Cyber Case Study Program

Digital Forensics Under Pressure: Technical and Legal Conflicts in Cyber Forensics

Case Number ACI-07-2025

Dr. Hyungbae Park

Editor in Chief: Karen Guttierri, PhD
Lead Editor: Volker Franke, PhD
Managing Editor: Anne Chance, PhD

About Case Studies

The ACI-TRENDS Global Cybersecurity Case Program is administered by the Army Cyber Institute at the United States Military Academy at West Point and publishes cybersecurity-related teaching cases, simulations and interactive exercises for use in academic and professional classrooms.

What are case studies?

Case studies are high-impact interactive learning tools structured around real or realistically simulated events placing learners in the role of decisionmakers confronting complex problems, tradeoffs, and uncertainty. Case studies immerse participants in the problem and its dilemmas.

Why use case studies?

Immersing participants cognitively and emotionally in this way requires them to grapple with ambiguity, incomplete information, and competing priorities while developing plausible courses of action.

Case studies are particularly important because cyber incidents unfold across technical, organizational, legal, and human domains simultaneously.

Case studies make invisible systems and cascading consequences visible, demonstrate how theory and policy apply under pressure, and build the analytical judgment required to anticipate, assess, and respond to real-world cyber threats.

Where to find ACI case study series.

More information on the case method can be found:

1. At the Trends Global Website: https://trendsglobal.org/whats-trending/
2. "Decision-Making under Uncertainty: Using Case Studies for Teaching Strategy in Complex Environments. by Dr. Volker Franke https://jmss.org/article/view/57957
3. [If there is a link to an ACI or WPP publication]

About the Author

Dr. Hyungbae Park is an Associate Professor of Computer Science and Cybersecurity at the University of North Georgia. He earned his Ph.D. in Computer Science from the University of Missouri-Kansas City.

His research focuses on AI-driven cybersecurity and software development, as well as the scalability and resilience of Software-Defined Networking (SDN), big data analytics for network failures, location privacy in Wireless Sensor Networks (WSNs), and smartphone-based localization and authentication.

In addition to his academic research, Dr. Park brings extensive practical expertise supported by industry-recognized certifications such as GIAC Certified Forensic Examiner (GCFE), GIAC Penetration Tester (GPEN), GIAC Reverse Engineering Malware (GREM), GIAC Cloud Security Essentials (GCLD), and GIAC Machine Learning Engineer (GMLE).

His expertise spans a broad range of cybersecurity domains including computer and network forensics, reverse engineering, cryptography, cyber-physical systems security, ethical hacking, and network security.

With a strong foundation in both academic research and hands-on technical practice, he bridges theoretical advances and real-world cyber defense challenges and contributes to cybersecurity workforce development through hands-on training, capture-the-flag (CTF) coaching, and curriculum design aligned with ABET accreditation standards.

Digital Forensics Under Pressure: Technical and Legal Conflicts in Cyber Forensics

Narrative

May 14, 2010 – Peyton, Colorado: FBI agents executed a search warrant at the residence of defendant Ramona Fricosu, a Colorado woman suspected of orchestrating a mortgage and financial fraud scheme. During the search, six computers were seized, including three laptops. Two laptops were unencrypted and examined. The third, a Toshiba Satellite M305 found in Ms. Fricosu's bedroom, was protected with PGP Full Disk Encryption. The laptop was active, logged into Fricosu's user account, and visibly in the process of deleting files. The investigative team faced an immediate crisis: the laptop's solid-state drive (SSD) was performing TRIM operations, automatically erasing deleted data blocks. Any delay or improper handling could result in permanent loss of digital evidence.

The investigative team faced an immediate crisis: the laptop's solid-state drive (SSD) was performing TRIM operations, automatically erasing deleted data blocks.

They quickly recognized several complicating factors:

- The laptop uses a solid-state drive (SSD). SSDs employ wear-leveling and TRIM, meaning that once files are deleted, the underlying data blocks may be erased very quickly by the hardware.[1][2][3]
- The laptop is also protected by full-disk encryption. Because it is currently unlocked, investigators can access the contents[4]. However, if they power it off to preserve the SSD's state, the disk will be locked. Unless the suspect provides the password or the encryption key can be extracted from memory, the disk contents will become unreadable.
- Investigators consider the option of capturing system RAM to preserve potential decryption keys or plaintext passphrases. However, if the key or passphrase has already been wiped from memory, the effort may yield nothing, and the very act of running memory capture software could overwrite the remnants they are attempting to recover.[5][6]

1 Kumar, Manish (2021). Solid State Drive Forensics Analysis – Challenges and Recommendations. Accessed 2/17/2026: https://scholar.google.com/scholar?hl=en&as_sdt=0%2C11&q=Solid+state+drive+forensics+analysis%E2%80%94Challenges+and+recommendations&btnG=

2 Iqbal, M., & Soewito, B. (2020). Digital forensics on solid state drive (SSD) with TRIM feature enabled and deep freeze configuration using static forensic methods and ACPO framework. International Journal of Computer Science and Information Security (IJCSIS), 18(11), pp.44-56. Accessed: 2/17/2026: https://scholar.google.com/scholar?hl=en&as_sdt=0%2C11&q=Digital+Forensics+on+Solid+State+Drive+%28SSD%29+with+TRIM+Feature+Enabled+and+Deep+Free ze+Configurtion+Using+Static+Forensic+Methods+and+ACPO+Framework&btnG=

3 Srinivasan, A. (2025, October). Security and Forensics–Is Solid State Drive a Friend or a Foe?. In Proceedings of the International Symposium on Memory Systems (pp. 148-158). Accessed 2/17/2026: https://dl.acm.org/doi/pdf/10.1145/3767110.3767138

4 Mancilla, Emilia A. (2022). Enhancing the Admissibility of Live Box Data Capture in Digital Forensics: Creation of the Live Box Computer Preservation Response (LBCPR) and Comparative Study Against Dead Box Data Acquisition (pp.24-40). Accessed 2/17/2026:https://hammer.purdue.edu/articles/thesis/Enhancing_the_Admissibility_of_Live_B ox_Data_Capture_in_Digital_Forensics_Creation_of_the_Live_Box_Computer_Prese rvation_Response_LBCPR_and_Comparative_Study_Against_Dead_Box_Data_Acquisition/21671555/1/files/38419520.pdf

5 Hamid, Ishrag et al. (2024). A Comprehensive Literature Review on Volatile Memory Forensics. Accessed 2/17/2026: https://www.mdpi.com/2079-9292/13/15/3026

Beyond the immediate technical dilemma, the investigative team had to consider formal evidence-handling requirements. The investigators recognized that failure to maintain a properly documented chain of custody could result in suppression of critical evidence, regardless of its relevance to the alleged fraud scheme.[7] Because the laptop was actively running and potentially destroying data, any decision made at the scene could later be scrutinized in court. Before interacting with the laptop, the team carefully documented the scene. Photographs were taken showing the laptop's physical condition, screen state, logged-in user account, running applications, system time, and visible file activity. Investigators recorded who first observed the device, who touched it, and the exact sequence of actions taken. A contemporaneous activity log was initiated to establish a defensible chain of custody from seizure through laboratory analysis.

These technical and procedural decisions were not merely operational; they directly affected the admissibility of evidence. If defense counsel could demonstrate improper handling, failure to maintain integrity verification, or breaks in the chain of custody, critical digital evidence might be suppressed despite its substantive value.

These technical and procedural decisions were not merely operational; they directly affected the admissibility of evidence.

January 23, 2012 – Legal escalation

Prosecutors filed a motion to compel Fricosu to decrypt her hard drive based on the urgency of evidence recovery. Defense counsel objected under the Fifth Amendment, asserting that revealing the passphrase would constitute testimonial self-incrimination.[8] [9] The court ultimately ruled that Fricosu must produce an unencrypted version of the data under the foregone conclusion doctrine because the government already knew the drive existed and that Fricosu had control over it.[10] [11] [12] Judge Robert E. Blackburn granted the application under the All Writs Act and ordered production of an unencrypted copy, explaining:

6 Nyholm, H., Monteith, K., Lyles, S., Gallegos, M., DeSantis, M., Donaldson, J., & Taylor, C. (2022). The evolution of volatile memory forensics. Journal of Cybersecurity and Privacy, 2(3), pp.556-572. Accessed 2/17/2026: https://www.mdpi.com/2624-800X/2/3/28

7 D'Anna, T., Puntarello, M., Cannella, G., Scalzo, G., Buscemi, R., Zerbo, S., & Argo, A. (2023, February). The chain of custody in the era of modern forensics: from the classic procedures for gathering evidence to the new challenges related to digital data. In Healthcare (Vol. 11, No. 5, p. 634). MDPI. Accessed 2/16/2025: https://www.mdpi.com/2227-9032/11/5/634

8 Kessler, Gary C. et al. (2020). Cryptography, Passwords, Privacy, and the Fifth Amendment. Journal of Digital Forensics, Security and Law, Vol. 15, No. 2. Accessed 10/26/2025: https://commons.erau.edu/cgi/viewcontent.cgi?article=1678&context=jdfsl

9 Morrison, C. Myers (2012). Passwords, Profiles, and the Privilege Against Self-Incrimination: Facebook and the Fifth Amendment. Accessed 10/26/2025: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2005989

10 Horth, Brittany (2012). U.S. v. Fricosu: District Court Holds that Defendant Cannot Refuse to Decrypt Hard Drive under Fifth Amendment. Accessed 10/26/2025: https://jolt.law.harvard.edu/digest/u-s-v-fricosu

11 Kravets, David (2012). Feds Urge Court to Reject Laptop Decryption Appeal. Accessed 10/26/2025: https://www.wired.com/2012/02/laptop-decryption-appeal/

12 CBS Colorado (2012). Colorado Woman Must Turn Over Computer Password. Accessed 10/26/2025: https://www.cbsnews.com/colorado/news/colorado-woman-must-turn-over-computer-password/

"There is little question here but that the government knows of the existence and location of the computer's files. The fact that it does not know the specific content of any specific documents is not a barrier to production. … Additionally, I find and conclude that the government has met its burden to show by a preponderance of the evidence that the Toshiba Satellite M305 laptop computer belongs to Ms. Fricosu, or, in the alternative, that she was its sole or primary user, who, in any event, can access the encrypted contents of that laptop computer."[13]

Accordingly, the court concluded that "the Fifth Amendment is not implicated by requiring production of the unencrypted contents of the Toshiba Satellite M305 laptop computer," and directed that by February 21, 2012 Fricosu "SHALL PROVIDE counsel for the government in this case with an unencrypted copy of the hard drive," while precluding the government from using her act of production against her (use-and-derivative-use protection for the act).[14]

As shown above, several constitutional complications are recognized:

- Prosecutors sought to compel Fricosu to produce an unencrypted version of the drive. Defense counsel argued that revealing the passphrase would constitute testimonial self-incrimination, raising the constitutional question whether decryption is a physical act or a communicative act protected by the Fifth Amendment.
- The government argued that it already knew the laptop existed and that Fricosu controlled it. However, the remaining question was whether prior knowledge of the device alone was sufficient, or whether the government must also know the specific contents of the encrypted files.
- Although the court prohibited using Fricosu's act of production against her, concerns persisted that the decrypted contents themselves could implicitly convey testimonial assertions, thereby creating potential derivative-use issues.

…the constitutional question whether decryption is a physical act or a communicative act protected by the Fifth Amendment.

13 Judge Blackburn, Robert E. (2012). Criminal Case No. 10-cr-00509-REB-02. Accessed 10/26/2025: https://www.eff.org/files/filenode/fricosu_order.pdf

14 Judge Blackburn, Robert E. (2012). Criminal Case No. 10-cr-00509-REB-02. Accessed 10/26/2025: https://www.eff.org/files/filenode/fricosu_order.pdf