



# DIGITAL FORENSIC ANALYSIS

**Technology—it's embedded into most every aspect of our business and personal lives today. With this reliance on modern technology, investigating digital devices is a necessity to avoid missing crucial details regarding the activities and communications that could be otherwise unknown.**

## THE ISSUES — STATISTICS RELATED TO DIGITAL FORENSIC ANALYSIS



**NEARLY 50 PERCENT OF EMPLOYEES WHO QUIT A JOB OR WHO ARE ASKED TO LEAVE ARE TAKING CONFIDENTIAL INFORMATION, ACCORDING TO SYMANTEC.**

[https://www.ciosummits.com/media/solution\\_spotlight/OnlineAssett\\_Symantec\\_WhatsYoursIsMine.pdf](https://www.ciosummits.com/media/solution_spotlight/OnlineAssett_Symantec_WhatsYoursIsMine.pdf)



**Annual losses for the US are estimated at between \$10 billion and \$12 billion from cybercrime targeting IP and perhaps \$50 billion to \$60 billion globally.**

<https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf>



**53% of polled companies confirmed insider attacks against their organization in the previous 12 months**

<https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf>

## SERVICES — WHY LBMC?

**When responding to a potential insider threat, there are three things to keep in mind:**

- ✓ **Identify and preserve all technology used by the suspect**
- ✓ **Don't turn on the devices used**
- ✓ **Ensure that only a qualified forensics expert analyzes the data**

**LBMC INFORMATION SECURITY HAS INVESTED IN "BEST OF BREED" COMPUTER FORENSICS SOFTWARE PLATFORMS AND TOOLS TO EFFICIENTLY AND EFFECTIVELY PRESERVE AND ANALYZE COMPUTERS, STORAGE MEDIA, AND MOBILE DEVICES OF ALL TYPES TO RECOVER ARTIFACTS THAT MAY OTHERWISE HAVE NOT BEEN UNKNOWN.**

What are the dos and dont's of digital forensic investigations? What are some situations in which you might need digital forensic services? These questions and more can be answered by LBMC Information Security's digital forensic services and professionals.

### LBMC INFORMATION SECURITY'S DIGITAL FORENSIC ANALYSIS

#### Forensic Analysis

LBMC Information Security's certified forensic analysts follow strict evidence handling procedures and employ a forensics analysis methodology that has been built on more than 10 years of experience to assist you.

#### The basics of this methodology include:

- Developing detailed timelines of detailed computer activity
- Identifying and recovering electronic communications outside of conventional email (webmail, text messaging, etc.)
- Analyzing Internet activities
- Determining and analyzing "cloud" storage usage (Google docs, Dropbox, etc.)
- Investigating social media activities
- Recovering and analyzing deleted information
- Understanding application histories regarding execution
- Recovering and analyzing videos and pictures
- Detailing removable media usage (USB drives, printers, etc.)
- Determining documents created, opened, printed, etc.

#### Digital Forensic Services include:

- Incident Response
- Incident Response Plans
- Incident Response Programs and Training
- Litigation Support and Electronic Discovery
- Penetration Testing
- Other Security and Compliance Services

**60+**

Healthcare Data Security Experts

**5/8**

of the Largest U.S. For-Profit Health Systems are Our Clients

**60%**

of Our Clients are in or Related to the Healthcare Industry

## OUR EXPERIENCE — TESTED AND TRUSTED



Awarded as a Top Ten Cybersecurity Provider

**20+**

20+ years of information technology experience



Qualified as an expert witness in Federal and numerous State courts



Sole endorsed provider of security risk assessments for several state trade associations

#### LBMC Information Security has experience in the following cybersecurity frameworks:

- HIPAA/HITECH
- PCI DSS
- ISO 27001
- COBIT
- HITRUST
- NIST CSF &800 SERIES
- CMS
- JCAHO
- OCR
- MARS-E

**We can help with digital forensic analysis needs. Our professionals are ready to offer a discreet consultation, so contact us today!**