - How much data (approximately) is backed up on the tape(s)? Example: 700MB.
  - Was compression used?
  - What tool did the system's administrator use to create the tape? Include all option settings and/or command lines options. If the backup tool is a commercial product, include the version number. Examples include tar/cvf/dev/rmt/0*; Backup Exec for Windows 2000 Version 8; and ArcServe for Novell Version 9.

Tips for submitting a Log File?

If submitting a detection log file, please submit it in electronic form. Electronic log files enhance the analysts' ability to interpret the log more effectively, ultimately providing a better result for the customer. Paper logs will be processed. However, an increased time may be associated with your request.

If network intrusion detection logs or other detection type logs are associated with the respective investigation (examples: ASIM logs and Government Sniffer logs), please provide them in electronic formats if possible.

Tips for submitting Digital Multimedia

In order for DCFL to achieve the best audio or video enhancement, original tapes should be submitted when possible. Please submit copies only as a last resort. Copies of the original are often of a degraded quality and may limit the enhancement request.

If you have advanced knowledge of surveillance, please contact DCFL and we will provide you with assistance which will help us handle your media more efficiently.

The following information will assist in completing Form 1, Section 48: Service Requested of the Forensics Media Analysis Request if Digital Multimedia support is requested. Answers to these questions will expedite tape recovery.

- Audio Media Request Example:
  - Enhance and improve the recording to allow better understanding of the conversation.

- Video Media Request Example:
  - Enhance and improve the recording to better see what is happening between time position (HH:MM:SS) and (HH:MM:SS) of the recording.
  - Enhance and improve the recording to better see what is happening while (THIS EVENT) is taking place.

<u>For each tape submitted, please include the following information:</u>

- Approximate dimensions of the location where the recording was made.
- Approximate number of voices recorded.
- Diagram of location where recording was made with microphone/camera location(s) identified.
- Where possible, specify microphone/camera model number and serial number.
- Information about the contents of the tape.
- Any peculiarities about the content/recording.
- Physical location or time marking (HH:MM:SS-HH:MM:SS) on the tape where the target information is located.