DoD CYBER CRIME CENTER (DC3)
SUBMITTING DATA TAPES, LOG FILES, & MULTIMEDIA

Cyber Forensics Laboratory

Submitting Data Tapes

Data tapes often contain valuable clues for your case. It's important that you collect and document the proper information at the time you seize and/or create a tape as evidence. Provide the information listed below with each tape submitted with a service request.

System Administrator Contact Information

If possible, identify the System Administrator responsible for the network, including their full name and phone number.

Evidence Collector Contact Information

If possible, identify the person who physically conducted the backup process or seized the evidence, including their full name, phone number, and agency mailing address.

Physical Tape Information

- Is the data tape in storage? If so, retrieve the tape from its storage location.
- On seizure, write-protect each data tape:
  - On 4mm tapes, ensure tape tab remains in OPEN position.
  - On 8mm tapes, ensure tape tab remains in CLOSED position.
  - On DLT/SDLT and LTO tapes, ensure tape tab shows ORANGE.
- If you create a backup set, ensure all tapes are labeled properly by writing the tape number out of the total number of tapes. Example: Tape 3 of 4
- Write the password you used during the backup process on the tape's label.

Hardware

- Does the system use a robotic tape arm? If so, seize the device. This might also require seizing the server; many robotic arms use a special card that's installed on the server to which the device is attached.
- 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 (crucial information for Intrusions exams). Example: IP=13X.1X.6X.X, Name=This.is.the.domain

Operating System

On which operating system was the tape created? If possible, include the exact version number and server type.

Backup Information

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

Data Backup Volume

- Approximately how much data is backed up on the tape(s)? Example: 700GB
- Was compression used?
- What tool did the System Administrator use to create the tape? Include all option settings and/or command lines options.

When the preceding information isn't recorded or provided, data tape recovery becomes exceedingly difficult and will impact our Technicians' ability to provide results. We will still analyze your evidence without this information; however, such requests are often associated with significantly more time in the Lab.

Submitting Log Files

If you're submitting a detection log file, submit it in electronic format. Electronic log files enhance the Analysts' ability to interpret the log more effectively, ultimately providing you with better results. We will still process paper logs; however, such requests are often associated with significantly more time in the Lab.

If network-intrusion-detection logs or other detection-type logs are associated with your investigation (such as ASIM logs, Government Sniffer logs), provide the logs in electronic format if possible.

Submitting Digital Multimedia

For Examiners to enhance audio and/or video optimally, submit original tapes. Submit copies **only as a last resort**. Copies often are a degraded quality, which limits enhancement capabilities.

If you know about the surveillance before it happens, contact the Lab before submitting your request. We will provide you with assistance that will help us handle your media more efficiently.

Audio Media Request Example

"Enhance/improve recording to understand the conversation better"

Video Media Request Example

- "Enhance/improve recording to see what's happening between [HH:MM:SS] and [HH:MM:SS] better"
- "Enhance/improve recording to see what's happening while [certain event] is taking place better"

Required Information for Each Tape Submitted

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