# Project Bid - Cloud Forensics

**Names:** Lisa Bazis
Collin Daily
Lyle Reinholz
Sanjar Hamidi
Sarah Noles

**Email addresses:** lbazis@unomaha.edu
cdaily@unomaha.edu
lreinholz@unomaha.edu
shamidi@unomaha.edu
snoles@unomaha.edu

**University:** University of Nebraska-Omaha

**Faculty Advisor:** Dr. Matt Hale

**Project:** Cloud Forensics

**Project Agency (optional):** National Security Agency

**Technical Director / External Customer:** Albert Holt

**Reason for wanting this project:**

As cloud computing becomes continually more pervasive, all aspects of a person's life seems to be stored in the cloud. A common cloud computing use case that many individuals utilize is the cloud-based document storage repositories, such as Dropbox, Box, or Google Drive, which often include the capability to sync seamlessly between the cloud and desktop spaces.

While convenient for the user of the service, the use of such products introduces many security and forensics implications. Research into the forensics artifacts left behind by software that syncs between cloud content storage solutions and desktop environments has the potential to reveal interesting findings, including recovering contents or documents from a user's account, recovering deleted files, and potentially even recovering information about the user's account related to syncing and authentication.

**Project Scope:**

The team will utilize industry standard tools to test the forensic artifacts left behind during the software syncs. AccessData tools such as Forensics Toolkit, FTK Imager, and Registry Viewer along with DB Browser for SQLite, Scalpel, and MSAB XRY Extract (if access provided by the university) will be used to examine the local machine to find leftover artifacts from the following cloud content storage products; Dropbox, Box, and iCloud.

The team will develop a scenario testing Dropbox, Box, and iCloud with the sync client installed on a clean copy of Windows 10 OS in a virtual environment only used for this project. A predetermined set of files will be used to test with and the file hash will be determined to prove

integrity throughout testing. The predetermined files will have uploaded to the cloud storage service, and an image of the sync drive will be taken to validate hash for integrity purposes.

Then the files will be accessed through local OS, Windows 10. Afterwards all network connections will be disabled and the forensics analysis of local OS using above mentioned forensic tools will be being in an effort to find any left-over artifacts from cloud storage on the local machine. The artifacts we hope to find will include but are not limited to file metadata, thumbnails, and copies of original files.

**Qualifications:**

- Lisa Bazis is a graduate student in Cybersecurity at the University of Nebraska Omaha. She currently works in the Information Security Office at the University of Nebraska Medical Center/Nebraska Medicine. Her background is in network security and risk assessments. She has a strong understanding of cloud architecture which will help with this INSuRE project.
- Collin Daily is a senior in his last semester studying Cybersecurity at the University of Nebraska at Omaha. His passion is in network security and forensics. After he completes his bachelor's degree, he will look to start working full time while pursuing his master's degree.
- Lyle Reinholz is an undergraduate student majoring in Cybersecurity and minoring in Computer science. His passion is to be a penetration tester and to be able to make networks more secure in doing so.
- Sanjar Hamidi is a student of UNO's integrated Undergraduate/Graduate program. MS in Cybersecurity with concentration in Cyber operations; and BS in Cybersecurity with minors in Computer Science and Management Information Systems. Sanjar is an intern with a security company focusing on cybersecurity integration in systems currently used by the U.S. government. Sanjar has developed a strong understanding of Forensics Science, and Forensics tools used in the industry; which he will utilize within this INSuRE project.
- Sarah Noles is a graduate student studying Cybersecurity at the University of Nebraska at Omaha. She currently works as a security analyst at a software development company focusing on penetration testing and automation. She has strong programming and analysis skills that will assist in this graduate capstone.