Theft of Intellectual Property

A Guide For First Responders

Data Specialist Group | 877-787-7075 | www.DataSpecialistGroup.com
Note:

- The objective of this document is to guide you through the process of preserving data and documenting the chain of custody as it relates to electronically stored information (ESI).

- The ESI you preserve may be necessary to prosecute or defend any legal action as admissible evidence.

- These are general principals to be used as a guideline when responding to any company event that involves work product and electronic technology.

- Some of these principals should be used for employees separating from the company, even if litigation is not anticipated to the extent litigation may commence years after the departure.
Basics

- The basics of forensics are to preserve item(s) “as is” or prevent changes by other means
- Data is perishable and easily altered, lost, or written over
- The basic function of the first responder is to preserve data and/or prevent the loss of data
- Reasonable, necessary, and documented actions are accepted
- Theft of intellectual property (IP) and the deliberate destruction of work product have civil and criminal remedies; therefore associated electronic devices shall be processed in the same manner you would process any other crime scene
Golden Rules

- Take immediate steps to preserve the data
- If the computer is off, leave it off
- If the computer is on, leave it on and physically disable all communications, unless you have reason to believe a process is destroying data
- Do not start searching the computer, accessing files, or allowing anyone else to use it
- Use a camera to document what is on the computer screen, the desk area, drawers, front and back of the computer as well as the surrounding office area
- Be sure to obtain images of all cables and connectors
- Immediately begin a log of any and all of your actions
- Contact a Digital Forensics Expert if necessary
Camera Of Choice

- The smart phone should be used to take photographs
  - Geo Location
  - Time & Date
  - Dynamic Range
  - Back up to log
  - Images and metadata are easily transmitted
  - Photograph item > Tag item > Photograph tagged item
Random Access Memory (RAM)

- RAM is the most perishable of all memory
- RAM can be the most valuable evidence in a cyber breach or theft of work product
- To preserve RAM the device must be kept alive
- If available use hardware or software to keep the device alive (virtual “mouse jiggler”)
- Contact your digital forensics expert to assist you in preserving RAM
Smart Phones

- If possible, obtain the unlock code from the employee or swipe code on Android phones
- Do not allow employees to delete any data even if it is alleged to be their “own”
- If the phones is on and unlocked, place it in airplane mode
- Do not open, close, or access other applications
- If the phone screen is unlocked, disable the screen lock feature
- If screen is locked, place the phone in a faraday bag that provides shielded charging
- If a faraday bag is not available and the screen is locked, it may be necessary to power off the device to prevent loss of data
- Log all of your actions; photograph the device; tag the device; and store in a secure location with the least amount of access
Running Stand Alone Computer

1. Use images to document any software active on the computer screen
2. If a network cabled is attached, remove it
3. If a wifi adapter is attached, photograph and remove it (If not removable, disable it)
4. Do not manipulate or search the computer
5. Use images to document all devices, cables, and hardware peripherals that are attached to the computer
6. If theft of intellectual property is suspected, guard the scene until a digital forensics expert arrives to preserve RAM (It may be necessary to move the mouse to prevent the computer from hibernating)
1. Shake the mouse and wait 1 minute to make sure the computer is off

2. If the computer is off, label all connections paying special attention to USB connections

3. Document each of your labels with images, as well as any other labels, decals, serial numbers or service tags

4. As you unplug each device, log the name and the number assigned to the device, photograph and place in box

5. After all connections are removed, place the computer in a box or plastic bag; tape closed; sign and date across tape; then assign an item number and log

6. After you have processed the work area, store in a secure location with the least amount of access
Laptops

- If the device is closed it could be off, on, in sleep mode or hibernating (the “lid” switch is programmable)

- If the device is on and RAM data needs to be preserved, all communications to the device must be terminated by:
  - Disconnecting network cable
  - Turning off mobile wireless and broadband services by switch or keyboard combination
  - Unplugging any and all wireless and/or broadband adapter(s)
  - Placing it in a faraday bag if available
  - In some cases it may be necessary to move the mouse to keep the laptop from shutting down or hibernating to preserve data in RAM
  - Plug in the device if it is running on battery

- If it is believed that the device is destroying data, unplug the device and remove the battery

- If the device is off, leave it off and follow the instructions for a stand alone computer
Storage Media

- Do not plug any storage media into the subject computer for any reason at any time.
- Do not attempt to access data on storage media in efforts to determine if the contents are relevant.
- Data on storage media can be altered, hidden, or encrypted (files that may seem insignificant can be the key to unlocking encrypted or password protected files).
- Special attention should be given to coins, pens, watches, and other devices that can be hidden storage media.
- When in doubt, photograph, tag, log, and retain.
Processing The Work Area

1. Search the desktop, drawers, laptop bags and file cabinets for any and all electronic devices and media storage (memory cards, CD’s, USB drives, and mobile devices)

2. Be thorough, look inside other containers and items such as cigarette packs and envelopes

3. Search under desk blotters and photograph any and all items found, they may contain passwords and documentation of policy breaches

4. Include note pads and scraps of paper

5. Be sure to secure all data cables, manuals, and chargers

6. Label and log each device found and place in a box

7. Mark the box fragile; seal the box; sign/date across the seal; affix a copy of the log; then store with the computer in a secure location with the least amount of access
Network Servers And Storage Devices

- Network storage devices are beyond the scope of the office first responder.

- To the extent that most enterprise systems cannot be interrupted, the preservation of ESI on servers should be conducted by forensic experts, cyber security experts, and/or server administrators trained in forensic preservation.
Purpose Of Preservation

- Portable media, devices, and cloud storage provide a medium for employees to steal data.

- The small and medium sized companies are the most susceptible due to lack of written and enforced policies, infrastructure, and information technology support.

- The greatest threat to small and medium sized businesses is the lack of a written “Bring Your Own Device” (BYOD) policy, followed by companies that allow employees to use personal devices for business.

- Most employees do not regard stealing projects they worked on as intellectual property.

- Most employees believe it is their right to delete their work, emails, texts, and personal data.

- A separated employee may commence litigation years after departing the company.

- Work product theft or deletion can go unnoticed for days, months, or years.
- Web based desktop applications like JoinMe, Logmein, and GotomyPC can allow undetectable access to corporate systems.

- Corporate VPN networks provide employee access to systems.

- The second greatest threat to all companies are substandard Information Technology professionals who fail to properly install or monitor systems.

- Properly preserved data is necessary to investigate theft of IP as well as prosecute or defend legal actions that may involve ESI.

- All companies should forensically preserve a departed employee’s data from their computers, network shares, and mobile devices immediately.
Theft of Intellectual Property
by Dwayne Denny of Data Specialist Group

www.DataSpecialistGroup.com
Client.Services@DataSpecialistGroup.com
877-787-7075