[This file is supplemental material to Straight, *Grey Areas and Egress: Artifact-Based Collaborative Learning in Cybersecurity Ethics*, prompt 10.2 (2026), doi: 10.31719/pjaw.v10i2.280]

# EXODUS Case Excerpts

Selected Artifacts from the Full Case Study

Ryan M. Straight

*This supplemental file accompanies Ryan M. Straight, "Grey Areas and Egress: Artifact-Based Collaborative Learning in Cybersecurity Ethics," Prompt: A Journal of Academic Writing Assignments, Issue 10.2 (2026). It presents three excerpted artifacts from the full EXODUS case study to give readers a working sense of the artifact-based materials students encounter. The full case appears in* Cyber Dimensions: Immersive Case Studies Across Digital Domains *(Straight, 2025; Kendall Hunt) and is available only through the textbook.*

## Case Orientation

Alex Chen is a quantum computing engineer at Quantum Frontier, a leading AI company with government contracts in defense and intelligence. After five years of high-impact work on Project Daedalus (the company's flagship quantum machine-learning initiative), Chen accepts a position at NexGen Cybernetics, a competitor known for an open-source, collaborative approach to AI development.

Before departing, Chen copies portions of the quantum AI algorithms she worked on at Quantum Frontier to personal cloud storage. Her stated intent, later recorded in the exit interview, centers on two threads: using some material as a portfolio piece, and continuing to develop algorithms she feels personally invested in. Quantum Frontier detects the exfiltration. The FBI investigation that follows produces charges under the Computer Fraud and Abuse Act (CFAA) and the Economic Espionage Act (EEA).

The three artifacts below are drawn from the larger documentary record students encounter. They are not the full case. They are a representative triad showing how the case creates interpretive ambiguity through contradictory evidence. Students must reconcile the security team's account of sophisticated exfiltration with the exit interview's account of a conscientious professional acting on convictions about open science.

### Artifact One: Internal Security Memo

To: David Kumar, CTO
From: Cybersecurity Team
Date: July 5, 2026
Subject: Unusual Data Exfiltration Detected (Critical Alert)

**CONFIDENTIAL | HIGH PRIORITY**

Mr. Kumar,

Our advanced AI-driven Security Information and Event Management (SIEM) system has flagged critical anomalies associated with the account of Alex Chen (Employee ID: QD-3782). We've detected a sophisticated data exfiltration attempt from our secure quantum development servers. Here are the technical details:

1. **Volume and Timing:**
   - Approximately 1.2TB of data transferred over the past two weeks
   - Transfers primarily occurring between 0100 and 0400 hours local time
   - Unusual pattern of large data bursts followed by periods of dormancy
2. **Data Characteristics:**
   - Targeted repositories include core quantum ML algorithm source code
   - Exfiltrated data encompasses both compiled binaries and raw source files
   - Metadata analysis suggests selective extraction of key AI model architectures
3. **Exfiltration Methodology:**
   - Use of custom-built data segmentation tool to obfuscate transfer volumes
   - Implementation of quantum-resistant encryption (likely AES-256 with quantum key distribution)
   - Evidence of steganographic techniques to hide data within innocuous file transfers
4. **Network Behavior:**
   - Detected use of a sophisticated covert channel leveraging DNS tunneling
   - Traffic shaped to mimic normal network patterns, evading traditional DLP systems
   - Possible use of a distributed peer-to-peer (P2P) network for data staging
5. **Endpoint Analysis:**
   - Traces of a custom kernel module on Chen's workstation, potentially used to bypass system logging
   - Evidence of memory manipulation techniques to evade endpoint detection and response (EDR) solutions
   - Use of volatile memory-only malware, complicating forensic analysis
6. **Possible Insider Threat Indicators:**

- Detected attempts to access servers outside of Chen's immediate project scope
- Unusual queries to HR databases, possibly attempting to identify other high-access employees
- Spike in off-hours VPN connections from Chen's account over the past month

*Immediate Actions Taken*

1. Implemented real-time monitoring on Chen's account activities
2. Activated our quantum encryption modules on all outgoing data packets
3. Deployed honeypot servers with falsified algorithm data to trace potential exfiltration paths
4. Initiated full-spectrum scan of our network for any planted persistent threats

*Recommended Next Steps*

1. Authorize full forensic analysis of Chen's workstation and all associated cloud accounts
2. Implement network segmentation to isolate quantum computing resources
3. Rotate all access keys and certificates across our infrastructure
4. Conduct emergency incident response team meeting to develop containment strategy
5. Consider engaging our FBI liaison given the sensitive nature of the quantum AI projects involved

Given the highly sensitive nature of our quantum AI projects and the potential national security implications, we recommend an immediate and thorough investigation. We've already initiated our advanced containment protocols, but given Ms. Chen's high-level access, additional measures may be necessary.

We also strongly advise informing relevant government agencies, as per our federal contracts' requirements. The sophistication of the exfiltration techniques suggests this could be more than a simple case of intellectual property theft.

We're standing by to brief you in person and to execute any additional security measures you deem necessary.

Respectfully,
Dr. Samantha Reeves
Chief Information Security Officer
Quantum Frontier Cybersecurity Team

### Artifact Two: Exit Interview Transcript Notes

Interviewer: Dr. Sarah Martinez, Division Head, HR
Interviewee: Alex Chen
Date: July 10, 2026

- Chen expressed deep gratitude for her time at Quantum Frontier, highlighting the growth opportunities and innovative projects she was part of.
- When asked about her future plans, Chen mentioned a "new opportunity that aligns more closely with my personal ethics and vision for AI development." She didn't specify the company but emphasized a desire to work on more open and collaborative projects.
- Discussing ongoing projects, Chen seemed hesitant but assured all her work was properly documented. She mentioned leaving detailed notes for her team about the quantum entanglement optimization algorithm she was working on.
- When reminded about the non-disclosure agreement and company policies regarding proprietary information, Chen nodded and stated, "I understand the importance of intellectual property rights, but I also believe in the power of open collaboration in advancing AI for the benefit of humanity."
- Chen signed all required exit paperwork but paused briefly before signing the IP assignment confirmation, muttering something about "the ethics of owning ideas."

*Observations*

- Chen's body language suggested discomfort when discussing proprietary information.
- She seemed particularly passionate when talking about open-source contributions and the ethical implications of AI development.
- There was a noticeable shift in Chen's demeanor when the quantum entanglement optimization algorithm was mentioned. She became more guarded and her responses more measured.

*Action items*

- Revoke all access credentials immediately following the interview.
- Conduct comprehensive equipment check-in procedure, including deep scan of returned devices.
- Schedule follow-up with Chen's team to ensure smooth transition and identify any potential knowledge gaps.
- Flag Chen's file for potential IP concerns and recommend a review of her recent

contributions to company projects.

*Additional Note*

Given Chen's expertise and the sensitive nature of her work, recommend a more thorough debriefing process and possibly a temporary non-compete agreement review with legal.

### Artifact Three: Timeline of Events (Selected)

The case also includes a chronological scaffold that students use to situate the artifacts relative to one another. Selected entries:

**June 15, 2026.** Alex Chen receives a job offer from NexGen Cybernetics, a direct competitor of Quantum Frontier.

**June 18, 2026.** Chen engages in an encrypted chat with an unknown party about her future plans, discussing her upcoming move and the importance of bringing certain information with her.

**June 20, 2026.** Chen begins copying code from Quantum Frontier's secure quantum computing servers to her personal cloud storage.

**June 25, 2026.** Chen submits her two weeks' notice to Quantum Frontier.

**July 1, 2026.** Chen contributes to an open-source project, sparking internal debate at Quantum Frontier about potential IP issues.

**July 5, 2026.** Quantum Frontier's AI-driven security monitoring system flags unusual data access patterns associated with Chen's account. The cybersecurity team sends the internal memo reproduced above.

**July 10, 2026.** Chen's last day at Quantum Frontier. Exit interview conducted by Dr. Sarah Martinez, Head of HR.

**July 15, 2026.** Quantum Frontier discovers the full extent of the copied code, approximately 1.2TB. The company contacts law enforcement.

**July 20, 2026.** FBI launches an investigation into potential CFAA violations.

### Reading These Artifacts Pedagogically

The memo describes a sophisticated, deliberate exfiltration operation. The exit interview describes a conscientious professional acting on open-science convictions. Both accounts describe the same two-week period. Both are, on their own terms, plausible.

Students in the assignment must reconcile these documents without the benefit of authorial intervention. The security memo's technical detail (covert channels, steganography, custom kernel modules) reads as inculpating. The exit interview's normative register (gratitude, ethical hesitation, concern for open collaboration) reads as exculpatory. Neither document alone resolves the question of what Chen actually did and why.

This interpretive ambiguity is load-bearing pedagogically. It is what allows the same six analytical tasks (ethical framework application, stakeholder analysis, legal analysis, military-AI ethics, corporate response evaluation, policy development) to yield genuinely different conclusions in different groups, rather than converging on a single "right" answer. The artifacts provide evidence without interpretation. Students construct meaning across contradictory possibilities.

The full EXODUS case continues with a corporate counsel memo, FBI investigation excerpts, an encrypted chat log, defense-attorney internal materials, a news article, social media response, and an ethics blog post. Instructors adopting the assignment access the complete case through the published textbook, *Cyber Dimensions: Immersive Case Studies Across Digital Domains* (Kendall Hunt). Instructors who instead want to author their own artifact-based cases in other domains can consult the Cyber Dimensions OER Toolkit for methodology and the Cyber Dimensions Case Study Demo for a complete worked implementation (the CIRCUIT case), with full source available for inspection.

> *The artifacts provided in this document are reproduced with the permission of the publisher under the author's retained right to use case materials in research publications.*