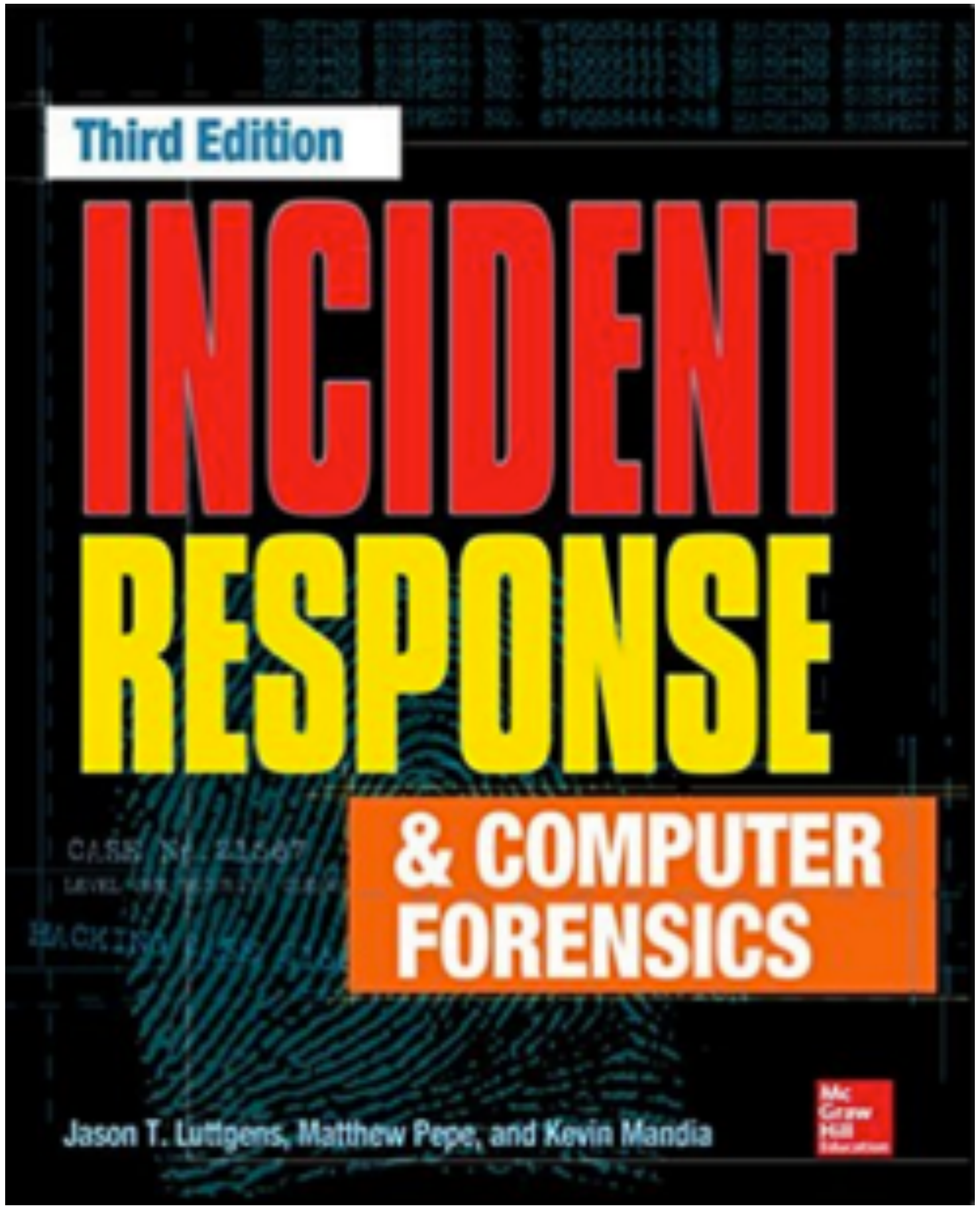
CNIT 121: Computer Forensics



4 Getting the Investigation Started on the Right Foot

Collecting Initial Facts

- **You need specific information**
- **Such as IP Addresses and times**
- **Validate facts and check context**

Time Zones

- **A big problem**
- **Simple solution: use UTC for everything**

Five Checklists

- **Incident summary**
- **How the incident was detected**
- **Individual system details**
- **Network details**
- **Malware details**

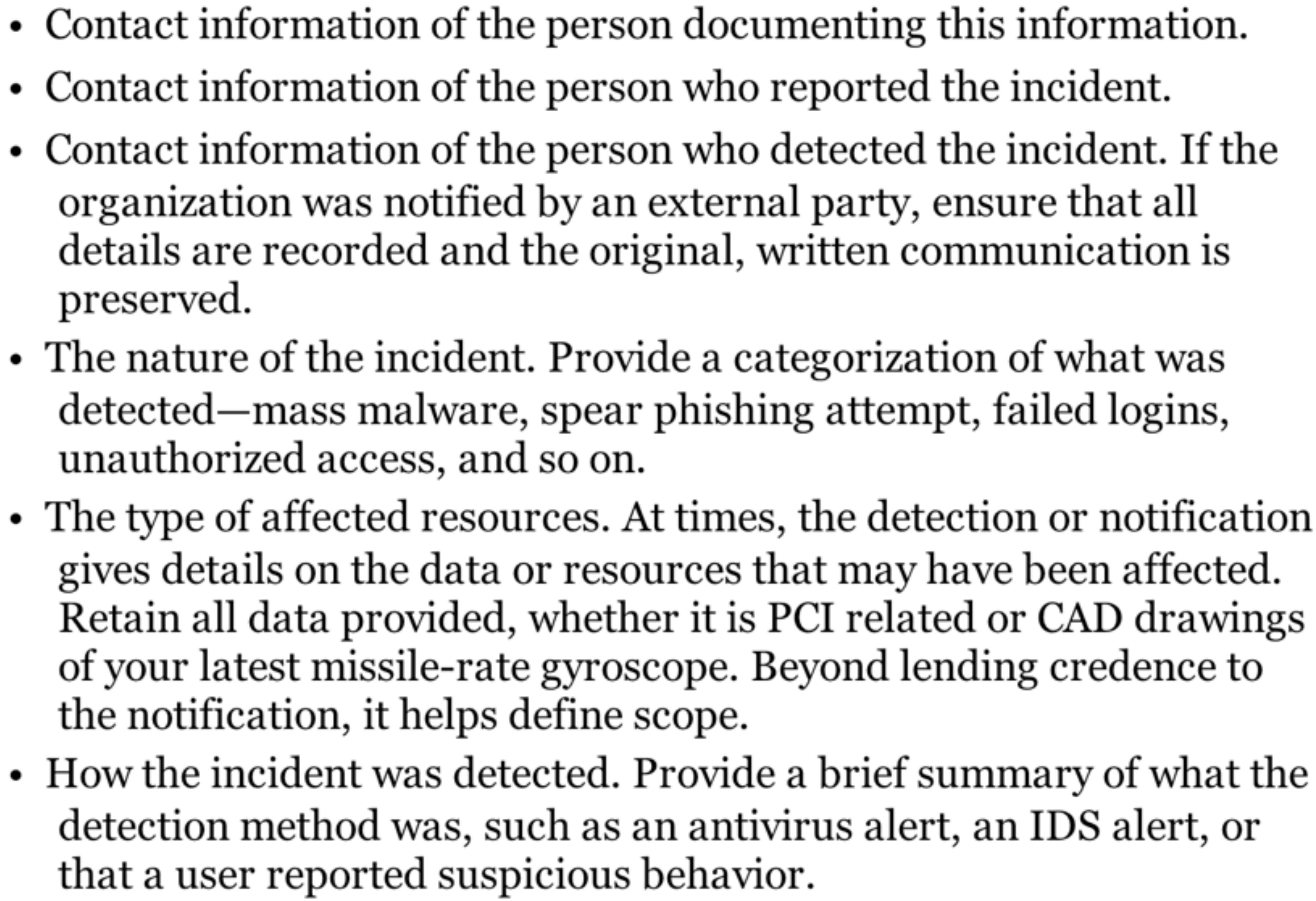
Documentation

- **Use your own incident documentation system**
  - **File share (with limited and audited access)**
  - **Or a Request Tracker for Incident Response**
- **Don't trust any part of the target's network**
  - **It could be compromised**

Incident Summary Checklist

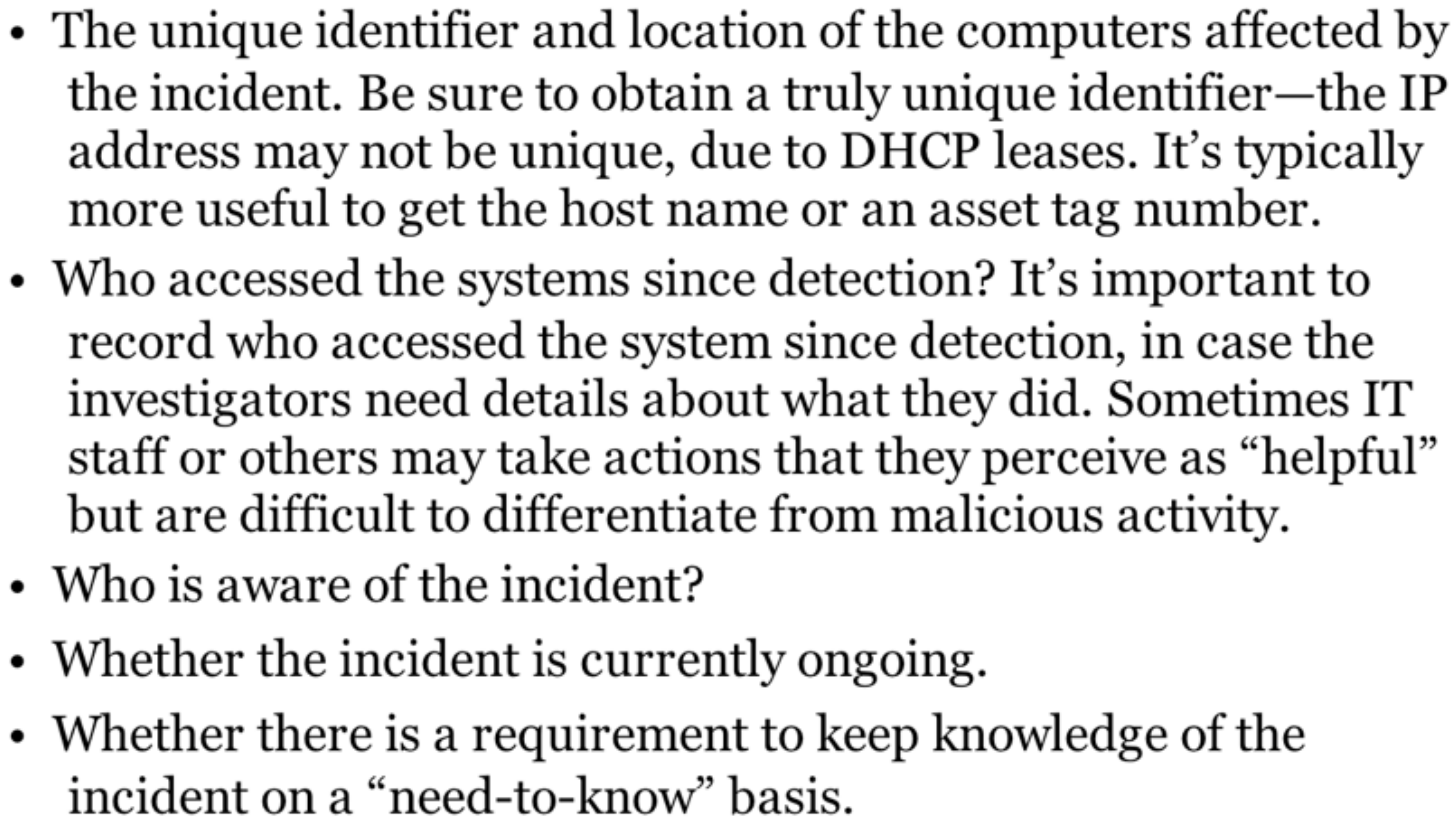
- Date and time the incident was reported. Record the date and time that an individual or automated system initially brought the issue to the IR team's attention.
- The date and time the incident was detected. Normally, the time an incident is reported is more recent than the actual detection time. Be sure to track down and record when the issue was actually detected.

Incident Summary Checklist



- Contact information of the person documenting this information.
- Contact information of the person who reported the incident.
- Contact information of the person who detected the incident. If the organization was notified by an external party, ensure that all details are recorded and the original, written communication is preserved.
- The nature of the incident. Provide a categorization of what was detected—mass malware, spear phishing attempt, failed logins, unauthorized access, and so on.
- The type of affected resources. At times, the detection or notification gives details on the data or resources that may have been affected. Retain all data provided, whether it is PCI related or CAD drawings of your latest missile-rate gyroscope. Beyond lending credence to the notification, it helps define scope.
- How the incident was detected. Provide a brief summary of what the detection method was, such as an antivirus alert, an IDS alert, or that a user reported suspicious behavior.

Incident Summary Checklist



- The unique identifier and location of the computers affected by the incident. Be sure to obtain a truly unique identifier—the IP address may not be unique, due to DHCP leases. It's typically more useful to get the host name or an asset tag number.
- Who accessed the systems since detection? It's important to record who accessed the system since detection, in case the investigators need details about what they did. Sometimes IT staff or others may take actions that they perceive as "helpful" but are difficult to differentiate from malicious activity.
- Who is aware of the incident?
- Whether the incident is currently ongoing.
- Whether there is a requirement to keep knowledge of the incident on a "need-to-know" basis.

Incident Detection Checklist

- **Was the detection through an automated or manual process?**
- **What information was part of the initial detection?**
- **What sources provided the data?**
- **Has the source data been validated as accurate?**
- **Is the source data being preserved?**

Incident Detection Checklist

- **How long have the detection sources been in operation and who runs them?**
- **What are the detection and error rates?**
- **Has anything related to the data sources changed?**

Collect Additional Details

- **Individual systems**
  - **Physical location, asset tag number**
  - **System's make and model, OS, primary function**
  - **Responsible administrator or user**
  - **IP address, hostname, domain**
  - **Critical information stored on the system and backups**

Collect Additional Details

- **Individual systems**
  - **Whether the system is still connected to the network**
  - **List of malware detected, back as far as log data goes**
  - **List of remediation steps that have been taken**
    - **It can be difficult to tell attacker actions from administrator actions, such as changing passwords**
  - **Data that is being preserved by staff**

Collect Additional Details

- **Network details**
  - **All external malicious IPs and domain names**
  - **Whether network monitoring is being conducted**
  - **List of remediation steps that have been conducted**
  - **Is data being preserved?**
  - **Updates to network diagrams and configurations**

Collect Additional Details

- **Malware details**
  - **Date, time, and how malware was detected**
  - **List of systems where malware was found**
  - **Malware filenames, directories**
  - **Findings of detection mechanism: name and family of the malicious file**
  - **Is malware active? What network connections are present?**

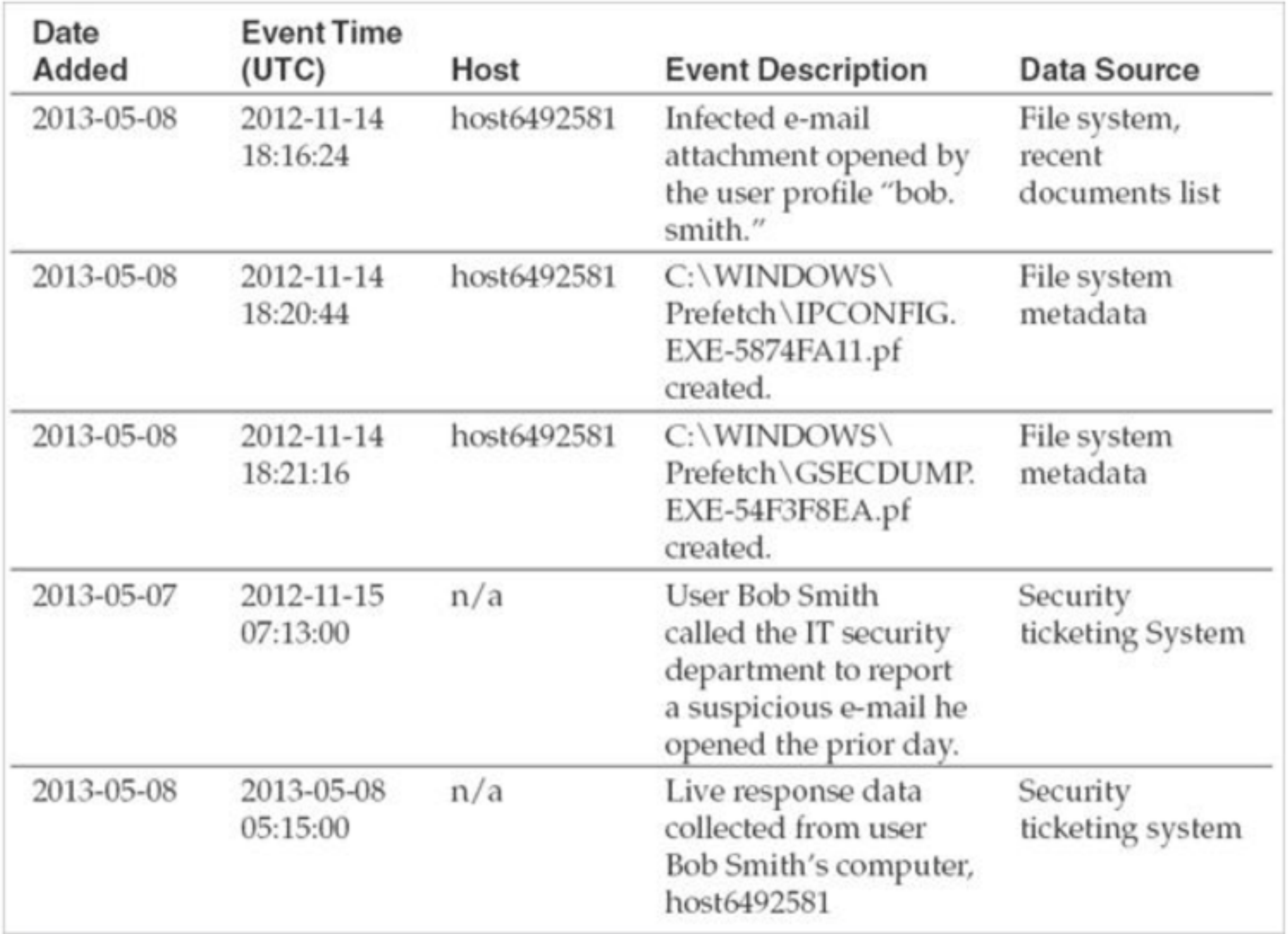
Collect Additional Details

- **Malware details**
  - **Is a copy of the malware preserved?**
  - **Status of any analysis: network and host indicators of compromise**
  - **Was malware submitted to any third party?**

Case Notes

- **Record the main actions your team takes**
- **Be professional--your case notes may be discoverable**

Attack Timeline



Date Added	Event Time (UTC)	Host	Event Description	Data Source
2013-05-08	2012-11-14 18:16:24	host6492581	Infected e-mail attachment opened by the user profile "bob. smith."	File system, recent documents list
2013-05-08	2012-11-14 18:20:44	host6492581	C:\WINDOWS\ Prefetch\IPCONFIG. EXE-5874FA11.pf created.	File system metadata
2013-05-08	2012-11-14 18:21:16	host6492581	C:\WINDOWS\ Prefetch\GSECDUMP. EXE-54F3F8EA.pf created.	File system metadata
2013-05-07	2012-11-15 07:13:00	n/a	User Bob Smith called the IT security department to report a suspicious e-mail he opened the prior day.	Security ticketing System
2013-05-08	2013-05-08 05:15:00	n/a	Live response data collected from user Bob Smith's computer, host6492581	Security ticketing system

Investigative Priorities

- **Common priorities**
  - **Who broke in**
  - **When its occurred**
  - **What they accessed**
  - **Are they still inside?**

Investigative Priorities

- **Special cases**
  - **PCI: list of potentially compromised account numbers and dates**
- **Plan with legal counsel for**
  - **Copyright infringement**
  - **Larceny**

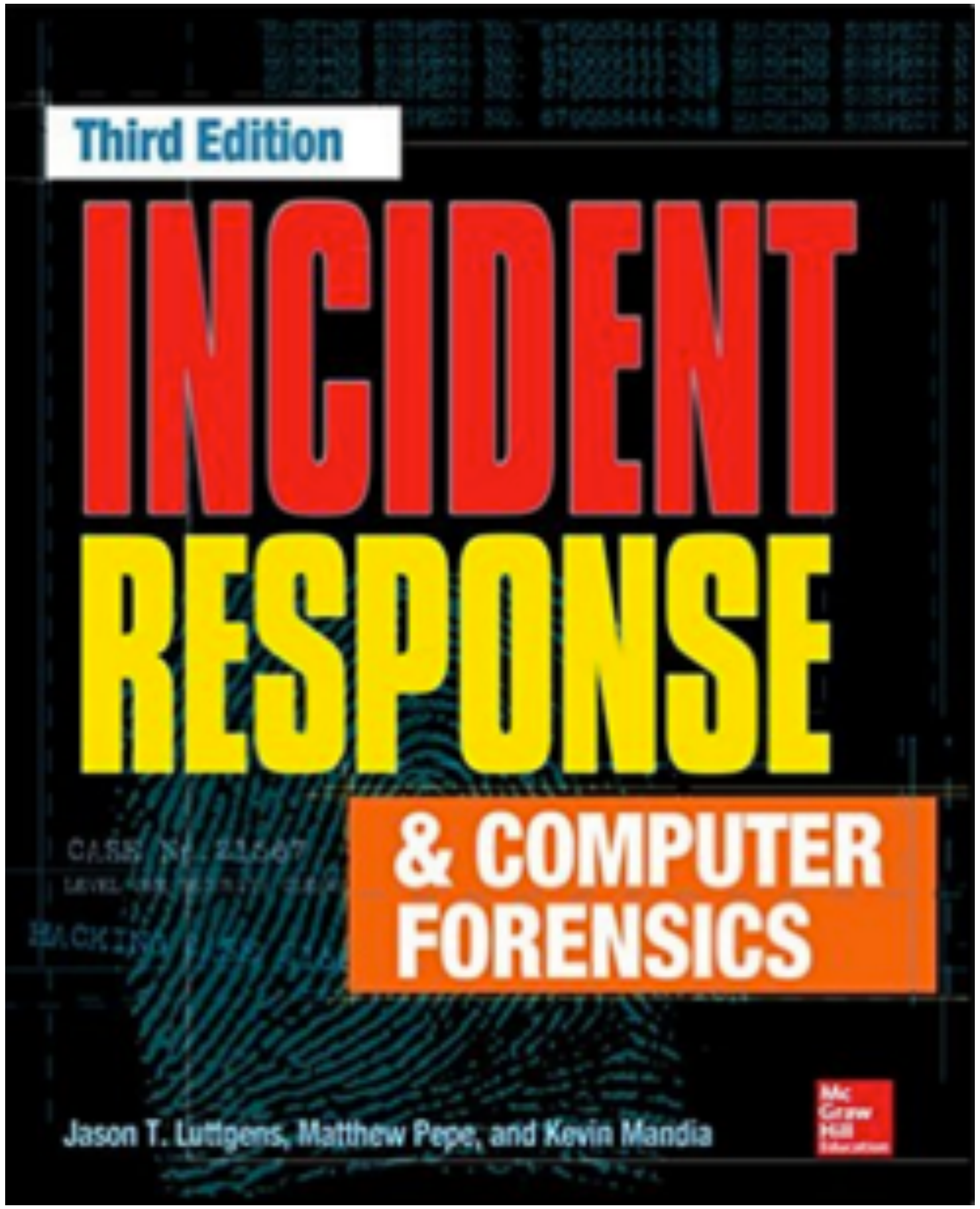
Management Expectations

- **Set reasonable goals**
- **Consider sources of evidence, type of incident, questions, and time constraints**
- **Network intrusions often use overseas jump points--making legal action difficult or impossible**
- **If breach was months or years ago, much evidence may be lost**

Case: Warez Site

- Someone ran an automated vulnerability scan on a web server
- Entered through management interface
- Set up a Warez site (selling stolen or illegal files)
- Management wanted to find and prosecute the attacker
- But this is a common, automated attack
- More realistic to just find and patch the vulnerability

CNIT 121: Computer Forensics

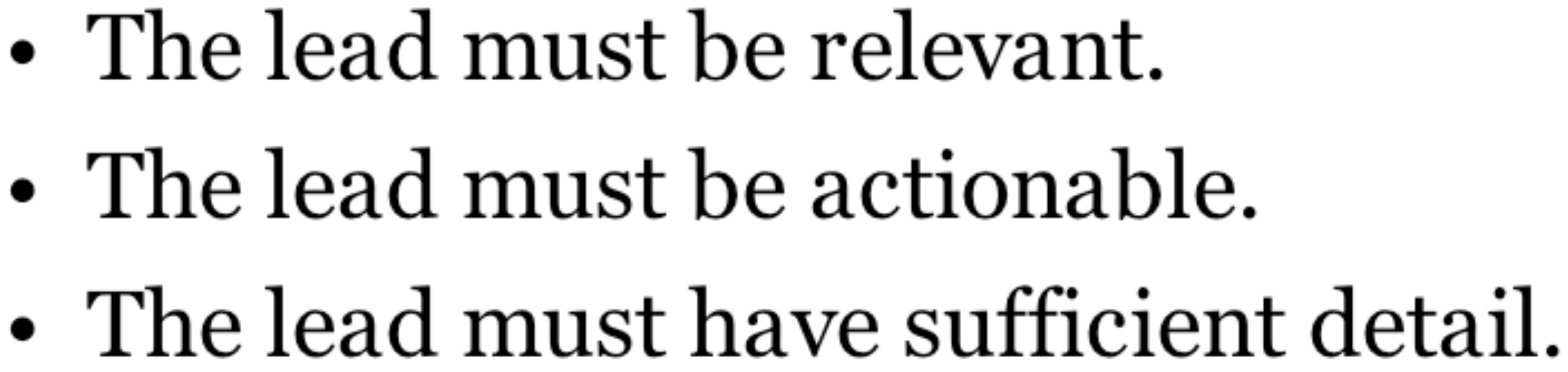


5 Initial Development of Leads

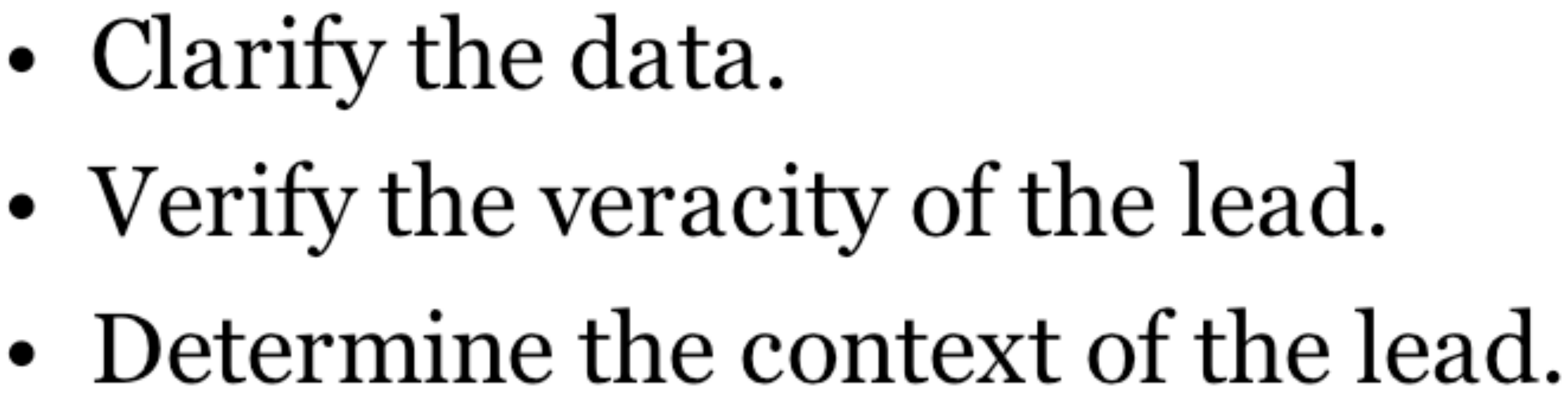
Leads

- **Actionable items about stolen data (tasks to perform), like**
  - **Network indicators**
  - **Identities of potential subjects**
  - **Issues that led to compromise or a security incident**

Defining Leads of Value



- The lead must be relevant.
- The lead must be actionable.
- The lead must have sufficient detail.



- Clarify the data.
- Verify the veracity of the lead.
- Determine the context of the lead.

Example: NIDS

- **Network Intrusion Detection System generates an alert**
  - **Connection to a command-and-control server**
- **Identify internal origin if NAT obscures it**
- **Inspect raw packets**
- **Search other connections made by that host**

Veracity and Context

- **Especially important when humans are the source**
- **Humans may be misinterpreting normal traffic**
  - **Automated systems sometimes do too**

Acting on Leads

- **Turn leads into viable indicators**
  - **That can detect ongoing events and future attacks**
- **Detect suspicious conditions beyond the leads you already have**

Turning Leads into Indicators

- **Property-based indicators**
  - **Observable characteristics of malicious software or actions**
  - **Registry key, MD5 hash, mutex with an unique name**
    - ***mutex* is an internal Windows object used for inter-process communication**
    - **Often used by malware to avoid repeat infections**

Turning Leads into Indicators

- **Methodology-based or anomaly-based indicators**
    - **Less specific leads, where a combination of characteristics is suspicious**
    - **Unexpected executables in the \Windows\Help directory**

Lifecycle of Indicator Generation

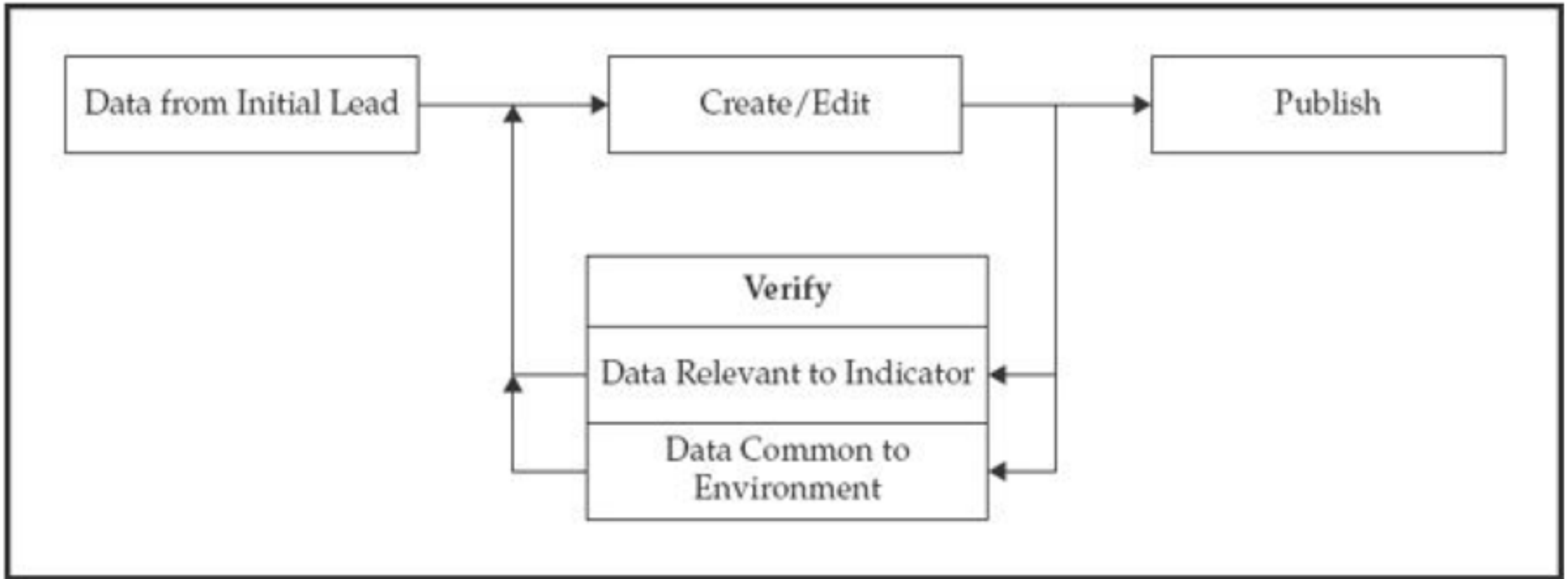


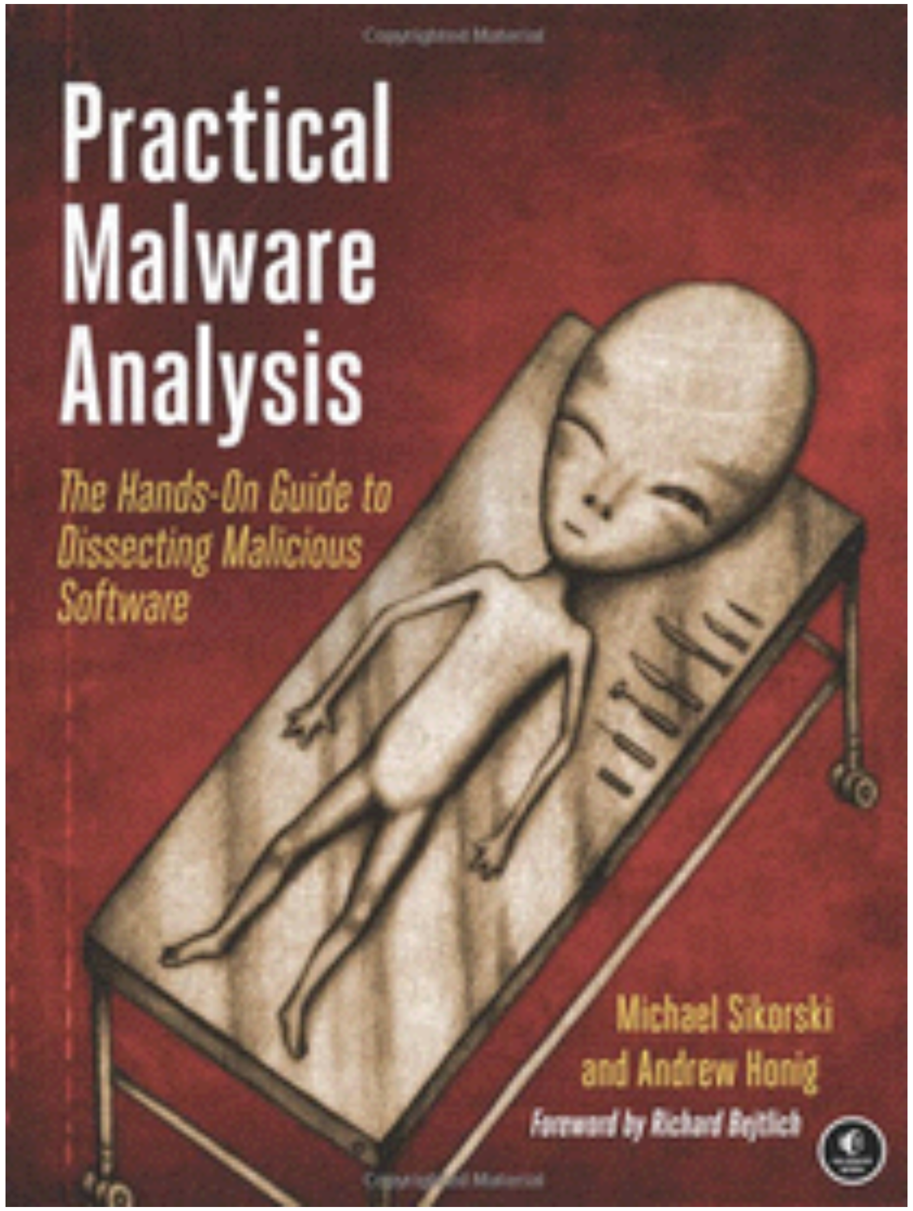
Figure 5-1. Indicator development lifecycle

Editing Host-based Indicators

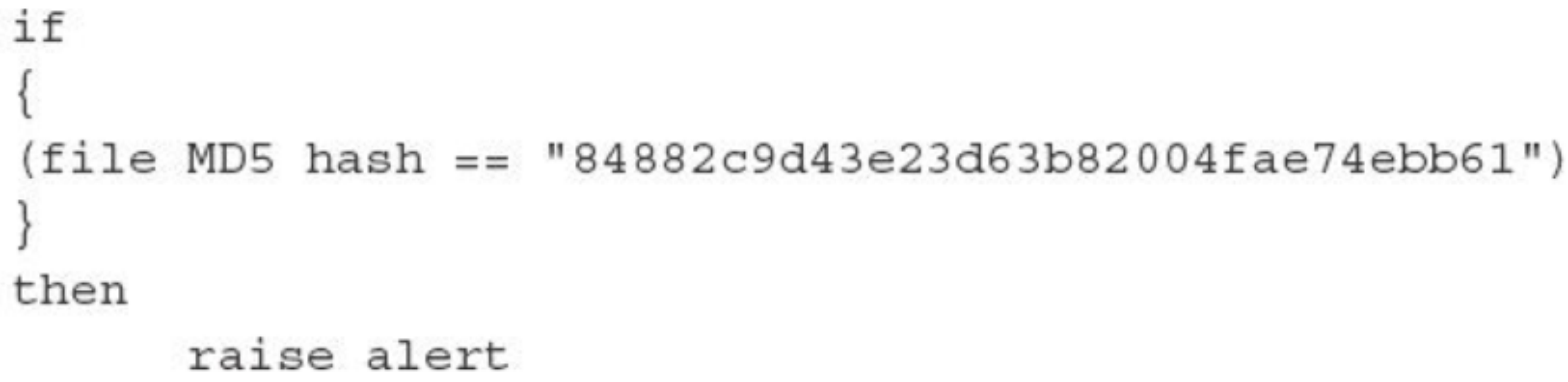
- **Binary classification: endpoint is either of interest to the investigation, or not**
- **Assemble a set of observables that are suspicious**

Practical Malware Analysis

- **Malware samples from this book**
- **Used in CNIT 126**


Copyrighted Material
Practical Malware Analysis
The Hands-On Guide to Dissecting Malicious Software
Michael Sikorski and Andrew Honig
Foreword by Richard Bejtlich
Copyrighted Material

File MD5 Hash



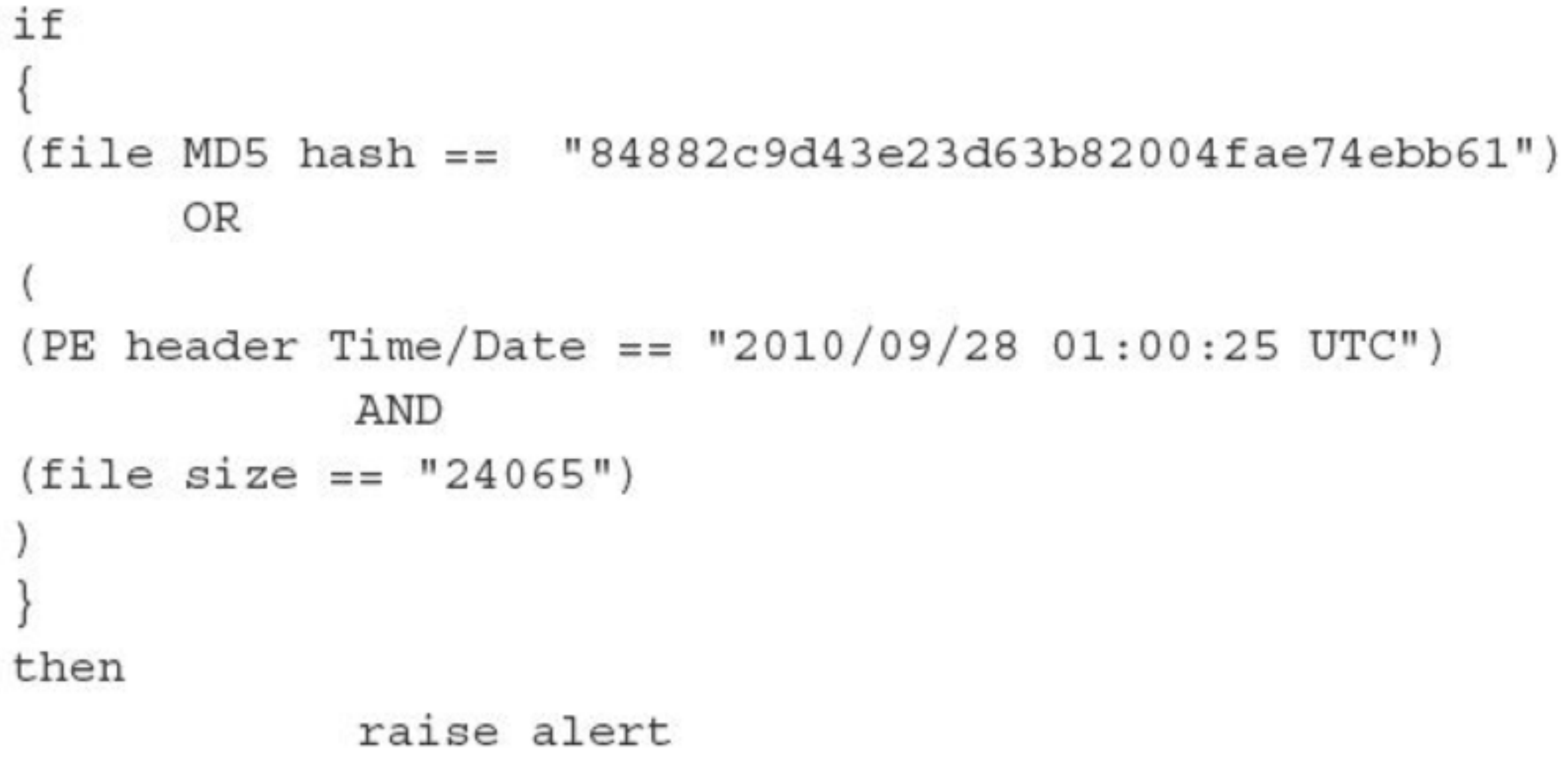
```
if
{
(file MD5 hash == "84882c9d43e23d63b82004fae74ebb61")
}
then
      raise alert
```

- **Low false positive rate, but limited**
    - **Any change in file causes indicator to fail**
    - **Won't be effective for long**

Windows PE Headers

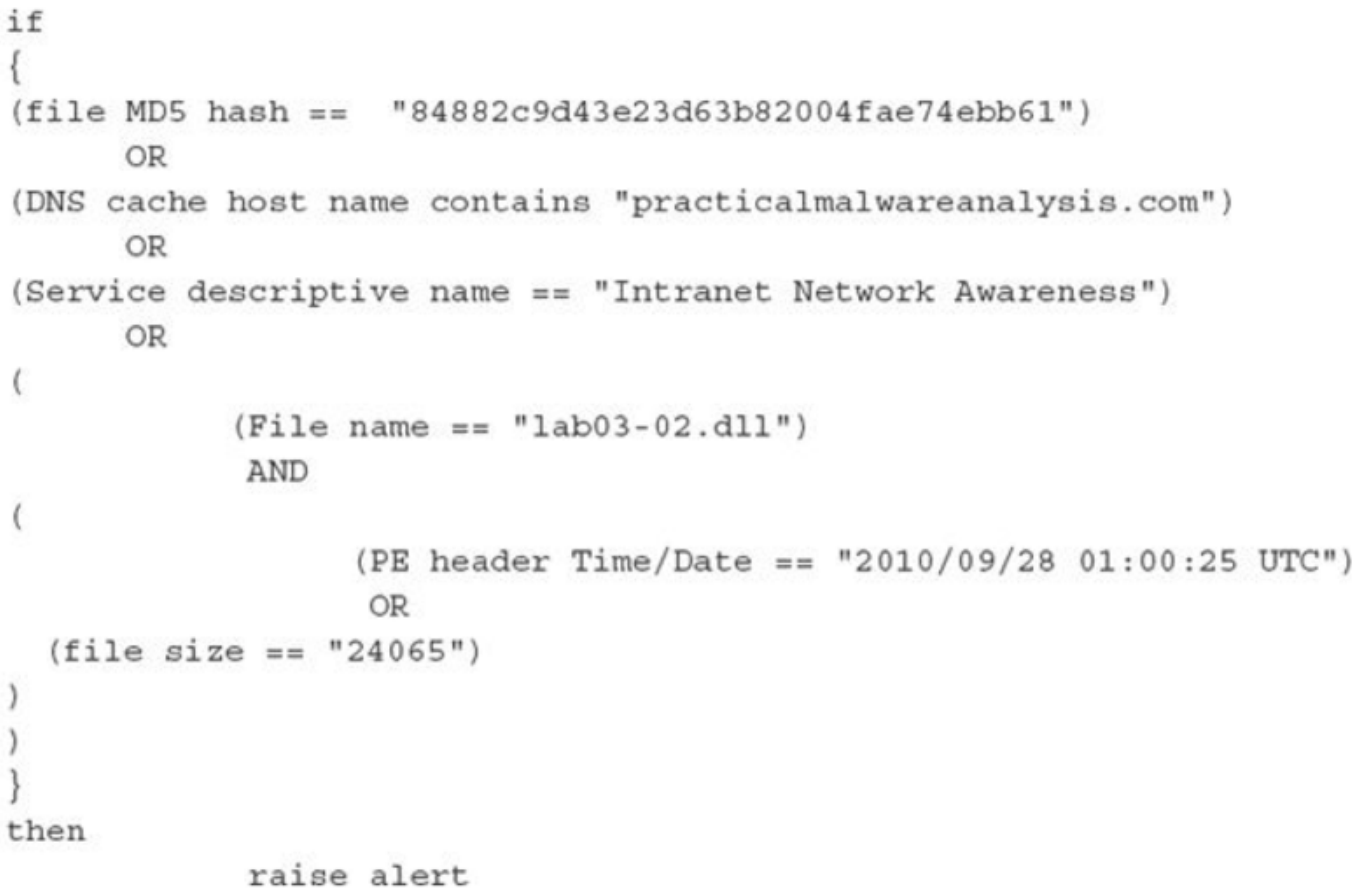
- **Windows programs are Portable Executable (PE) files**
  - **.exe, .com, or .dll**
- **The PE format has a header that specifies general information about the file**

Windows PE Headers



```
if
{
(file MD5 hash ==  "84882c9d43e23d63b82004fae74ebb61")
      OR
(
(PE header Time/Date == "2010/09/28 01:00:25 UTC")
            AND
(file size == "24065")
)
}
then
            raise alert
```

Include DNS Cache



```
if
{
(file MD5 hash ==  "84882c9d43e23d63b82004fae74ebb61")
      OR
(DNS cache host name contains "practicalmalwareanalysis.com")
      OR
(Service descriptive name == "Intranet Network Awareness")
      OR
(
           (File name == "lab03-02.dll")
            AND
(
                 (PE header Time/Date == "2010/09/28 01:00:25 UTC")
                  OR
  (file size == "24065")
)
)
}
then
            raise alert
```

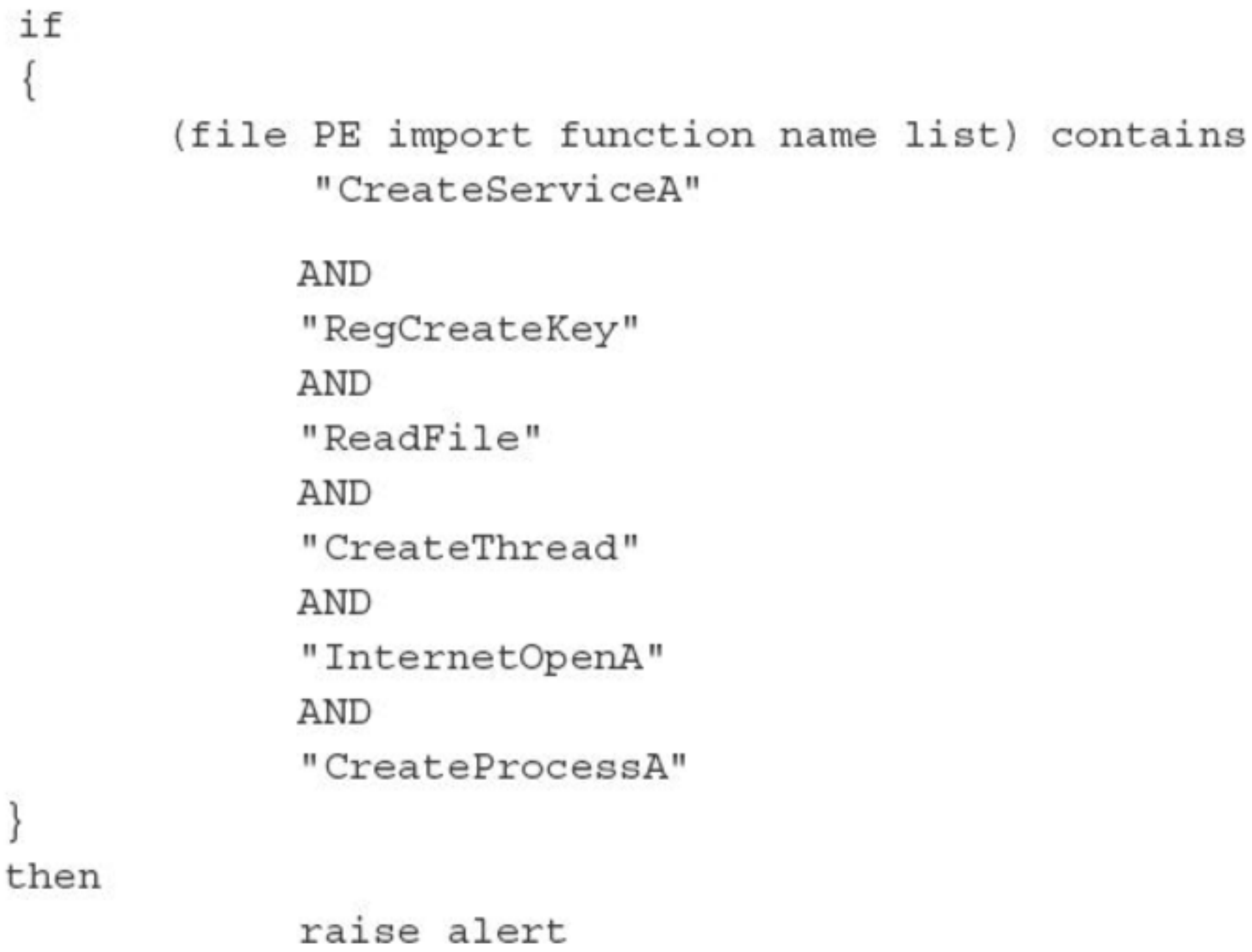
Balance

- Goal: enough information to reliably detect files
- But not too much time lost analyzing malware
- And not too slow for scanner to process
    - Snort drops packets when rules are too complex

Import Table

- **Part of PE header**
- **Lists libraries required to run the program**
- **Normal programs use libraries in common, predictable patterns**
- **Malware often uses strange patterns of libraries**

Import Table IOC



```
if
{
        (file PE import function name list) contains
                "CreateServiceA"

               AND
               "RegCreateKey"
               AND
               "ReadFile"
               AND
               "CreateThread"
               AND
               "InternetOpenA"
               AND
               "CreateProcessA"
}
then
               raise alert
```

Non-Malware IOC

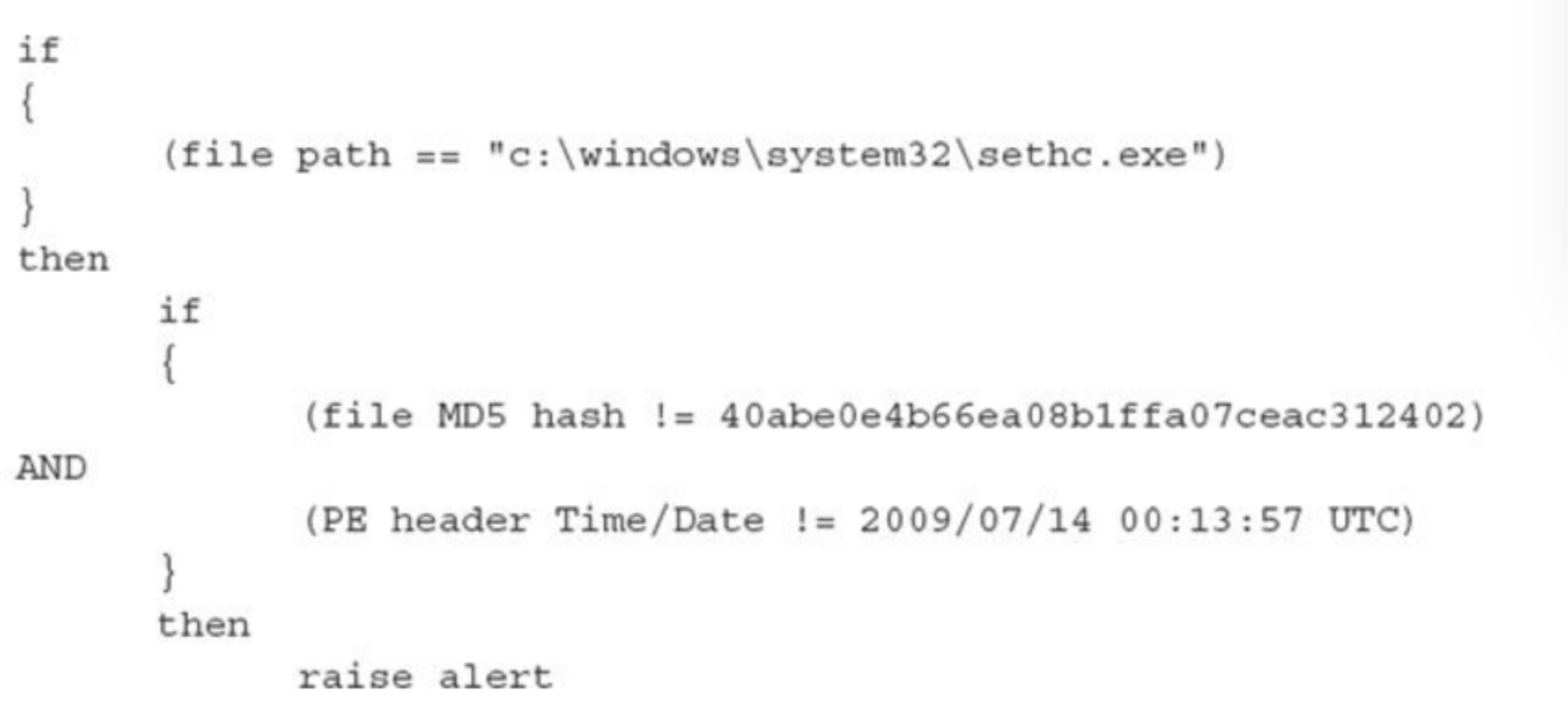
- **Actions an attacker may perform**
- **Example: sethc.exe replacement attack**
    - **sethc.exe enables handicapped accessibility**
    - **Press Shift key five times before login**
    - **Windows offers accessible login options**
    - **By launching sethc.exe with System privileges**

Seth.exe Replacement

- **Replace the file at C:\Windows\System32\sethc.exe, or**

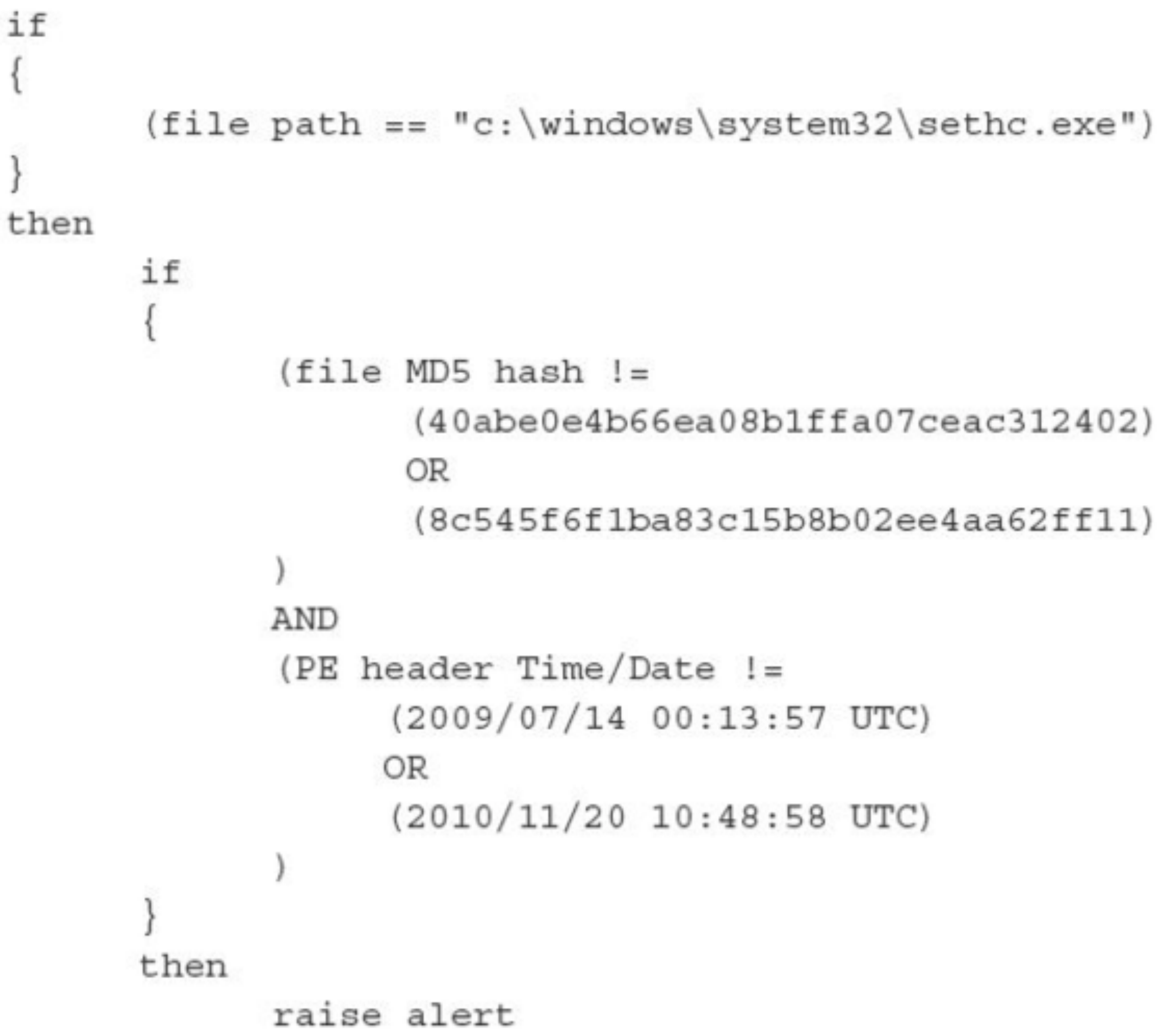
- **Add cmd.exe to the seth executable's debug handler in the registry**

Detect File Replacement



```
if
{
        (file path == "c:\windows\system32\sethc.exe")
}
then
        if
        {
                (file MD5 hash != 40abe0e4b66ea08b1ffa07ceac312402)
AND
                (PE header Time/Date != 2009/07/14 00:13:57 UTC)
        }
        then
                raise alert
```

Two Windows Versions



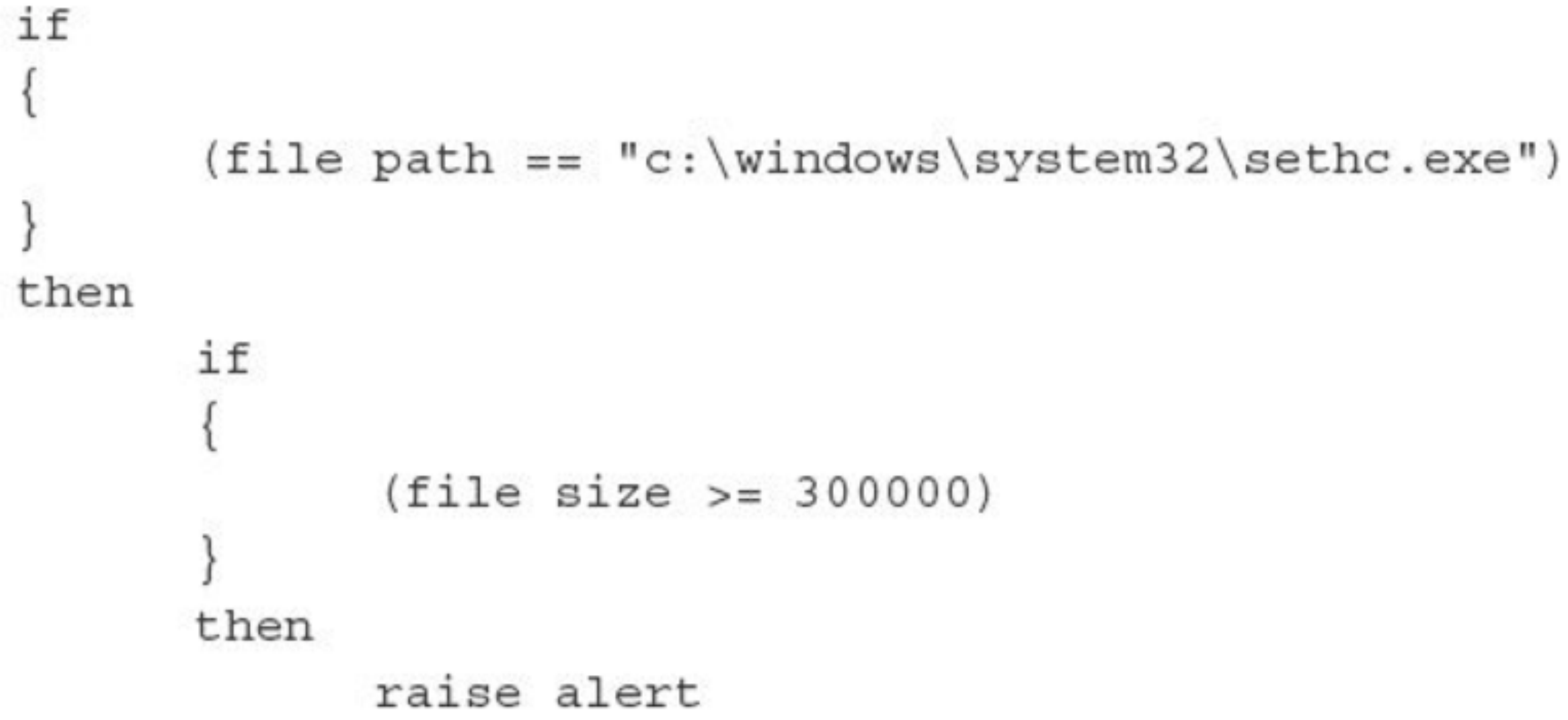
```
if
{
      (file path == "c:\windows\system32\sethc.exe")
}
then
      if
      {
            (file MD5 hash !=
                  (40abe0e4b66ea08b1ffa07ceac312402)
                  OR
                  (8c545f6f1ba83c15b8b02ee4aa62ff11)
            )
            AND
            (PE header Time/Date !=
                 (2009/07/14 00:13:57 UTC)
                 OR
                 (2010/11/20 10:48:58 UTC)
            )
      }
      then
            raise alert
```

Another Way

- **In practice, attackers always replaces sethc.exe with cmd.exe**

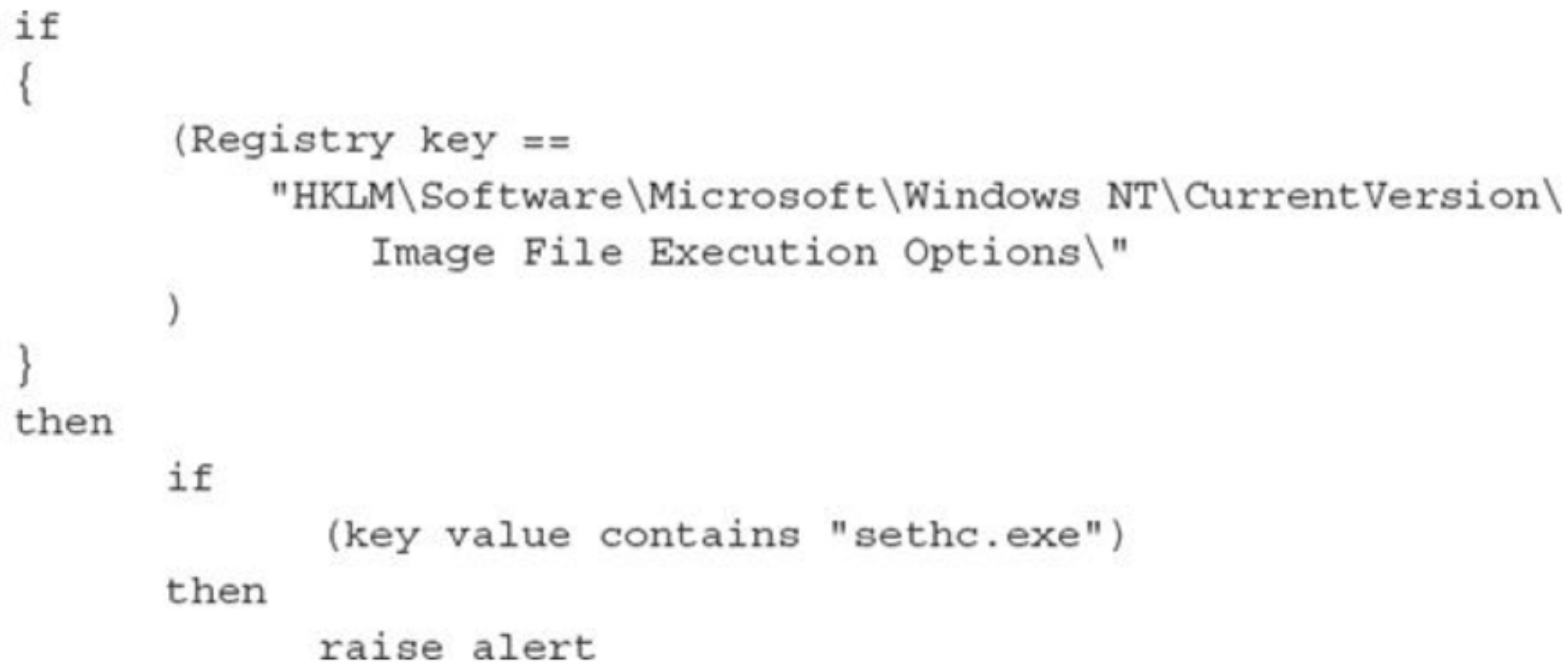
- **And cmd.exe was always 10% or more larger that the largest seth.exe**

Much Simpler IOC



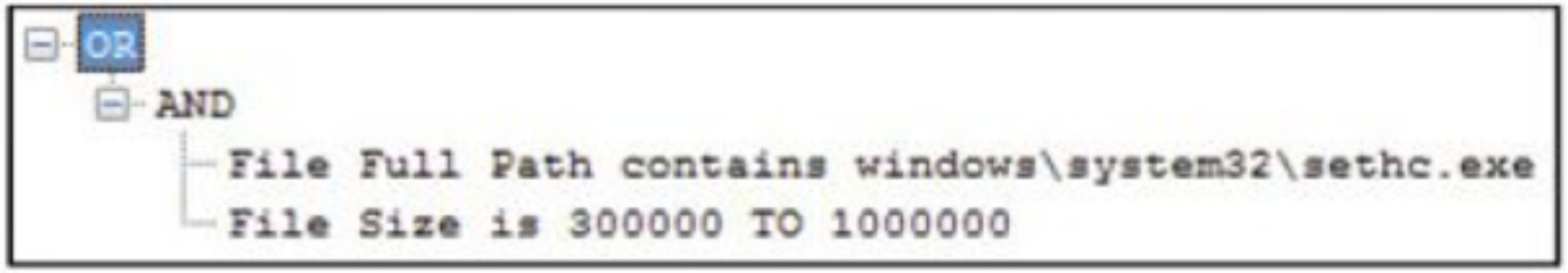
```
if
{
        (file path == "c:\windows\system32\sethc.exe")
}
then
        if
        {
                (file size >= 300000)
        }
        then
                raise alert
```

Detect Debugger Key



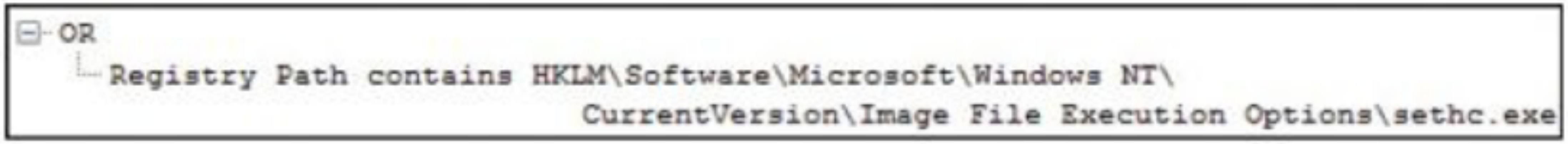
```
if
{
      (Registry key ==
          "HKLM\Software\Microsoft\Windows NT\CurrentVersion\
              Image File Execution Options\"
      )
}
then
      if
            (key value contains "sethc.exe")
      then
            raise alert
```

OpenIOC Format



```
OR
  AND
    File Full Path contains windows\system32\sethc.exe
    File Size is 300000 TO 1000000
```

Figure 5-2. File system indicator for sethc.exe replacements



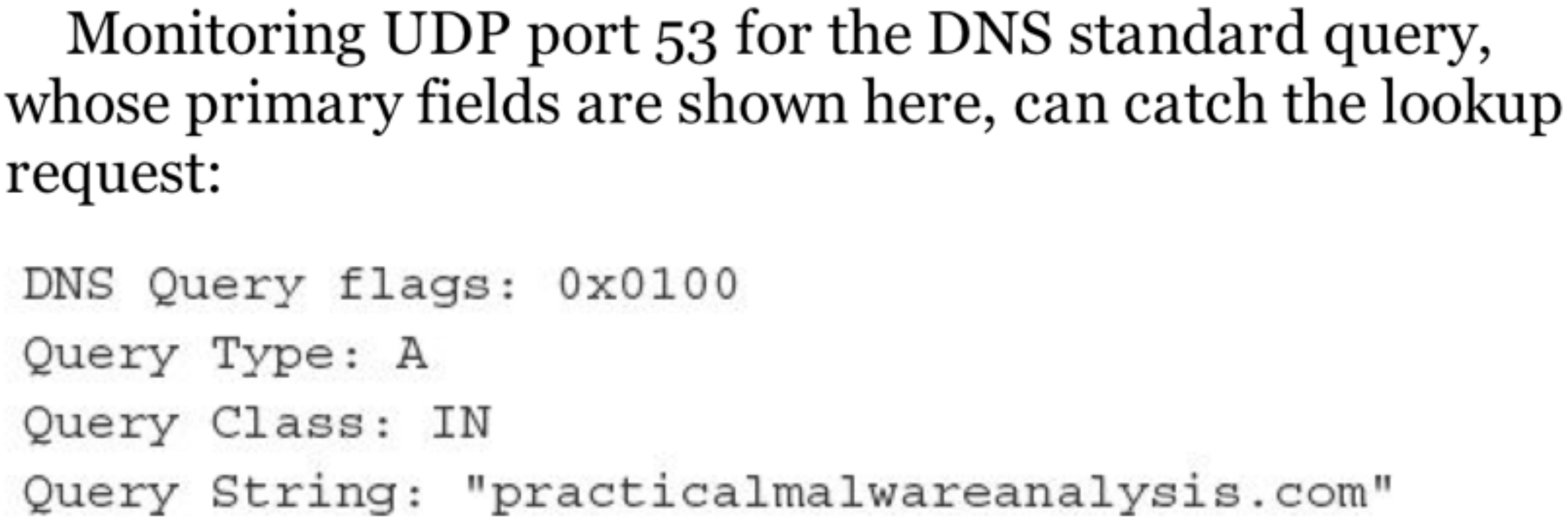
```
OR
  Registry Path contains HKLM\Software\Microsoft\Windows NT\
                         CurrentVersion\Image File Execution Options\sethc.exe
```

Figure 5-3. Registry indicator for sethc.exe debuggers

Editing Network-Based Indicators

- **Rapid determination of whether a session is relevant to the investigation**
  - **"If a set of bytes are present in the first n bytes of a session, raise an alert"**
- **As malware changes, the network signatures require editing**

DNS Monitoring

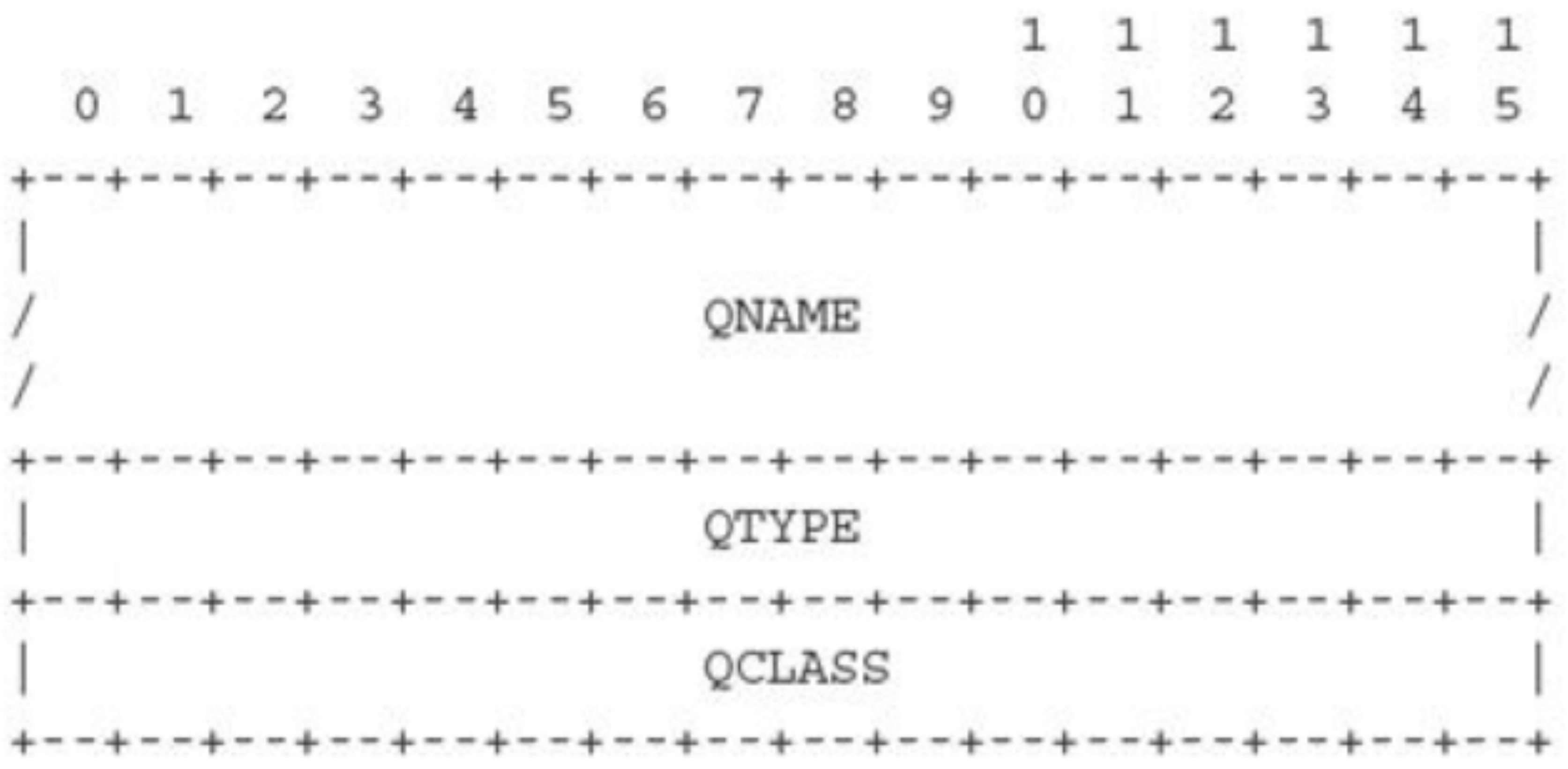


Monitoring UDP port 53 for the DNS standard query, whose primary fields are shown here, can catch the lookup request:

```
DNS Query flags: 0x0100
Query Type: A
Query Class: IN
Query String: "practicalmalwareanalysis.com"
```

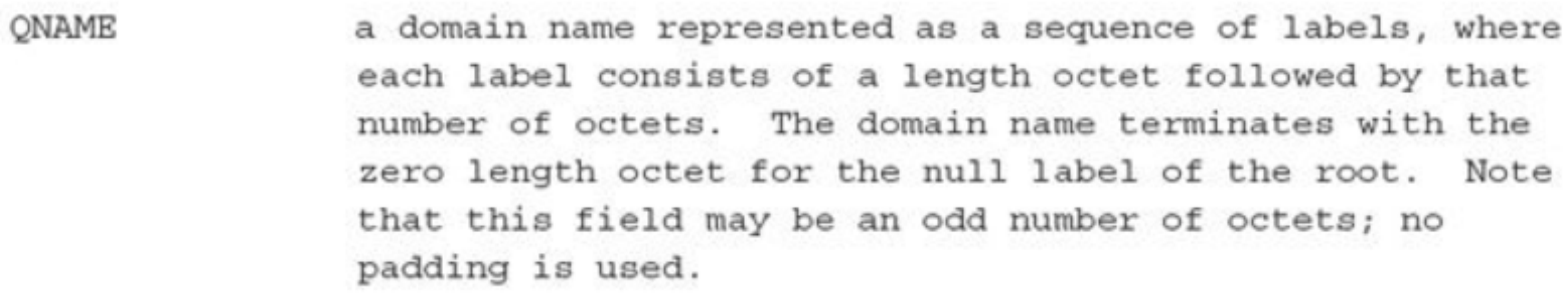
DNS from RFC 1035

- **Query section**



```
                                1  1  1  1  1  1
  0  1  2  3  4  5  6  7  8  9  0  1  2  3  4  5
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                                               |
/                     QNAME                     /
/                                               /
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                     QTYPE                     |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                     QCLASS                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
```

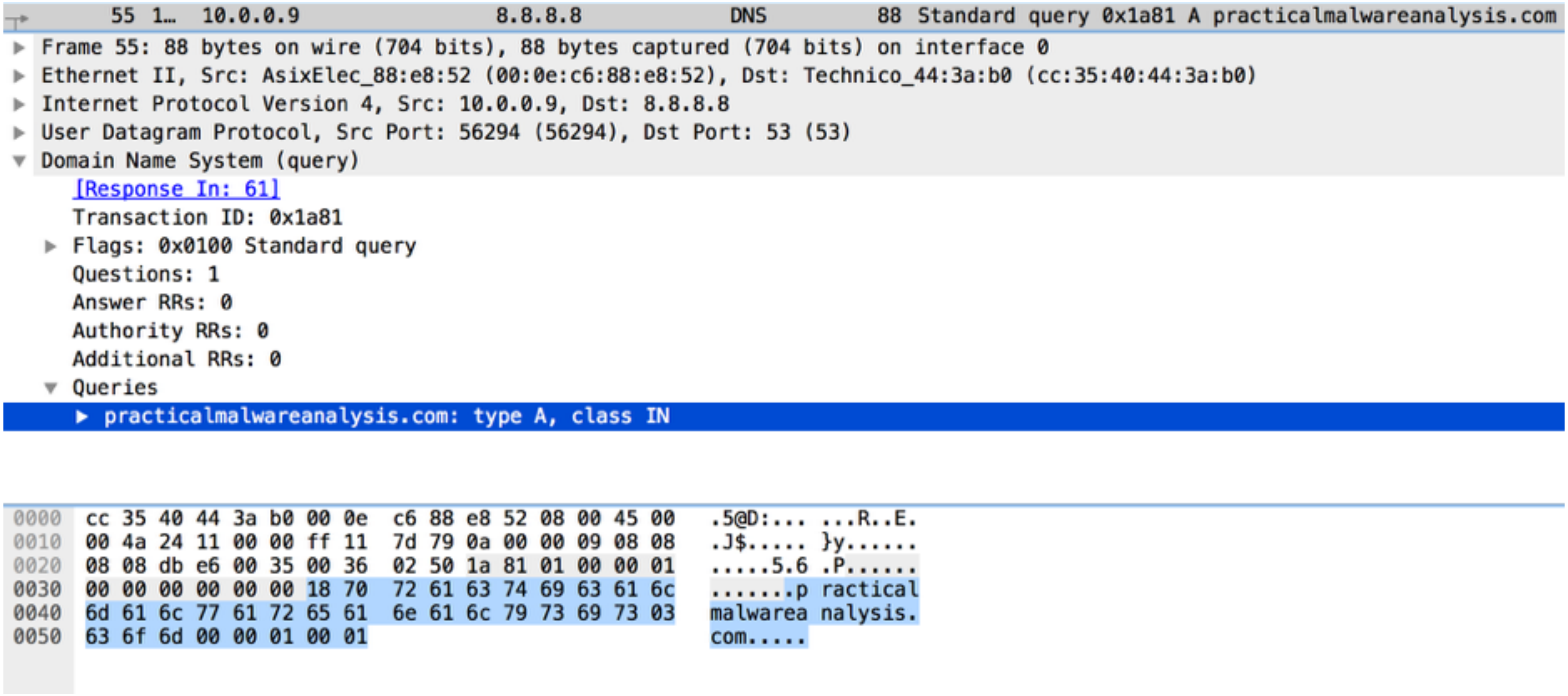
QNAME Format



```
QNAME           a domain name represented as a sequence of labels, where
                each label consists of a length octet followed by that
                number of octets.  The domain name terminates with the
                zero length octet for the null label of the root.  Note
                that this field may be an odd number of octets; no
                padding is used.
```

- **Domain names are split into labels**
- **Length before each label**
- **No periods are used**
  - **18   practicalmalwareanalysis**
  - **3   com**

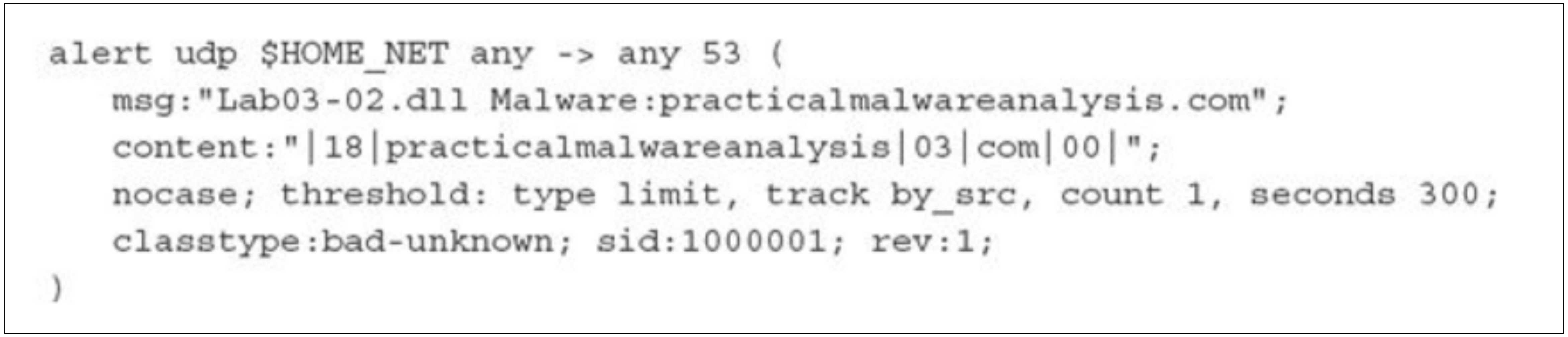
Wireshark Capture



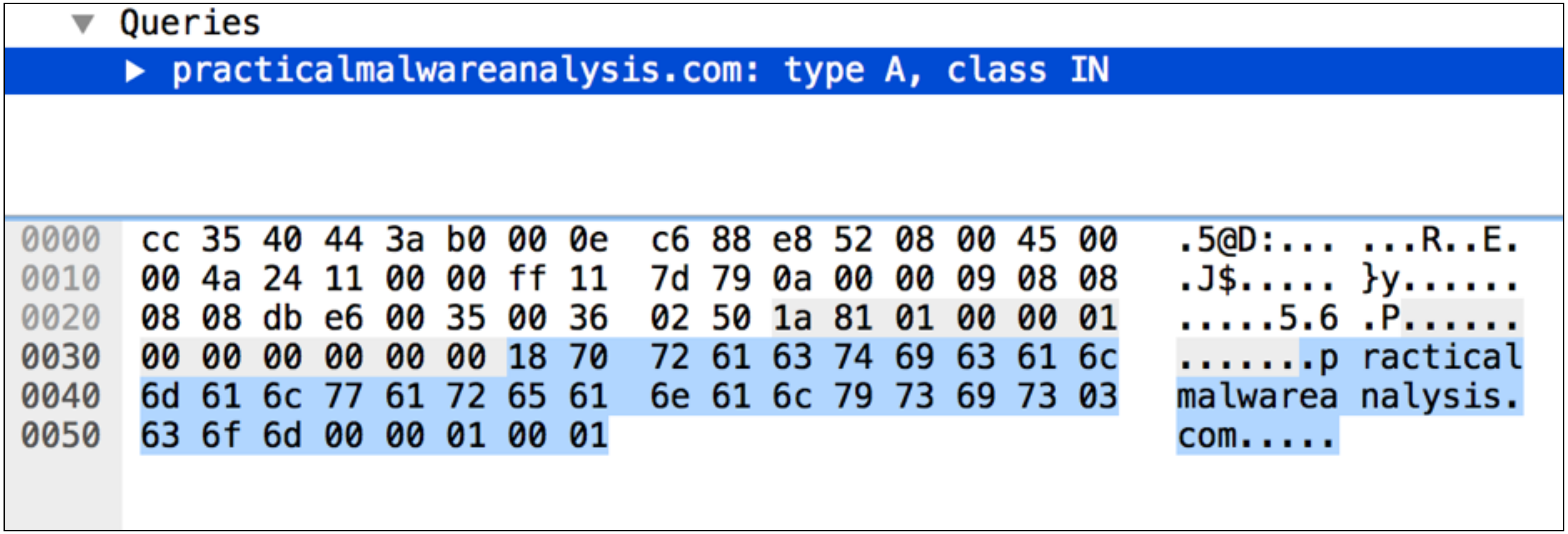
```
     55 1…  10.0.0.9             8.8.8.8            DNS        88 Standard query 0x1a81 A practicalmalwareanalysis.com
▶ Frame 55: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface 0
▶ Ethernet II, Src: AsixElec_88:e8:52 (00:0e:c6:88:e8:52), Dst: Technico_44:3a:b0 (cc:35:40:44:3a:b0)
▶ Internet Protocol Version 4, Src: 10.0.0.9, Dst: 8.8.8.8
▶ User Datagram Protocol, Src Port: 56294 (56294), Dst Port: 53 (53)
▼ Domain Name System (query)
    [Response In: 61]
    Transaction ID: 0x1a81
  ▶ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▶ practicalmalwareanalysis.com: type A, class IN


0000  cc 35 40 44 3a b0 00 0e  c6 88 e8 52 08 00 45 00   .5@D:... ...R..E.
0010  00 4a 24 11 00 00 ff 11  7d 79 0a 00 00 09 08 08   .J$..... }y......
0020  08 08 db e6 00 35 00 36  02 50 1a 81 01 00 00 01   .....5.6 .P......
0030  00 00 00 00 00 00 18 70  72 61 63 74 69 63 61 6c   .......p ractical
0040  6d 61 6c 77 61 72 65 61  6e 61 6c 79 73 69 73 03   malwarea nalysis.
0050  63 6f 6d 00 00 01 00 01                            com.....
```

Snort Signature



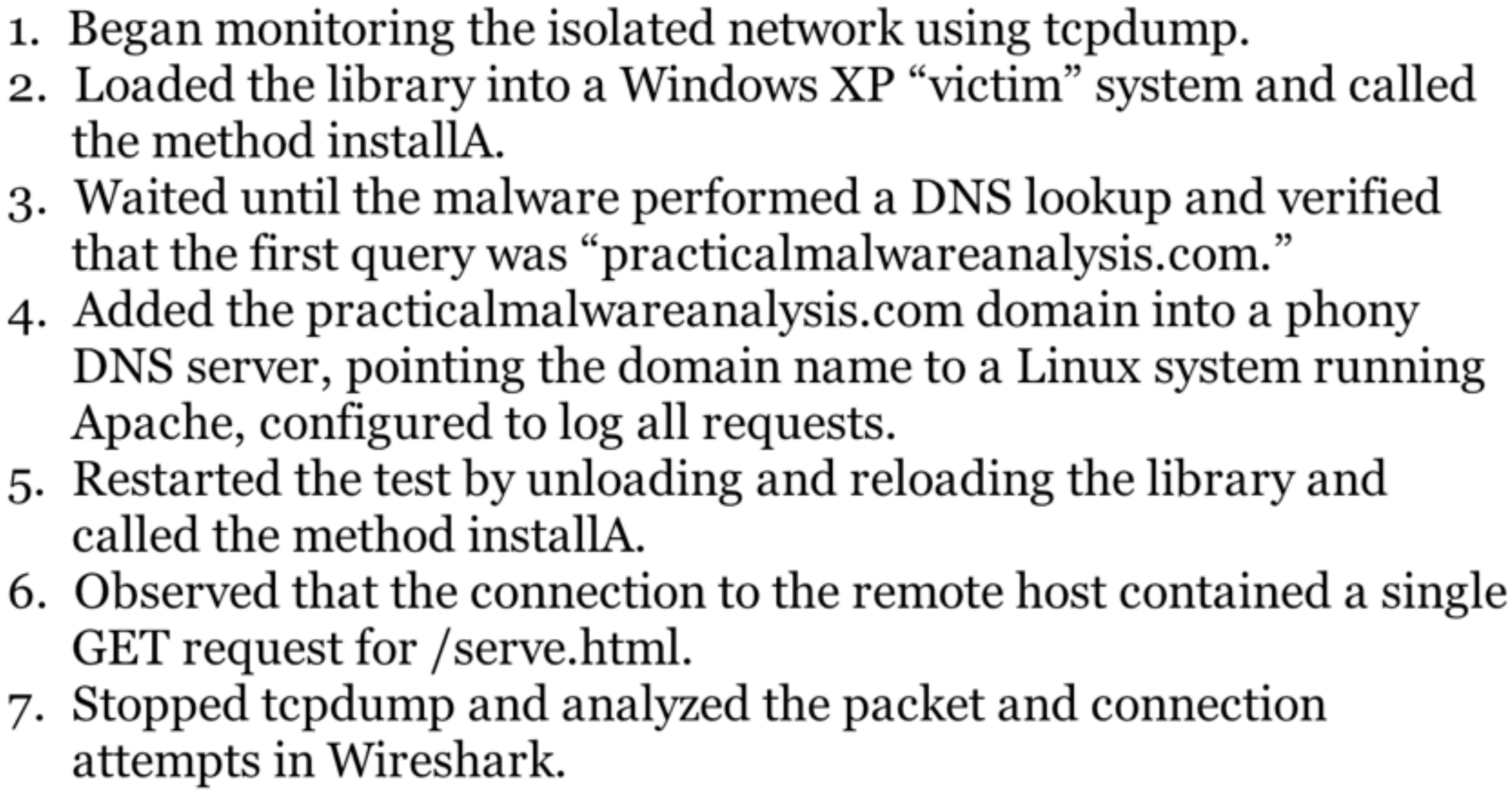
```
alert udp $HOME_NET any -> any 53 (
   msg:"Lab03-02.dll Malware:practicalmalwareanalysis.com";
   content:"|18|practicalmalwareanalysis|03|com|00|";
   nocase; threshold: type limit, track by_src, count 1, seconds 300;
   classtype:bad-unknown; sid:1000001; rev:1;
)
```



```
▼ Queries
    ▶ practicalmalwareanalysis.com: type A, class IN

0000  cc 35 40 44 3a b0 00 0e  c6 88 e8 52 08 00 45 00   .5@D:... ...R..E.
0010  00 4a 24 11 00 00 ff 11  7d 79 0a 00 00 09 08 08   .J$..... }y......
0020  08 08 db e6 00 35 00 36  02 50 1a 81 01 00 00 01   .....5.6 .P......
0030  00 00 00 00 00 00 18 70  72 61 63 74 69 63 61 6c   .......p ractical
0040  6d 61 6c 77 61 72 65 61  6e 61 6c 79 73 69 73 03   malwarea nalysis.
0050  63 6f 6d 00 00 01 00 01                            com.....
```

Dynamic Analysis

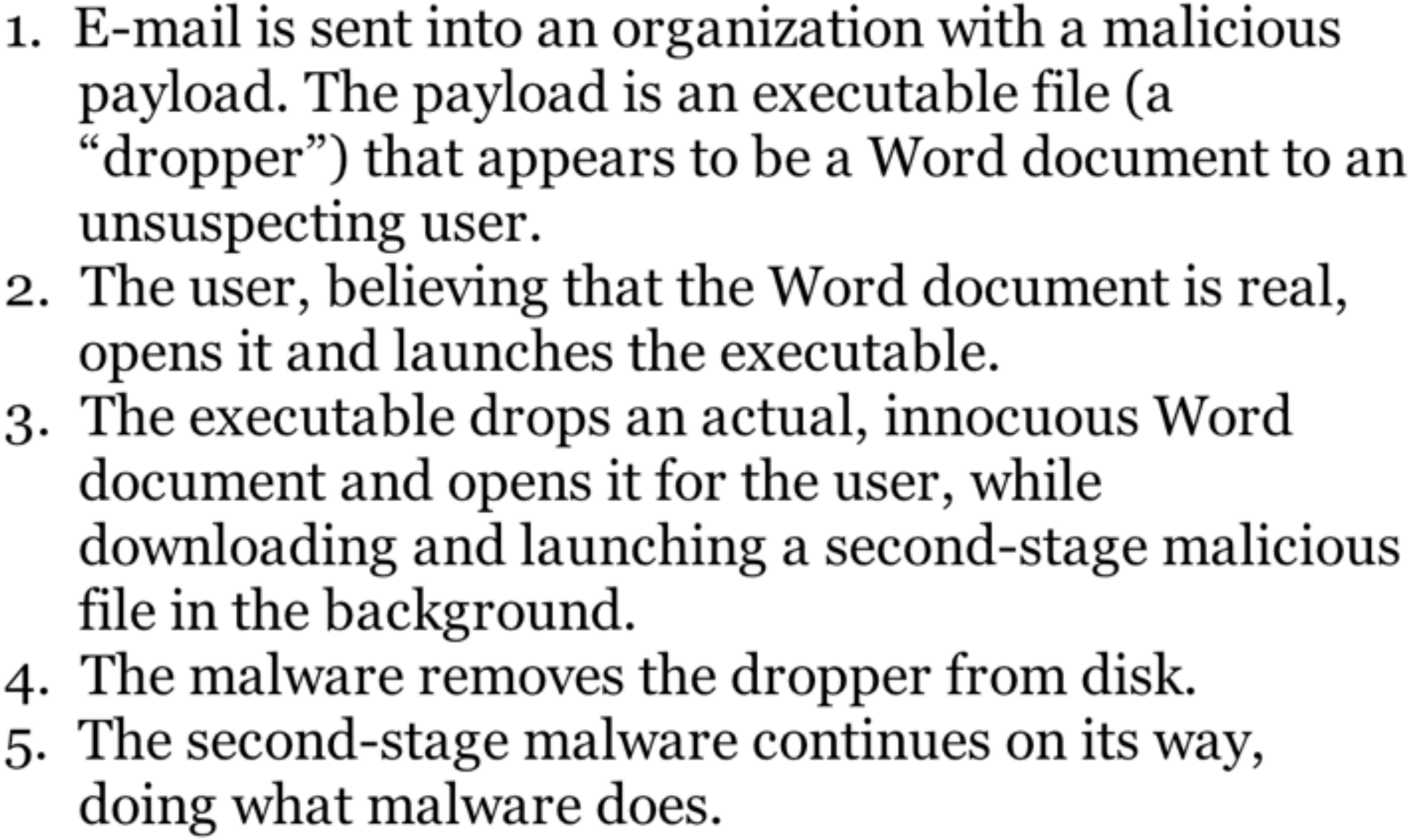


1. Began monitoring the isolated network using tcpdump.
2. Loaded the library into a Windows XP "victim" system and called the method installA.
3. Waited until the malware performed a DNS lookup and verified that the first query was "practicalmalwareanalysis.com."
4. Added the practicalmalwareanalysis.com domain into a phony DNS server, pointing the domain name to a Linux system running Apache, configured to log all requests.
5. Restarted the test by unloading and reloading the library and called the method installA.
6. Observed that the connection to the remote host contained a single GET request for /serve.html.
7. Stopped tcpdump and analyzed the packet and connection attempts in Wireshark.

Verification

- **Before scanning thousands of systems, test IOP rules on a representative sample**
- **Two reviews**
  - **Data Relevant to Indicator**
  - **Data Common to Environment**

Attack Lifecycle

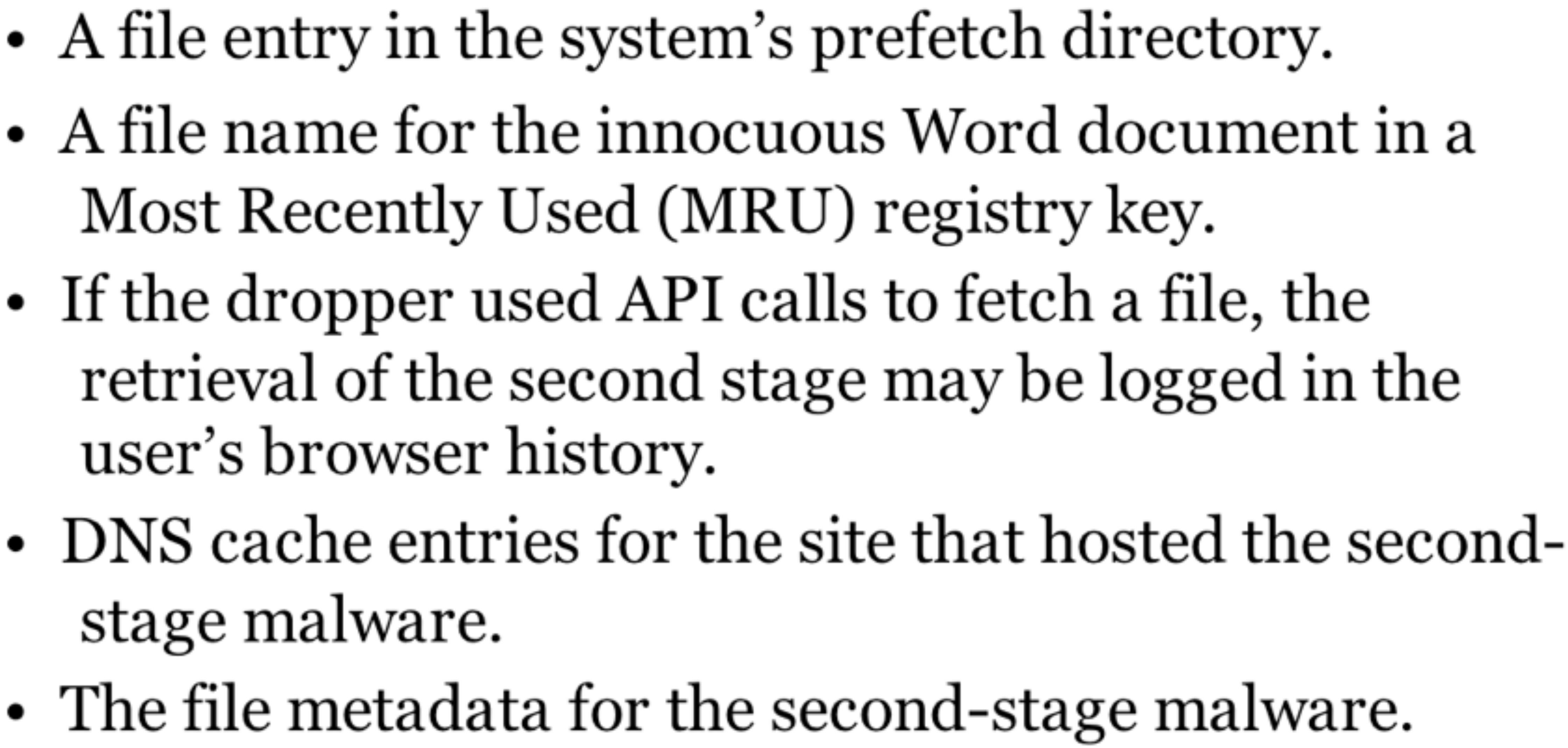


1. E-mail is sent into an organization with a malicious payload. The payload is an executable file (a "dropper") that appears to be a Word document to an unsuspecting user.
2. The user, believing that the Word document is real, opens it and launches the executable.
3. The executable drops an actual, innocuous Word document and opens it for the user, while downloading and launching a second-stage malicious file in the background.
4. The malware removes the dropper from disk.
5. The second-stage malware continues on its way, doing what malware does.

Less Effective Indicator

- **Properties of the dropper**
  - **MD5 hash**
  - **File name**
- **Automated email scanners typically generate this information**

More Effective Indicators



- A file entry in the system's prefetch directory.
- A file name for the innocuous Word document in a Most Recently Used (MRU) registry key.
- If the dropper used API calls to fetch a file, the retrieval of the second stage may be logged in the user's browser history.
- DNS cache entries for the site that hosted the second-stage malware.
- The file metadata for the second-stage malware.

Data Common to Environment

- **Run indicator on a sample of clean workstations**
- **Ensure that parameters don't match**
- **If they do, modify indicators to reduce false positives**

Impact on Environment

- **Run indicator on a representative subset of systems, including servers**
- **Use a resource manager to see the load on the systems**
- **If you bring down important systems with the scan, your customer won't be happy**

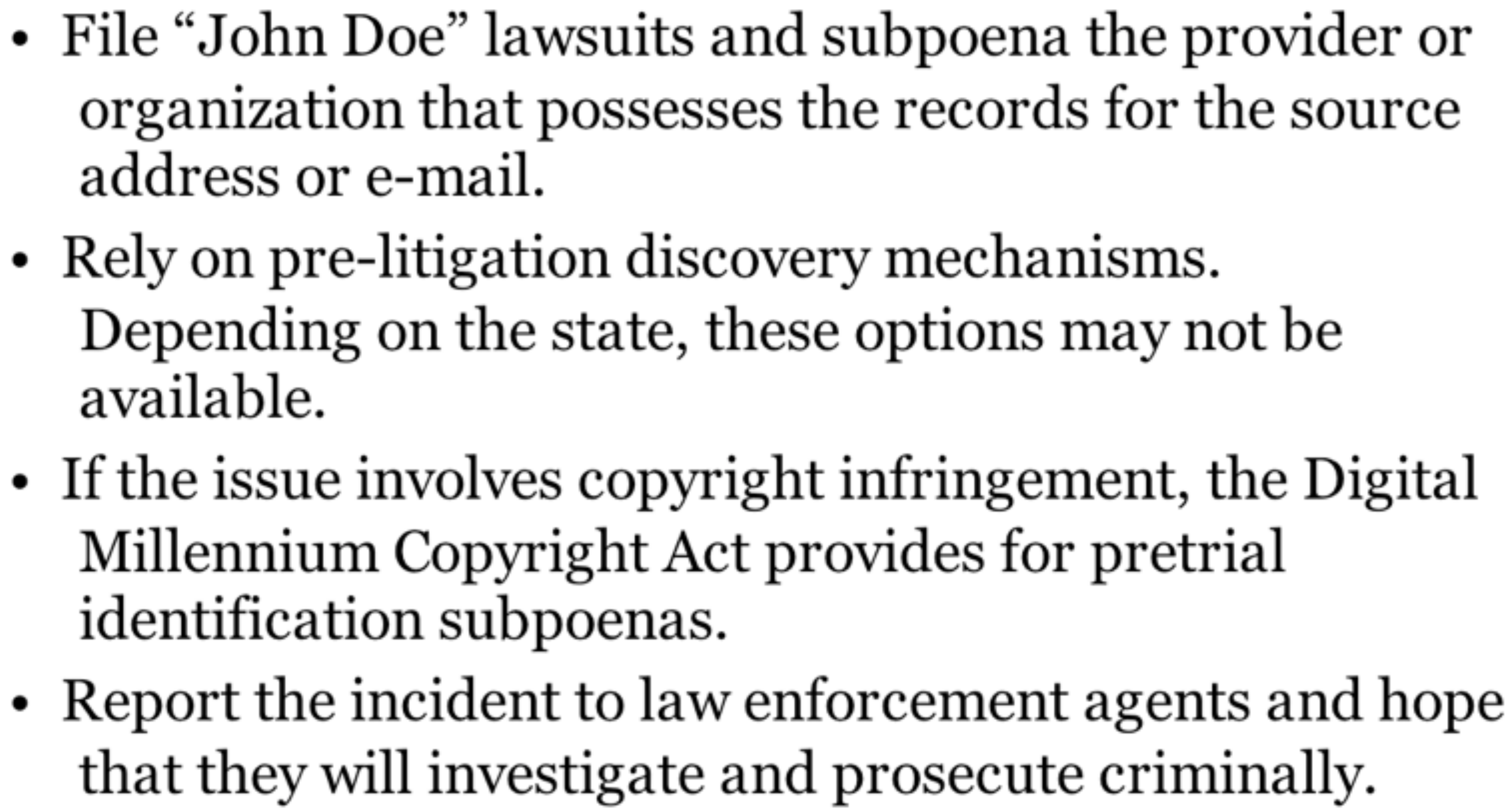
Resolving Internal Leads (from humans)

- **Thoroughly document any statement**
- **Allow the interviewee to tell a story**
- **Avoid leading questions, and ones that require yes/no answers**
- **Collect the facts before allowing interview to opine; don't criticize or confront**
- **Know when to get others involved**

Resolving External Leads

- **External parties are not usually nobliged to provide you with information**
  - **They may do so, if it does not cause undue risk**
- **Private organizations cannot serve grand jury subpoenas, 2703(d) court orders, or subpoenas**

Legal Options



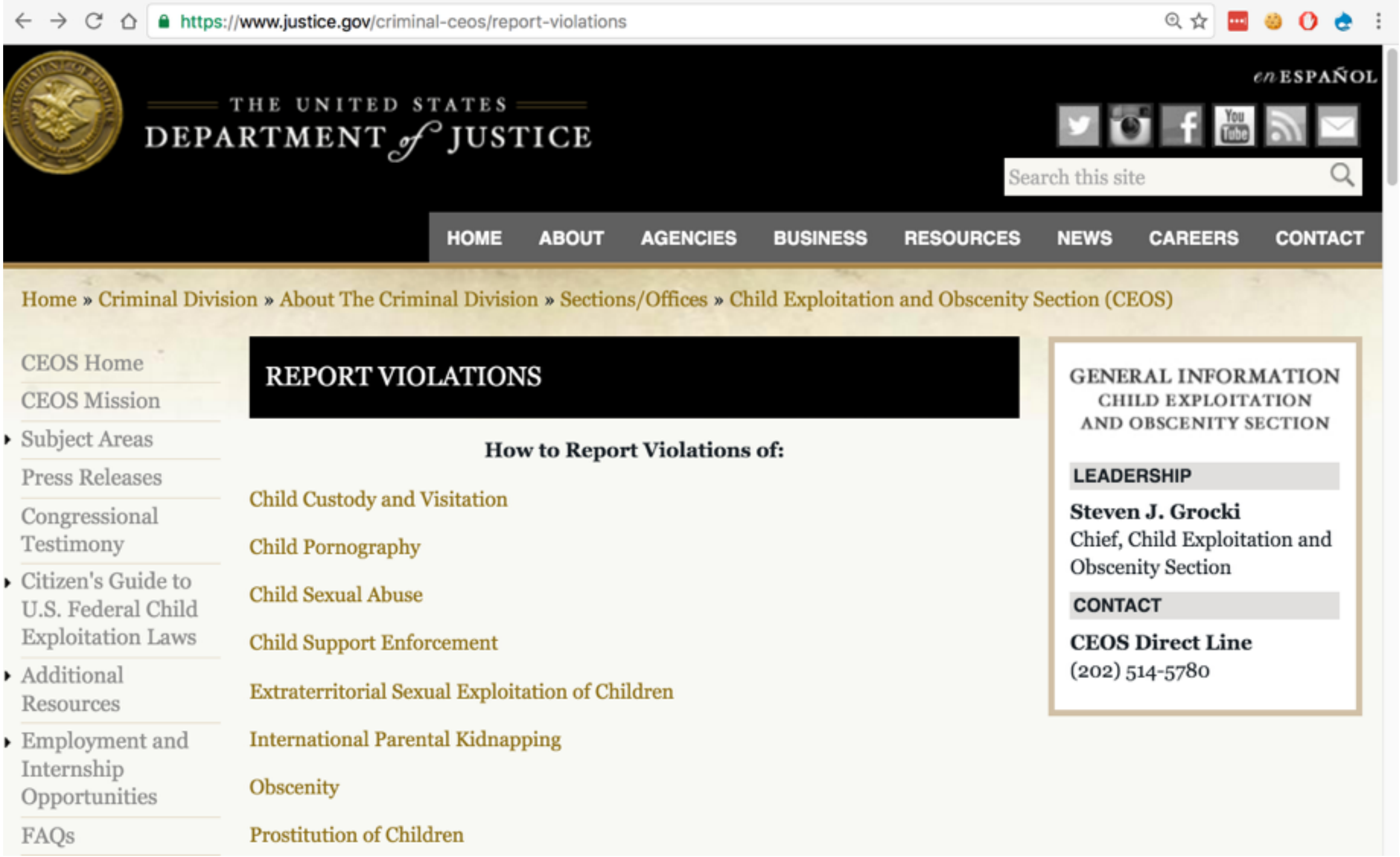
- File “John Doe” lawsuits and subpoena the provider or organization that possesses the records for the source address or e-mail.
- Rely on pre-litigation discovery mechanisms. Depending on the state, these options may not be available.
- If the issue involves copyright infringement, the Digital Millennium Copyright Act provides for pretrial identification subpoenas.
- Report the incident to law enforcement agents and hope that they will investigate and prosecute criminally.

Filing a Subpoena to Perform Discovery

- **Your legal counsel files a complaint which leads to civil discovery**
- **This can compel an organization, such as an ISP, to divulge information about a subscriber**

Reporting an Incident to Law Enforcement

- **Most organizations avoid this, to prevent a public relations issue**
- **US very rarely requires notification of criminal acts**
  - **Child pronography requires you to contact the**


https://www.justice.gov/criminal-ceos/report-violations
en ESPAÑOL
THE UNITED STATES
DEPARTMENT of JUSTICE
Search this site
HOME
ABOUT
AGENCIES
BUSINESS
RESOURCES
NEWS
CAREERS
CONTACT
Home » Criminal Division » About The Criminal Division » Sections/Offices » Child Exploitation and Obscenity Section (CEOS)
CEOS Home
CEOS Mission
Subject Areas
Press Releases
Congressional Testimony
Citizen's Guide to U.S. Federal Child Exploitation Laws
Additional Resources
Employment and Internship Opportunities
FAQs

REPORT VIOLATIONS

How to Report Violations of:

Child Custody and Visitation

Child Pornography

Child Sexual Abuse

Child Support Enforcement

Extraterritorial Sexual Exploitation of Children

International Parental Kidnapping

Obscenity

Prostitution of Children

GENERAL INFORMATION
CHILD EXPLOITATION
AND OBSCENITY SECTION

LEADERSHIP

Steven J. Grocki
Chief, Child Exploitation and Obscenity Section

CONTACT

CEOS Direct Line
(202) 514-5780

- **Link Ch 5a**

Foreign Entities

- **ISPs or hosting sites**
- **Quite complicated**
- **Require civil requests through formal channels**
- **State Dept. and Federal law enforcement agencies**

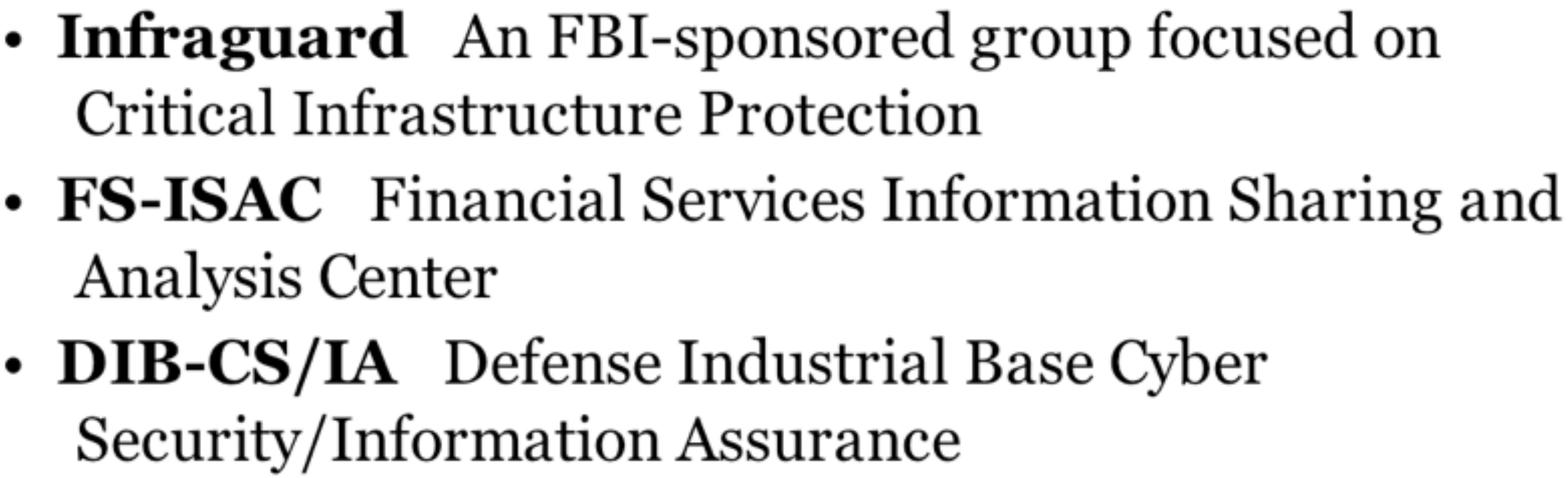
Advantages of Law Enforcement

- **Greater capacity to investigate and prosecute**
- **Quicker response to subpoenas and court orders**
    - **And target is not notified**
- **Can bring criminal action at no cost to your organization**
    - **Or a small cost preparing materials**

Preparing for Law Enforcement Involvement

- **Document the incident appropriately**
- **Maintain chain of custody of evidence**
- **Clear and concise picture of the unlawful activity that took place**
- **Convey the information in a clear and simple manner**

Information Sharing



- **Infraguard** An FBI-sponsored group focused on Critical Infrastructure Protection
- **FS-ISAC** Financial Services Information Sharing and Analysis Center
- **DIB-CS/IA** Defense Industrial Base Cyber Security/Information Assurance