A Linear Algebra Unit for Critical Infrastructure Defense

Cybersecurity education, workforce development

Donna Beers[1] Clifton Morrow[2]

[1]Simmons University
[2]Taylor Business Institute

April 12, 2026

The Trailhead: Introduction

Welcome to Our Forest Jaunt

1. Identify the Analytical Gap
2. Isolate the Threat Model
3. Evaluate the Geometries
4. Scale the Architecture

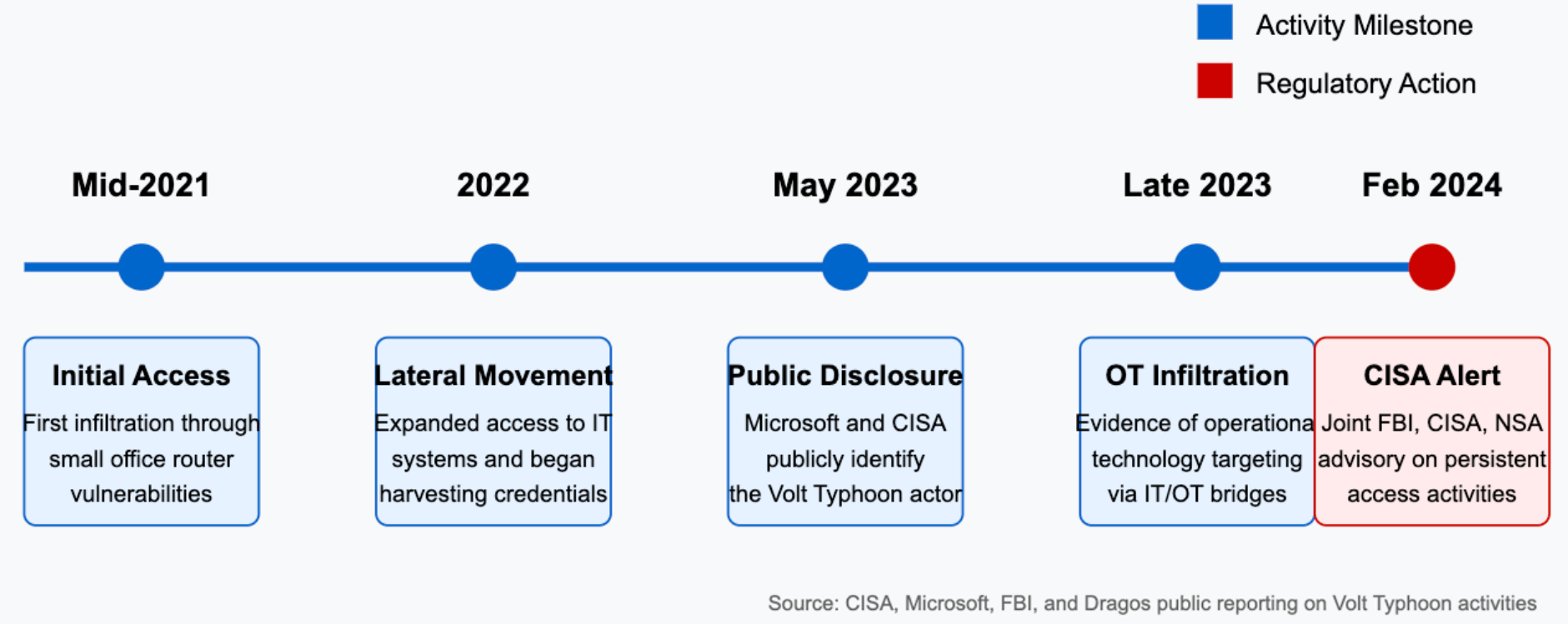
The Trailhead: Meet Your Guides

Donna Beers, Clifton Morrow

- Donna Beers is Professor of Mathematics at Simmons University in Boston, where she promotes student success in STEM through research experiences. She partners on the NASA-funded DREAM-WSTEM program, a year-long, tiered mentorship initiative that includes student research on the Muddy River's water chemistry and microbiology.
- She also collaborates with Brown University's Community Noise Lab.
- Clifton Morrow is Professor at Taylor Business Institute in Chicago, Illinois, where he teaches mathematics and STEM topics. Taylor Business Institute offers degrees in electronics and information technology.
- He co-developed and chaired the Minisymposium, *Undergraduate Research using the Mathematics of Soft Target Risk Assessment,* for the Third Joint SIAM/CAIMS Annual Meeting (AN25) (SIAM, 2025)

The Trailhead: Phase 1, Identify the Analytical Gap

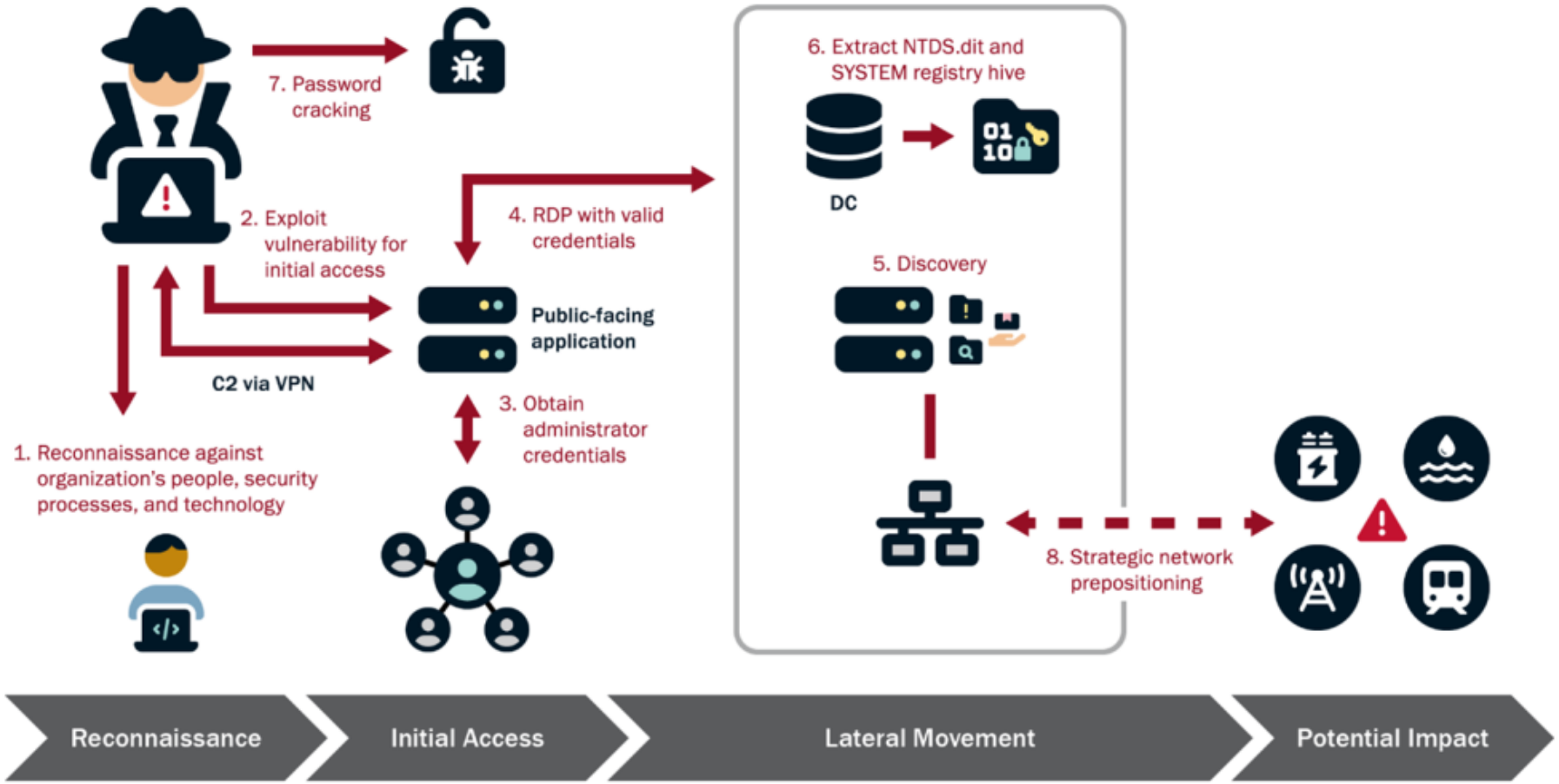
Examine the Volt Typhoon Timeline



(Waldman, 2024) Volt Typhoon and the rise of Signature-Proof protocol tunneling.

The Trailhead: Phase 1, Identify the Analytical Gap

Analyze Volt Typhoon Methods



(CISA, 2024) Volt Typhoon methodology.

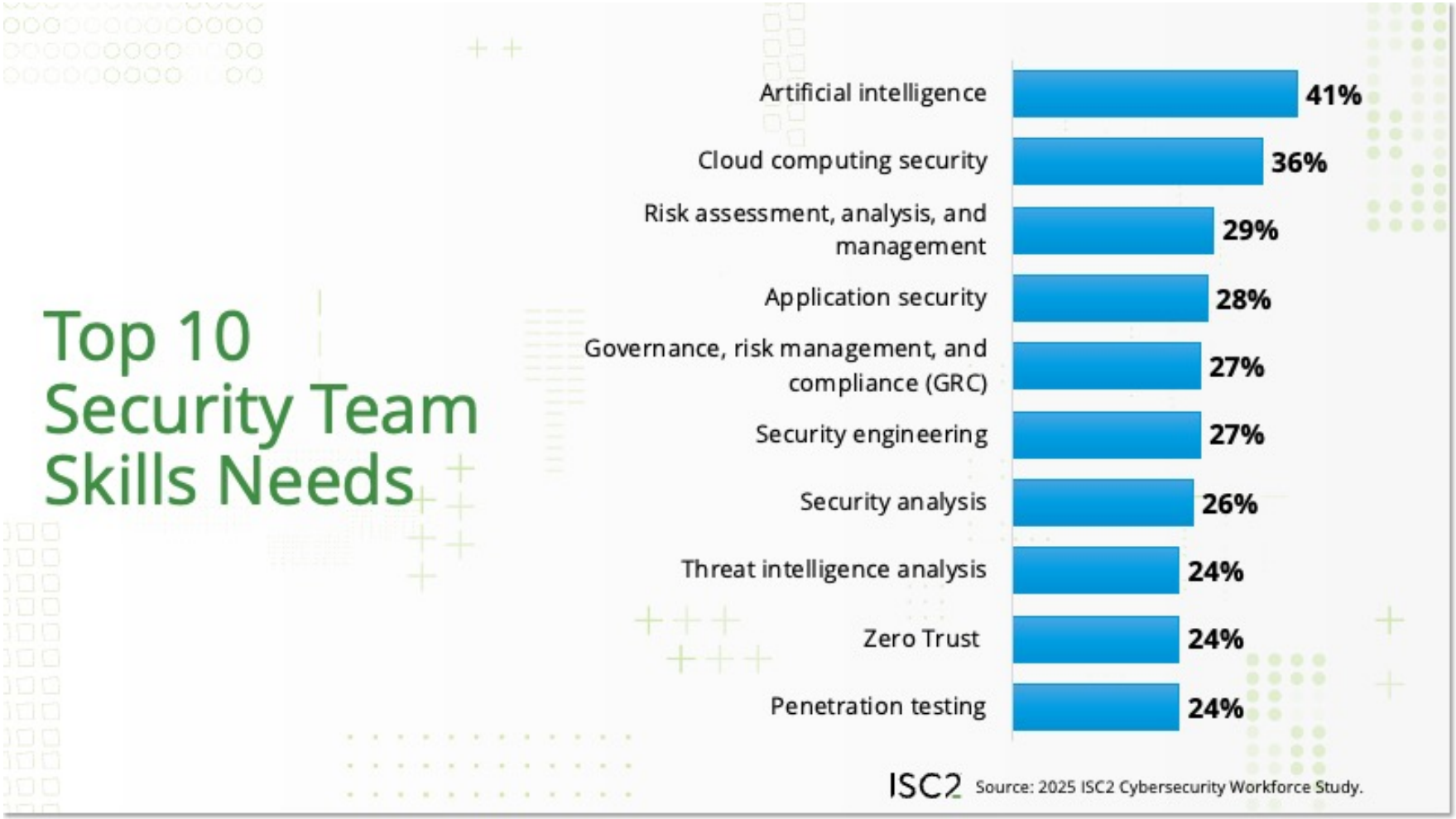
The Thicket: Gaps and Problems

Outline Security Team Skill Needs

Standard technical certifications (CySA+, GCIA) focus heavily on rule-based heuristics and signature matching. (ISC2, 2025)

The Thicket: Gaps and Problems

Rank the Top 10 Skill Needs



Algorithmic defense (Machine Learning) is treated as an opaque black box. (ISC2, 2025)

The Thicket: Gaps and Problems

Review Certification Core Focus Areas

Certification	Core Focus Areas	Heuristics / Behavioral	Signature / IOC
CompTIA CySA+	Security analytics, threat detection, SIEM, incident response	Behavioral analytics used to identify abnormal activity and threats; emphasis on analyzing anomalous activity and patterns (CompTIA, 2023)	Use of Indicators of Compromise (IOCs) such as IPs, hashes, and domains in detection and response workflows (CompTIA, 2023)
GIAC GCIA	Intrusion detection, packet analysis, IDS/IPS, traffic analysis	Detection of anomalous network behavior and deviations from baseline traffic patterns (Laman, 2026)	Strong emphasis on IDS signatures and rule-based detection (e.g., Snort) (GIAC, 2026)

The Thicket: Gaps and Problems

Review Certification Techniques

Certification	Core Focus Areas	Heuristics / Behavioral	Signature / IOC
CompTIA CySA+ (Techniques)	SOC detection methods	Heuristic detection through identification of suspicious patterns without reliance on known signatures (Chapple and Seidl, 2023)	Signature-based detection using threat intelligence feeds and known indicators integrated into SIEM/EDR platforms (CompTIA, 2023)
GIAC GCIA (Advanced)	IDS tuning, traffic forensics	Identification of normal vs anomalous protocol behavior through deep packet analysis (Laman, 2026)	Development and tuning of intrusion detection rules to detect malicious traffic patterns (GIAC, 2026)

The Thicket: Threat Model

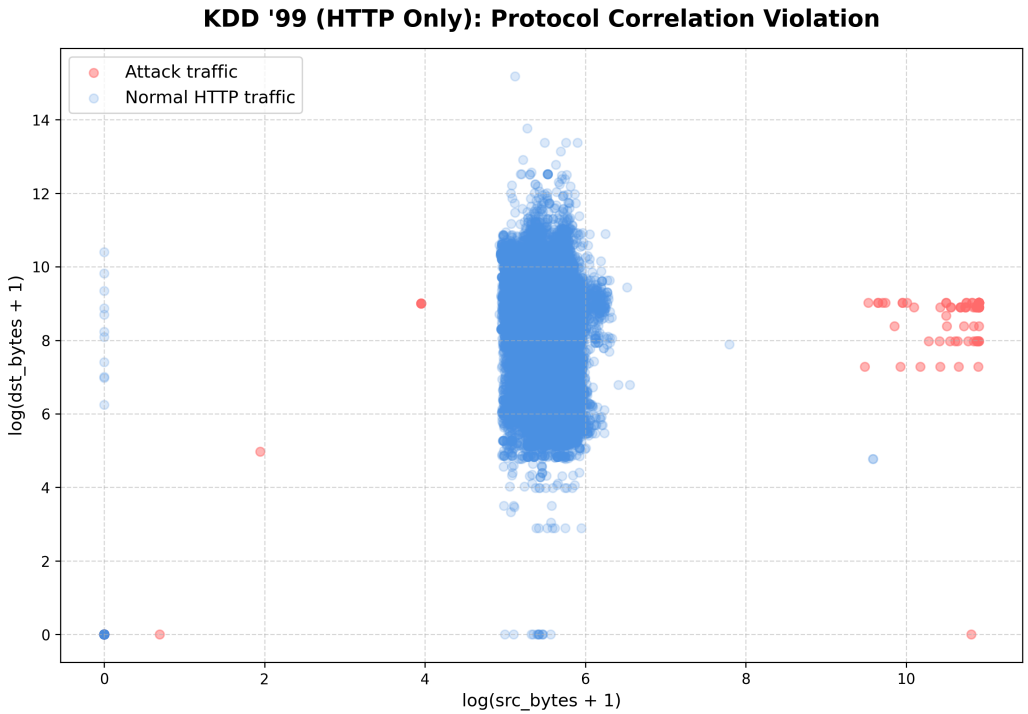
Recognize Signature-Proof Exfiltration

- Adversaries utilize protocol mimicry (Wagner and Soto, 2002) to evade standard firewall rules.
- Attackers tunnel data out via HTTP, keeping byte sizes strictly within the expected minimum and maximum historical bounds.
- Geometric thresholds and min/max rules fail by design.

The Thicket: Phase 2, Isolate the Threat Model

Apply the Scientific Method

- The Setup: Why we use the KDD '99 (UCI Machine Learning Repository, 1999) Micro-Slice (The 7×2 Janus (Ovidius Naso, 2004) Matrix).
- The Justification: It isolates a perfect Rank-1 linear correlation (Request $\propto$ Response) that students can calculate by hand, stripping away the noise of modern $n = 100$ datasets.



The Thicket: Pedagogical Glass Box

Formulate the Janus Matrix ($X \in \mathbb{R}^{7\times 2}$)

We extract a micro-slice from the KDD Cup '99 dataset.
Features: src_bytes vs. dst_bytes.

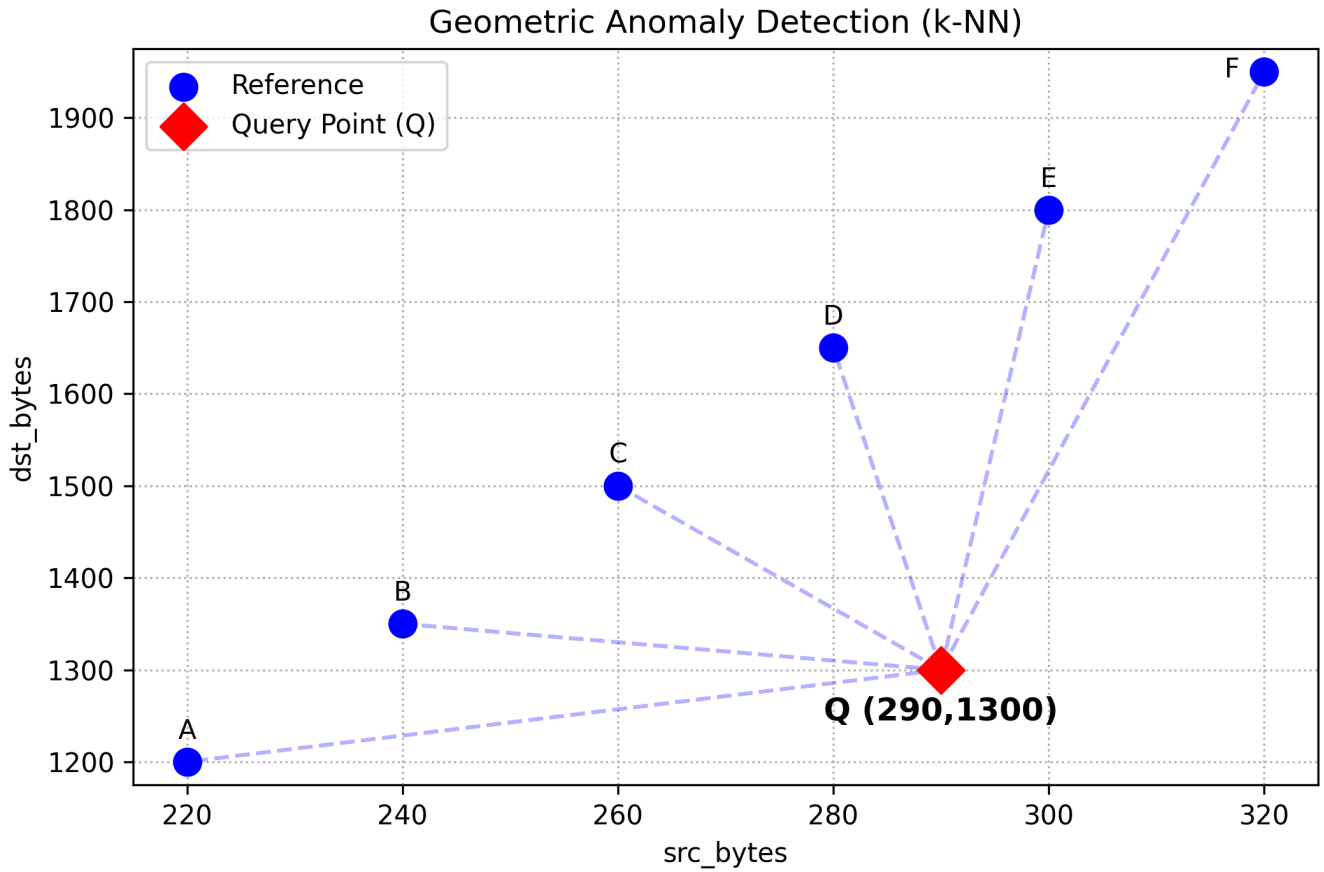
$$X = \begin{bmatrix} 220 & 1200 \\ 240 & 1350 \\ 260 & 1500 \\ 280 & 1650 \\ 300 & 1800 \\ 320 & 1950 \\ \mathbf{290} & \mathbf{1300} \end{bmatrix} \begin{matrix} \leftarrow \text{A} \\ \leftarrow \text{B} \\ \leftarrow \text{C} \\ \leftarrow \text{D} \\ \leftarrow \text{E} \\ \leftarrow \text{F} \\ \leftarrow \text{Q} = \text{query point to analyze} \end{matrix}$$

Why: It isolates a perfect Rank-1 linear correlation (Request $\propto$ Response) small enough for students to calculate by hand.
Why not use a modern dataset like UNSW-NB15 (Moustafa and Slay, 2015): high dimensionality makes them pedagogically opaque.

The Thicket: Pedagogical Glass Box

Visualize the Janus Matrix

Visualization of the 7-point dataset. The query point Q is geometrically distant from the reference points even though its coordinates reside in the benign range of both dimensions.



The Janus Lens: Phase 3, Evaluate the Geometries

Interpret the Findings

- k-NN (Duda et al., 2001) Failure. The attacker successfully hides in the gap.
- SVD (Golub and Van Loan, 2013) Success. Explain the shift from spatial proximity to orthogonal covariance.
- Spheres (k-NN) vs. Cylinders (SVD). Why an analyst must understand both geometries.

The Janus Lens: Baseline Detection (k-NN)

Measure Euclidean Distance

Evaluating the anomaly (Q) using standard Euclidean distance.
We calculate the (closest, median, furthest) distances in this table.

Point	**Coord**	**Distance** $d(Q, P_i)$
B	(240, 1350)	$\sqrt{50^2 + 50^2} \approx \mathbf{70.7}$
D	(280, 1650)	$\sqrt{10^2 + 350^2} \approx \mathbf{350.1}$
F	(320, 1950)	$\sqrt{30^2 + 650^2} \approx \mathbf{650.7}$

With $k = 3$, the nearest neighbors are $\{B, A, C\}$. A naïve voting algorithm would classify Q as Benign.
We have Query Distance: $\bar{d}_Q \approx 316.0$

The Janus Lens: Baseline Detection (k-NN)

Compute Internal Cohesion

Point i	**Point** j	**Distance** $d(P_i, P_j)$
A	**B**	151.33
B	**C**	151.33
...	...	...
A	**E**	605.31
A	**F**	756.64

A more thorough application of k-NN also fails on this dataset. This table shows that the average internal cohesion of the reference set is $\bar{d}_{internal} \approx 353.1$

The Janus Lens: k-NN Failure

Diagnose the False Negative

We have

$$316.0 < 353.1$$

$$\text{query distance} < \text{internal cohesion}$$

$$\bar{d}_Q < \bar{d}_{internal}$$

The query point is closer to the cluster center than the valid points are to each other.
The naïve voting algorithm classifies Q as Benign.
The attacker has successfully hidden in the spatial gap.

The Janus Lens: Algebraic Shift (SVD)

Model Structural Covariance

- We abandon spatial proximity and model the invariant subspace.
- The covariance structure is decomposed: $X_{cov} = V \Lambda V^T$ (Duda et al., 2001)
- This forces students to identify the correlation rule, not just the bounding box.

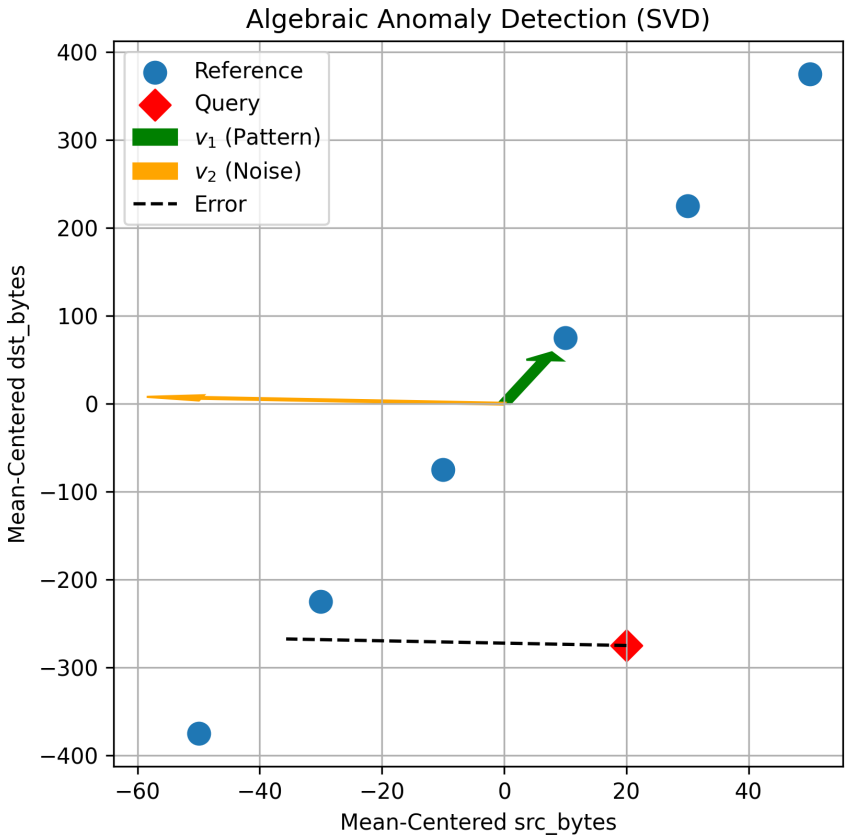
The Janus Lens: Subspace Decomposition

Extract the Rules of Traffic

$$V^T \approx \begin{bmatrix} 0.13 & 0.99 \\ -0.99 & 0.13 \end{bmatrix}$$

Row 1 (v_1): The Traffic Pattern (Valid HTTP Request/Response ratio).
Row 2 (v_2): The Noise Axis (Forbidden orthogonal variance).

Visualization of the mean-centered data and the eigenvectors (scaled by $50\times$ for visualization)



The Janus Lens: Projection Test

Detect the Variance Violation

We project the centered query point Q_c onto the noise axis v_2.

$$\begin{aligned} \text{Score} &= |Q_c \cdot v_2| \\ &= |(20)(-0.99) + (-275)(0.13)| \\ &\approx 55.6 \end{aligned}$$

This high projection score (55.6) contrasts sharply with the reference set, which has near-zero projection on v_2. Thus, SVD mathematically reveals the anomaly by detecting the variance violation, succeeding where geometric distance failed.

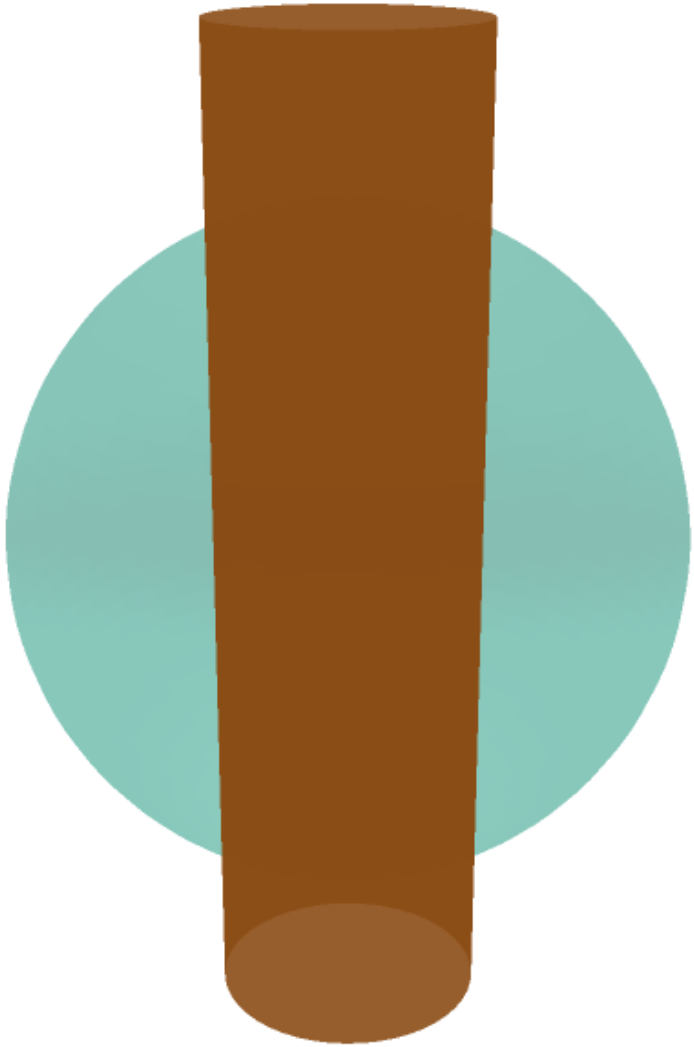
The Janus Lens: Algorithmic Synthesis

Compare Spheres vs. Cylinders

k-NN: Models radial geometric bounds (A Sphere).

SVD: Models orthogonal variance limits (A Cylinder).

Neither algorithm universally dominates; they measure fundamentally different constraints.



The Janus Lens: Opposite Case

Contrast SVD Failure with k-NN Success

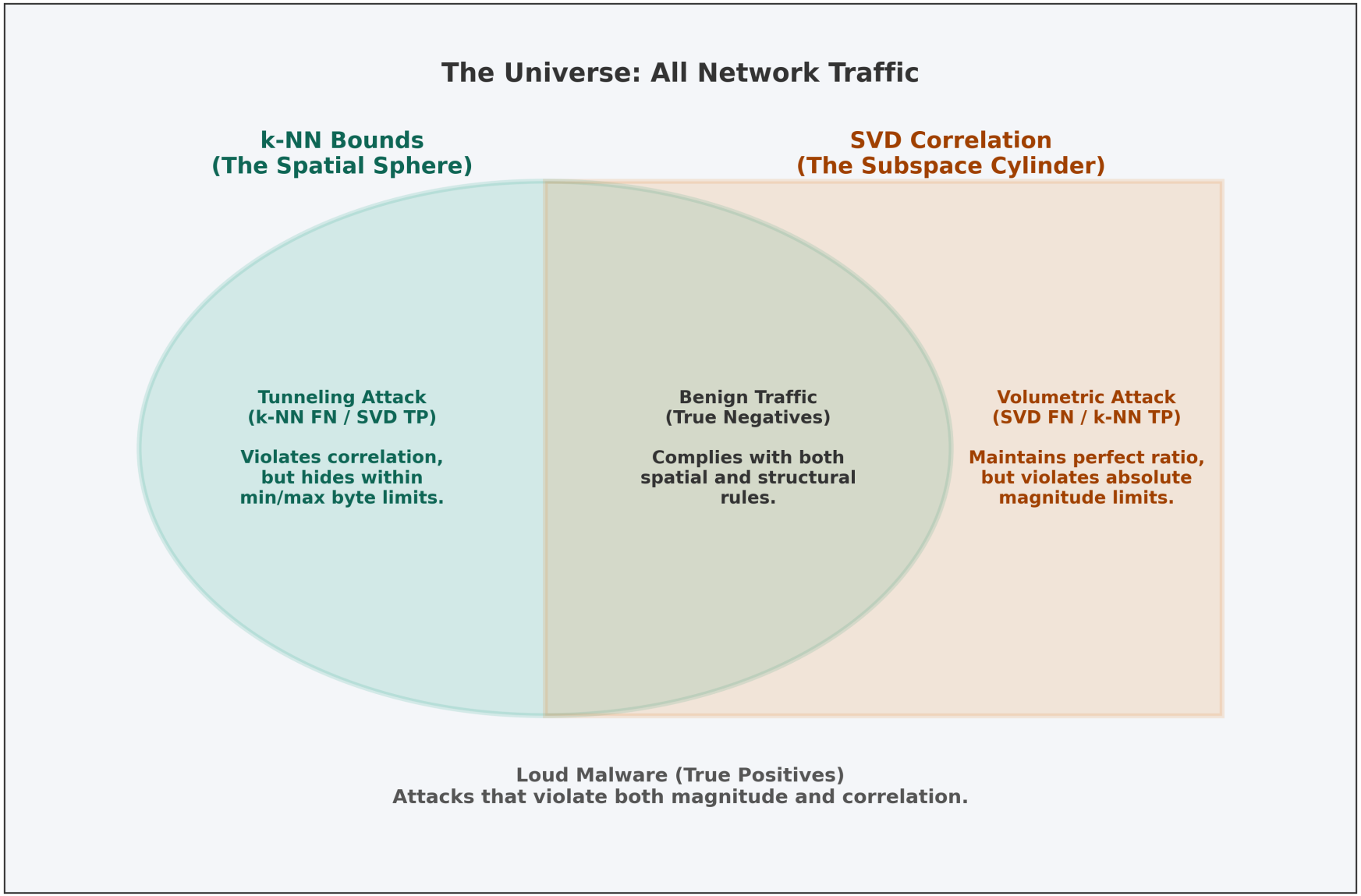
Consider a massive exfiltration event that perfectly mimics the correct byte ratio.

The point lies perfectly on the v_1 subspace (SVD projection error is zero $\rightarrow$ False Negative).

However, its massive magnitude pushes it outside the k-NN sphere (k-NN $\rightarrow$ True Positive).

The Janus Lens: k-NN Sphere vs. SVD Cylinder

Map the Venn Confusion Matrix



The Vista: System Complexity

Calculate the Cost of Defense

- Heuristics require $O(n^2)$ manual rule configurations by human analysts.
- SVD algorithmically learns the entire feature space simultaneously.

The Vista: Conclusion

Empower the Analyst

- Moving beyond black-box vendor alerts.
- Providing analysts with the algebraic fluency to understand, tune (Liu et al., 2025), and trust (Phillips et al., 2021) hybrid detection (Chandola et al., 2009) models.
- Conclusion: By teaching the underlying manifold geometry (Duda et al., 2001), we empower junior analysts to tune detection models rather than blindly trusting vendor alerts.

Review References I

Chandola, V., Banerjee, A., and Kumar, V. (2009). Anomaly detection: A survey.

Chapple, M. and Seidl, D. (2023). *CompTIA CySA+ Study Guide: Exam CS0-003*. Wiley, 3 edition.

CISA (2024). Prc state-sponsored actors compromise and maintain persistent access to u.s. critical infrastructure. [Online; accessed 9-Apr-2026].

CompTIA (2023). Cysa+ (cs0-003) exam objectives. [Online; accessed 11-April-2026].

Duda, R. O., Hart, P. E., and Stork, D. G. (2001). *Pattern Classification*. John Wiley & Sons, New York, 2 edition.

GIAC (2026). Giac certified intrusion analyst certification (gcia). [Online; accessed 11-April-2026].

Golub, G. H. and Van Loan, C. F. (2013). *Matrix Computations*. Johns Hopkins University Press, 4 edition.

ISC2 (2025). Cybersecurity professionals navigate evolving workplaces while seizing new opportunities. [Online; accessed 10-Apr-2026].

Laman, A. (2026). Sec503: Network monitoring and threat detection in-depth. [Online; accessed 11-April-2026].

Liu, X., Huang, D., Yao, J., Dong, J., Song, L., Wang, H., Yao, C., and Chu, W. (2025). From black box to glass box: A practical review of explainable artificial intelligence (xai).

Moustafa, N. and Slay, J. (2015). Unsw-nb15: a comprehensive data set for network intrusion detection systems (unsw-nb15 network data set). In *2015 Military Communications and Information Systems Conference (MilCIS)*, pages 1–6. IEEE.

Ovidius Naso, P. (2004). *Fasti*. Oxford World's Classics. Oxford University Press, Oxford. See Book I for Janus.

Phillips, P. J. et al. (2021). Four principles of explainable artificial intelligence.

SIAM (2025). Ms40: Undergraduate research using the mathematics of soft target risk assessment. also listed in the program available at https://www.siam.org/media/f3wpi00w/an25_glance_v5.pdf.

UCI Machine Learning Repository (1999). Kdd cup 1999 data. Subset: HTTP src_bytes vs dst_bytes.

Wagner, D. and Soto, P. (2002). Mimicry attacks on host-based intrusion detection systems. In *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pages 255–264. ACM.

Waldman, A. (2024). U.s. agencies continue to observe volt typhoon intrusions. [Online; accessed 9-Apr-2026].

Image Credits I

-  **File:Parsonsia straminea stems and foliage on Corymbia intermedia 7th Brigade Park, Chermside IMGP4141.jpg — Wikimedia Commons, the free media repository** (2025) by Wikimedia Commons. https://commons.wikimedia.org/w/index.php?title=File:Parsonsia_straminea_stems_and_foliage_on_Corymbia_intermedia_7th_Brigade_Park,_Chermside_IMGP4141.jpg&oldid=1043652214

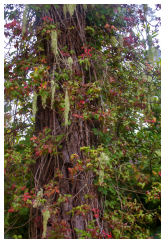
-  **Vines Growing On Tree Trunk** (n.d.) by Linnaea Mallette. https://www.publicdomainpictures.net/en/view-image.php?image=264413&picture=vines-growing-on-tree-trunk

Image Credits II

-  **File:Astrolabe, c. 1601, Isa ibn Allahdad, Indo-Persian, brass - Art Institute of Chicago - DSC09729.JPG — Wikimedia Commons, the free media repository** (2026) by Wikimedia Commons.
`https://commons.wikimedia.org/w/index.php?title=File:Astrolabe,_c._1601,_Isa_ibn_Allahdad,_Indo-Persian,_brass_-_Art_Institute_of_Chicago_-_DSC09729.JPG&oldid=1154265044`

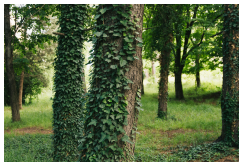
-  **Green Leaves on Tree Trunks** (n.d.) by Aleksey Vecherin.
`https://www.pexels.com/photo/green-leaves-on-tree-trunks-9562443/`

Image Credits III

-  **File:Eugène Atget (French, 1857-1927) - Trees and Roots - 2019.85 - Cleveland Museum of Art.jpg — Wikimedia Commons, the free media repository** (2024) by Wikimedia Commons. https://commons.wikimedia.org/w/index.php?title=File:Eug%C3%A8ne_Atget_(French,_1857-1927)_-_Trees_and_Roots_-_2019.85_-_Cleveland_Museum_of_Art.jpg&oldid=908107768

-  **A Tree By the Water** (n.d.) by Wolfgang Weiser. https://www.pexels.com/photo/a-tree-by-the-water-20753236/

Image Credits IV

-  **File:Mango (Mangifera indica) Probably crown gall caused by Agrobacterium tumefaciens (32589809932).jpg — Wikimedia Commons, the free media repository** (2025) by Wikimedia Commons. https://commons.wikimedia.org/w/index.php?title=File:Mango_(Mangifera_indica)_Probably_crown_gall_caused_by_Agrobacterium_tumefaciens_(32589809932).jpg&oldid=1116139395

-  **Stream Through Deep Valley** (n.d.) by Ken Kistler. https://www.publicdomainpictures.net/en/view-image.php?image=92563&picture=stream-through-deep-valley

-  **Compass on a Table** (n.d.) by Derwin Edwards. https://www.pexels.com/photo/compass-on-a-table-11209280/

Image Credits V

-  **Question Mark** (2017) by Arvin61r58.

  https://openclipart.org/detail/286084/question-mark

-  **File:Thank-you-word-cloud.jpg — Wikimedia Commons, the free media repository** (2024) by Wikimedia Commons.
  https://commons.wikimedia.org/w/index.php?title=File:Thank-you-word-cloud.jpg&oldid=971862242

The Vista

Thank You, Questions, Contact

Donna Beers
donna.beers@simmons.edu

Clifton Morrow
clifton.morrow@tbiil.edu