

The Witness

Read a modem's heat, not its logs, and prove a covert miner the firewall never saw

Dr. Ahmet Furkan Aydogan | aydogana@uncw.edu

Department of Computer Science, University of North Carolina Wilmington

Track	Cyber Operations (CYBR 358)	Deliverable	The completed Word worksheet
Term	Fall 2026	Points	100
Instructor	Dr. Ahmet Furkan Aydogan	Assigned / Due	_____

Abstract. *In September 2026 scientists published the first complete wiring map of a fruit fly's whole nervous system: about 140,000 neurons, driven in part by a few cells that steer the fly toward warmth it likes and away from heat it does not. A fly is, among other things, a tiny walking thermometer. This lab borrows that idea. You are the attacker on a compromised home modem that is secretly mining cryptocurrency. The modem has a firewall that will block and alarm if you flood it, so you must mine quietly, just under its rate limit. You will find that no matter how quiet you keep the network traffic, the work still heats the modem's case, and the flies in the room desert the warm modem for a comfortable ring around it. The firewall and the logs see nothing. The flies see everything. Part I explains why a physical side channel like heat escapes a network defense; Part II is the graded operation you carry out on the class board.*

Source and honesty. The fly is real: the whole-nervous-system connectome was released in 2026 (FlyEM / Janelia, the Cambridge Connectomics Group and Google Research). Thermal and power *side-channel* attacks are a real, established class of security problem. Everything you touch here, the modem, the miner, the firewall and the flies, is a synthetic simulation: no real device is used, no credentials or personal data are involved, and the flag is a harmless synthetic string.

1. PART I. Why heat tells on a quiet attacker

The one-line story

A cheap home modem is compromised and put to work mining cryptocurrency. Mining is just a lot of computation, and computation costs the processor work, and work turns into heat. The attacker keeps the network side quiet so the modem's own firewall never notices. But the heat has to go somewhere. The modem's plastic case warms by several degrees, and the insects that share the room, which steer by temperature, stop resting on the now too-hot modem and settle in a ring a short distance away. Their positions, not the network logs, are what reveal the intrusion.

Overview and learning objectives

By the end of this lab you will be able to:

- explain, in plain language, what a side channel is and why heat is one;
- describe how a rate-limit firewall decides what to block, and what it cannot see;
- find the highest request rate that mines effectively while staying under that limit;
- read a simple physical detector (the flies' positions) and say what it proves; and
- judge why a network-only defense misses a low-and-slow abuse that a physical channel still exposes.

Key terms

Each term is defined once, in plain words, with an everyday comparison.

- **Side channel.** Information that leaks through a by-product of a system rather than through its normal output. A locked office reveals nothing through the door, yet a warm doorknob still says someone was just inside. Here the by-product is heat.
- **Thermotaxis.** An animal's movement guided by temperature. A fruit fly has a strong preferred temperature, near 24 degrees, and walks away from anything much hotter, the way you edge back from a fire that is too close.
- **Cryptomining.** Running heavy repeated computation to earn cryptocurrency. On a hijacked device it is theft of electricity and compute; more mining means more processor load.
- **Rate limit (firewall).** A rule that caps how many requests per second a device will accept. Ask politely within the cap and you are served; hammer past it and the excess is dropped, and if you keep hammering the connection is cut and an alert is raised. Think of a ticket window that serves a steady line but calls security when someone shoves.
- **Covert versus overt.** An overt attack trips the alarm; a covert one stays under every threshold the defender set. The whole point of this lab is a covert miner: quiet on the network, loud in the physical world.
- **Detector.** Anything that turns a signal into a decision. Here the flies are the detector: their move from the modem to a ring is the alarm the firewall never sounded.

The same mechanism from two chairs

Heat rises with processor load. That one fact is the whole lab, read two ways.

The mechanism on the attacker's side. You want to mine as much as possible. More requests means more load means more coins. But push past the firewall's rate limit and you are blocked and flagged, so your yield drops to zero and you are caught on the network. The move is to sit just under the limit: the maximum quiet rate.

Now flip it. The mechanism on the defender's side. You cannot see the mining in the network logs, because the attacker stayed under your limit. But you can measure the modem's temperature, or watch anything in the room that responds to temperature. The load that was invisible to the firewall is plain in the heat.

Key finding. A rate-limit firewall answers one question, "is the traffic within my cap," and a patient attacker can always answer yes. Heat answers a different question the attacker cannot suppress, "is this device working hard," and that is the question that catches a covert miner.

2. PART II. The operation

Where your answers go

Do NOT hand in a blank document. Open the file "The Witness, Student Worksheet.docx" that came with this lab. Every step and question below has a matching answer line, box, or table in that worksheet: record your flag, paste your screenshots, and write your explanations there. The completed worksheet is what you submit.

Practise first: the offline simulator

Your kit contains a single self-contained page, `simulator/witness_sim.html`. Double-click it to open it in any web browser; nothing is installed and no network is needed. It has two modes:

- **Auto incident** plays a full simulated day in which the miner fires twice on the modem. Watch the flies leave the modem during each burst and the detector line rise. This shows you the effect before you cause it.

- **Manual (terminal)** hands you the controls. Type `help`, then `fw.status` to read the firewall's rate limit, then write a short `miner.js` in the editor and Run it. Raise the rate and watch the modem's case temperature climb and the flies back off to the ring.

Use the simulator until you can reliably heat the modem without tripping its firewall. Then do it for grades on the class board.

The class board (your environment)

You will not install any server. The instructor runs the modem's control board and gives each student a private board keyed by Student ID. Two things are keyed to your ID and to no one else's: your firewall's exact rate limit, and your flag. You cannot use a classmate's numbers; you must do your own recon.

The board is reached in your web browser at:

- **Board address:** <https://tennessee-shall-agree-discussing.trycloudflare.com>
- **Entry page:** open the board address, then type your Student ID to open your own board.
- **Your board:** shows your firewall's rate limit (your recon), and a form to run the miner.

Note on the address. This is a temporary class tunnel. If it stops working, your instructor will post a new address; the lab is identical on the new link.

Worked example (how to open your page). Suppose your Student ID is 23914242. Open <https://tennessee-shall-agree-discussing.trycloudflare.com>, type 23914242, and confirm the page shows your own ID at the top and a firewall rate limit for your board. Use *your own* Student ID, not 23914242, which is only an example; your limit and your flag are tied to your ID.

Your job: mine at the highest quiet rate, then read the heat

1. **Recon.** Read your firewall's rate limit from your board (Step 1 card). This is the ceiling.
2. **Mine.** Choose a request rate just under that ceiling, a duration long enough to heat the case, name the device the anomaly is on, and say in one line what the flies do.
3. **Submit.** The board runs your plan, shows the resulting case temperature, and marks each of five checks green or red.
4. **Read the witness.** When all five are green, the board reports that the firewall logged nothing yet the case ran hot and the flies gave it away, and it relays your flag.

How the gate scores you

When you submit, the board checks five things and marks each green (present) or red (missing).

Check	What it wants
Under the limit	Your rate is at or below your firewall's limit, so no alert fires. Over it, you are blocked.
Highest quiet rate	Your rate is within 60 req/s below the limit: mine hard, do not leave yield on the table.
Sustained	Your duration is at least 60 seconds, long enough for the case to actually heat.
Correct device	You name <code>modem</code> as the anomaly. The oven, TV and fridge also warm on their own schedules; only one is the mining host.
Understands the tell	You state in a few words what the flies do (leave the hot modem, form a ring) that the firewall and the logs never record.

All five green, and the flag appears. Any red, and the board tells you exactly what to fix.

Where each part comes from (how to discover it)

You are not expected to guess. Everything is shown on your board or is learnable in the simulator first.

Part	Where you find it	How
Firewall limit	your board (Step 1), or <code>fw.status</code> in the simulator	The board prints your ceiling; the simulator's <code>fw.status</code> prints the same kind of policy.
The quiet maximum	the simulator	Raise the rate in Manual mode until just before the firewall trips; that band is your target.
Duration	the simulator	Watch how long the case takes to heat once mining starts; pick a duration past that.
Anomaly device	the simulator	In Auto mode, see which device the flies desert during the bursts.
The tell	the simulator	Describe what the flies do: they leave the modem and settle in a ring.

Setup and procedure

Put the lab folder on your Desktop. Open `simulator/witness_sim.html` in a browser to practise. When you are ready, open the announced board address and enter your Student ID. Do the steps in order.

1. **Open your board.** Enter your Student ID and confirm the page shows your own ID and your firewall's rate limit.
2. **Practise in the simulator.** In Manual mode, run `fw.status`, then mine at several rates and watch the case temperature and the flies. Find the highest rate that never trips the firewall.
3. **Plan your run.** Write down a rate just under your board's limit, a duration of at least 60 seconds, the device (`modem`), and one line on what the flies do.
4. **Submit it.** Enter your plan on the board and read the resulting case temperature and the five-part verdict.
5. **Fix the red parts and resubmit.** Correct whatever is red. Each verdict moves you one step closer; this is not guessing.

6. **Capture the flag.** When all five parts are green, the board relays your flag. Take a screenshot showing your Student ID and the flag together.

[Screenshot 1 goes here]

A sample board verdict

Result of your run

modem case temperature: 33.7 C

Physical witness: the flies backed off to a ring; the thermal witness fired.

Gate feedback

[check] Under the firewall limit (no alert)

[check] Mining at the highest quiet rate

[check] Sustained long enough to heat

[check] Correct anomaly device

[check] Understands the thermal side channel

3. Analysis questions

Answer each in a few sentences in the worksheet, using what you observed.

1. **The measurement.** In the simulator, record the modem's case temperature at rest and again while mining at your quiet maximum. Why is a change from a baseline a better alarm than any single temperature reading on its own?
2. **Identify.** Name the five devices in the simulated home and say which one is the anomaly and why the other four are decoys. What makes the modem's heat different from the oven's?
3. **In your own words.** Your miner never tripped the firewall and left the network logs clean. Explain to a first-year student how the flies still caught it, using an analogy that is not the one used in this handout.
4. **Limits of the evidence.** The flies moving to a ring proves the modem got hot. Does it prove the cause was mining, or only that the device was working hard? What else could heat a modem, and how would a defender tell the difference?
5. **Trade-off and judgment.** From the defender's chair, name one physical or behavioural signal you would monitor to catch covert mining, and one real cost it imposes. From the attacker's chair, say in one sentence why staying under the firewall's limit was still not enough to stay hidden.

4. Deliverable, grading, and ethics

Deliverable. Fill in the provided Word worksheet, "The Witness, Student Worksheet.docx": record your flag, paste your required screenshot, complete the observation log, and answer Q1 to Q5. Save it as `Lastname_Firstname_Witness.docx` (or export to PDF) and upload it. A screenshot clearly showing your Student ID and your flag, with all five parts green, is mandatory.

Criterion	Points
Evidence captured: screenshot of your flag (your Student ID and flag, all five parts green)	30
Observation log completed (at least three runs recorded, with rate and case temperature)	15
Q1 to Q2: correct measurement and identification of the anomaly versus the decoys	25
Q3 to Q5: thoughtful judgment on side channels, causation, and defense	20
Clarity, structure, and correct use of terms	10

Academic integrity, scope, and ethics. This is individual work. Everything here is a synthetic simulation: no real device, credential, or personal data is involved, and the flag is a harmless synthetic string. Work only on the class board and your own machine. Your firewall limit and flag are tied to your Student ID, so use your own. Studying how a covert miner is caught is defensive knowledge: the lesson is that a network limit and a physical by-product can disagree, and the by-product wins. The technique is neutral; the target and the authorization are what make it right or wrong. A correctly reported “I could not pass yet,” with your runs recorded, earns partial credit; an invented flag earns zero. AI may help you understand the tools, but run every step yourself.

Questions? Email the instructor at aydogana@uncw.edu.