# PACS FORENSIC EVIDENCE PACKET

## Scenario 5: "Carbon Copy" — IT/Cybersecurity Reference

Distribute to IT/Cybersecurity Team (Team B) at Exercise Start
FOR TRAINING USE ONLY

## EXHIBIT A: PACS EVENT LOG — BADGE NCIA-2847 (LAST 72 HOURS)

The following is the full PACS event log for badge NCIA-2847 (Carlos Mendez, SkyWay Catering) for the 72 hours preceding the duplicate credential alert. Events highlighted in **bold** are anomalous.

| Timestamp | Door | Location | Result | Reader Freq | Notes |
|---|---|---|---|---|---|
| Tue 06:52:14 | S-4 | Conc A Boundary | GRANTED | 13.56 MHz | Normal — Mendez morning shift start |
| Tue 07:01:33 | K-2 | Concourse A Kitchen | GRANTED | 13.56 MHz | Normal — SkyWay catering prep area |
| Tue 12:15:08 | S-4 | Conc A Boundary | GRANTED | 13.56 MHz | Normal — Lunch break exit |
| Tue 12:48:22 | S-4 | Conc A Boundary | GRANTED | 13.56 MHz | Normal — Return from lunch |
| Tue 15:30:45 | S-4 | Conc A Boundary | GRANTED | 13.56 MHz | Normal — End of shift |
| Wed 06:48:07 | S-4 | Conc A Boundary | GRANTED | 13.56 MHz | Normal — Morning arrival |
| Wed 07:05:11 | K-2 | Concourse A Kitchen | GRANTED | 13.56 MHz | Normal — Catering prep |
| Wed 10:22:38 | V-1 | Vendor Break Room | GRANTED | 125 kHz ■ | **ANOMALOUS: This reader is 125 kHz legacy. First time Mendez badge read at 125 kHz in 30 days.** |
| Wed 10:23:05 | V-1 | Vendor Break Room | GRANTED | 125 kHz ■ | **Second read 27 seconds later. Same door. Why badge twice?** |
| Wed 12:10:44 | S-4 | Conc A Boundary | GRANTED | 13.56 MHz | Normal — Lunch |
| Wed 15:28:19 | S-4 | Conc A Boundary | GRANTED | 13.56 MHz | Normal — End of shift |
| Thu 06:55:30 | S-4 | Conc A Boundary | GRANTED | 13.56 MHz | Normal — Mendez morning arrival |
| Thu 07:04:18 | K-2 | Concourse A Kitchen | GRANTED | 13.56 MHz | Normal — Catering prep |
| **Thu 07:38:12** | **S-4** | **Conc A Boundary** | **GRANTED** | **125 kHz ■** | **ALERT EVENT 1 — 125 kHz read. But Mendez is already inside (entered at 06:55). Why is his badge at S-4 again?** |
| **Thu 07:39:41** | **R-7** | **Ramp — Baggage** | **GRANTED** | **13.56 MHz** | **ALERT EVENT 2 — 89 sec after S-4. Mendez would have to be in two places at once.** |
| **Thu 07:44:09** | **M-3** | **Maint Corridor B** | **GRANTED** | **125 kHz ■** | **Clone continues — Maintenance corridor, 125 kHz reader. Leads to mechanical rooms.** |
| **Thu 07:51:33** | **E-2** | **Electrical Room B** | **GRANTED** | **125 kHz ■** | **Clone accesses Electrical Room B — houses network switch closet for Concourse B.** |
| **Thu 08:03:17** | **M-3** | **Maint Corridor B** | **GRANTED** | **125 kHz ■** | **Clone exits via maintenance corridor.** |
| **Thu 08:07:44** | **S-6** | **Conc B Boundary** | **GRANTED** | **125 kHz ■** | **Clone exits to non-sterile side via S-6 (125 kHz legacy reader).** |

## EXHIBIT B: READER FREQUENCY ANALYSIS

NCIA's PACS system includes a mix of modern and legacy badge readers. The following analysis shows which readers still operate in legacy 125 kHz mode:

| Door | Location | Reader Model | Frequency | Encryption | Clone Risk |
|---|---|---|---|---|---|
| S-1, S-2, S-3 | Main terminal boundary | HID iCLASS SE R40 | 13.56 MHz | AES-128 | LOW |
| **S-4** | **Conc A boundary** | **HID multiCLASS SE** | **DUAL: 13.56 MHz + 125 kHz** | **13.56: AES-128 125: NONE** | **HIGH — accepts unencrypted legacy cards** |
| S-5 | Conc B boundary | HID iCLASS SE R40 | 13.56 MHz | AES-128 | LOW |
| **S-6** | **Conc B boundary (secondary)** | **HID ProxPoint Plus** | **125 kHz ONLY** | **NONE** | **CRITICAL — legacy reader, no encryption** |
| R-1 thru R-6 | Ramp access doors | HID iCLASS SE R40 | 13.56 MHz | AES-128 | LOW |
| R-7 | Ramp — baggage makeup | HID iCLASS SE R40 | 13.56 MHz | AES-128 | LOW |
| **V-1** | **Vendor Break Room** | **HID ProxPoint Plus** | **125 kHz ONLY** | **NONE** | **CRITICAL — legacy reader, no encryption** |
| K-1, K-2 | Kitchen / Catering | HID iCLASS SE R40 | 13.56 MHz | AES-128 | LOW |
| **M-1 thru M-4** | **Maintenance corridors** | **HID ProxPoint Plus** | **125 kHz ONLY** | **NONE** | **CRITICAL — legacy readers, no encryption** |
| **E-1, E-2** | **Electrical rooms** | **HID ProxPoint Plus** | **125 kHz ONLY** | **NONE** | **CRITICAL — houses network infrastructure** |

## Key Finding

The clone was read at 125 kHz at every door it accessed (S-4, M-3, E-2, S-6). The real Mendez badge was read at 13.56 MHz at every door he accessed (S-4 at 06:55, K-2, R-7). This means the clone is a **125 kHz proximity card** — a cheap copy of the unencrypted legacy credential number. It can only pass through doors that still have legacy 125 kHz readers or dual-mode readers in legacy-compatible mode.

# EXHIBIT C: NCIA DOOR MAP — CLONE MOVEMENT OVERLAY

The clone's path through the airport, based on PACS logs:

| Time | Door | Action | What This Tells Us |
|---|---|---|---|
| **07:38:12** | S-4 (125 kHz) | Clone enters sterile side via Concourse A boundary | Clone enters through a dual-mode reader using the legacy 125 kHz credential. The real Mendez entered through S-4 at 06:55 using 13.56 MHz — he's already inside. |
| **07:44:09** | M-3 (125 kHz) | Clone enters Maintenance Corridor B | The clone is heading away from the gate area and toward the mechanical infrastructure. This is not a passenger area — it's back-of-house. |
| **07:51:33** | E-2 (125 kHz) | Clone enters Electrical Room B | CRITICAL: Electrical Room B houses the Concourse B network switch closet — a Layer 2 switch, fiber patch panel, and a wireless access point. The clone spent approximately 12 minutes inside. |
| **08:03:17** | M-3 (125 kHz) | Clone exits back through maintenance corridor | Retracing their route. They got what they came for. |
| **08:07:44** | S-6 (125 kHz) | Clone exits to non-sterile side via Concourse B boundary | Exit through a different door than entry — S-6 instead of S-4. Classic counter-surveillance: don't use the same path twice. |

### The 12-Minute Question

The clone was inside Electrical Room B for **12 minutes** (07:51:33 to 08:03:17). That room contains a Cisco Catalyst 2960 Layer 2 switch, a fiber optic patch panel, a Ruckus wireless access point serving Concourse B, and a UPS battery backup. Twelve minutes is enough time to:

- Install a rogue network device (e.g., a network tap, a Raspberry Pi, or a rogue wireless AP)
- Capture MAC addresses and VLAN tags from the switch's management interface
- Physically tap the fiber with a passive optical splitter
- Photograph the switch configuration, patch panel labeling, and cable routing
- Connect a laptop to an open port and perform network reconnaissance

**The IT team needs to physically inspect Electrical Room B immediately.**