Forensics Incident Response Playbook

A Field Guide for the First 72 Hours

This playbook is written for business owners, IT managers, finance leaders, and in-house counsel who just learned something is wrong. Maybe an email flagged a wire transfer after it went out. Maybe an executive lost control of a phone number. Maybe a wallet is empty. Maybe a ransom note is on every server.

You do not have time to read a textbook right now. You need a checklist of what to do, what not to do, and who to call. That is what this book is.

Petronella Technology Group is a Raleigh-based firm founded in 2002. Craig Petronella holds Licensed Digital Forensic Examiner credential DFE #604180, along with CMMC-RP, CCNA, CWNE, and an MIT artificial intelligence certificate. The team is CMMC-RP certified across the board. The firm is a CMMC-AB Registered Provider Organization (RPO #1449), BBB accredited A+ since 2003, and holds PPSB accreditation. Petronella's forensic specialties are SIM swap response, crypto theft triage, pig butchering scam evidence, ransomware triage, business email compromise recovery, and insider threat investigations. Our scope goes through a trusted partner network.

This document is not legal advice. It is an operational checklist. Share it with your incident commander, your attorney, and your insurance broker before you need it.

Incident line: (919) 348-4912 **Consult form**: petronellatech.com/contact-us/

Petronella Technology Group

Licensed Digital Forensic Examiner
CMMC-AB Registered Provider Organization #1449
Raleigh, North Carolina

DRAFT FOR REVIEW

2026 Edition

Table of Contents

Chapter 1: The First 60 Minutes After You Suspect a Breach

The first hour after you notice something is wrong is the hour that decides whether evidence survives. Most victims destroy their own case in the first ten minutes because they panic. This chapter is for whoever is holding the incident when the alarm fires. Read it before you touch anything.

What NOT To Do

1. Do not power off the machine. Volatile memory holds attacker processes, decryption keys, and running malware. If you shut down, those go away.
2. Do not re-image or wipe the drive. You destroy artifacts that establish the attack timeline.
3. Do not call the phone number the attacker gave you. It confirms you as an engaged target and can trigger the next stage of the scam.
4. Do not pay anything, sign anything, or click anything in the ransom note until a forensics resource is on the phone with you.
5. Do not post to social media or customer email about the incident yet. Early disclosure without scope often triggers regulatory notice clocks you are not ready to start.
6. Do not run your own antivirus scan to "clean it up." You overwrite artifacts.
7. Do not let staff log in to check email on the suspect machine.

Minute-by-Minute Triage

Minutes 0 to 5: Contain without destroying.

1. Pull the ethernet cable. Disable Wi-Fi at the adapter level, not by powering off.
2. Photograph every screen with a phone camera. Include ransom notes, unusual processes, browser tabs, and running dialogs.
3. Note the exact time. Write it down. All later timestamps refer back to this.
4. Identify which user was logged in, what they were doing, and the last action before the alarm.

Minutes 5 to 15: Call the right people.

1. Call your incident response firm first. Petronella incident line: (919) 348-4912.
2. Call your cyberinsurance carrier second. Most policies require notice within 24 to 72 hours or benefits drop. Do this on a different device than the one that is compromised.
3. Notify your attorney. Privilege attaches better when counsel is engaged early.

Minutes 15 to 60: Preserve and contain.

1. Identify other machines on the same network. Assume lateral movement until proven otherwise. Isolate them the same way.
2. Preserve firewall logs, endpoint detection and response logs, authentication logs, and cloud console audit logs. Download to external media. Do not delete anything.

3 Capture a memory image if you have the tooling. If not, wait for the forensics team to arrive before touching the machine.

4 Document who has been told what, in writing, with timestamps. This becomes the incident journal.

Evidence Preservation

- Use an external drive you own. Do not write evidence to the cloud before talking to counsel.
- Hash everything with SHA-256 as you copy it. Write the hash on a sticky note and photograph it.
- Keep the original machine powered on and network-isolated until the forensic examiner says you can shut it down.
- Store physical evidence like USB drives, phones, and written ransom notes in a locked drawer. Log who touches what and when.

When to Escalate

Escalate to a Licensed Digital Forensic Examiner any time you see any one of these:

- A ransom note or extortion message.
- A wire transfer you did not authorize.
- Loss of access to your own phone number or email.
- Executive or admin credentials confirmed compromised.
- Customer data exfiltration alerts.
- Regulated data (PHI, CUI, PCI) in scope.

Petronella Services Referenced in This Chapter

Petronella's incident response team handles initial triage, evidence preservation, and forensic imaging for the categories covered in this playbook. Schedule a confidential forensics consult at petronellatech.com/contact-us/ or call (919) 348-4912. The team is a CMMC-AB Registered Provider Organization and includes Licensed Digital Forensic Examiner credentials for court-admissible work.

Chapter 2: SIM Swap Triage

A SIM swap is when an attacker convinces your mobile carrier to move your phone number to a SIM card they control. Once that happens, every two-factor text, every password reset link, every bank verification call goes to them. The window to respond is short. Usually four to seventy-two hours before the attacker has drained what they came for.

This chapter is for the person who just realized their phone says "No Service" for no reason, or whose executive cannot receive calls.

What NOT To Do

1. Do not try to reset accounts from the phone you suspect was swapped. The attacker will intercept the codes.
2. Do not ignore a sudden loss of signal as a carrier glitch. Losing service on a normal day in a normal coverage area with a working phone is the warning sign.
3. Do not call your carrier from the compromised number. Call from a separate line.
4. Do not share the new recovery codes over SMS. Use a secondary email or authenticator app.

Minute-by-Minute Triage

Minutes 0 to 15: Confirm and lock down the carrier.

1. Call your carrier from a different phone. Go to the fraud or account security menu, not general support.

- T-Mobile: 1-800-937-8997 then request the fraud department.
- Verizon: 1-800-922-0204 then ask for the fraud team and "port freeze."
- AT&T: 1-800-331-0500 then request "port protection" and "wireless account lock."

1. Request a full account lock, port freeze, and SIM change hold. Verify in writing (text, email, or portal screenshot) that the lock is active.
2. Ask the carrier for the timestamp of the last SIM swap or port request and the requesting channel (store, phone, portal).

Minutes 15 to 60: Protect the downstream accounts.

1. On a clean device, change passwords for: email, bank, broker, cryptocurrency exchange, and password manager. In that order.
2. Move two-factor for those accounts from SMS to an authenticator app or hardware security key.
3. Revoke active sessions on email and financial accounts.
4. Check email for recent password-reset emails you did not initiate. Those reveal which accounts the attacker already touched.

Hours 1 to 24: Widen the net.

1. Notify your bank's fraud team by phone. Ask for a transaction review for the last seven days.

2 If you hold cryptocurrency on an exchange, contact exchange support and request a withdrawal freeze.

3 File an FBI IC3 report at ic3.gov. Include timestamps, carrier ticket numbers, and a summary of affected accounts.

4 File a police report with your local jurisdiction. Insurance and banks often require the report number.

Evidence to Capture

- Carrier account audit log (request in writing from fraud team).
- Recent port-in or SIM-change request records.
- Support ticket transcripts from the carrier.
- Screenshots of any two-factor texts or password-reset emails you received before the swap.
- Timeline of the loss-of-signal moment, from your own call log or a witness.

When to Escalate

Escalate to a forensic examiner when the swap is confirmed and any financial loss is suspected, when an executive or board member is the victim, or when two-factor-protected business accounts (email, file sync, remote access) were in scope. Petronella coordinates carrier subpoenas for the port-request origination IP and handles evidence preservation for downstream account-takeover investigations.

Petronella Services Referenced in This Chapter

SIM swap response is one of Petronella's core forensic specialties. The team preserves carrier records, traces downstream account compromise, and prepares the declaration an insurance carrier or civil attorney will ask for. Schedule a confidential forensics consult at petronellatech.com/contact-us/ or call (919) 348-4912.

Chapter 3: Crypto Theft Triage

If a wallet is empty and you did not authorize the withdrawal, read this chapter before you do anything else. Every minute you spend clicking around in block explorers while still logged in to the compromised wallet increases the chance the attacker takes the rest.

This chapter is for the self-custody wallet holder, the exchange account holder, and the finance team that just lost operational funds.

What NOT To Do

1. Do not reconnect a compromised wallet to any decentralized application. The approval that let them drain it is likely still live.
2. Do not sign any transaction on a hardware wallet you suspect is compromised, even a "test" transaction.
3. Do not message the scammer to "negotiate." You confirm you are a target.
4. Do not share your seed phrase with anyone claiming to be recovery support. Real recovery firms never ask for the seed.
5. Do not move remaining funds to another address created on the compromised machine. The attacker owns that machine.

Minute-by-Minute Triage

Minutes 0 to 10: Freeze what is left.

1. Disconnect the compromised machine from the internet.
2. If a hardware wallet is involved, physically unplug it. Do not enter the PIN again on the compromised host.
3. On a clean device, generate a brand-new wallet with a new seed phrase. Write the new seed on paper, not on a computer.
4. Move remaining funds from the compromised wallet to the new wallet. Use the compromised host only if you have no alternative, and use a clean machine if you can.

Minutes 10 to 60: Capture the chain evidence.

1. Open the drain transaction in a block explorer. Use Etherscan for Ethereum and EVM chains, Blockchair for Bitcoin, Solscan for Solana, and the chain-native explorer otherwise.
2. Screenshot the transaction page. Save the transaction hash. Note the block number, timestamp, sender, recipient, and amount.
3. Follow the funds through two to three hops. Screenshot each hop. Note any exchange-tagged addresses the funds touched. That tag is what law enforcement uses to subpoena the exchange for the recipient's identity.
4. Export your wallet's transaction history to CSV if the software allows it.

Hours 1 to 24: Report and trace.

1. If the destination address is tagged to a regulated exchange (Coinbase, Kraken, Binance.US), contact their compliance or law enforcement response team immediately. Provide the transaction hash, your identity, and a police report number if you have one. Some exchanges will freeze the incoming deposit if notified within hours.
2. File with FBI IC3 at ic3.gov. Include all transaction hashes and the trace.
3. File a Suspicious Activity Report-relevant disclosure with your bank if the funds originated from a bank transfer. Some banks can reverse a wire within 24 hours.
4. File a local police report.

Evidence to Capture

- Transaction hashes, block numbers, and timestamps for every hop.
- Wallet software version and install source.
- Browser extension list at the time of the drain.
- Any signed approval (Etherscan's "Approved Tokens" tab) that the attacker may have exploited.
- Communications with the scammer if pig butchering or social engineering was involved (see Chapter 4).
- A hash-verified copy of the compromised machine's disk for later forensic work.

When to Escalate

Escalate to a forensic examiner when the loss is over a threshold your firm considers material, when an executive or custodial wallet is compromised, or when the funds are still moving and you need a trace submitted to an exchange within a short window. Petronella coordinates on-chain tracing with the trusted partner network and prepares victim declarations for law enforcement submission.

Recovery Paths

- Exchange freeze: only works if funds land at a regulated exchange and you report fast.
- Civil clawback: possible when the recipient's identity is known. Requires counsel.
- Criminal referral: FBI, Secret Service (for large losses), and local police.
- Insurance: some crime policies cover cryptocurrency theft. Check the endorsement.

Nobody should promise recovery. Most self-custody theft is not recovered. The point of fast response is to maximize the small window where recovery is possible and to preserve evidence for insurance and tax-loss purposes.

Petronella Services Referenced in This Chapter

Crypto theft triage is a Petronella specialty. The team handles on-chain evidence preservation, exchange notification coordination, and forensic imaging of the compromised host. Schedule a confidential forensics consult at petronellatech.com/contact-us/ or call (919) 348-4912.

Chapter 4: Pig Butchering Scam Response

Pig butchering is a long-running relationship scam. An attacker spends weeks or months building trust over text, dating apps, or social platforms, then convinces the victim to deposit funds into a fake investment platform. By the time the victim tries to withdraw, the "platform" demands taxes, fees, or more deposits, and eventually disappears.

This chapter is for the family member, the estate attorney, or the finance lead who just figured out the "investment account" the victim was watching grow for six months is not real.

What NOT To Do

1. Do not shame the victim. Shame shuts down the evidence you need. The scam is designed to work on smart people.
2. Do not delete the chat history, the dating-app conversation, or the investment-platform account. That is all evidence.
3. Do not pay the "tax" or "release fee" the fake platform is asking for. It is another layer of the scam.
4. Do not call the number the scammer gave the victim. It confirms the target and can trigger the recovery-scam follow-on.
5. Do not promise the victim recovery. Most losses are not recovered. Set expectations honestly.

Minute-by-Minute Triage

Hours 0 to 4: Preserve conversations.

1. On the victim's phone, open the platform or chat app and enable airplane mode before the attacker can delete the thread remotely.
2. For WhatsApp, Telegram, Signal, and iMessage: use the export-chat function to produce a full transcript. Save the export to external storage.
3. Screenshot every conversation screen, scrolling top to bottom. Include timestamps, profile pictures, phone numbers, and any voice-note or video-message thumbnails.
4. Screenshot the fake investment-platform pages showing balance, fake transactions, and the withdrawal denial.
5. If the victim received any email from the platform, forward the full-headers version to a secure account.

Hours 4 to 24: Capture the money trail.

1. Pull bank statements covering the entire relationship, not just the last transfer. Mark each deposit to the scam with date, amount, beneficiary name, and receiving bank SWIFT or ABA routing number.
2. If wires went international, note the intermediary banks on the wire advice.
3. For cryptocurrency deposits, follow Chapter 3's evidence capture steps on every transaction.
4. List every phone number, social handle, email, and platform URL the scammer used. Scammers rotate handles. Capture all of them.

Evidence to Capture

- Full chat exports (WhatsApp, Telegram, Signal, iMessage, Line, WeChat as applicable).
- Screenshots of the fake investment platform, including URL and login page.
- Wire-transfer receipts, routing numbers, and intermediary bank information.
- On-chain transaction hashes for any crypto deposits.
- Timeline of the relationship, from first contact to discovery, with approximate dates and platform.
- Scammer's claimed name, photo, employer, and location (almost always false but still evidence).

Law Enforcement Referral

Pig butchering is a priority for the FBI. File at ic3.gov with all evidence attached. Use the following structure in the narrative:

1. Platform of first contact (dating app, Facebook, Instagram, LinkedIn, WhatsApp cold message).
2. Approximate date range of grooming.
3. Date of first deposit and total deposits.
4. Receiving bank or crypto address for each deposit.
5. Date and nature of the "withdrawal denial" event.
6. Any attempts at contact since discovery.

Also file with the Federal Trade Commission at reportfraud.ftc.gov and with your local FBI field office if the loss is large.

When to Escalate

Escalate to a forensic examiner when a wire transfer is within the twenty-four-hour bank reversal window, when the victim is a fiduciary with downstream exposure, when elder-abuse thresholds are involved, or when the loss is material to an estate or business.

Petronella Services Referenced in This Chapter

Petronella preserves chat evidence to a court-admissible standard, coordinates with the FBI and the trusted partner network on bank and crypto reversals, and prepares the victim declaration civil counsel will need. Schedule a confidential forensics consult at petronellatech.com/contact-us/ or call (919) 348-4912.

Chapter 5: Ransomware Triage

A ransomware event is the most expensive incident most small and mid-sized businesses will ever face. The average business is down for days to weeks. The decision of whether to pay, negotiate, restore, or rebuild depends on evidence you collect in the first few hours.

This chapter is for the business owner, the IT director, and the CFO who are staring at a ransom note right now.

What NOT To Do

1 Do not pay before you know whether your backups work.

2 Do not pay before you know whether your insurance covers it and whether the carrier requires pre-approval.

3 Do not pay before checking the Treasury OFAC sanctioned-entity list. Paying a sanctioned group is a federal violation.

4 Do not negotiate on your own without a professional negotiator. Every message is evidence and every misstep raises the price.

5 Do not wipe machines before imaging them. You destroy the evidence the forensic investigator and insurer will require.

6 Do not restore from backup until you know the backup is clean.

Minute-by-Minute Triage

Hours 0 to 1: Contain and notify.

1 Isolate every machine from the network. Pull cables. Disable Wi-Fi at the switch level. Disconnect cloud-sync clients.

2 Photograph the ransom note on every affected machine. Note the strain name if shown, the Bitcoin or Monero address, and the negotiation URL.

3 Call your cyberinsurance carrier. Most policies require notice within 24 to 72 hours. The carrier will dispatch a panel response team. Use them unless they fail the quality bar.

4 Call your incident response firm and legal counsel. Engage under privilege.

Hours 1 to 4: Test backup viability.

1 Identify your backup system: on-site, off-site, immutable cloud, tape.

2 Verify the backup has not been encrypted. Many ransomware crews now attack backups first.

3 Perform a test restore of a single non-production system. Confirm data integrity and a bootable state.

4 Estimate your Recovery Time Objective (RTO) based on the test restore's speed projected across full production.

Hours 4 to 24: Build the decision framework.

1 Calculate three numbers: the ransom cost, the estimated recovery cost if you rebuild from backup, and the estimated revenue loss per day of downtime.

2 Decide whether your insurance covers the ransom (check the extortion endorsement) and what your co-pay is.

3 If you do not have clean backups, escalate the decision to your executive team with your attorney on the call. Do not negotiate without a professional negotiator from the trusted partner network on your side.

Restore-vs-Pay Decision Framework

Favor restore when: backups are verified clean, RTO is acceptable, the attacker has not exfiltrated data (no double-extortion), and the insurance policy covers the recovery labor.

Favor negotiated settlement only when: backups are confirmed unusable or partially destroyed, the encryption is confirmed irreversible without the decryptor, insurance has approved the payment, the entity is not on the OFAC list, the counsel and the negotiator both support it, and the decryptor has been proven to work on a sample file.

Almost no scenario justifies paying without professional negotiation. Petronella works with a trusted partner network for negotiation and Bitcoin brokerage.

Backup Verification

Before any restore, confirm:

- Backup date and time precedes the known compromise.
- Backup files are not encrypted or modified.
- Restore targets (hardware or cloud) are clean of persistence.
- Active Directory and identity systems are rebuilt or restored from a known-good state, not from the compromised copy.
- Endpoint detection and response is running on every restored machine before it goes live.

Evidence to Capture

- Full disk images of at least one representative affected system.
- Memory images while systems still run.
- Firewall, domain controller, and endpoint detection logs for at least thirty days back.
- The ransom note itself, plus any negotiation portal screenshots.
- Indicators of compromise: attacker IP addresses, command-and-control domains, file hashes.
- Timeline: earliest suspicious activity through ransom-note deployment.

When to Escalate

A ransomware event always escalates to a Licensed Digital Forensic Examiner, counsel, and the insurance carrier's panel. There is no "small ransomware" case. Regulatory notice clocks start running the moment you have reason to believe regulated data is in scope.

Petronella Services Referenced in This Chapter

Petronella handles ransomware incident triage, forensic imaging, backup validation, and coordination with the insurance panel and the trusted partner network for negotiation. The team does not perform the

negotiation itself. Schedule a confidential forensics consult at petronellatech.com/contact-us/ or call (919) 348-4912.

Chapter 6: Business Email Compromise

Business email compromise is the most common cause of reported financial loss from cybercrime according to FBI IC3 annual reports. The attacker either takes over a legitimate mailbox or spoofs one, then redirects a wire transfer to an account they control. The window to reverse a wire is short. Usually twenty-four to seventy-two hours.

This chapter is for the controller, CFO, or accounting manager who just discovered a wire went to the wrong account, or who is looking at an email that "feels off."

What NOT To Do

1. Do not reply to the suspect email from the same mailbox. The attacker is reading it.
2. Do not authorize the next wire in the thread, even if it "confirms" you replied to the last one.
3. Do not delete the email. Headers are critical evidence.
4. Do not change only the password of the suspect mailbox. You must also revoke active sessions and rotate any app passwords.
5. Do not assume it was only one mailbox. BEC often involves lateral movement through shared delegations.

Minute-by-Minute Triage

Minutes 0 to 15: Stop the money.

1. Call your bank's wire-fraud team immediately. The line is usually in the fraud department, not general service. Reference SWIFT FFIS (Financial Fraud Kill Chain) for recalls across banks.
2. Provide the wire date, amount, originating account, beneficiary name, beneficiary account number, and beneficiary bank.
3. Request a SWIFT recall or ACH reversal depending on rail. Follow up in writing within the hour.

Minutes 15 to 60: Lock down the mailbox.

1. On a clean device, change the password of the compromised mailbox. Use a long passphrase.
2. Revoke all active sessions in the Microsoft 365 or Google Workspace admin console.
3. Disable any forwarding rules, mail flow rules, or delegations you do not recognize. Screenshot each rule before deleting.
4. Rotate app passwords and OAuth tokens on the mailbox.
5. Enable a conditional-access policy that forces reauthentication for all users in the organization.

Hours 1 to 4: Scope the compromise.

1. Pull the mailbox audit log for the last ninety days. Look for: mailbox sign-ins from unfamiliar IP addresses, rule changes, unusual item deletions, and access to the "Sent Items" folder by non-owner identities.
2. Pull the unified audit log in Microsoft 365 or the audit log in Google Workspace for the same window.

3 Identify what else the compromised identity had access to: file shares, SharePoint sites, CRM, ERP, payroll.

Email Header Analysis

A real email from a vendor normally shows:

- A **Received:** chain that originates from the vendor's mail provider.
- **SPF:** Pass, or at least a soft-fail that aligns with the vendor's published SPF record.
- **DKIM:** Pass, with a selector matching the vendor's domain.
- **DMARC:** Pass, with alignment.

A BEC email often shows one or more of:

- A Received chain that originates from a residential or hosting-provider IP.
- SPF fail, or SPF pass from a lookalike domain (vendor-co.com instead of vendor.com).
- DKIM missing or failing.
- DMARC none or reject with alignment broken.
- A "reply-to" header that does not match the "from" header.
- A sender display name that matches the vendor but an email address that does not.

Save the full message headers before anyone deletes the email.

MFA Bypass Indicators

Even with multi-factor authentication on, attackers can compromise a mailbox by:

- Stealing an active session token (often through phishing into an attacker-in-the-middle page).
- Tricking a user into approving a push notification fatigue attack.
- Registering their own authenticator through a compromised account recovery.

Indicators that a bypass happened:

- Sign-ins from unusual countries within minutes of a legitimate sign-in.
- New MFA methods registered that the user does not recognize.
- Token-based sign-ins with no interactive authentication in the same session.

Evidence to Capture

- Full message headers of the fraudulent email and any related emails.
- Mailbox rules at the time of discovery.
- Audit-log exports for the compromised identity.
- Bank confirmation of the wire transfer and any recall attempt.
- Any phone calls with the attacker, logged.
- Contracts or invoices the attacker may have altered.

When to Escalate

Always escalate a BEC to a Licensed Digital Forensic Examiner and counsel. Regulatory notice obligations may apply depending on data accessed. Insurance crime coverage almost always requires a third-party forensic report.

Petronella Services Referenced in This Chapter

Petronella handles BEC mailbox forensics, attacker-in-the-middle kit identification, wire-recall coordination, and the third-party forensic attestation the insurance carrier will want. Schedule a confidential forensics consult at petronellatech.com/contact-us/ or call (919) 348-4912.

Chapter 7: Network Forensics Basics

Network forensics answers the questions that host forensics cannot: where the attacker came from, where they went next, what data left the building, and how much of it. This chapter is for the IT lead or security analyst who needs to understand what to capture and what the captured data is good for.

What NOT To Do

1. Do not delete old firewall logs. The attacker was probably inside before you noticed. You need at least thirty to ninety days of backward lookup.
2. Do not mirror traffic to a cloud tool the attacker may also have access to.
3. Do not try to "observe" an active attacker by leaving everything connected. Containment beats observation in most business-impact cases.
4. Do not share packet captures outside the investigation team without redaction. They often contain credentials and sensitive data.

Packet Capture Basics

A full packet capture (PCAP) records every byte of every packet on the wire. Netflow records only the metadata: source, destination, port, bytes, duration. Use the right tool for the question.

Use a full PCAP when you need to see: the exact content of an attacker's command-and-control channel, the file contents that were exfiltrated, the specific HTTP or DNS query that matters for attribution.

Use Netflow when you need to see: volume trends, unusual destinations over a long window, first-seen host-to-host relationships, broad east-west lateral movement.

Tools

tcpdump is the baseline Linux packet-capture tool. A basic capture:

```
tcpdump -i eth0 -s 0 -w /tmp/capture.pcap host 10.1.2.3
```

This captures full-size packets on interface eth0 to or from 10.1.2.3. Rotate the file with the `-G` and `-W` flags for long runs.

Wireshark is the analysis tool. It reads the PCAP, decodes protocols, and lets you filter by conversation, stream, or content. Use the "Follow TCP Stream" feature to reconstruct an attacker's session.

Zeek (formerly Bro) produces structured logs from traffic. It is better for long-term monitoring than raw packet capture.

Netflow is exported by most enterprise firewalls and routers. Capture and aggregate it centrally.

Log Timeline Reconstruction

A useful incident timeline pulls from at least four sources:

1. **Firewall logs**: inbound and outbound connections, blocked traffic, VPN sign-ins.
2. **Active Directory (or identity provider) logs**: sign-ins, privilege changes, Kerberos activity.
3. **Endpoint detection and response logs**: process execution, file writes, network connections from each host.
4. **Email and cloud audit logs**: mailbox access, file access, sharing changes.

Normalize the timestamps to UTC and feed them into a single chronological view. Use a spreadsheet or a purpose-built log tool. The picture that emerges is usually:

- First foothold (often a phishing email or an exposed remote service).
- Privilege escalation.
- Lateral movement.
- Data staging.
- Data exfiltration.
- Ransom or impact event.

Knowing the first-foothold time tells you what backups are safe to restore from.

Evidence to Capture

- Thirty to ninety days of firewall logs.
- Thirty to ninety days of identity-provider sign-in logs.
- Endpoint detection and response logs covering every affected host.
- Email audit logs for any identity in scope.
- A PCAP of any active command-and-control channel if the attacker is still live and containment allows observation.
- Netflow from the core switch and internet edge, if collected.

When to Escalate

Escalate when the incident touches more than one host, when regulated data is in scope, when the attacker is believed to still have access, or when insurance or regulators will require a forensic report. Raw packet capture analysis at scale is specialized work.

Petronella Services Referenced in This Chapter

Network forensics is a Petronella specialty. The team performs log timeline reconstruction, PCAP analysis, and command-and-control attribution. Schedule a confidential forensics consult at petronellatech.com/contact-us/ or call (919) 348-4912.

Chapter 8: When to Bring in a Licensed DFE and Expert Witness

A Licensed Digital Forensic Examiner is credentialed to produce work that holds up in court. That is different from a generalist IT person or even a skilled security engineer. When a case may land in civil litigation, criminal prosecution, an insurance claim dispute, or a regulatory proceeding, the chain of custody from the first touch of evidence has to withstand cross-examination.

This chapter is for the attorney, the general counsel, the insurance claims adjuster, or the business owner deciding whether to engage a credentialed examiner.

What Court-Admissible Chain of Custody Requires

Chain of custody is the documented path of every piece of evidence from acquisition to courtroom. To stand up in court, it requires:

1. **Acquisition documentation**: who acquired the evidence, when, where, by what method, and with what tools. The tool must be a known, verifiable forensic suite with verifiable versioning.
2. **Hash verification**: a cryptographic hash (SHA-256 or stronger) of the original evidence calculated at acquisition and verified before every analysis session. If hashes diverge, the evidence is tainted.
3. **Storage**: evidence held in a secure location (locked cabinet, tamper-evident bag, controlled-access server). Every access logged.
4. **Analysis record**: every tool run, every filter applied, every export, logged with timestamp, examiner name, and output hash.
5. **Expert declaration**: a written statement by the examiner describing methodology, findings, and limitations, signed under penalty of perjury.
6. **Courtroom availability**: the examiner must be available to testify and be cross-examined.

A generalist IT team usually cannot provide steps 1, 4, 5, and 6 at the standard a court requires. That is where a Licensed DFE comes in.

Craig Petronella's DFE Credential

Craig Petronella holds Licensed Digital Forensic Examiner credential DFE #604180. He has served as expert witness in cases involving SIM swap, cryptocurrency theft, business email compromise, network intrusion, and related matters. He does not perform private investigator work, mobile-device forensics using Cellebrite, traditional e-discovery, or EnCase-tool-specific work. Cases requiring those capabilities are referred to the trusted partner network.

Expert Witness Declaration Format

A typical declaration produced by Petronella's examiner includes:

- Qualifications of the examiner, with credentials and prior testimony.
- Summary of the matter.
- Evidence received, with acquisition method and hash.
- Methodology applied.

- Findings, stated as conclusions with supporting facts.
- Limitations and caveats.
- Signature block, typically under penalty of perjury.

Preservation Holds

A preservation hold, also called a litigation hold, is the legal notice that an entity must stop destroying evidence. When counsel anticipates litigation, they issue the hold. The forensic examiner's role is to capture evidence in a way that proves preservation, often through memory and disk imaging at a specific moment, with hash and chain documented.

Preservation holds apply to:

- Email mailboxes of every custodian named in the matter.
- Cloud storage (OneDrive, Google Drive, Dropbox).
- Collaboration tools (Slack, Teams).
- Endpoint images of custodian devices.
- Server logs and audit trails.
- Third-party records that may be subpoenaed later.

When to Engage the DFE

Engage at any of these triggers:

1. Counsel anticipates litigation (civil or criminal).
2. The insurance carrier requires third-party forensic attestation.
3. A regulator or auditor has asked for a forensic report.
4. Criminal referral is on the table.
5. The loss is material enough that the case will probably be litigated.
6. Evidence is at risk of spoliation without formal chain of custody.

Petronella Services Referenced in This Chapter

Petronella's Licensed Digital Forensic Examiner work includes evidence acquisition, chain of custody, expert witness declaration, and testimony. Schedule a confidential forensics consult at petronellatech.com/contact-us/ or call (919) 348-4912.

Chapter 9: Insurance Claim Preparation

Every cyberinsurance policy has notice requirements, documentation requirements, and coverage limits. The claim you submit is only as strong as the evidence and the timeline behind it. This chapter is for the risk manager, CFO, or business owner preparing a cyber claim.

What NOT To Do

1. Do not miss the notice window. Most policies require notice within 24 to 72 hours. Some are tighter. Miss it and benefits drop or disappear.
2. Do not engage a forensic vendor off the carrier's panel without pre-approval. Many policies will only reimburse panel vendors.
3. Do not pay a ransom before getting carrier pre-approval. Unapproved payments are often excluded from reimbursement.
4. Do not communicate with regulators, law enforcement, or media before counsel reviews the message. Even a well-meaning statement can create waiver.
5. Do not destroy evidence after the claim is filed. Spoliation claims can reduce or void coverage.

What Cyberinsurance Carriers Actually Want

Policies vary, but most carriers want some combination of these items, in this general order:

Within 24 to 72 hours:

1. Notice of loss, submitted through the carrier's claim portal or broker.
2. A description of what is known so far. Keep this factual and bounded. Do not speculate.
3. The name of engaged counsel and incident response firm.
4. Confirmation of initial containment steps.

Within 1 to 2 weeks:

1. Preliminary forensic findings: scope, confirmed affected systems, confirmed data types in scope.
2. Initial timeline from the forensic examiner.
3. Preliminary estimate of business interruption loss, if the policy has BI coverage.
4. Identification of any regulated data in scope (PHI, PCI, CUI, PII).

Within 30 to 90 days:

1. Final forensic report, including chain of custody and expert declaration.
2. Full business interruption loss documentation: revenue impact, extra expense, documented restoration costs.
3. Regulatory notice records if notices were sent.
4. Third-party demands and legal hold notices.
5. Reconciliation of incurred expenses against policy sublimits.

Digital Forensics Attestation

Most policies require a third-party digital forensics attestation to release certain benefits, especially:

- Ransomware extortion coverage.
- Data breach notification cost coverage.
- Business interruption loss.
- Regulatory fines and defense.

The attestation is a signed statement from a credentialed forensic examiner describing what happened, when, how, and what data was in scope. It is not the same as an IT status report. It carries the weight of the examiner's credentials and liability. Petronella's Licensed Digital Forensic Examiner produces this attestation for the specialties covered in this playbook.

Incident Timeline from the SOC

The carrier will ask for a timeline that answers:

- First signs of compromise (with timestamp and source).
- First detection by the victim.
- First containment action.
- First exfiltration event, if any.
- First impact event (ransom deployment, wire transfer, account takeover).
- Full remediation completion.

Pull the timeline from log sources listed in Chapter 7. Normalize to UTC. Annotate with the evidence source for every entry. This becomes an exhibit in the claim file.

Evidence to Capture for the Claim

- All items from the host and network chapters above.
- Every invoice from every vendor engaged in the response, with service description.
- Business interruption data: revenue comparison period, affected systems, and labor cost.
- Regulatory notices sent and received.
- Communications with counsel (privileged, but referenced in the claim).
- Communications with the carrier and broker.

When to Escalate

Escalate to specialty counsel and a forensic examiner on any claim where:

- The ransom or loss amount approaches the policy sublimit.
- The carrier denies or reserves rights on any coverage part.
- Regulated data is in scope.
- The attacker group appears on the OFAC list.
- Business interruption exceeds a few days.

Petronella Services Referenced in This Chapter

Petronella provides the forensic attestation cyberinsurance carriers require, incident timelines, and evidence packages for the claim file. The team coordinates with carrier-panel counsel and panel vendors as needed. Schedule a confidential forensics consult at petronellatech.com/contact-us/ or call (919) 348-4912.

Closing: The Call That Matters

If you are reading this after an incident, stop reading and make the call. Petronella's incident line is (919) 348-4912. The consult is confidential. Early engagement is always cheaper than late engagement.

If you are reading this before an incident, share it with your executive team, your IT lead, your finance lead, and your outside counsel. Add the phone number to your business continuity plan. Know your cyberinsurance notice window. Confirm your backups restore. Run one tabletop exercise a year.

The first hour decides most of the outcome. Be ready before it starts.

Petronella Technology Group Licensed Digital Forensic Examiner DFE #604180 CMMC-AB Registered Provider Organization #1449 BBB Accredited A+ since 2003 Founded 2002 5540 Centerview Dr, Raleigh, NC (919) 348-4912 petronellatech.com