# Matthew R. Considine

**539 W SECOND ST., LEXINGTON, KY 40508 | 845-264-8829 | MRC@CYBERAGENTSINC.COM**

**BACHELOR OF SCIENCE IN COMPUTER AND DIGITAL FORENSICS**

**GRADUATED: DECEMBER 2014 | CHAMPLAIN COLLEGE, BURLINGTON, VT**

## SUMMARY:

College graduate with a Bachelor's degree in Computer and Digital Forensics, has also attended CEIC 2015 and EnFuse 2016 and 2017 to maintain up-to-date knowledge on proper forensic processes. 28 months workplace experience and has been responsible for multiple data recovery and forensic acquisition jobs. Has completed computer examinations without compromising data integrity, and has provided reports on findings. Has acquired forensic images of iOS and Android cell phones for forensic examination. Has examined forensically acquired cell phone data for criminal and civil cases. Has provided written reports regarding information on examined cell phones and cell tower data. Experience during trials as an expert consultant.

## CURRENT EMPLOYER:

Cyber Agents, Inc. 535 W Second St, Ste. 209, Lexington, KY 40508 859-523-9081

- Perform data recovery of hard drives, cell phones, and network servers.
- Examine and analyze evidence to establish a report for legal teams.
- Maintain Chain of Custody for criminal and civil litigation.

## EDUCATION:

Bachelors of Science in Computer and Digital Forensics
Champlain College in Burlington, VT
Graduated December 2014

## RECENT WORK:

Digital Forensic Consulting and Examinations

- **USARMY v Fitch**: Sexual Assault, advise on proper cross-examination questioning and review material pertaining to deleted emails and cell phone data.
- **USNAVY v Jackson**: Sexual Assault, review authenticity of email evidence and attorney consult.
- **US v Day**: Possession of CP, examine laptop and Android cell phone used by defendant to obtain and view CP material, and review FBI and LE reports and consult with attorney.
- **KY v Hughes:** Rape, examine Snapchat conversations, review discovery material, and consult with attorney
- **KY v Curtis:** Possession of CP, review of torrent client logs and government reports
- **KY v Probus:** Kidnapping and Assault, review cell phone data and consult with the attorneys, expert testimony in digital forensics and cell phone forensics

Computer Examinations

- Assemble and disassemble laptops and desktops to gain access to the hard disk drive (HDD) or solid state drive (SSD).
- Use write-blocking hardware and software to ensure no changes are made to evidence during imaging process.
- Forensically image laptop and desktop HDDs using EnCase Acquisition, Voom Hardcopy, FTK Imager, and LogiCube Forensic Dossier or Forensic Falcon.
- Maintain Chain of Custody documentation.
- Use EnCase, Internet Evidence Finder, Forensic Explorer, and NetAnalysis to examine forensic images (E01, L01, DD, etc.) and Virtual Hard Drives (VHD, VMDK).
- Examine system events to determine user behavior.
- Examine Internet history to determine user actions online.
- Examine Windows registry to determine user activity on the file system.
- Determine the cause of specific events based on the contextual evidence.
- Report findings and professional opinion on evidence in question.
- Review torrent file logs to determine file requests from specified IP address.
- Perform bit-level searches for file headers/footers for data carving purposes

Cell Phone Extraction

- Image Android cell phones and Apple iPhones.
- Ensure no changes made to phone prior to acquisition.
- Examine and extract SMS, MMS message data.
- Examine and extract picture, video, voice, and web data.
- Provide information about picture metadata.
- Perform keyword searches for specific messages or web data.
- Perform ADB extractions via command line in Windows

Data Recovery

- Image a RAID system through a network connection using EnCase.
- Image and organize multiple drives in RAID separately.
- Reconstruct RAID using forensic software.
- Extract and mount virtual backups from a forensic image file.
- Locate and extract specific files.
- Maintain spreadsheet containing dates/times of backups and specified files.

**EXPERIENCE WITH:**

Software

- EnCase (v6, 7, 8)
- Access Data FTK Imager
- Magnet Forensics Internet Evidence Finder
- Forensic Explorer
- Net Analysis and History Extractor
- Cellebrite UFED Physical Analyzer
- Android Debug Bridge (ADB)
- Microsoft Office
- Windows OS (XP, Vista, 7, 8, 8.1, 10)
- VMWare Workstation

Hardware

- Desktop and laptop hardware (HDDs, assembly/disassembly)
- Smart phones (iPhone and Android)
- Logicube Forensic Dossier/Falcon
- Tableau T35i Writeblocker
- Voom Hardcopy (2 and 3)
- Cellebrite UFED Touch and Touch 2

## PROFESSIONAL DEVELOPMENT:

CEIC 2015 and EnFuse 2016, 2017 Las Vegas, NV:

- Took several courses to stay current on forensic software and procedures.
- Communicate with other members of the digital forensic community.
- Passed Phase 1 of EnCE certification test, currently on Phase 2.

2014 Senior Capstone (Final Thesis)

- Formulate a way to test creation and modification of shellbag artifacts.
- Test tools to determine reliability of results and compatibility with Windows 10.
- Determine the activity related to Windows 10 shellbags.
- Compare findings to those of previous versions of Windows.
- Determine the forensic value of these artifacts.

Training at Cyber Agents, Inc. (2015-Present):

- Develop and implement testing for WinMX (P2P software)
- Receive training from Trent Struttmann and Eric Lakes regarding the examination of Limewire forensic artifacts
- Update educational material to better reflect the current trends in information technology
- Research on white papers and case studies involving data relevant to current cases
- Utilize and research methods of extracting data from specific model cell phones