Forensics Lab 4

C16406984

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Single Evidence Form  Case No.  **PLEASE COMPLETE FORM IN UPPERCASE** | | | | | | | | | | | | | | | | | | | Evidence No. | | | | | | | | |  |  |  |  | | |  | Digital Forensics Lab | | | | | | |
| **Section B: Evidence Collection** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Date/Time Collected | | | | D D | | | M | M | | Y Y | |  | H H **:** M M | | | | | | Collected by | | | | | | | | | | | | | | | | | | | | | | |
| Site Address | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Section C: Evidence Details** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Date/Time Stored | | | | D D | | | M | M | | Y Y | |  | H H **:** M M | | | | | |  |  |  |  |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  |  |  |
| Storage Location | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Device Type | | | | | | | | | | | | | | | | | | | Capacity | | | | | | | | | | | | | | | | | | | | | | |
| Manufacturer | | | | | | | | | | | | | | | | | | | Model | | | | | | | | | | | | | | | | | | | | | | |
| Serial No. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| MD5 Sum |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | | | | | | | |
| SHA-1 Sum |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Additional Information... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Note any damage, marks and scratches | | | | | | | | | | | | | | | | | | | Digital Image Taken | | | | | | | | |  |  |  | Yes | | |  | No | | | | | | |
| **Section D: Image Details** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Date/Time Imaged | | | | D D | | | M | M | | Y Y | |  | H H **:** M M | | | | | | Imaged by | | | | | | | | | | | | | | | | | | | | | | |
| Storage Location | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Image Filename | | | | | | | | | | | | | | | | | | | Image Size | | | | | | | | |  |  |  |  | | |  | (inc. unit) | | | | | | |
| Additional Information... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| This form is to be used when collecting a hardware device containing data that may be of interest in a case. Guidelines:  •**Ensure that this form only refers to one item of evidence and that one is completed for each item of evidence**  •**This form must be accompanied by Chain of Custody forms which detail the individuals that have handled the evidence**  •**Further remarks can be noted overleaf in Section E: Remarks**  •**It is important that these forms are kept with the evidence at all times**  •**Upon handover or disposal please complete Section F: Evidence Handover** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |



|  |  |
| --- | --- |
| Single Evidence Form | |
| **Section E: Remarks** | |
| **Section F: Evidence Handover / Disposal** | |
| Date/Time | |
| Submitted by | Signature |
| Received by | Signature |
| Witnessed by | Signature |



|  |  |  |
| --- | --- | --- |
| Chain of Custody Form for use with a Single Evidence form  Page No.  Case No. Evidence No.  **This form must accompany a Single Evidence form and it’s respective evidence** | | |
| **Chain of Custody** | | |
| **SUBMITTER** | | **RECEIVER** |
| Name: |  | Name: |
| Signature: |  | Signature: |
|  | Evidence Modified: |  |
| Date & Time: | Yes / No | Date & Time: |
| **SUBMITTER** | | **RECEIVER** |
| Name: |  | Name: |
| Signature: |  | Signature: |
|  | Evidence Modified: |  |
| Date & Time: | Yes / No | Date & Time: |
| **SUBMITTER** | | **RECEIVER** |
| Name: |  | Name: |
| Signature: |  | Signature: |
|  | Evidence Modified: |  |
| Date & Time: | Yes / No | Date & Time: |
| **SUBMITTER** | | **RECEIVER** |
| Name: |  | Name: |
| Signature: |  | Signature: |
|  | Evidence Modified: |  |
| Date & Time: | Yes / No | Date & Time: |
| **SUBMITTER** | | **RECEIVER** |
| Name: |  | Name: |
| Signature: |  | Signature: |
|  | Evidence Modified: |  |
| Date & Time: | Yes / No | Date & Time: |
| **SUBMITTER** | | **RECEIVER** |
| Name: |  | Name: |
| Signature: |  | Signature: |
|  | Evidence Modified: |  |
| Date & Time: | Yes / No | Date & Time: |
| **SUBMITTER** | | **RECEIVER** |
| Name: |  | Name: |
| Signature: |  | Signature: |
|  | Evidence Modified: |  |
| Date & Time: | Yes / No | Date & Time: |
| **If this form is full please continue on another page** | | |



Q2.

Columbia Pictures, Inc. v. Bunnell, C.D. California

In this case the plaintiff Columbia Pictures are suing the defendants who operate the TorrentSpy network, an online tool for searching .torrent files that allow users to download copyrighted material, for knowingly profiting off and distributing pirated material.

The judge based on this suit, ordered that the defendants produce logs which provide the IP addresses of Users who downloaded .torrent files, the times, dates etc

The defendants however disputed this, stating that these logs are only found temporarily in RAM and therefore not “electronically stored information”.

The judge however disagreed and stated that Rule 34 of the Federal Rule of Civil Procedure covered all forms of computer storage future and current and that it did not require any degree of permanency.

Therefore since the defendants were clearly capable of producing it, they were required to do so.

This is the closest case I could find that deals with ram/volatile memory. Prevailing Computer Seizure procedure seems to favour plugging out a computer instantly to prevent automated programs or remote access from interfering with the hard drive which is regarded as much more important.

Therefore live data recovery seems to be a rarity in legal cases, even cold boot attacks which don’t require the PC to be on and can be used to recover encryption keys seem to be rare.