A Forensics Approach

for Quantum Computers

Jonathan Metzger

CY5210 Information System Forensics

December 15th, 2022

# Introduction

When Quantum Computing becomes a reality soon, all classical asymmetric cryptography algorithms will be obsolete. We need a Post-Quantum solution to cryptography to protect our assets and a Post-Quantum solution to forensics to recover malicious activity.

Forensics investigators today use tools like AccessData FTK Imager, RegRipper, USB Detective, and command line scripts to analyze data on a system. Windows machines can view registry hives like SOFTWARE, SYSTEM, or NTUSER to analyze user applications, operating system components, or user information. From here, they can judge whether something malicious happened to the system. This can be done to an extent with classical techniques. However, forensic investigators will need to start thinking about analyzing data on a quantum computer.

Forensic Investigators will need to observe future quantum systems when they become more mainstream. Today, a few quantum computers exist at large companies like IBM and Google. The latest announcement of the most powerful Quantum System will be late next year when IBM releases the IBM Quantum System. As big companies are making processes in developing modern quantum systems for commercial use, forensic investigators will need to keep up to secure these new systems from any malicious threats or activity. First, Quantum Computers will be discussed, how forensic investigators apply them, challenges that come with Quantum Forensics, and summarize a path forward.

# Quantum Computers

For over a century, physicists have studied and worked on Quantum Mechanics. It is the cornerstone of chemistry, physics, and modern technologies like computer chips. Richard Feynman and Yuri Marin first proposed them in the 1980s as a theory that was hard to implement since the technology was ahead of their time. In 1994, Peter Shor came up with Shor’s Algorithm to solve a complex problem on a classical system that relates to factoring and provides the ability to process data exponentially quicker and can break many of the public key cryptosystems.[[1]](#footnote-2) This has become a massive evolution in how we process data on our computer systems. Once these theories become a reality and new quantum systems are built for public use, malicious actors will try to exploit this new technology to hack systems or steal confidential information from institutions for profit.

Two properties of quantum mechanics called Superposition, the equal probability of a qubit to be in a 0, 1, or both states [[2]](#footnote-3), and Entanglement, the dependence of two qubits when interacting[[3]](#footnote-4), are essential to understanding our quantum systems, and their low-level qubits operate to try to understand what is happening in the system. Right now, classical computers use classical logic gates, or algorithms and functions, to process data. These algorithms are usually coded high enough to be understandable to the human eye. As we analyze the algorithm on a lower level, like assembly or binary, the manipulation of registers or bit changes can be observed.

Quantum Forensics

As classical system users carry out these actions, they can be traced by forensic investigators to the chain of custody of the evidence. That becomes difficult when analyzing the activities carried out by quantum system users. New quantum forensics tools will need to be created to use these new functions and gate changes to track the timeline of system usage and collect digital forensics artifacts.

As stated by Richard E Overill, “It is not possible to clone an exact copy of an arbitrary unknown quantum state for preservation and subsequent analysis” However, it is possible to approximate the quantum states by creating copies and performing Gate Reversal to undo the chain of events. [[4]](#footnote-5) Observation would collapse the state of the system. We need to undo the operations to get the data back. It is difficult to hold the system's state since it can change in milliseconds.

Dayton Closser and Elias Bou-Harb of the University of Texas at San Antonio have established a Live Digital Forensics Approach for Quantum Mechanical Computers. This approach has been summarized into three simple steps Preparation, Execution of the Quantum State, and Measurements. The most important step, preparation, needs to create the logic to use with the qubit circuits. Once that logic is established, using quantum simulator editors like Python Jupyter-Notebooks, the reason can be reversed to retrieve the system's actions. Next, the Quantum State is analyzed when the reason is executed quickly. This is the most challenging state to capture the state of the qubit for analysis. In addition, third parties can utilize entanglement to manipulate the qubit states and send messages before them are written. This is like how man-in-the-middle attacks of classical systems are carried out. The IBM Quantum Experience is already working on this, an open community to share and implement quantum logic solutions and system simulators like the real Noisy Intermediate-Scale Quantum, or NISQ, systems, to focus on error correction. Last, the results of the logic are measured and recorded as part of the chain of custody to track the system properties at the time of malicious intent and be proof of evidence of a crime on a quantum system.[[5]](#footnote-6)

# Challenges

Challenges are met when analyzing forensic data on a quantum system. First, quantum computing theories have yet to be tested enough on actual quantum systems because of their novelty. It will be a long time after these theories become realities that forensic investigators will be able to identify the timeline of the events occurring in the quantum system.

To handle this theory, quantum systems must be developed to address this computing power, with the temperature to remain at absolute 0. The current goal is to develop these systems for warmer and room temperature heat.[[6]](#footnote-7) Another goal is to combat noise in the quantum system with error correction or fault-tolerant quantum computing. Since particles are moving faster than our current technology can handle, there are still high error rates with noise emissions.[[7]](#footnote-8)

# Conclusion

To combat these challenges faced in Quantum Forensics, there is a path forward. There will need to be Quantum Anti-Forensics deferred measurements to detect this application of scientific methods trying to influence the existence of evidence at a crime scene negatively.[[8]](#footnote-9) Currently, if a forensics investigator performs a live acquisition or when the system was left on when the system was analyzed, the state can still be manipulated at runtime, especially if connected to the internet. If that system is turned off or examined by a dead/offline acquisition, the state is untouched but may cause a loss of data, such as running processes and network connections. [[9]](#footnote-10)

This needs to be applied for Quantum post-mortem forensics since the state of the qubits is constantly changing. The only way to track the system’s actions is in a dead state. Lastly, quantum analyzing is only in theory since the systems' hardware is still being developed. Once the hardware catches up, quantum algorithms and forensics tools will need to be applied to analyze these systems. It will be a challenge in the coming decades, but Quantum Computers are the future. Malicious actors can use this technology to bypass our computer security cryptographic algorithms to steal confidential data.

# Bibliography

Biercuk, Michael. “Quantum Computer Error Correction Is Getting Practical.” IEEE Spectrum, September 4, 2021. https://spectrum.ieee.org/quantum-computer-error-correction-is-getting-practical.

Caltech Science Exchange. “What Is Entanglement and Why Is It Important?” n.d. https://scienceexchange.caltech.edu/topics/quantum-science-explained/entanglement.

Caltech Science Exchange. “What Is Superposition and Why Is It Important?” n.d. <https://scienceexchange.caltech.edu/topics/quantum-science-explained/quantum-superposition>.

Closser, Dayton, and Elias Bou-Harb. “A Live Digital Forensics Approach for Quantum Mechanical Computers.” DFRWS, March 24, 2022. Accessed December 10, 2022. <https://dfrws.org/presentation/a-live-digital-forensics-approach-for-quantum-mechanical-computers/>.

Conover, Emily. “New Quantum Computers Can Operate at Higher Temperatures.” Science News, April 15, 2020. https://www.sciencenews.org/article/new-quantum-computers-can-operate-higher-temperatures.

LopezBravo, Sonia. “Quantum Computing History - Azure Quantum.” Microsoft Learn, November 7, 2022. Accessed December 10, 2022. <https://learn.microsoft.com/en-us/azure/quantum/concepts-overview>.

Kolhe, Mahesh, and Purnima Ahirao. “Live Vs. Dead Computer Forensic Image Acquisition.” IJCSIT - International Journal of Computer Science and Information Technologies, 2017. Accessed December 10, 2022. https://ijcsit.com/docs/Volume%208/vol8issue3/ijcsit2017080331.pdf.

Overill, Richard E. *Digital Quantum Forensics: Challenges and Responses*, 2011. https://www.researchgate.net/publication/225960273\_Digital\_Quantum\_Forensics\_Challenges\_and\_Responses.

Shree, Divya, Anjan K Koundinya, and Bharathi R. “Anti-Forensics of Data in Classical and Quantum Systems Over the Classical Communication Channels.” IJCSN - International Journal of Computer Science and Network, August 202AD. Accessed December 10, 2022. http://ijcsn.org/IJCSN-2020/9-4/Anti-Forensics-of-Data-in-Classical-and-Quantum-Systems-Over-the-Classical-Communication-Channels.pdf.

1. LopezBravo, Sonia. “Quantum Computing History - Azure Quantum.” (2022) [↑](#footnote-ref-2)
2. Caltech Science Exchange. “What Is Superposition and Why Is It Important?” [↑](#footnote-ref-3)
3. Caltech Science Exchange. “What Is Entanglement and Why Is It Important?” [↑](#footnote-ref-4)
4. Overill, Richard E. Digital Quantum Forensics: Challenges and Responses, 2011 [↑](#footnote-ref-5)
5. Closser, Dayton, and Elias Bou-Harb. “A Live Digital Forensics Approach for Quantum Mechanical Computers.” [↑](#footnote-ref-6)
6. Conover, Emily. “New Quantum Computers Can Operate at Higher Temperatures.” [↑](#footnote-ref-7)
7. Biercuk, Michael. “Quantum Computer Error Correction Is Getting Practical.” [↑](#footnote-ref-8)
8. Shree, Divya “Anti-Forensics of Data in Classical and Quantum Systems Over the Classical Communication Channels.” [↑](#footnote-ref-9)
9. Kolhe, Mahesh“Live Vs Dead Computer Forensic Image Acquisition.” [↑](#footnote-ref-10)