# CIT 430/530 – Lab #5 – Pcap File Analysis

Pcap files are the captured traffic from a network protocol analyzer, such as Wireshark or tshark. In this lab, you’ll use Wireshark to analyze a pcap file and answer questions related to computer forensics investigation.

### Wireshark resources

* Wireshark User Guide – <https://www.wireshark.org/docs/wsug_html/>
  + [Section 6 – Working with Capture Packets](https://www.wireshark.org/docs/wsug_html/#ChapterWork)
  + [Section 7 – Advanced Topics](https://www.wireshark.org/docs/wsug_html/#ChapterAdvanced)

## Part 1: Getting Started

|  |  |
| --- | --- |
| **Case Background** | After being released on bail, Ann Dercover disappears! Fortunately, investigators were carefully monitoring her network activity before she skipped town. “We believe Ann may have communicated with her secret lover, Mr. X, before she left,” says the policy chief. “The packet capture may contain clues to her whereabouts.” |
| **Forensic Tasks** | 1. Provide any online aliases or addresses and corresponding account credentials that may be used by the suspect (Ann) under investigation. |
| 1. Who did Ann communicate with? Provide a list of email addresses and any other identifying information. |
| 1. Extract any transcripts of Ann’s conversations and present them to investigators |
| 1. If Ann transferred or received any files of interest, recover them. |
| 1. Are there indications of Ann’s physical whereabouts? If so, provide supporting evidence. |
| **Suspect Information** | * Ann Dercover Laptop MAC: 00:21:70:4D:4F:AE * Ann’s Internal (home) Network: 192.168.30.0/24 * DMZ: 10.30.30.0/24 * The “Internet”: 172.30.1.0/24 |

From your SIFT Workstation download the pcap file from Canvas, then use the following command to open the file using Wireshark.



Once Wireshark opens, complete the following steps to gather background information and find evidence supporting the forensic tasks listed above.

Select Statistics in the menu bar, then Protocol Hierarchy

1. **Provide the upper-layer network protocols and their percentages associated with emails exchanged over a network**

|  |  |
| --- | --- |
| **Protocol** | **Percent** |
| **Simple mail transfer protocol** | **10.8** |
| **SMB mailslot protocol** | **0.7** |

Close the Statistics Window then apply a filter to show packets from Discover, Offer, Request, Acknowledgement ([DORA](https://ipwithease.com/understanding-dora-process-in-dhcp/)) process when Ann last logged on to her network.

**eth.addr = 00:21:70:4d:4f:ae**

In the first DHCP request packet, expand the Bootstrap Protocol to determine the following information:

|  |  |
| --- | --- |
| **Type of laptop used by Ann** | Dell |
| **IP address of the requesting device** | 192.168.30.108 |

Select the DHCP Acknowledge (ACK) packet and from within the packet details window, expand the various headers to find the following information:

|  |  |
| --- | --- |
| **IP address of the DHCP server** | 192.168.30.10 |
| **Ann’s IP lease information** | 3600s or 1 hour |
| **IP Address of Ann’s DNS server** | 10.30.30.20 |

**Leave Wireshark running**.

## Part 2: Key Word Search

Key word searches are significant to the computer forensics process, particularly during a network forensics analysis. Searching for known strings or words that may be of interest help identify potential evidence quickly. In this section, you’ll use ngrep to parse the pcap evidence.

* [ngrep (network grep)](https://www.tecmint.com/ngrep-network-packet-analyzer-for-linux/) is a simple yet powerful network packet analyzer. It is a grep-like tool applied to the network layer – it matches traffic passing over a network interface. It allows you to specify an extended regular or hexadecimal expression to match against data payloads (the actual information or message in transmitted data, but not auto-generated metadata) of packets.

**In a new terminal**, change to the Downloads directory and issue the following command:

**ngrep “Ann Dercover” -N -t -q -I evidence-packet-analysis.pcap**

The returned output should be seven (7) packets containing the string “Ann Dercover”. Use these packets to complete the table below.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Source IP | Source Port | Destination IP | Destination Port | Timestamp | Packet Number [A] in Wireshark |
| 1 | **192.168.30.108** | **1684** | **64.12.168.40** | **587** | **19:33:07** | **1587** |
| 2 | **192.168.30.108** | **1685** | **205.188.58.10** | **143** | **19:33:08** | **1615** |
| 3 | **205.188.58.10** | **143** | **192.168.30.108** | **1686** | **19:33:21** | **1655** |
| 4 | **192.168.30.108** | **1687** | **64.12.168.40** | **587** | **19:34:16** | **1749** |
| 5 | **192.168.30.108** | **1688** | **205.188.58.10** | **143** | **19:34:18** | **1779** |
| 6 | **192.168.30.108** | **1689** | **64.12.168.40** | **587** | **19:35:16** | **1825** |
| 7 | **192.168.30.108** | **1690** | **205.188.58.10** | **143** | **19:35:24** | **2164** |

## Part 3: SMTP Analysis

The same information returned with ngrep can also be found using Wireshark, but organizes the data in a somewhat friendly manner.

Back in Wireshark clear the previous eth.add filter and create a new filter using the destination IP returned in the first packet by ngrep. Next, find this same packet in Wireshark.

**ip.dst == destination\_IP**

In the “Info” column of this packet you should see a statement about the packet being a DATA fragment. The nice thing about Wireshark is that it can take this packet and find the other packets that are a part of this specific network communication.

Select this packet in the packet window, right-click, then go to Follow TCP Stream. What is returned, is the conversation for this communication. Use Wireshark to follow the TCP Streams for all seven packets returned by ngrep and answer the following questions:

|  |  |
| --- | --- |
| 1. **Any online aliases, addresses or corresponding account credentials that may be used by Ann Dercover.** | * **Text    Description automatically generated** * **Graphical user interface, text, application    Description automatically generated** |
| 1. **Email addresses or other identifying information related to individuals Ann may have communicated with.** | * [**Inter0pt1c@aol.com**](mailto:Inter0pt1c@aol.com) |
| 1. **Extract (i.e. screenshot) any transcripts of Ann’s conversations and summarize the timeline of events using this content, IP address information and timestamps** | **Graphical user interface, text, application  Description automatically generated**   * **Graphical user interface, application    Description automatically generated** |

## Extra Credit (optional)

By now you should have an idea of what Ann has done, but there’s additional information that can be collected/recovered. Answer the remaining questions and provide a brief summary of your procedure (i.e. packet of interest, data carving technique, commands used, etc.)

1. **Recover Ann’s attachment**
2. **Find any indications of Ann’s physical whereabouts**.

**Hints:**

* This will require data being carved from one of the packets in the SMTP Analysis section, which can be found in its TCP Stream.
  + All the information in this packet (minus the header information) will be needed or else an error will be reported when trying to open the carved file.
* The data to carve is in base64 and will need to be decoded. The following commands will be useful. Use the man pages if needed.
  + **fromdos -b Filename\_of\_copied\_data**
  + **base64 -d Filename\_of\_copied\_data > NewFile**

## Submission:

Upload a completed copy of the lab to Canvas by the due date.