OFFICIAL USE ONLY

DIGITAL EVIDENCE FORENSIC REPORT

Your Logo Here	Your address here

CASE INFORMATION:

Agency Case #:		Originating Agency Case #:	

[removed] #:		[removed] #:		Remedy#:	
Distribution:	☐ [removed] ☐ [removed] ☐ [removed] ☐ IT ☐ [removed] ☐ Internal Audit ☐ Emp. Relations ☐ CI ☐ Other:				

Date/Time Report Completed:		Date/Time Incident Occurred:	

Type of Report:	Initial

INVOLVED:

☐ Involved ☐ Witness ☐ Complainant ☐ Mentioned
Name: Last: _____ First: _____ Title: _____
Mailstop: _____ Email: _____
Cell Phone: _____ Work Phone: _____ Employee #: _____

☐ Involved ☐ Witness ☐ Complainant ☐ Mentioned
Name: Last: _____ First: _____ Title: _____
Mailstop: _____ Email: _____
Cell Phone: _____ Work Phone: _____ Employee #: _____

☐ Involved ☐ Witness ☐ Complainant ☐ Mentioned
Name: Last: _____ First: _____ Title: _____
Mailstop: _____ Email: _____
Cell Phone: _____ Work Phone: _____ Employee #: _____

CLASSIFICATION LEVEL HERE
May be exempt from public release under the Freedom of Information Act (5 U.S.C. 552) exemption number and category: **7, Law Enforcement**

Department of Name of Agency review required before public release
Name/Org: Your name/org Date:
Guidance (if applicable):

SUMMARY:

EVIDENCE SUBMITTED:

Item #	

SOFTWARE UTILIZED

All software utilized in this examination is fully licensed and registered to [Agency Name] or its agents. All software and forensic hardware has been validated pursuant to [Agency Name] policies and procedures.

FORENSIC EXAMINATION OF EVIDENCE
ITEM #1

Item #1 – Can be described as

[insert photo here] [insert photo here]
[insert photo here] [insert photo here]

HASH OF ORIGINAL EVIDENCE

The original media was connected to a forensic hardware write blocker (asset tag #) and the write blocker connected to a forensic computer (asset tag #). Prior to doing anything with the original media, the media was hashed to obtain a baseline hash value. This allows the hash value of the original media to later be compared to the hash value of the forensic image created of the original media. By comparing the hash values of the original media and that of the forensic image, the forensic image can be authenticated as an exact duplicate copy of the original evidence.

The hash values obtained from the original evidence were as follows:

☐ MD5:
☐ SHA1:
☐ Other:

FORENSIC IMAGING

After obtaining the hash value(s) of the original media, a forensic image was created. The forensic image was placed on a:

☐ Government owned, forensically wiped hard drive
☐ Government owned, forensically wiped Storage Area Network (SAN)

The forensic imaging software utilized in this process creates an imaging report, detailing the hash value(s) of the newly created forensic image. The hash value(s) of the forensic image was compared to the original hash value obtained prior to imaging the device. The hash value(s) of the forensic image:

☐ Matched exactly the hash value(s) of the original media.
☐ Did not match the original hash value(s) of the media. If checked, provide explanation below.

VIRUS AND MALWARE

The original media was scanned for malware. Prior to the scan, all malware definitions were updated. The results were:

☐ No malware detected.
☐ Malware detected. If checked, identify and report on malware located below.

DRIVE GEOMETRY

BIOS EXAMINATION

Once the hard drive was removed, the computer was turned on and the BIOS (Basic Input/Output System) checked. The following was found:

☐ The date and time were accurate.
☐ The date was accurate, but the time was inaccurate. List time offset from correct time:
☐ The time was accurate, but the date was inaccurate. List date offset from correct date:
☐ Forensic computer was adjusted to compensate for any time differences.

What was used as a time reference:

☐ Cellular phone set by network.
☐ Other:

FORENSIC EXAMINATION OF FILES

DISPOSITION

EVIDENCE DISPOSITION

[insert scanned signature here]
Insert Name
Insert Title

[Agency] Case #:

FORENSIC EXAMINER'S CONCLUSION

DISPOSITION

ATTACHMENTS

APPROVALS

Report Author Digital Signature:

Report Approver Digital Signature:

[insert scanned signature here]
Insert Name
Insert Title