Digital Property
Spring 2026
Final Exam

I was pleased with your answers. While everyone got some things right and some things wrong, on the whole you displayed a solid understanding of the course's core concepts and great imagination in applying them to realistic fact patterns.

The sample answers that follow are meant to be comprehensive, rather than something I expected you to produce under time-limited exam conditions. It took me more than two hours to type up these answers—and I was the one who wrote the questions! Many of the questions could go in several different directions, and I gave full credit for any of them, as long as you did it well.

True/False

6 questions, 5 points each (30 points total) / 50 words each

Answer each of the following questions with "true," "false," or "it depends." Justify your answer in a sentence or two.

1. Zaphod sold a car to Arthur, who paid in Bitcoin. Unbeknownst to Arthur, Zaphod obtained the Bitcoin by hacking a Sirius Cybernetics Corporation computer. True or false: *Arthur must return the Bitcoin to Sirius?*

There was a mistake in this question: it should have read, "Unbeknownst to Zaphod, Arthur obtained the Bitcoin …" instead of the other way around. Unfortunately, this resulted in a question that is ambiguously wrong, and for which there is not an unambiguously correct fix. As a result, I gave everyone full credit. The answer to the question as intended is:

False. UCC § 12-104(e) makes Bitcoin fully negotiable. Because Arthur was a qualifying purchaser without notice of Sirius's claim, Arthur has good title free of Sirius's claim.

2. Magrathea Industries has a block of 16,384 IP addresses allocated by ARIN. It is short on cash and would like to raise money by selling the addresses, but ARIN rules prohibit selling IP addresses or transferring them without ARIN's permission. True or false: *Magrathea can sell the addresses, despite ARIN's policies to the contrary?*

True or It Depends. ARIN's policies do not necessarily resolve whether the IP addresses are property that Magrathea can sell. As seen in the FullNet/EBOX purchase agreement, Magrathea can make a valid contract to sell the IP addresses contingent on ARIN's approval of the transfer, which it will probably give.

3. Tricia has stored a collection of family photos in the online storage service HeartOfGold. Rob obtained Tricia's password in a phishing attack and deleted the photos. True or false: *Rob is liable to Tricia for conversion?*

True. Under *Thyroff*, files in digital storage can be property subject to conversion, and Rob has deprived Tricia of all use of those files.

4. Marvin has been playing the online game Pan-Galactic for years. Ford correctly guessed Marvin's (weak) password and transferred 200,000 "space credits" to his own account. True or false: *Marvin cannot turn to the legal system for relief against Ford, because Pan-Galactic is only a game?*

False or It Depends. If Roosevelt follows the persuasive decision in *Lakeman*, valuable in-game objects can be property that the legal system will protect.

5. Fenchurch has an account with Hactar Bank. Jeltz robs Fenchurch at gunpoint, takes Fenchurch's debit card, and uses it to withdraw $2,000 from her account. True or false: *Hactar must restore the funds to Fenchurch's account, because this was an unauthorized transaction under Regulation E?*

True. The card is an "access device" but it was obtained from the "consumer" (Fenchurch) by robbery, so the transfer is unauthorized.

6. Frankie makes an NFT of the Statute of Liberty. Benjy also wants to make an NFT of the Statute of Liberty. True or false: *Frankie can prevent Benjy from making their own NFT because there can only be one NFT representing any given thing?*

False. No technical or legal rule prevents there from being multiple NFTs that purport to represent the same thing. The Statute of Liberty is public property and in the public domain, so Frankie has no exclusive rights to it.

Short Answer

3 questions, 15 points each (45 points total) / 250 words each

7. Grunthos has created a free, ad-supported poetry history website, Azguide, with tens of thousands of poems, arranged by author and year. (All of the individual poems are old enough that they are no longer subject to copyright.) Grunthos is concerned that the Vogon Corporation, which is creating a generative-AI model specialized for writing poetry, will try to scrape Azguide to use the poems as training data. *Identify three bodies of law that Grunthos could use to try to stop Vogon, and explain why each would or would not work.*

There were more than three correct answers, but I gave credit (up to 5 points each) for any three. Here are some examples.

Copyright: Although the poems are in the public domain, Grunthos could try to assert copyright in compilation. This probably won't work. The selection might be original, but the arrangement by author and year is probably not. Under *Bartz*, the AI training process itself is likely to be a fair use. Any outputs that are similar to training data will not be similar to a copyrighted work owned by Grunthos. And the scraping process itself is not using pirated works (as in *Bartz*); these poems were placed online by Grunthos itself.

Trespass to chattels: Vogon is accessing Grunthos's tangible personal property: the servers. This is unlikely to work. Trespass to chattels only applies when there is damage to the property or interference with the owner's ability to use it. Unless Vogon's scraping imposes a severe technical burden on the servers, this case will be like *Hamidi* and the use will not be actionable.

Computer Fraud and Abuse Act: The CFAA protects against unauthorized access to computers. This is unlikely to work. *HiQ* held that when data on a computer is not walled off behind a password gate, it is not a CFAA violation to scrape it, even when the computer owner has demanded that the scraper stop.

Contract: Accessing a computer in violation of terms of service can be actionable as a breach of contract, so Grunthos could put a no-scraping

clause in its terms. This might work but requires sacrificing some usability. The challenge is forcing Vogon to agree to Grunthos's terms of service. Grunthos would probably need to make all users click through a screen requiring them to accept the terms of service, which would be a hassle for other users.

8. Eddie registered the domain name disasterarea.com through the registrar Deep Thought. He provided a Gmail email address as his point of contact. Gmail suspended Eddie's account for alleged terms of service violations (sending spam, which he disputes). As a result, Eddie, who forgot his password at Deep Thought., was unable to renew the registration to disasterarea.com, which expired. Colin then registered the domain name at Deep Thought. *Can Eddie recover the domain name? Why or why not?*

The key issue here is abandonment/expiration (discussed in the first paragraph), which was worth 10 points. I gave up to 5 additional points for good discussion of any of the additional issues raised by the problem.

The domain name is intangible property under *Kremen*. The key issue is whether Eddie abandoned the domain name. Abandonment ordinarily requires a voluntary act to relinquish control over an asset. Domain names, however, automatically expire at the end of a registration term unless they are affirmatively renewed. Eddie did not renew his registration on disasterarea.com**, and so it should probably be treated as abandoned. That made the domain name unowned and available for anyone to claim. Colin's registration made him the first possessor of the domain name, and so he is the owner. Eddie cannot recover it from Colin.**

One exception might be if Eddie has trademark rights in the phrase "Disaster Area." If so, and if Colin registered the domain name to draw in users looking for Eddie's site or for the business associated with the phrase, then Eddie might be able to recover the domain name under the UDRP or ACPA.

Eddie does not have a claim against Deep Thought. Unlike Network Solutions in *Kremen*, Deep Thought did not breach any duty it owed to Eddie. Instead, it allowed the domain name to expire at the end of its registration term, as presumably specified in its contract with Eddie.

Policy considerations support this result. The clarity of title provided by the domain name system would be undermined if the end of a registration were to become uncertain due to claims by previous registrants. Eddie was in the best position to prevent an unwanted abandonment—and he could have retained the domain name if he had not forgotten his password.

Finally, the fact that Google locked Eddie out of his Gmail account does not change the answer. As in *CRS Recovery*, control of one item of property—here, the Gmail account—effectively gives control over another—the domain name. Although Eddie disputes whether he violated Gmail's terms of service, those terms of service probably give Google the exclusive discretion to terminate accounts. Matters might be different if Colin took control of the account to take control of the domain name, because then Eddie might be able to recover the domain name as a remedy for the wrongful account takeover.

9. We have seen that plaintiffs have attempted to use the tort of conversion to protect many different kinds of property. *Give three examples of things that are protected by the tort of conversion in different ways, explain briefly what kind of a thing each of them is, and say what kind of conduct would constitute conversion.*

I gave credit (up to 5 points each) for any three answers that included different types of property. Here are some examples. Additional possible answers include a social media account, a social-media handle, an NFT, and a recording protected by state copyright law.

A domain name is a kind of intangible property. It gives the possessor the ability to direct Internet users to a particular server when they look up the domain name in the domain name system. Conversion of the domain name involves taking away that ability—for example, redirecting the domain name to point to a different server and taking away the owner's control over the name. This could involve either changing the password and credentials at the registrar, or transferring the domain name to a different registrar.

Bitcoin are a kind of intangible property. Their exclusivity is enforced by the Bitcoin blockchain. Their main use is as money: to circulate as a

form of payment. Possession of Bitcoin is achieved through control of the private key required to transfer them. Conversion of a Bitcoin involves making an unauthorized transfer to a blockchain address with a private key not controlled by the owner.

Files in storage are a kind of information property. While many people can have the same information, each of them possesses the unique copies of that information under their control. As seen in *Thyroff*, conversion of files involves completely depriving the owner of the ability to access them—for example, by deleting them.

A computer is tangible personal property. It gives the possessor the ability to use it to run programs—and also to use its physical properties, e.g., as a paperweight. It can be converted by physically destroying it or by physically taking control of the tangible object and moving it somewhere the owner cannot enter or control.

Funds in a bank account are intangible financial property. Their exclusivity is enforced by the account's access controls (e.g., a user password) and the bank's database software. They can be converted through an unauthorized transfer that drains the funds and sends them somewhere not controlled by the account owner, such as a wire transfer or cash withdrawal.

A supplemental type certificate (STC) (as seen in *G.S. Rasmussen*) represents FAA approval to safely modify a class of aircraft in a specified way. It is intangible regulatory property. It can be converted by using the certificate to obtain an airworthiness certificate from the FAA without a license from the STC owner.

Long Answer

45 points / 750 words

10. Matt Watney, a professional content creator and space enthusiast, created a fictional "moon mission." He sealed himself in a replica of an actual capsule for several days, using the Telescope streaming platform to stream himself carrying out all of the tasks that actual astronauts would. The highlight of the event was the "landing," in which he emerged from the capsule and explored the "lunar landscape" (actually his backyard).

Watney created 100 access tokens that would allow a viewer to watch the landing livestream on Telescope. If a second device attempted to watch on the livestream using the same access token, Telescope would turn off the first device's stream and start streaming to the second device instead.

The access tokens were created and managed by a smart contract written by Watney and deployed on the Martian blockchain. Watney sold the tokens for the MARS cryptocurrency (the native currency of the Martian blockchain) at a price that was equivalent to $3,000 each. Unfortunately, several incidents disrupted the experience:

- Kristin Montrose, an employee of Telescope, allowed several of her friends to watch the livestream without access tokens.
- Jessica Lewis bought a token and printed out the passcode, which she left on the desk in her office. Donald Purnell, who was there for a meeting, took a photo of the printout. Lewis started watching the livestream, but was blocked after a few minutes when Purnell used the token to start streaming instead.
- Halfway through the stream, an unknown hacker going by the name "Ares" found a bug in the smart contract and was able to transfer a token held by Aksel Vogel to a hosted wallet ending in `-6a7e`, on the Martian blockchain run by Pathfinder, a cryptocurrency exchange. Vogel was able to watch the complete livestream; no one else tried to log in using the token.

Watney is furious. He believes that these incidents ruined the livestream for him and his loyal fans.

Who can Watney and his fans sue for violating their digital property rights, what can they sue for, and what remedies will they be able to receive?

Each access token (effectively an NFT) is an item of intangible property, with control managed by the smart contract. Watney is the initial owner, and his transfers to purchasers give good title. The ability to watch the stream may or may not be "property" as such; it is non-rival because additional people can watch without interfering with each other.

Montrose

Montrose's actions are like those of the defendants in *Turoff*: she used her privileged access to allow more of something (streaming or operating taxis) than were authorized. Montrose and/or her employer, Telescope could be liable to Watney.

The first problem is identifying a cause of action. Conversion does not fit because Montrose did not deprive Watney or any of his viewers of anything; this is not a trespass to chattels because she did not interfere with the functioning of a computer; it is arguably not a CFAA violation because she was authorized to use Telescope's computers. Watney might be able to claim a breach of his contract with Telescope (it depends on what the contract says) or copyright infringement for streaming in excess of the license from Watney (which also depends on the contract). Another possible theory is trade-secret misappropriation, based on the idea that live access to the stream was supposed to be tightly controlled.

The second problem is identifying an appropriate measure of damages. Because there was no deprivation, Watney suffered no out-of-pocket losses. It does not appear that Montrose's friends paid her for access, so she has no unjust enrichment to disgorge. The best measure of damages might be the $3,000 per stream that Watney charged his viewers.

Purnell

Purnell probably did not misappropriate anything when he took a photograph of Lewis's printout of the passcode [i.e., the private key to her access token on the Martian blockchain]. It's probably not a *trade* secret in Lewis's hands, as she was using it for her own entertainment. There are no copyrights or other IP rights in the information in the passcode, so it was not a tort for him to make a copy of that information. At the

same time, however, Lewis did not voluntarily transfer the access token to Purnell, so he acquired no rights in it.

Purnell may have violated Lewis's rights when he logged into the livestream using her access token. It's a CFAA violation, because he was not authorized to watch the livestream from Telescope's computers (Lewis was), and access was controlled by the technical barrier of the access tokens. Lewis, however, suffered only $3,000 in loss (the cost of the access token), so she probably cannot sue Purnell. He may have converted the access token; it depends on whether she could have logged back in to the livestream using it. [This was ambiguous in the problem; it depends on how Telescope was configured and on the relationship between the passcode and the access token.] If watching the stream was a form of property, then he converted it by logging in and locking her out.

Ares

A strict "code is law" view of blockchains would say that Ares was authorized to transfer the token because the smart contract allowed them to do it. A view more consistent with the cases in the course materials would say that they were not authorized because the bug was not part of how the contract was intended and understood to function. [Whether that access was also a CFAA violation depends on subtle questions about how the CFAA applies to blockchains, which we did not discuss in this course.]

As a result, the transfer to the -6a7e wallet was effectively a form of theft. Ares converted Vogel's access token and deprived Vogel of control over it. But because whoever received the access token did not attempt to view the livestream, Vogel might be entitled only to nominal damages from Ares. Even if viewing the stream live in real time is property, that property was not converted or interfered with.

Vogel might or might not be able to recover the access token. The problem is not securing control over it. As in *AA v. Persons Unknown*, Pathfinder can be ordered to freeze the hosted wallet and turn over the token to Vogel if he prevails in court. But because the access token is a controllable electronic record under UCC article 12, the unknown owner of the -6a7e wallet might benefit from the take-free rule of § 12-104(e). It depends on whether the owner is a qualifying purchaser who gave val-

ue for the token and whether they knew of the theft, neither of which can be answered for certain without more information on who they are and the facts of the transaction.