

CPSC 6240 Biyang Fu Chenxi Hu

CPSC 4240/6240 Spring 2020

Try It 3

50 points

Due date: 4/15/2020 before 9pm.

Instructions:

This homework is done in *teams of two*, or *individually*, your choice. If you are working with another student, that student must be from the same level as you are (4240 or 6240).

You are allowed to use search engines, textbook/s, lecture notes, and any other sources you wish. But you are *not* allowed to copy paste from Internet, or help other teams with their work, either by giving them hints or solutions.

You will take a number of screenshots. All screenshots should be clearly legible and illustrate without a doubt what you are doing. You can open them in an image editor of your choice and trim off the parts you do not need, just to make images smaller. Insert them when answering the question, do not submit them separately as image files. Since this is an editable word document, you can make space between the questions and type your answers and insert screenshots here. Please do not type in red, any other color is fine. I read everything you write, so if you just type in black, I will not miss your answer



What and how to submit

If working with one other student, please include both of your names on top of that doc or pdf file, as well as your course # 4240 or 6240. No name → no credit. Submit your answer file to canvas.

Grading and Points

Every question indicates how many points it is worth. 4000-level and 6000-level are graded differently, with points indicated as (x/y), where x is 4240 and y is 6240.

Exercises

1. Investigate algorithms used in steganography. Find and describe two of them. Are there programs that use the same algorithm? Can you hide a message in an image using one software program, and then retrieve the message using different software? If so, what two programs, if any, are compatible with each other? In this exercise one of your steganography programs will be Invisible Ink, and another is any program of your choice. (10/8)

(1) Two steganography algorithms:

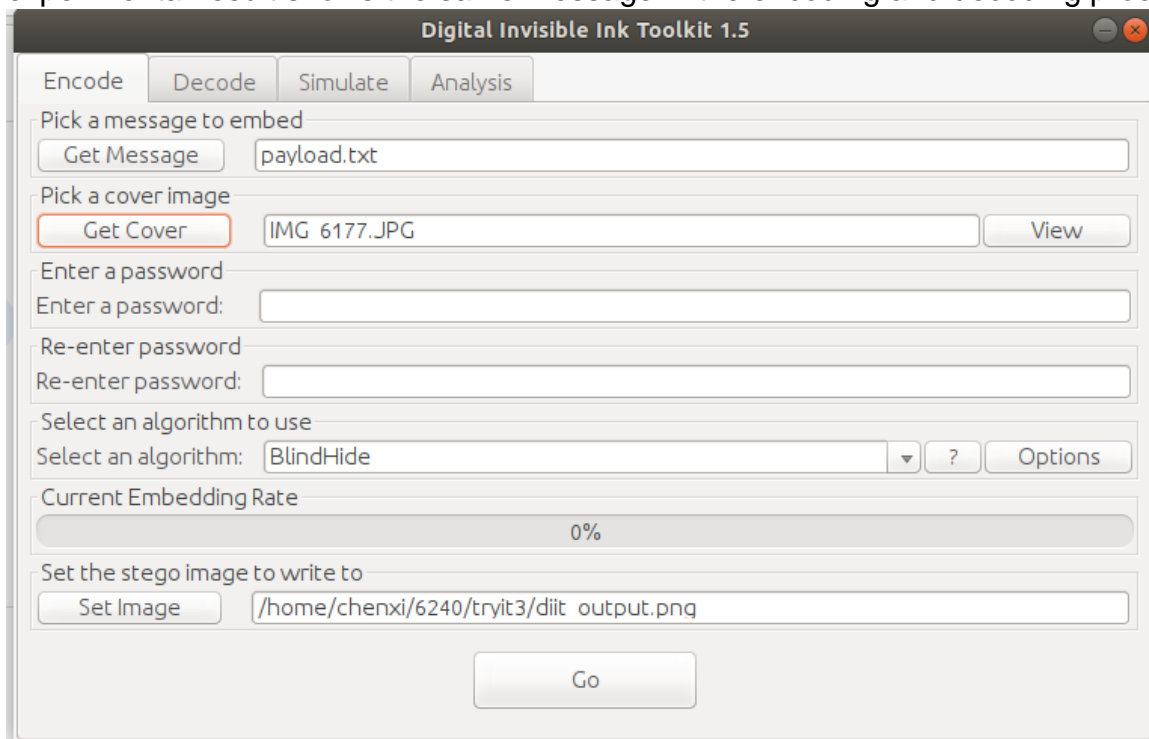
a). Least Significant Bit (LSB) Algorithm

LSB is one of the easiest image steganography algorithms that embeds the payload into the carrier so that it cannot be detected by a casual observer. The main idea of this algorithm is hiding messages inside an image by substituting the least significant bit of image with the bits of message to be hidden.

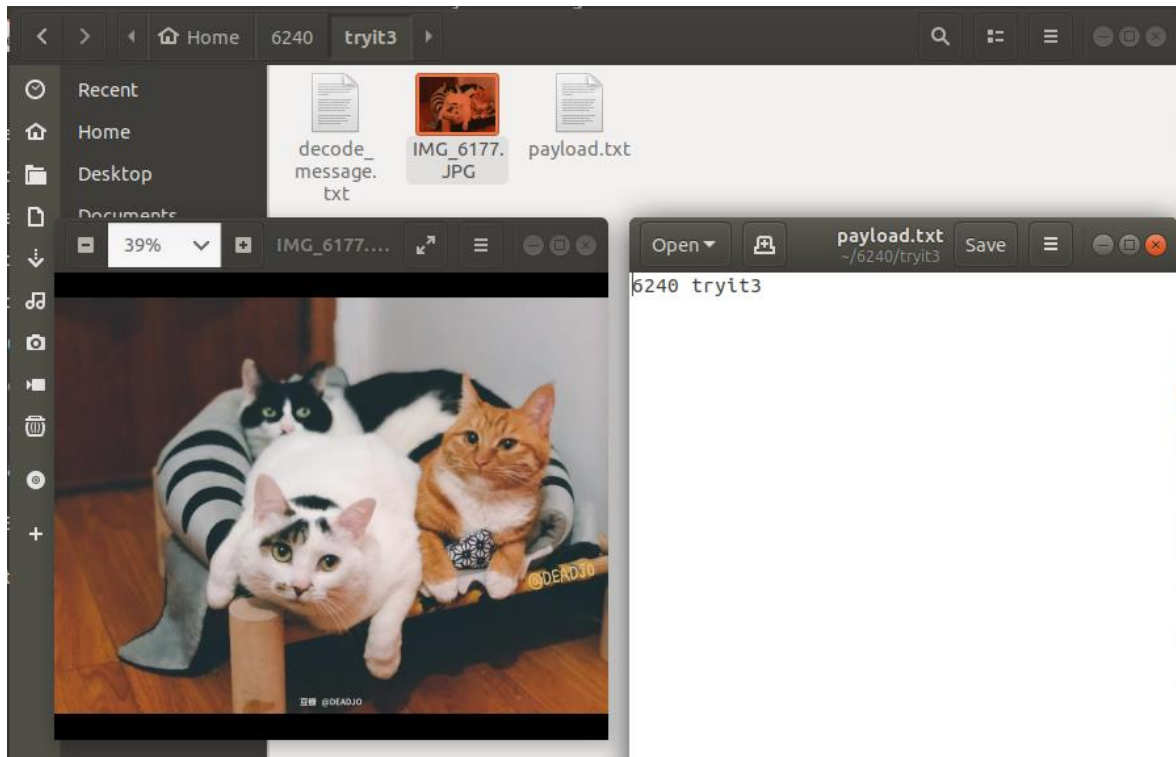
b). Discrete Cosine Transform (DCT)

DCT is another image steganography algorithm which transforms an image from the spatial domain to the frequency domain. It separates the image into parts of differing importance and applies a general equation to obtain DCT matrix.

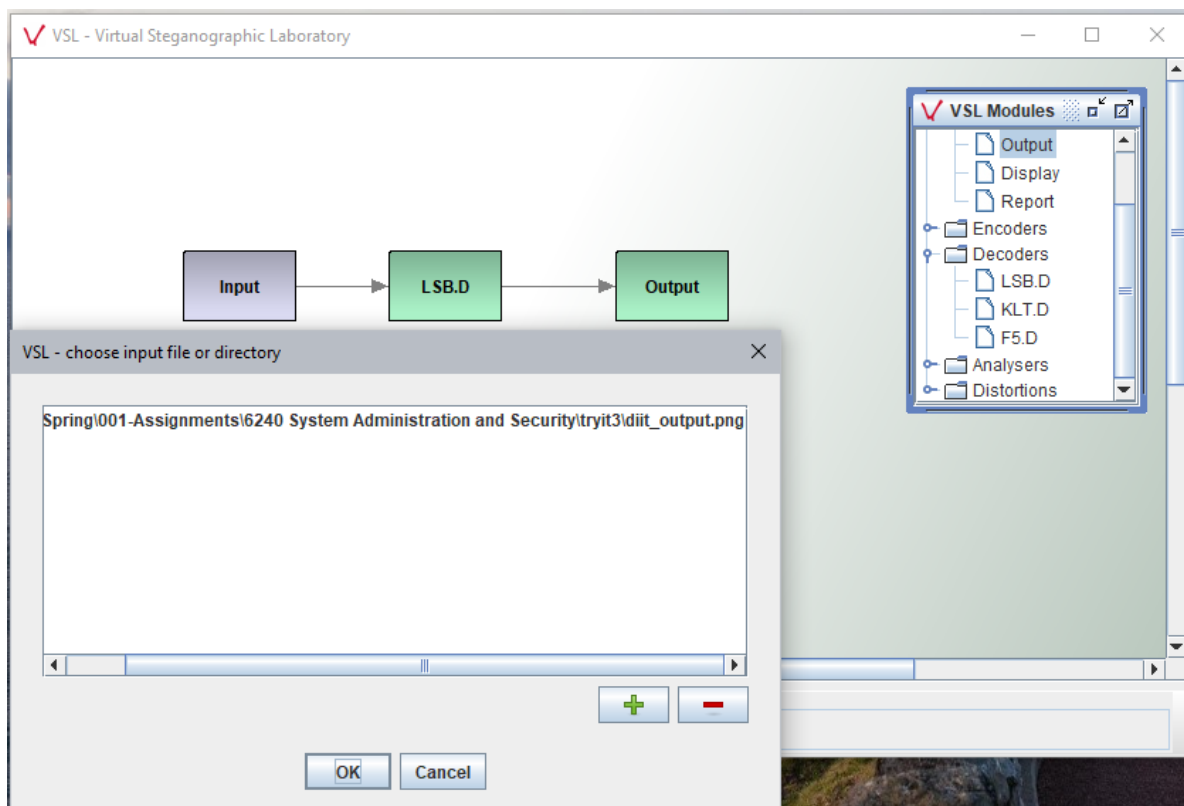
(2) Invisible Ink and Virtual Steganographic Laboratory for Digital Images (VSL) use the same blindhide (LSB) algorithm. We try to encode the message file (payload.txt) into the image file (IMG_6177.JPG) with Invisible Ink to obtain an output image (diit_out.png), and then decode message from the output image (diit_out.png) into a txt file (.). The experimental result shows the same message in the encoding and decoding processes.



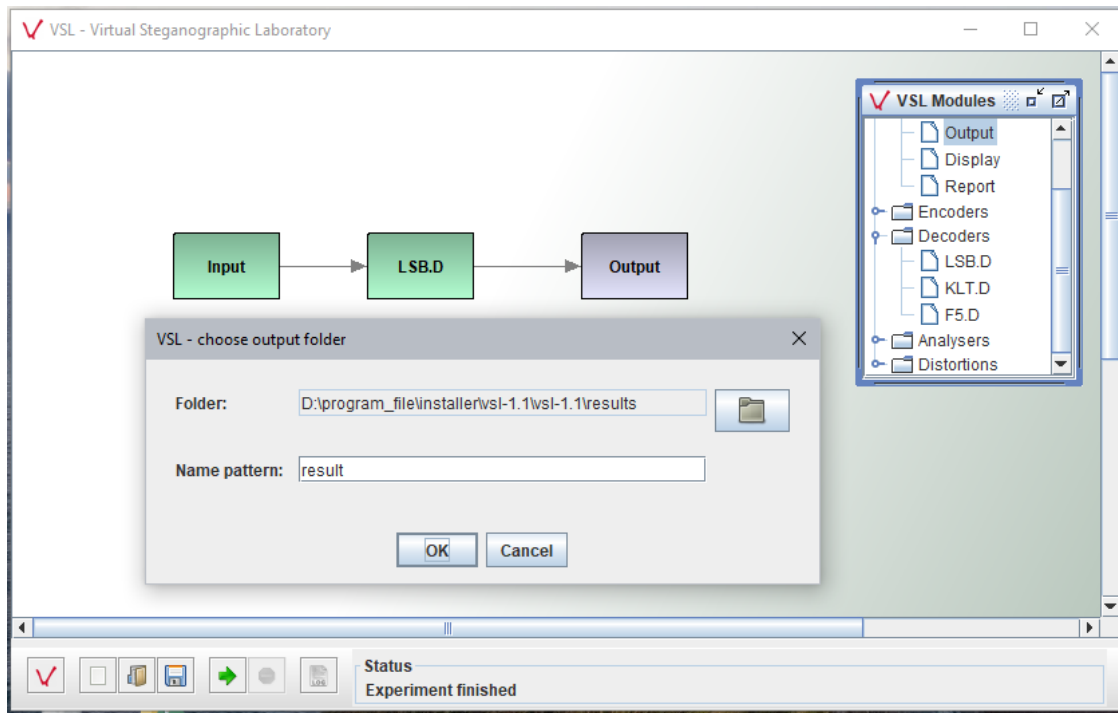
1 - Digital Invisible Ink Toolkit encoding configurations



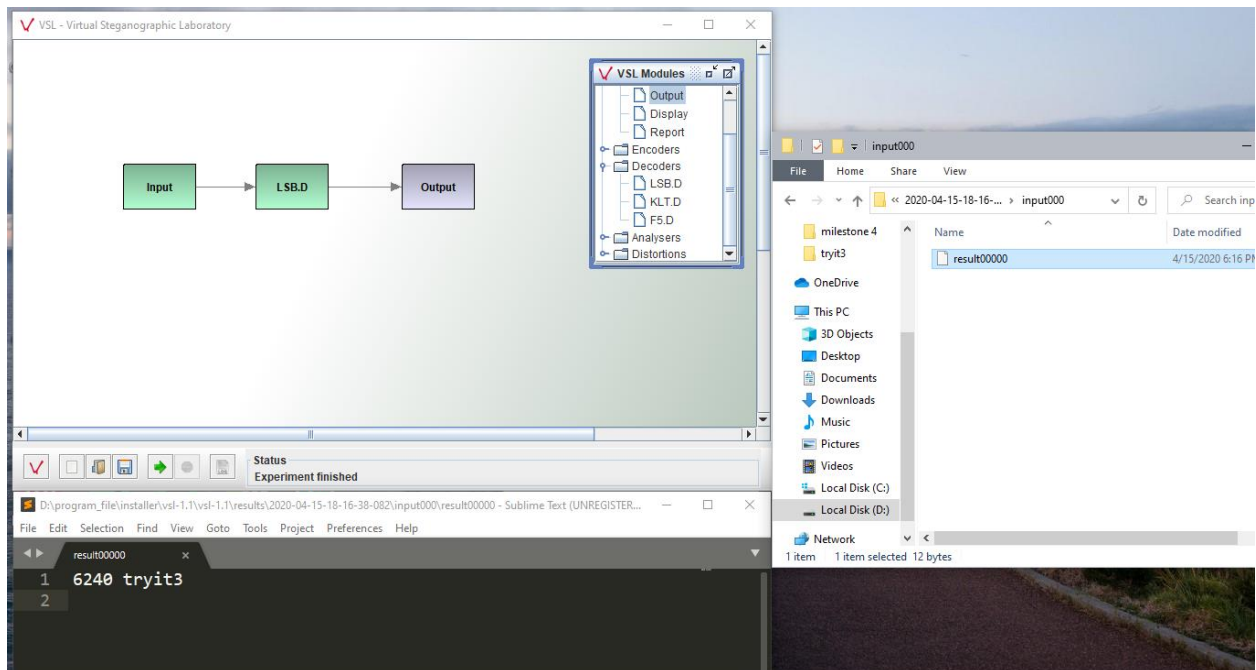
2 - Files



3 - VSL decoding configurations of input image



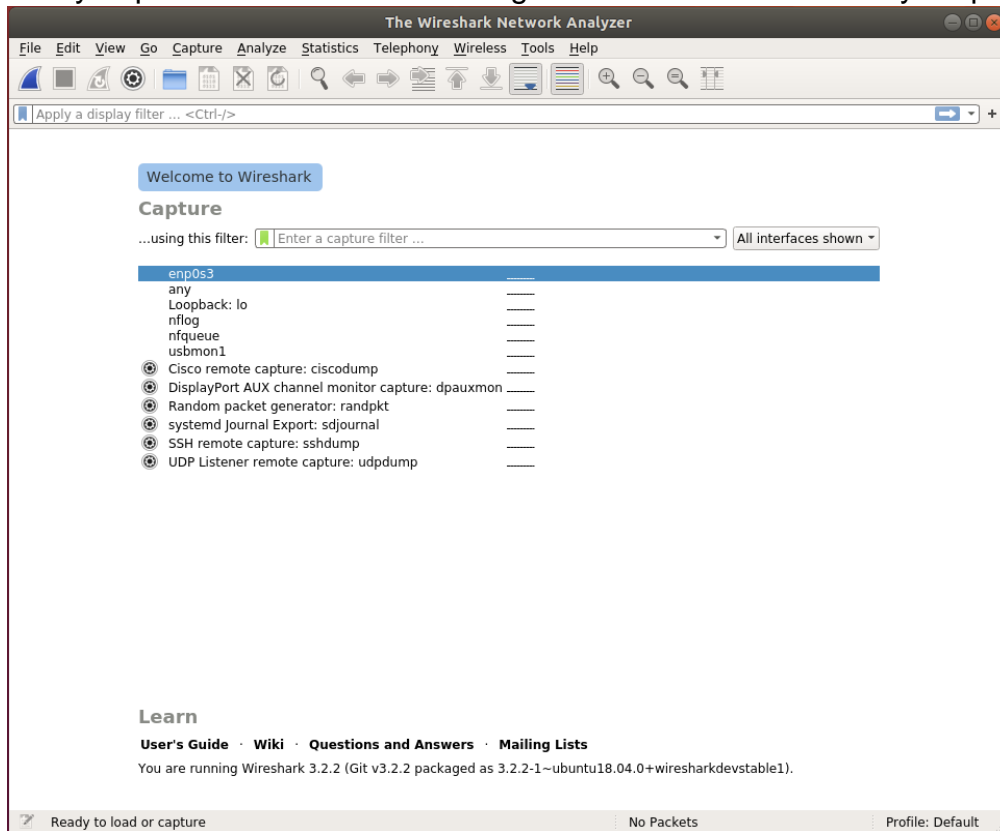
4 - VSL decoding configurations of output file



5 - VSL decoding results

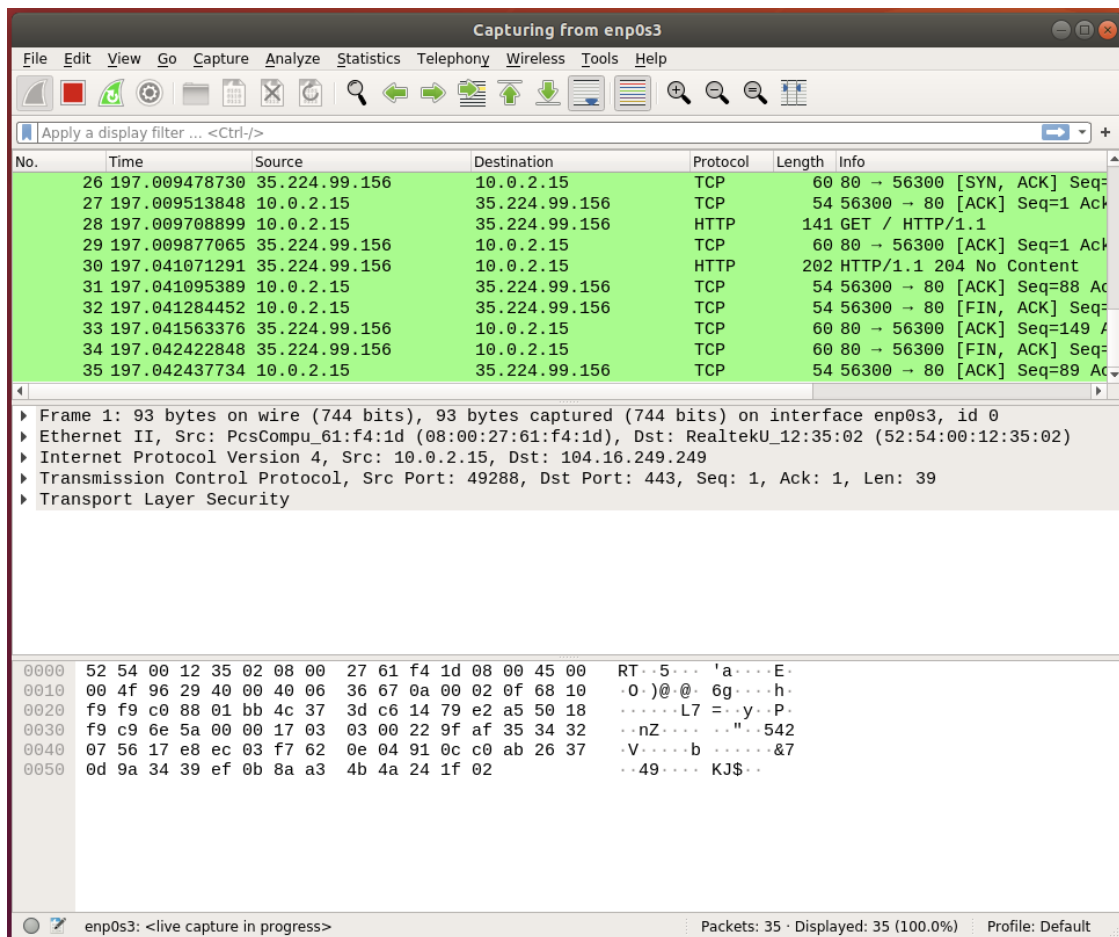
2. In this exercise you will experiment with an open source packet analyzer Wireshark (formerly known as Ethernet). Download/install Wireshark and look for a tutorial online. When you are done with the tutorial, experiment with Wireshark and show how someone with malicious intent could use it to obtain useful

information. What useful information could they obtain using Wireshark? Is there a way to prevent this? Include enough screenshots to illustrate your points. (10/8)

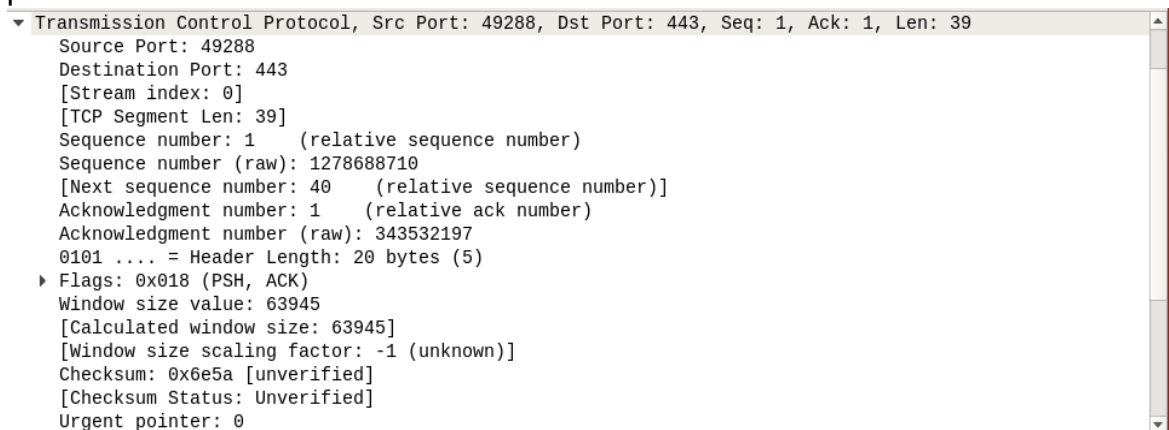


Wireshark uses WinPCAP as an interface to directly exchange data packets with the network card. Users can choose the interface to capture network packets. Depending on the interface on your system, this screen may be different from yours.

We chose enp0s3 to capture the network traffic of this interface. After selecting the interface, the network packets of all devices on our network begin to fill (refer to the screenshot below):



Malicious attackers can use Wireshark to capture network traffic on the attacker's specific interface. The captured data includes TCP messages, HTTP messages, DNS messages, etc. And the attacker can also analyze these data to obtain the specific content of each message. For example, the TCP protocol shown in the following figure, we can get the source port number, destination port number, sequence number, confirmation number, header length and so on of the TCP packet.



By default, the permission of `tcpdump` is `root: root`, ordinary users running Wireshark can not call `tcpdump`, which will lead to unable to capture packets. In

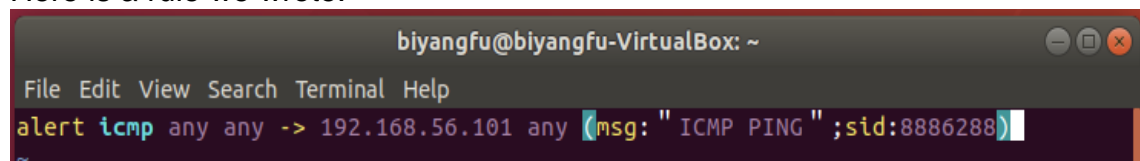
order to allow ordinary users to use Wireshark, the attacker needs to add the current user and tcpdump to the Wireshark user group. Therefore, users need to protect their own passwords, and often check whether other strange users are added to the Wireshark group.

3. In this exercise you will experiment with Snort for Linux, an open source network intrusion detection system. You can search for an online tutorial on how to use it. Download/install it. Describe how this NIDS works. How is intrusion detected? What can you do if intrusion is detected? Include some screenshots to illustrate your narrative. (10/10)

The Snort workflow is divided into the following four main parts:

1. Packet capture / decoding engine: First, use libpcap to capture data packets on the network from the network card, and then the data packets are filled into the link layer protocol packet structure through the decoding engine to decode high-level protocols, such as TCP and UDP ports.
2. Pre-processor plug-in: Next, the data packets are sent to various pre-processors for inspection and operation before being processed by the detection engine. Each preprocessor checks whether the packet should pay attention, alert or modify something.
3. Rule analysis and detection engine: Then, the packet is sent to the detection engine. The detection engine performs a single and simple detection of the characteristics and package information of each package through different options in various rule files. The detection engine plug-in provides additional detection functions for packages. Each keyword option in the rule corresponds to a detection engine plug-in, which can provide different detection functions.
4. Output plug-in: Snort outputs alarm through detection engine, pre-processor and decoding engine.

Here is a rule we wrote:

A screenshot of a terminal window titled 'biyangfu@biyangfu-VirtualBox: ~'. The terminal shows a menu bar with 'File Edit View Search Terminal Help'. Below the menu bar, a Snort rule is displayed: 'alert icmp any any -> 192.168.56.101 any (msg: "ICMP PING ";sid:8886288)'. The rule is color-coded: 'alert' is red, 'icmp' is blue, 'any' is green, 'any' is green, '->' is red, '192.168.56.101' is green, 'any' is green, '(' is blue, 'msg: "ICMP PING "' is red, ';' is blue, 'sid:8886288)' is red. The cursor is at the end of the rule.

```
biyangfu@biyangfu-VirtualBox: ~  
File Edit View Search Terminal Help  
alert icmp any any -> 192.168.56.101 any (msg: "ICMP PING ";sid:8886288)
```

We can use snort to listen to packets matching this rule and issue an alert.


```

-----
pcap DAQ configured to passive.
Commencing packet processing
++ [0] enp0s3
04/14-00:54:26.766481 [**] [1:8886288:0] "ICMP PING" [**] [Priority: 0] [AppID
: ICMP] {ICMP} 10.0.2.15 -> 192.168.56.101
04/14-00:54:27.789002 [**] [1:8886288:0] "ICMP PING" [**] [Priority: 0] [AppID
: ICMP] {ICMP} 10.0.2.15 -> 192.168.56.101
04/14-00:54:28.812263 [**] [1:8886288:0] "ICMP PING" [**] [Priority: 0] [AppID
: ICMP] {ICMP} 10.0.2.15 -> 192.168.56.101
04/14-00:54:29.836234 [**] [1:8886288:0] "ICMP PING" [**] [Priority: 0] [AppID
: ICMP] {ICMP} 10.0.2.15 -> 192.168.56.101
04/14-00:54:30.860227 [**] [1:8886288:0] "ICMP PING" [**] [Priority: 0] [AppID
: ICMP] {ICMP} 10.0.2.15 -> 192.168.56.101
04/14-00:54:31.884297 [**] [1:8886288:0] "ICMP PING" [**] [Priority: 0] [AppID
: ICMP] {ICMP} 10.0.2.15 -> 192.168.56.101


```

Users can let snort listen to the network by writing specific intrusion rules. Once snort captures intrusion packets that match the rule, it will issue a warning and write it to the log.

We can use snort in combination with other firewall software, such as PfSense, to prevent intrusion. When snort detects an intrusion, it will send an alarm to inform the firewall, and then the firewall will take the corresponding fire prevention strategy to prevent the intrusion.

4. Investigate three different websites of your choice in terms of their authentication requirements: what is the length of the passwords that they require? What are password rules on that site? Are reused passwords allowed? Do they use account lockout? For how long? How often do users have to change these passwords? If a user forgot the password, what is the password reset procedure? Does the website use CAPTCHA? Answer all of these questions. As a conclusion to this exercise, please state which of the three websites has the strongest password security, and explain why it is so. (10/8)

Authentication Requirements	Clemson canvas	www.amazon.com	www.bankofamerica.com
(1). Length of the passwords.	≥ 4 characters.	≥ 6 characters.	8 - 20 characters.
(2). Password rules.	Not mentioned. But provides 'CCIT Strong Password Guidelines'.	Not mentioned. But provides 'Choose a Strong Password' guidelines.	<ul style="list-style-type: none"> Contain 8 to 20 characters. Have at least 1 uppercase letter, 1 lowercase letter, and 1 number. Not repeat the same number or letter more than 3 times in a row. Not include spaces, and contain only the following special characters: @ # * () + = { } / ? ~ ; , . - _
(3). Allow reused passwords or not.	Not mentioned.	Yes.	No. Passcode must be different from the previous 5 Passcodes.

(4). Account lockout or not. If so, how long.	Yes. Wait 15 minutes for automatically lockout clear, or call (864)656-3494 to get your lockout cleared immediately.	Yes. Contact a locksmith for assistance.	Yes. Couple minutes
(5). Passwords expiration.	From admission to one year after graduation.	Not mentioned.	Not mentioned.
(6). Password reset procedure.	<ul style="list-style-type: none"> Employee Username passwords are reset by Computer Resources, Student passwords are reset by the Help Desk. Verification of some personal information will need to be provided in order to complete this request. 	<ul style="list-style-type: none"> Tap Forgot Password link on the login screen. Follow the on-screen instructions. 	<ul style="list-style-type: none"> Tap Forgot Password link on the login screen. Follow the on-screen instructions.
(7). Use CAPTCHA or not.	Yes. Duo Mobile app.	Yes. Copy the text from a picture in a text entry box	No.
(8). Strongest password security.			 <p>The strongest password security based on the maximum limit compared to another two websites.</p>

5. System administrators are often tasked with selecting and even installing the proper video surveillance system for the organization. Please do an online research and find three candidate video security systems. The cost of the system should be no more than \$1200 USD. The motion activated system should have recording capabilities, night vision, and other useful features. It should be accessible for monitoring over the internet. Ease of installation should also be considered. Justify why you are recommending your selected systems. Which one is the best of the three? (10/8).

(1) Three candidate video security systems & their justification.

a). ADT - Authorized Premier Provider:

- Competitive 6-month money-back guarantee

- 24/7 service and monitoring come standard
- Real-time video surveillance from any device
- Over 150 security system installation service centers
- Homeowners Insurance Certificate

b). Vivint

- Professional installation + \$0 activation
- Free 4.5-star smart home app
- 24/7 continuous video recording

c). Protect America

- 24/7 Professionally monitored security by 5x redundant monitoring stations nationwide
- Trusted emergency response in seconds.
- Security systems built around your needs.
- A quick, simple DIY setup means no costly installation fees or strangers in your home.
- Complete remote system control via iOS and Android smartphone app.

(2) For us, the best video surveillance system among three of the above is ADT, because of its security certificate, nice installation service and price advantage.

Graduate Students:

6. Investigate two other IDS for Linux. What are they, and what is the cost of such system, if any. Do they work the same as Snort? (8)

OSSEC:

OSSEC is a host-based and application-based intrusion detection system that monitors important enterprise servers and various applications to avoid corporate resources from being attacked and misused. OSSEC is an open source intrusion detection system, owned and maintained by OSSEC Foundation. Unlike Snort based on rule base search and matching, OSSEC manages and configures the connection of Manager, the organization of Agents, the creation of policies, etc. through the Administrator. The OSSEC Agent is installed in a server or workstation to monitor all behaviors in the system. When an attack is discovered, perform corresponding actions such as notifying the user, sending an email, notifying the administrator, terminating the session, shutting down the machine, etc.

Suricata:

Suricata is an open source network intrusion detection and prevention engine developed by the Open Information Security Foundation (OISF) and the providers it supports. The engine is multi-threaded, with built-in IPv6 support, can load preset rules, and supports Barnyard and Barnyard2 tools. Like Snort, Suricata is also based on rule sets, but the supported rules are not completely consistent. Both Snort and Suricata have the ability to detect attacks based on rule signatures. However, Snort detects based on rules and thresholds to track when the rule is triggered, and Suricata introduces session variables (for example, through flowint) to create counters. Then, manual rules can use these variables to trigger events.