

# پروژه درس امنیت

بسته ی سوم

یاسمین مدنی - پریسا ظفری



## سوال اول - یافتن وب سرور



```
1 # find web server
2 import requests
3
4 def web_server(url):
5     response = requests.get(url)
6     if response.status_code == 200:
7         print('Success!')
8         print(response.headers['server'])
9     elif response.status_code == 404:
10         print('Not Found.')
11
```



```
1 web_server('https://www.coursera.org/')

```



Success!  
envoy



```
1 web_server('https://github.com/')

```

Success!  
GitHub.com



## سوال اول-یافتن لوکیشن

```
[ ] 1 import json
    2 import urllib.request
    3
    4 def location(url):
    5     GEO_IP_API_URL = 'http://ip-api.com/json/'
    6
    7     IP_TO_SEARCH = url
    8
    9     # Creating request object to GeoLocation API
   10     req = urllib.request.Request(GEO_IP_API_URL+IP_TO_SEARCH)
   11
   12     # Getting in response JSON
   13     response = urllib.request.urlopen(req).read()
   14
   15     # Loading JSON from text to object
   16     json_response = json.loads(response)
   17
   18     print(json_response['country']+"/"+json_response['city'])
   19
```



1 location('coursera.org')



United States/Washington



1 location('github.com')

United States/San Francisco



## سوال اول - پیدا کردن پورت های باز

```
9
10 def port_scan(port):
11     """
12     Scan a port on the global variable `host`
13     """
14     try:
15         s = socket.socket()
16         s.connect((host, port))
17     except:
18         with print_lock:
19             print(f"{host:15}:{port:5} is closed ", end='\r')
20     else:
21         with print_lock:
22             print(f"{host:15}:{port:5} is open ")
23     finally:
24         s.close()
```

```
1 if __name__ == "__main__":
2     host = 'coursera.org'
3     start_port = 1
4     end_port = 800
5     ports = [ p for p in range(start_port, end_port)]
6
7     main(host, ports)
```

```
➡ coursera.org : 80 is open
   coursera.org : 443 is open
```



## سوال اول - یافتن ایمیل های سایت

```
[ ] 27
28     # extract base url to resolve relative links
29     parts = urlsplit(url)
30     base_url = "{0.scheme}://{0.netloc}".format(parts)
31     path = url[url.rfind('/')+1] if '/' in parts.path else url
32
33     # get url's content
34     print("Crawling URL %s" % url)
35     try:
36         response = requests.get(url)
37     except (requests.exceptions.MissingSchema, requests.exceptions.ConnectionError):
38         # ignore pages with errors and continue with next url
39         continue
40
41     # extract all email addresses and add them into the resulting set
42     new_emails = set(re.findall(r"[a-z0-9\.\-+_]+@[a-z0-9\.\-+_]+\.[a-z]+", response.text, re.I))
43     emails.update(new_emails)
44     print(emails)
45     with open('emails.txt', 'a', encoding='utf-8') as f:
46         for email in new_emails:
47             f.writelines(email + "\n")
48
49     # create a BeautifulSoup for the html document
50     soup = BeautifulSoup(response.text, 'xml')
51
52     # Once this document is parsed and processed, now find and process all the anchors i.e. linked urls in this document
53     for anchor in soup.find_all("a"):
54         # extract link url from the anchor
55         link = anchor.attrs["href"] if "href" in anchor.attrs else ''
56         # resolve relative links (starting with /)
57         if link.startswith('/'):
58             link = base_url + link
59         elif not link.startswith('http'):
60             link = path + link
61         # add the new url to the queue if it was not in unprocessed list nor in processed list yet
```

# سوال اول - نمونه خروجی موجود در فایل emails

```
emails (1).txt - Notepad
File Edit Format View Help
launch-codes-mona@1x.mp
launch-codes-mona-fallback@2x.jpg
launch-codes-mona@2x.mp
launch-codes-mona-fallback@1x.jpg
bg@2x.hevc.mov
bg@1.5x.webm
copilot-safety@github.com
bg-poster@2x.webp
bg@1.5x.hevc.mov
bg@1x.webm
bg@2x.webm
bg@1x.hevc.mov
hearts@2x.mov
laughing@2x.mov
laughing@2x.webm
sparkles-fast@2x.mov
hearts@2x.webm
mind-blown@2x.webm
mind-blown@2x.mov
sparkles-fast@2x.webm
email@example.com
Company-Cloud-Community-Product@2x.png
1200.630-Global@2x-1.png
1200.630-Productivity-wLogo@2x.png
you@example.com
startups@github.com
you@example.com
you@company.com
nick@domain.com
```



## سوال دوم-بخش اول

! Your evaluation period ends in 30 days. 1. Get a license key

### Virtual Network Editor

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Auto-bridging	-	-	-
VMnet1	Host-only	-	Connected	Enabled	192.168.71.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.48.0

VMnet Information

☒ Bridged (connect VMs directly to the external network)

Bridged to: Automatic Automatic Settings...

☐ NAT (shared host's IP address with VMs) NAT Settings...

☐ Host-only (connect VMs internally in a private network)

☐ Connect a host virtual adapter to this network  
Host virtual adapter name: VMware Network Adapter VMnet0

☐ Use local DHCP service to distribute IP address to VMs DHCP Settings...

Subnet IP: Subnet mask:

Restore Defaults Import... Export... OK Cancel Apply Help

### Virtual Network Editor

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Auto-bridging	-	-	-
VMnet1	Host-only	-	Connected	Enabled	192.168.71.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.48.0
LAN	Host-only	-	Connected	-	10.0.0.0

Add Network... Remove Network Rename Network...

VMnet Information

☐ Bridged (connect VMs directly to the external network)

Bridged to: Automatic Automatic Settings...

☐ NAT (shared host's IP address with VMs) NAT Settings...

☒ Host-only (connect VMs internally in a private network)

☒ Connect a host virtual adapter to this network  
Host virtual adapter name: VMware Network Adapter VMnet11

☐ Use local DHCP service to distribute IP address to VMs DHCP Settings...

Subnet IP: 10 . 0 . 0 . 0 Subnet mask: 255 . 255 . 255 . 0


Restore Defaults Import... Export... OK Cancel Apply Help



## سوال دوم-بخش اول

- [Download pfSense Community Edition](#)
- **NETGATE 4100 BASE PFSENSE+ SECURITY GATEWAY**

Buy Cloud | Buy Appliance | Support | Blog



Get Started | Cloud | Products | Services | Support | Training | Community | Download

Latest Stable version (Community Edition)

This is the most recent stable release, and the recommended version for all installations. Refer to the documentation for [Upgrade Guides](#) and [Installation Guides](#). For pre-configured systems, see the [pfSense® firewall appliances from Netgate](#).

RELEASE NOTES

SOURCE CODE

Select Image To Download

Version: 2.7.0

Architecture: 


Select

 ⓘ

Mirror: 

Austin, TX USA

DOWNLOAD

Supported by 

SHA256 Checksums for compressed (.gz) files

Subscribe To The Netgate Newsletter

Product information, pfSense software announcements, and special offers. See our [newsletter archive](#) for past announcements.

Email\*

Email Address

☐ I understand I am signing up to receive the newsletter, software announcements, and special offers from Netgate.\*

I'm interested in...

☐ pfSense Plus Appliances

☐ pfSense Plus on AWS

☐ pfSense Plus on Azure

☐ TNSR Appliances

☐ TNSR on AWS

☐ TNSR on Azure

☐ Network Security News & Updates

Subscribe



# سوال دوم-بخش اول

## HARDWARE SPECIFICATIONS:

CPU	Intel® Atom® C3338R with QAT, 2-core @ 1.8 GHz (Denverton family)
CPU Cores	Dual Core
Physical Network I/O ports	(2) Auto media detect 1 Gbps (RJ45 copper / SFP fiber) Combo WAN ports (4) 2.5 Gbps RJ-45 "direct" (unswitched) ethernet LAN ports
Storage	16 GB eMMC (onboard - soldered) upgradable to 128 GB NVMe M.2 SSD with <a href="#">4100 Max</a>
Memory	4 GB DDR4 w/o ECC, single channel



## سوال دوم-بخش اول

The image displays three sequential screenshots of the VMware Workstation Pro 17 'New Virtual Machine Wizard' dialog box.

**First Screenshot: Welcome to the New Virtual Machine Wizard**  
The window title is 'New Virtual Machine Wizard'. It features the VMware Workstation Pro 17 logo. The text reads: 'Welcome to the New Virtual Machine Wizard'. Below this, it asks 'What type of configuration do you want?'. There are two radio button options: 'Typical (recommended)' (selected) and 'Custom (advanced)'. The 'Typical' option description is 'Create a Workstation 17.x virtual machine in a few easy steps.' The 'Custom' option description is 'Create a virtual machine with advanced options, such as a SCSI controller type, virtual disk type and compatibility with older VMware products.' At the bottom are buttons for 'Help', '< Back', 'Next >', and 'Cancel'.

**Second Screenshot: Guest Operating System Installation**  
The window title is 'New Virtual Machine Wizard'. The section is 'Guest Operating System Installation'. It states: 'A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?'. Under 'Install from:', there are two radio button options: 'Installer disc:' (selected) and 'Installer disc image file (iso):'. The 'Installer disc:' option has a dropdown menu showing 'DVD RW Drive (E:)' and a 'Browse...' button. The 'Installer disc image file (iso):' option has an empty text field and a 'Browse...' button. At the bottom, there is a radio button option 'I will install the operating system later.' with the text 'The virtual machine will be created with a blank hard disk.' below it. At the bottom are buttons for 'Help', '< Back', 'Next >', and 'Cancel'.

**Third Screenshot: Select a Guest Operating System**  
The window title is 'New Virtual Machine Wizard'. The section is 'Select a Guest Operating System'. It asks: 'Which operating system will be installed on this virtual machine?'. Under 'Guest operating system', there are four radio button options: 'Microsoft Windows', 'Linux', 'VMware ESX', and 'Other' (selected). Under 'Version', there is a dropdown menu showing 'FreeBSD 11 64-bit'. At the bottom are buttons for 'Help', '< Back', 'Next >', and 'Cancel'.

## سوال دوم-بخش اول

**WORKSTATION PRO**

New Virtual Machine Wizard

**Specify Disk Capacity**

How large do you want this disk to be?

The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

Maximum disk size (GB):

Recommended size for FreeBSD 11 64-bit: 20 GB

☐ Store virtual disk as a single file

☒ Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

Virtual Machine Settings

Virtual Machine Settings

Hardware Options

Device	Summary
Memory	4 GB
Processors	2
Hard Disk (SCSI)	128 GB
CD/DVD (IDE)	Using file C:\Users\Asus\Down...
Network Adapter	NAT
USB Controller	Present
Display	Auto detect

**Device status**

☐ Connected

☒ Connect at power on

**Network connection**

☐ Bridged: Connected directly to the physical network

☐ Replicate physical network connection state

☐ NAT: Used to share the host's IP address

☐ Host-only: A private network shared with the host

☒ Custom: Specific virtual network

LAN (Host-only)

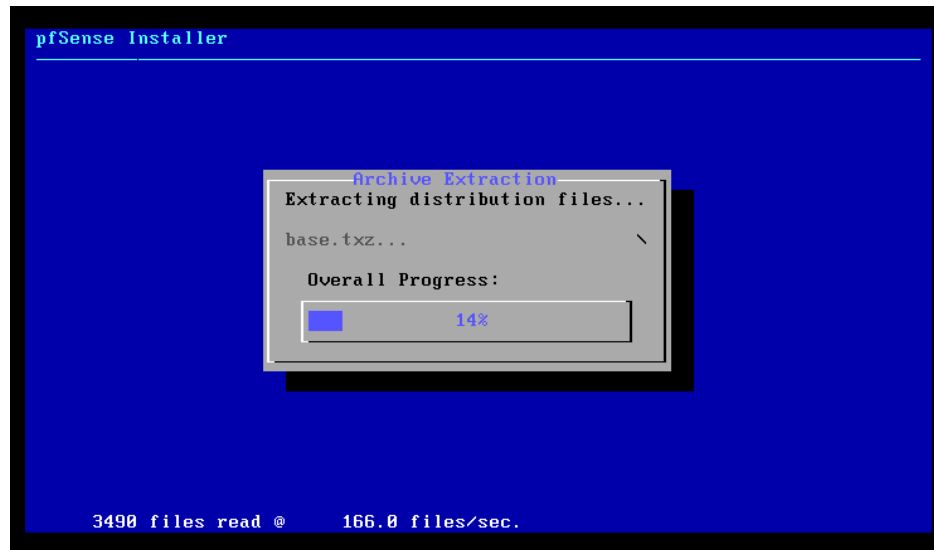
☐ LAN segment:

**Devices**

Memory	4 GB
Processors	2
Hard Disk (SCSI)	128 GB
CD/DVD (IDE)	Using file C:\Users...
Network Adapter	Custom (LAN)
USB Controller	Present
Display	Auto detect



## سوال دوم-بخش اول





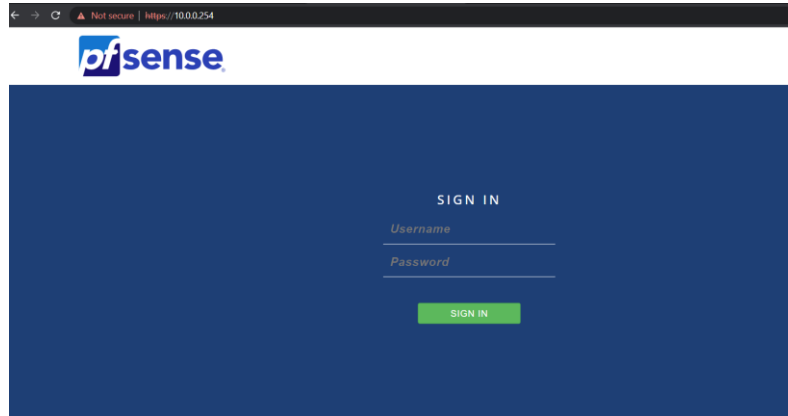
## سوال دوم-بخش اول

```
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***
```

```
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.233.133/24
LAN (lan)      -> em1      -> v4: 10.0.0.254/24
```

- |                                   |                                  |
|-----------------------------------|----------------------------------|
| 0) Logout (SSH only)              | 9) pfTop                         |
| 1) Assign Interfaces              | 10) Filter Logs                  |
| 2) Set interface(s) IP address    | 11) Restart webConfigurator      |
| 3) Reset webConfigurator password | 12) PHP shell + pfSense tools    |
| 4) Reset to factory defaults      | 13) Update from console          |
| 5) Reboot system                  | 14) Enable Secure Shell (sshd)   |
| 6) Halt system                    | 15) Restore recent configuration |
| 7) Ping host                      | 16) Restart PHP-FPM              |
| 8) Shell                          |                                  |

```
Enter an option:
```



# سوال دوم-بخش اول

Wizard / pfSense Setup / General Information

?

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname

pfSense

EXAMPLE: myserver

Domain

home.arpa

EXAMPLE: mydomain.com

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

Primary DNS Server

8.8.8.8

Secondary DNS Server

8.8.4.4

Override DNS

☒

Allow DNS servers to be overridden by DHCP/PPP on WAN

>> Next



## سوال دوم-بخش اول

**pfSense** COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Diagnostics / Ping ?

**Ping**


**Hostname**

**IP Protocol**

**Source address**   
Select source address for the ping.

**Maximum number of pings**   
Select the maximum number of pings.

**Seconds between pings**   
Select the number of seconds to wait between pings.

 Ping

**Results**

```
PING www.google.com (216.239.38.120) from 10.0.0.254: 56 data bytes
64 bytes from 216.239.38.120: icmp_seq=0 ttl=111 time=56.660 ms
64 bytes from 216.239.38.120: icmp_seq=1 ttl=111 time=59.131 ms
64 bytes from 216.239.38.120: icmp_seq=2 ttl=111 time=56.424 ms

--- www.google.com ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 56.424/57.405/59.131/1.224 ms
```

## سوال دوم-بخش اول

linux mint 17.1

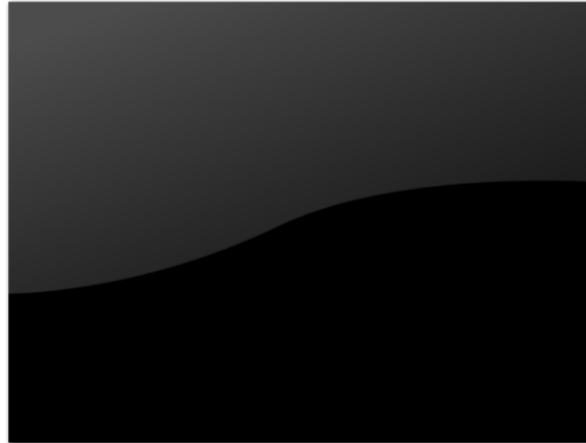
[Power on this virtual machine](#)  
[Edit virtual machine settings](#)

▼ **Devices**

Memory	4 GB
Processors	2
Hard Disk (SCSI)	40 GB
CD/DVD (SATA)	Using file C:\Use...
Network Adapter	Custom (LAN)
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

▼ **Description**

Type here to enter a description of this virtual machine.







## سوال دوم-بخش اول

- [DNS Lookup - WhatIsMyIP.com®](#)

What Is My IP? IP Address Lookup IP WHOIS Lookup DNS Lookup Internet Speed Test Tools

Find the IP Address of any Domain Name

<https://www.aparat.com/>

Lookup

IPv4 Address for <https://www.aparat.com/>

Domain Server IP: [185.147.178.13](#)

Domain Server IP: [185.147.178.11](#)

Domain Server IP: [185.147.178.12](#)

Domain Server IP: [185.147.178.14](#)

Firewall / Aliases / Edit



### Properties

Name

Aparat

The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and \_".

Description

A description may be entered here for administrative reference (not parsed).

Type

Host(s)

### Host(s)

Hint

Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.

IP or FQDN

185.147.178.11

Description

Delete

185.147.178.14

Description

Delete

185.147.178.13

Description

Delete

185.147.178.12

Description

Delete

Save

+ Add Host



## سوال دوم-بخش اول

Firewall / Rules / LAN

Floating WAN **LAN**

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	3 / 1.36 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0 / 3 KiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Add Delete Save Separator

Firewall / Rules / LAN

Floating WAN **LAN**

The changes have been applied successfully. The firewall rules are now reloading in the background. [Monitor](#) the filter reload progress.

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0 / 3.37 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0 / 0 B	IPv4 *	*	*	Aparat	*	*	none			
<input type="checkbox"/>	0 / 1 KiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Add Delete Save Separator



## سوال دوم-بخش اول

```
PING www.aparat.com (185.147.178.14) 56(84) bytes of data.  
^C  
--- www.aparat.com ping statistics ---  
24 packets transmitted, 0 received, 100% packet loss, time 23025ms
```



### Results

```
PING www.aparat.com (185.147.178.12) from 10.0.0.254: 56 data bytes
```

```
--- www.aparat.com ping statistics ---
```

```
3 packets transmitted, 0 packets received, 100.0% packet loss
```



## سوال دوم-بخش دوم

System / Package Manager / Package Installer

pfSense-pkg-suricata installation successfully completed.

Installed Packages

Available Packages

Package Installer

### Package Installation

RULES: Suricata IDS/IPS Engine comes without rules by default. You should add rules by yourself and set an updating strategy. To do so, please visit:

<http://www.openinfosecfoundation.org/documentation/rules.html>

<http://www.openinfosecfoundation.org/documentation/emerging-threats.html>

You may want to try BPF in zerocopy mode to test performance improvements:

```
sysctl -w net.bpf.zerocopy_enable=1
```

Don't forget to add net.bpf.zerocopy\_enable=1 to /etc/sysctl.conf

```
>>> Cleaning up cache... done.
```

```
Success
```



## سوال دوم-بخش دوم

### General Settings

**Enable** ☒ Checking this box enables Suricata inspection on the interface.

**Interface**

Choose which interface this Suricata instance applies to. In most cases, you will want to choose LAN here if this is the first Suricata-configured interface.

**Description**

Enter a meaningful description here for your reference. The default is the pfsense interface friendly description.

### Alert and Block Settings

#### Block Offenders

☒ Checking this option will automatically block hosts that generate a Suricata alert.

#### IPS Mode

Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Suricata inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.

Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Suricata can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers: bnxt, cc, cxgbe, cxl, em, ena, ice, igb, igc, ix, ixgbe, ixl, lem, re, vmx, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.

#### Kill States

☒ Checking this option will kill firewall states for the blocked IP. Default is Checked.

#### Which IP to Block

Select which IP extracted from the packet you wish to block. Choosing BOTH is suggested, and it is the default value.



## سوال دوم-بخش دوم

Services / Suricata / Global Settings ?

Interfaces Global Settings Updates Alerts Blocks Files Pass Lists Suppress Logs View

Logs Mgmt SID Mgmt Sync IP Lists

Please Choose The Type Of Rules You Wish To Download

Install ETOpen Emerging Threats rules

☒ ETOpen is a free open source set of Suricata rules whose coverage is more limited than ETPro.

☐ Use a custom URL for ETOpen downloads

Enabling the custom URL option will force the use of a custom user-supplied URL when downloading ETOpen rules.



## سوال دوم-بخش دوم

Services / Suricata / Updates





Interfaces   Global Settings   Updates   Alerts   Blocks   Files   Pass Lists   Suppress   Logs View

Logs Mgmt   SID Mgmt   Sync   IP Lists


## سوال دوم-بخش دوم

### Select the rulesets (Categories) Suricata will load at startup

-  - Category is auto-enabled by SID Mgmt conf files
-  - Category is auto-disabled by SID Mgmt conf files

Select All

Unselect All

 Save

Enabled

Ruleset:

Enabled

Ruleset: ET Open Rules

Snort Rules are not enabled.



emerging-dos.rules



## سوال دوم-بخش سوم

**Firewall Maximum Table  
Entries**

Maximum number of table entries for systems such as aliases, sshguard, snort, etc, combined.

Note: Leave this blank for the default. On this system the default size is: 400000



## سوال دوم-بخش سوم

**General Settings**

[Links](#) [Firewall Aliases](#) [Firewall Rules](#) [Firewall Logs](#)

**pfBlockerNG** ☒ Enable

**Note:** Context help is available on various pages by clicking the 'blue infoblock' icons: [→](#)

**Keep Settings** ☒ Enable

**Note:** With 'Keep settings' enabled, pfBlockerNG will maintain run state on Installation/Upgrade.  
If 'Keep Settings' is not 'enabled' on pkg Install/De-Install, all settings will be Wiped!

**Note:** To clear all downloaded lists, uncheck these two checkboxes and 'Save'. Re-check both boxes and run a 'Force Update|Reload'

**CRON Settings**

<input type="text" value="Every hour"/>	<input type="text" value="15"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Default: <b>Every hour</b> Select the Cron hour interval.	Default: <b>:00</b> Select the Cron update minute.	Default: <b>0</b> Select the Cron start hour.	Default: <b>0</b> Select the 'Daily/Weekly' start hour.



## سوال دوم-بخش سوم

IP Configuration	
Links	<a href="#">Firewall Aliases</a> <a href="#">Firewall Rules</a> <a href="#">Firewall Logs</a>
De-Duplication	<input checked="" type="checkbox"/> Enable Only used for IPv4 Deny Lists
CIDR Aggregation	<input checked="" type="checkbox"/> Enable Optimise CIDRs - merge contiguous CIDRs into larger CIDR blocks.
Suppression	<input checked="" type="checkbox"/> Enable Default enabled. This will prevent Selected IPs (and RFC1918/Loopback addresses) from being blocked. Only for IPv4 lists (/32 and /24). <a href="#">i</a>
Force Global IP Logging	<input type="checkbox"/> Enable The global logging option is only used to force logging for all IP Aliases, and not to disable the logging of all IP Aliases. This overrides any logging settings in the GeoIP/IPv4/v6 tabs.
Placeholder IP Address	<input type="text" value="127.1.7.7"/> Enter a single IPv4 placeholder address For IPv6 "::" will be prefixed to the placeholder IP. This address should be in an Isolated Range that is not used in your Network. This IP address will be used as a placeholder IP to avoid empty Feeds/Aliases.
ASN Reporting	<input type="text" value="Enabled - ASN entries cached for 1 hour"/> <a href="#">v</a> Query for the ASN (BGPIview.io API) for each block/reject/permit/match IP entry. ASN values are cached as per the defined selection.



## سوال دوم-بخش سوم



Category	Alias/Group	Description
IPv4	PRI1 > PRI6	Known Ransomware, malware, botnets, Command & Control (C&C) servers, bots, web scripts, phishing & compromised servers, malicious IP's found attacking SSH, SMTP, IMAP, TELNET, FTP end points and other known originators of malicious behaviour.
IPv4	Mail	Known sources of spam; useful for protecting mail servers
IPv4	Tor	Known Tor exit points; not inherently dangerous but you may want to isolate users anonymising their traffic.
IPv4	Internic	Contains root name servers needed to initialize the cache of Internet domain name servers

General
IP
DNSBL
Update
Reports
Feeds
Logs
Sync

Feed Settings

Pre-defined Alias/Group/Feeds

Links:
Firewall Aliases
Firewall Rules
Firewall Logs

The **Feeds Management** page is a collection of pre-defined Feeds arranged into Aliasnames/Groups. Review the **infoblock icons** beside each Alias/Group name for details about each Group.

**Number of Feeds per Category Type:**

IPv4:	91
IPv6:	15
DNSBL:	137

- Feeds are listed by Category (IPv4/IPv6/DNSBL). Links are provided for each Feed website and Feed URL.
- Clicking the "+" icon(s) in the Category column will import all Feeds in the Alias/Group at once, while clicking the "+" icon(s) on the right will only import the individual feed.
- Feeds with 'Alternative' URL(s) can be configured via the Radio button options.
- Unknown user-defined Feeds are listed in a table below pre-defined Feeds
- Permit Type feeds are listed with a green background.

Click here for Legend → ⓘ

**Disclaimer:** Use of the Feed(s) below are at your own risk! Note: Do not enable all Feeds at once.

Category	Alias/Group	Feed/Website	Header/URL
IPv4 Category ⓘ +	PRI1	Abuse Feodo Tracker	Abuse_Feodo_C2 +
IPv4	PRI1	➤ Abuse Feodo Tracker ⓘ	○ Abuse_Feodo_C2_med
IPv4	PRI1	➤ Abuse Feodo Tracker ⓘ	○ Abuse_Feodo_C2_Agr

# سوال دوم-بخش سوم

https://pulsedive.com/

## IPv4 Source Definitions

Auto	ON	https://feedotracker.abuse.ch/downloads/ipblocklist_recommended.tx	Abuse_Feodo_C2	Delete
Auto	ON	https://sbl.abuse.ch/blacklist/sblipblacklist.txt	Abuse_SSLBL	Delete
Auto	ON	https://cinsarmy.com/list/ci-badguys.txt	CINS_army	Delete
Auto	ON	https://rules.emergingthreats.net/rwrules/emerging-Block-IPs.txt	ET_Block	Delete
Auto	ON	https://rules.emergingthreats.net/blockrules/compromised-ips.txt	ET_Comp	Delete
Auto	ON	https://isc.sans.edu/block.txt	ISC_Block	Delete
Auto	ON	https://pulsedive.com/premium?key=49ec27415f85bf276ce8edac6c1c	Pulsedive	Delete
Auto	ON	https://www.spamhaus.org/drop/drop.txt	Spamhaus_Drop	Delete
Auto	ON	https://www.spamhaus.org/drop/edrop.txt	Spamhaus_eDrop	Delete
Auto	ON	https://talosintelligence.com/documents/ip-blacklist	Talos_BL	Delete
Format	State	Source	Header/Label	

Click here for Guidelines → ⓘ



## سوال دوم-بخش سوم

pfB\_PRI1\_v4

**Edit Firewall Rule**

**Action** Block

Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled** ☐ Disable this rule

Set this option to disable this rule without removing it from the list.

**Interface** LAN

Choose the interface from which packets must come to match this rule.

**Address Family** IPv4

Select the Internet Protocol version this rule applies to.

**Protocol** TCP/UDP

Choose which IP protocol this rule should match.

**Destination**

**Destination** ☐ Invert match any Destination Address /

**Destination Port Range** (other)  (other)

From Custom To Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

**Extra Options**

**Log** ☒ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

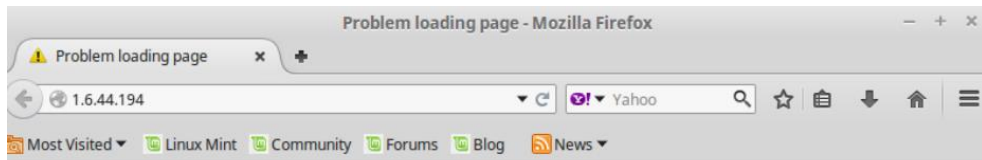
**Description** LAN Block PRI1

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

**Advanced Options** ⚙ Display Advanced

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	3 /10.03 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Logout Rule	
<input type="checkbox"/>	0 /0 B	IPv4 TCP/UDP	pFB_PRI1_v4	*	*	*	*	none		LAN Block PRI1	
<input type="checkbox"/>	0 /0 B	IPv4 *	*	*	Aparat	*	*	none		Block Aparat.com	
<input type="checkbox"/>	0 /36 KGB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add
 Add
 Delete
 Save
 Separator



## The connection was reset

The connection to the server was reset while the page was loading.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

Try Again



سوال دوم-بخش سوم



## سوال سوم:

### تکنیک دامنه فضایی (Spatial Domain Technique) :

تکنیک‌های استگانوگرافی حوزه فضایی، که به عنوان تکنیک‌های جایگزینی نیز شناخته می‌شوند، گروهی از تکنیک‌های نسبتاً ساده هستند که کانالی پنهان در قسمت‌های تصویر جلد ایجاد می‌کنند که در آن تغییرات در مقایسه با سیستم بینایی انسان (HVS) کمی ناچیز است.

یکی از راه‌های انجام این کار مخفی کردن اطلاعات در کمترین بیت (LSB) داده‌های تصویر است. عملیات جاسازی استگانوگرافی LSB با معادله زیر توصیف می‌شود:

$$Y_i = 2 \left\lfloor \frac{x_i}{2} \right\rfloor + m_i$$

. Steghide، S-tools، Steganos، و ابزارهای دیگر با استفاده از استگانوگرافی مبتنی بر LSB در دسترس هستند.

اگر  $\{xP, (0 \leq x \leq 1)\}$  توزیع کمترین بیت‌های تصویر جلد را نشان دهد، و  $\{mP, (0 \leq m \leq 1)\}$  نشان دهنده توزیع بیت‌های پیام دودویی مخفی پیام باید قبل از جاسازی فشرده یا رمزگذاری باشد تا از محرمانه بودن آن محافظت شود.

$$\{P_m(m=0) \approx P_m(m=1) \approx 1/2\}.$$

بر این اساس، توزیع پیام ممکن است برابر با توزیع متوسط فرض شود:





پنهان کردن بیت‌های پیام در تصویر با استفاده از الگوریتم‌های LSB: ترتیبی- پراکنده

Katzenbeisser و Petitcolas تغییرات متعددی را در تکنیک‌های پایه LSB توصیف می‌کنند. آنها همچنین یک تکنیک جایگزین برای جاسازی یک پیام مخفی در بیت‌های LSB پالت فرمت تصویر GIF یا BMP با استفاده از استگانوگرافی توصیف می‌کنند.

بیلی و کوران ارزیابی تکنیک‌های مختلف مربوط به استگانوگرافی فضایی را ارائه می‌کنند و چنین تکنیک‌هایی می‌توانند اصولاً برای تصاویر GIF اعمال شوند.

معایب: 1. به دلیل کوچک بودن آنها توسط چشم انسان بسیار دشوار . 2. تکنیک استفاده از هر پیکسل در تصویر

مزیت: چنین تکنیک‌هایی ساده و محبوب هستند.



## رمزگذاری داده‌ها:

مثال: پیام مخفی hello را در نظر بگیرید: شامل 5 حرف یا 5 بایت در کل  $5 \times 3 = 15$  پیکسل برای رمزگذاری نیاز داریم عکسی که در نظر می‌گیریم باید از بیشتر از 15 پیکسل داشته باشد نمونه‌ی اعدادی که داریم:

[(27, 64, 164), (248, 244, 194), (174, 246, 250), (149, 95, 232), (188, 156, 169), (71, 167, 127), (132, 173, 97), (113, 69, 206), (255, 29, 213), (53, 153, 220), (246, 225, 229), (142, 82, 175), (188, 156, 169), (71, 167, 127), (132, 173, 97), (113, 69, 206), (188, 156, 169), (71, 167, 127)]

برای هر حرف 3 مقدار rgb در نظر گرفته شده است:

1. باید مقادیر اسکی (ASCII) ها را پیدا کنیم
2. مقدار اسکی برای حرف H برابر 72 است.
3. سه پیکسل اول که (27, 64, 164), (248, 244, 194), (174, 246, 250) هستند را برمی‌داریم
4.  $01001000 = 72$
5. اعداد اصلاح شده = (26, 63, 164), (248, 243, 194), (174, 246, 250) خواهد بود.



## رمزگشایی داده:

- برای رمزگشایی، سه پیکسل در یک زمان خوانده می‌شود، تا زمانی که آخرین مقدار فرد باشد، به این معنی که پیام تمام شده است. هر 3 پیکسل حاوی یک داده باینری است که می‌تواند با همان منطق رمزگذاری استخراج شود. اگر مقدار فرد باشد، بیت باینری 1 باشد، در غیر این صورت (زوج باشد) برابر 0 است.



1. گرفتن عکس مورد نیاز و نوشته‌ای که می‌خواهیم مخفی کنیم :

```
# get image path and text
image_path = input("Please enter the path to image: ")
text = input("Please enter the text to be encoded: ")
```

2. گرفتن آدرس عکس و بازکردنش ، چون به RGB آن نیاز داریم با توجه به توابعی که برای image نوشته شده‌است آن را تبدیل می‌کنیم.

```
image = Image.open(image_path, 'r')
imrgb = image.convert("RGB")
```

3. به دست آوردن سایز عکس (طول متن که به پیکسل تبدیل می‌شود بیشتر از طول عکس نباشد) طول متن \* 3 یا تعداد پیکسل های عکس تقسیم بر 3

```
width, height = imrgb.size
num_pixels = width * height
encoding_places_len = int(num_pixels / 3)
```

```
#cut text to fit into image if needed
```

```
if len(text) > encoding_places_len:
```

```
    print("The text length is too long to be encoded in this image. The text will be cut to fit image size.")
```

```
    text = text[0:encoding_places_len]
```

4. اگر طول متن بیشتر شده باشد من متن را تا اندازه‌ی عکس تبدیل کردم و با بقیه‌ی حروف کار نداشتم.

5. برای هر حرفی که در متن وجود دارد را به عدد اسکی تبدیل کنیم و بعد به باینری آن را در آوردم.

```
def string_to_ascii8bit(text):
```

```
    binary_text = []
```

```
    for ch in text:
```

```
        # ord returns ascii code of character (as int)
```

```
        #format with string '{0:08b}' will format int into an 8 bit binary string
```

```
        binary_text.append('{0:08b}'.format(ord(ch)))
```

```
    return binary_text
```

6. تابع ord عدد اسکی یک حرف را برمیگرداند و و برای آنکه به باینری در بیاوریم از '{0:08b}'.format(ord(ch)) استفاده کرده‌ام.

7. تصویری که به rgb تبدیل کرده‌ایم را عدد هر پیکسل را در بیاوریم .

```
# get all pixels of image in a list and start iter() in them
```

```
pixels = list(imrgb.getdata())
```

```
imageiter = iter(pixels)
```

imrgb.getdata() را طبق یک نمونه از استک اورفلو همراه با خروجی نشان می‌دهم :

```
im = Image.open("composplot.gif")
imrgb = im.convert("RGB")
print(list(imrgb.getdata()))
```

Output:

```
[(255, 255, 255), (255, 255, 255), (216, 216, 216), (8, 8, 8), (19
```

تابع iter() :

```
# list of vowels
vowels = ['a', 'e', 'i', 'o', 'u']
vowels_iter = iter(vowels)

print(next(vowels_iter))    # 'a'
print(next(vowels_iter))    # 'e'
print(next(vowels_iter))    # 'i'
print(next(vowels_iter))    # 'o'
print(next(vowels_iter))    # 'u'
```

Run Code >>

## Output

```
a
e
i
o
u
```

با این کار هر پیکسل را جدا کرده‌ایم. حال ما داده‌هایی که نیاز داشته‌ایم را دریافت و به فرمتی که نیاز داشته‌ایم، درست کرده‌ایم.



## رمزگذاری :

۱. انتخاب ۳ پیکسل:

```
for i in range(len(binary_text)):
    # get the next three pixels
    next3 = [list(imageiter.__next__()), list(imageiter.__next__()), list(imageiter.__next__())]
```

۲. درون ۸ بیت بچرخیم و پیکسل و عدد بین rgb را انتخاب کنیم :

```
for i in range(len(binary_text)):
    # get the next three pixels
    next3 = [list(imageiter.__next__()), list(imageiter.__next__()), list(imageiter.__next__())]
    for j in range(8):
        pixidx = int(j / 3) # which pixel of next3 will be encoded this time
        rgbidx = j % 3 # which of the R,G,B values of the selected pixel will be encoded this time
        next3[pixidx][rgbidx] = change_pixel_value(next3[pixidx][rgbidx], binary_text[i][j] == '0')
```

۳. حال تابع change\_pixel\_value

```
# if bin_is_even = True the value will be decremented if it wasn't even before.
# Same happens with bin_is_even = False and the value will turn odd by being decremented
def change_pixel_value(value, bin_is_even):
    if bin_is_even and value % 2 == 1:
        value -= 1 # value turns even
    elif (not bin_is_even) and value % 2 == 0:
        value -= 1 # value turns odd
    return value
```

۴. چک کنیم آیا به رقم آخر رسیده‌ایم یا خیر :

```
if i == len(binary_text) - 1: #if this was the last character of text
    next3[2][2] = change_pixel_value(next3[2][2], False) # encode 1 at lsb of last pixel's blue value (the blue value is the last in RGB)
else:
    next3[2][2] = change_pixel_value(next3[2][2], True) # encode 0 at lsb of last pixel's blue value
for j in range(3):
    encoded_pixels.append(tuple(next3[j]))
```

۵. حال باید با داده‌هایی که تغییر داده‌ایم یک تصویر بسازیم و ذخیره کنیم:

```
encoded_image = gen_encoded_image(imrgb, encoded_pixels, width)

new_img_name = input("Please enter the path for the new image: ")
encoded_image.save(new_img_name, str(new_img_name.split(".")[1].upper()))
print("Successfully encoded image!\n\n\n")
```

۶. ساختن تصویر در تابع `gen_encoded_image` انجام می‌شود :

```
def gen_encoded_image(imrgb, encoded_pixels, width):
    for i in range(len(encoded_pixels)):
        row = int(i / width)
        col = i % width
        imrgb.putpixel((col, row), encoded_pixels[i])
    return imrgb
```





## 1. تابع decode()

2. گرفتن ادرس تصویر و تبدیل به پیکسل

3. گرفتن سه پیکسل و یک باینری اسکی با توجه به زوج و فرد بودن عدد rgb ذخیره می کنیم

4. عدد بدست آمده را به مبنا 10 می بریم و عدد اصلی که نشان دهنده ی حرف مخفی شده است را بدست می آوریم

5. نکست را پرینت می کنیم.

```
def decode():
    # get image path and text
    image_path = input("Please enter the path to image: ")
    text = ""

    #open image and extract its size info
    image = Image.open(image_path, 'r')
    imrgb = image.convert("RGB")
    width, height = imrgb.size
    num_pixels = width * height
    encoding_places_len = int(num_pixels / 3)

    # get all pixels of image in a list and start iter() in them
    pixels = list(imrgb.getdata())
    imageiter = iter(pixels)
    print("Decoding...\n")
    # decoding
    text = ""
    for i in range(encoding_places_len):
        # get the next three pixels
        next3 = [list(imageiter.__next__()), list(imageiter.__next__()), list(imageiter.__next__())]
        binary_ascii = ""
        for j in range(8):
            pixidx = int(j / 3) # which pixel of next3 will be encoded this time
            rgbidx = j % 3 # which of the R,G,B values of the selected pixel with be encoded this time

            if next3[pixidx][rgbidx] % 2 == 0:
                binary_ascii += "0"
            else:
                binary_ascii += "1"
        text += chr(int(binary_ascii, base=2))
        if next3[2][2] % 2 == 1: #text is complete
            break
    print(f"The decoded text is:\n{text}\n\n")
```

6. بر اساس زوج و فرد بودن عدد اسکی را در آورد و برگرداندن عدد اسکی به حرف است که در پایین نشان داده‌ام :

```
binary_ascii = ""
for j in range(8):
    pixidx = int(j / 3) # which pixel of next3 will be encoded this time
    rgbidx = j % 3 # which of the R,G,B values of the selected pixel will be encoded this time

    if next3[pixidx][rgbidx] % 2 == 0:
        binary_ascii += "0"
    else:
        binary_ascii += "1"

text += chr(int(binary_ascii, base=2))

if next3[2][2] % 2 == 1: #text is complete
    break
```

7. در main یک اینپوت می‌گیریم که نشان می‌دهد که می‌خواهیم از رمزگذاری یا رمزگشایی استفاده کنیم و طبق عدد وارد شده تابع مورد نظر استفاده می‌شود.

```
if __name__ == '__main__':
    while True:
        a = input("## Image Steganography Project ##\nWhat do you want to do?\n1. Encode\t2. Decode\t3. Exit\n")
        if a == "1":
            encode()
        elif a == "2":
            decode()
        elif a == "3":
            break
        else:
            print("Please enter one of the options 1, 2 or 3!\n\n")
```



نمونه‌های اجرای کد  
نمونه‌ی ورودی:

```
C:\Users\Alaie\Downloads\Telegram Desktop>python image-steganography.py
## Image Steganography Project ##
What do you want to do?
1. Encode      2. Decode      3. Exit
1
Please enter the path to image: D:\univercity\Term 8\Amniat\1397043116531862014819814.jpg
Please enter the text to be encoded: Secuirity
Encoding...

Please enter the path for the new image: D:\univercity\Term 8\Amniat\image_encoded.png
Successfully encoded image!
```



عکس داده شده :



عکس انکود شده :



نمونه ورودی و خروجی:

```
## Image Steganography Project ##
What do you want to do?
1. Encode      2. Decode      3. Exit
2
Please enter the path to image: D:\univercity\Term 8\Amniat\image_encoded.png
Decoding...

The decoded text is:
Secuirity
```



نمونه ورودی و خروجی:

```
## Image Steganography Project ##  
What do you want to do?  
1. Encode      2. Decode      3. Exit  
3  
  
C:\Users\Alaie\Downloads\Telegram Desktop>^Z
```



## بخش تحقیقاتی:

استگانوگرافی:

استگانوگرافی چیست؟

به فرآیند پنهان کردن داده‌ها در تصاویر یا فایل‌های صوتی گفته می‌شود تا کسی نتواند آن را ببیند

نحوه عملکرد:

در استگانوگرافی، می‌توان متن را در یک تصویر پنهان کرد و تصویر تفاوتی نخواهد داشت همچنین می‌توانیم یک تصویر دوم نیز در داخل تصویر اول پنهان کنیم. شما هرگز نمی‌توانید تفاوت بین عکس اصلی و تصویر استگو را فقط با نگاه کردن به آن تشخیص دهید. می‌توانید برخی از داده‌ها را در عکس پنهان کنید یا می‌توانید از آن برای ارسال پیام مخفی به فرد دیگری استفاده کنید.

انواع استگانوگرافی:

استگانوگرافی متن

تصویر استگو

استگو ویدیویی

استگو صوتی

استگو شبکه



تصویر استگنوگرافی:

محبوب‌ترین فرمت‌های فایل مورد استفاده در استگنوگرافی هستند دلیل ایجاد یک رسانه تصادفی شناخته شده‌اند. یکی از تکنیک‌های استگنوگرافی تصویر از «حفره‌ها» هستند.

فایل‌های تصویری:

تصویر به عنوان چینش اعداد تعریف می‌شود که نشان دهنده شدت‌های مختلف نور در قسمت‌های مختلف تصویر هستند. توصیف عددی: هر نقطه به نام پیکسل‌ها داده می‌شود. در یک طرح رنگی، تعداد بیت‌ها به عنوان عمق بیت شناخته می‌شود کوچکترین عمق بیت در طرح رنگ 8 است، یعنی 8 بیت برای نمایش رنگ هر پیکسل استفاده می‌شود. در تصاویر تک رنگ و هم در مقیاس خاکستری معمولاً از 8 بیت برای هر پیکسل استفاده می‌کنند این بیت‌ها می‌توانند تا 256 رنگ یا سایه خاکستری مختلف را نمایش دهند.

تصاویر رنگی دیجیتال به دلیل ذخیره شدن در فایل‌های 24 بیتی و استفاده از مدل رنگی RGB شناخته شده‌اند سه عبارت رنگی اصلی: قرمز، سبز و آبی

هر یک از این رنگ‌ها با 8 بیت نشان داده می‌شوند. این ترکیب رنگ می‌تواند به 256 برسد که به بیش از 16 میلیون ترکیب می‌رسد که در نهایت منجر به بیش از 16 میلیون رنگ می‌شود.

برجسته‌ترین فرمت‌های تصویر، منحصراً در اینترنت، فرمت تبادل گرافیکی (GIF)، فرمت گروه متخصصان عکاسی مشترک (JPEG) و تا حدی فرمت گرافیک شبکه قابل حمل (PNG) است برخی از مشارکت‌های ادبی از قالب بیت مپ (BMP)





تاکسونومی تکنیک‌های استگانوگرافی:

C نشان دهنده حامل پوشش

$\sim C$  تصویر استگو

K یک کلید اختیاری را نشان دهد

M پیامی باشد که باید ارسال شود

$Em$  یک پیام تعبیه شده

$Ex$  نشان دهنده پیام استخراج شده است

$$Em : C \oplus K \oplus M \rightarrow \tilde{C}$$
$$\therefore Ex(Em(c, k, m)) \approx m, \forall c \in C, k \in K, m \in M$$

برای تمایز بین تکنیک‌های مختلف استگانوگرافی، باید هم روش‌هایی که تصویر را تغییر می‌دهند و هم روش‌هایی که قالب فایل تصویر را تغییر می‌دهند، در نظر گرفت. روش‌های فشرده‌سازی با اتلاف منجر به اندازه‌های کوچک‌تر فایل تصویری می‌شوند، احتمال از بین رفتن جزئی پیام تعبیه‌شده را افزایش می‌دهند. فشرده‌سازی بدون اتلاف فایل تصویر را به اندازه کافی فشرده نمی‌کند.



تکنیک‌های استگانوگرافی که فایل‌های تصویری را برای مخفی کردن اطلاعات تغییر می‌دهند شامل موارد زیر است:

- حوزه فضایی (Spatial domain)
- تبدیل دامنه (Transform domain)
- گسترش طیف (Spread spectrum)
- روش‌های آماری (Statistical methods)
- تکنیک‌های اعوجاج (Distortion techniques)

تکنیک‌های استگانوگرافی که فرمت فایل تصویر را تغییر می‌دهند: جاسازی فایل - تعبیه

تکنیک‌هایی که عناصر موجود در تصویر بصری را تغییر می‌دهند: تکنیک تولید تصویر - تکنیک اصلاح عنصر تصویر

تکنیک‌های حوزه فضایی و تبدیلی: تکنیک استگانوگرافی تطبیقی



## تکنیک دامنه فضایی (Spatial Domain Technique) :

- به عنوان تکنیک‌های جایگزینی نیز شناخته می‌شوند
- گروهی از تکنیک‌های نسبتاً ساده هستند
- کانالی پنهان در قسمت‌های تصویر جلد ایجاد می‌کنند
- تغییرات در مقایسه با سیستم بینایی انسان (HVS) کمی ناچیز است
- مخفی کردن اطلاعات در کمترین بیت (LSB) داده‌های تصویر است
- روش جاسازی کمترین بیت‌های تصویر را می‌توان به عنوان نویز تصادفی در نظر گرفت
- در نتیجه به هیچ تغییری روی تصویر پاسخگو نمی‌شوند.

$$Y_i = 2 \left\lfloor \frac{x_i}{2} \right\rfloor + m_i$$

$$\{P_m(m=0) \approx P_m(m=1) \approx 1/2\}.$$



### تکنیک‌های تبدیل دامنه (Transform Domain Techniques) :

- فرآیند جاسازی داده‌ها در حوزه فرکانس سیگنال بسیار قوی‌تر از اصول تعبیه شده در حوزه زمان است.
- تکنیک‌های تبدیل دامنه نسبت به تکنیک‌های LSB برتری دارند
- برخی از تکنیک‌های دامنه تبدیل وابسته به قالب تصویر به نظر نمی‌رسند
- فرمت فایل JPEG رایج‌ترین فرمت فایل تصویری در اینترنت است

### فشرده سازی JPEG (JPEG compression) :

- ابتدا فضای رنگی RGB به یک نمایش YUV تبدیل می‌شود.
- از طریق این نمایش، جزء Y نشان دهنده روشنایی (یا درخشندگی) است و اجزای U و V مخفف رنگ (یا کرومینانس) هستند.
- برای تصاویر JPEG، تبدیل کسینوس گسسته (DCT) استفاده می‌شود.
- تبدیل DCT، یک سیگنال از نمایش یک تصویر به حوزه فرکانس تبدیل می‌شود،
- مرتب‌سازی پیکسل‌ها به بلوک‌های پیکسلی (8×8) و تبدیل این بلوک‌ها به ضرایب DCT-64
- مرحله کوانتیزاسیون فشرده سازی



## استگانوگرافی (JPEG Steganography):

- تصاویر JPEG محصول دوربین‌های دیجیتال، اسکنرها و سایر دستگاه‌های عکاسی عکس هستند.
- پنهان کردن اطلاعات مخفی در تصاویر JPEG ممکن است پوشش بهتری ایجاد کند.
- داده‌ها در بیشتر سیستم‌های استگانوگرافی در ضرایب تبدیل کسینوس گسسته غیر صفر (DCT) تصاویر JPEG جاسازی شده‌اند.

روش‌های اصلی استگانوگرافی JPEG را می‌توان به شرح زیر توصیف کرد:

- JSteg/JPHide : دو ابزار کلاسیک استگانوگرافی JPEG هستند
- توابع JSteg برای مخفی کردن داده‌های مخفی در یک تصویر جلد
- JPHide : LSB‌های ضرایب انتخاب شده را تغییر دهد و فرآیندی که در آن بیت‌های دومین صفحه بیت کم اهمیتیت به احتمال زیاد کار می‌شوند.
- F5 : به جای جایگزینی LSB‌های ضرایب DCT کوانتیزه شده با بیت‌های پیام، قدر مطلق ضریب توسط الگوریتم F5 در صورت نیاز به اصلاح یک کاهش می‌یابد.

علاوه بر جاسازی بیت‌های پیام در ضرایب DCT که به‌طور تصادفی انتخاب شده‌اند

هر دو، طول پیام و تعداد ضرایب غیر صفر در فرآیند جاسازی برای تعیین تعبیه ماتریس مورد نیاز برای کاهش تعداد تغییرات مورد نیاز در تصویر جلد مورد

نیاز است.

- OutGuess : دو نسخه منتشر شده بسیار شناخته شده برای آن وجود دارد: اولین مورد OutGuess 0.13b است که در معرض تجزیه و تحلیل آماری

قرار دارد و دومی OutGuess-0.2 است که شامل توانایی محافظت از ویژگی‌های آماری است.

اندکی بعد تغییراتی در ضرایب باقی مانده در طول جاسازی انجام می‌شود تا هیستوگرام DCT جهانی استگوا ایجاد شود.

تصویر با تصویر روی جلد مطابقت دارد. OutGuess

را نمی‌توان در معرض یک حمله chisquare قرار داد

- MB : یک چارچوب کلی برای انجام هر دو steganography و steganalysis با استفاده از یک مدل آماری از رسانه پوشش.

روش MB برای تصاویر JPEG قادر است ظرفیت پیام بالایی داشته باشد و در برابر بسیاری از حملات آماری مرتبه اول ایمن باقی بماند.

YASS : داده‌ها را مستقیماً در ضرایب JPEG DCT پنهان نمی‌کند. در عوض، یک تصویر ورودی در حوزه فضایی به بلوک‌هایی با اندازه بزرگ ثابت تقسیم می‌شود

که بلوک‌های بزرگ (یا بلوک‌های B) نامیده می‌شوند.

انتخاب تصادفی در هر بلوک B، یک بلوک فرعی  $8 \times 8$  است که به عنوان بلوک میزبان تعبیه شده (یا بلوک H) شناخته می‌شود.

کدهای تصحیح خطا، داده‌های مخفی کدگذاری شده و در ضرایب DCT بلوک‌های H جاسازی می‌شوند.

کل تصویر فشرده شده و به عنوان یک تصویر JPEG پس از معکوس کردن DCT بر روی بلوک‌های H توزیع می‌شود.



### تکنیک تبدیل موجک (Wavelet transform technique) :

اطلاعات حوزه مکانی را به اطلاعات حوزه فرکانس تبدیل می کند.

مدل استگنوگرافی تصویر استفاده می شود

نسبت به روش تبدیل کسینوس گسسته (DCT) ترجیح داده می شود

موجک ها توابع ریاضی هستند که داده ها را به اجزای فرکانس تقسیم می کنند که آنها را برای فشرده سازی تصویر ایده آل می کند

انتقال سفارشی علاقه مند به منطقه متصل همگن (HCRIOT) برای رمزگذاری و فشرده سازی

محققان از کوانتیزاسیون برداری، به نام Linde-Buzo-Gray (LBG) استفاده می کنند، که با کدهای بلوکی، معروف به کدهای BCH، و تبدیل موجک ها گسسته یک مرحله ای مرتبط است.

گروهی از دانشمندان در دانشگاه ایالتی ایووا در حال توسعه یک برنامه کاربردی پیشرفته به نام فناوری شبکه عصبی مصنوعی برای

استگنوگرافی (ANNTS) با هدف شناسایی تمام روش های استگنوگرافی فعلی هستند که شامل DCT، DWT و DFT می شود. آنها دریافتند

که تبدیل فوریه گسسته معکوس (IDFT) شامل یک خطای گرد است که DFT را برای کاربردهای استگنوگرافی نامناسب می کند.

یک تکنیک پنهان کردن داده ها در حوزه DWT وجود دارد که DWT با سطح اول برای تجزیه هر دو تصویر مخفی و پوشش استفاده

می شود، جایی که هر کدام به بلوک های جدا (4 × 4) تقسیم می شوند. سپس مقایسه ای بین بلوک های تصویر مخفی و بلوک های پوششی

برای تعیین بهترین تطابق انجام می شود. بعداً، بلوک های خطا تولید می شوند و در ضرایب بهترین بلوک های همسان در قسمت HL تصویر

جلد جاسازی می شوند.



تکنیک اسپرید اسپکتروم (Spread Spectrum Technique) :

انتقال طیف گسترده در ارتباطات رادیویی، پیام‌هایی را زیر سطح نویز برای هر فرکانس مشخصی ارسال می‌کند. تصویر جلد به عنوان نویز: سیستمی که تصویر جلد را به عنوان نویز در نظر می‌گیرد، می‌تواند یک مقدار واحد به آن تصویر جلد اضافه کند برای اجازه دادن به انتقال بیش از یک بیت، تصویر جلد باید به تصاویر فرعی تقسیم شود. شبه نویز: این تکنیک نشان می‌دهد که داده‌های پنهان در سراسر تصویر جلد پخش می‌شوند و به همین دلیل تشخیص آن دشوار می‌شود. استگانوگرافی طیف گسترده تصویر (SSIS) توصیف شده توسط مارول و همکاران، ارتباطات ترکیبی طیف گسترده، کدگذاری کنترل خطا و پردازش تصویر برای پنهان کردن اطلاعات در تصاویر، نمونه‌ای از این تکنیک است. طرح کلی تعبیه افزودنی را می‌توان به شرح زیر توصیف کرد:

$$Y_i = X_i + \gamma W_i \text{ for } i = 1, 2, \dots, N$$

در SSIS، فرآیند به این صورت پیش می‌رود: پیام در نویز پنهان می‌شود و سپس با تصویر جلد ترکیب می‌شود تا به یک تصویر استگانوگرافیک برسد. از آنجایی که قدرت سیگنال تعبیه شده بسیار کمتر از قدرت تصویر جلد است، تصویر تعبیه شده نه تنها برای چشم انسان بلکه از طریق تجزیه و تحلیل کامپیوتری بدون دسترسی به تصویر اصلی نامحسوس می‌شود.

● توالی مستقیم، پرش فرکانس و صدای جیر جیر



روش‌های آماری (Statistical Methods) :

این تکنیک‌ها که به عنوان تکنیک‌های مبتنی بر مدل نیز شناخته می‌شوند تکنیک‌های استگنوگرافی آماری از وجود یک «1 بیت» استفاده می‌کنند

این فرآیند به سادگی با تغییر تصویر جلد انجام می‌شود تا در صورت انتقال یک "1 بیت" نوعی تغییر قابل توجه در ویژگی‌های آماری ایجاد شود، در غیراین صورت بدون تغییر باقی می‌ماند.

برای ارسال چند بیت، یک تصویر به تصاویر فرعی تقسیم می‌شود

سیگنال پیام به گونه‌ای پردازش می‌شود که ویژگی‌های سیگنال پوشش دلخواه را مشاهده می‌کند

آمار ضرایب AC DCT کوانتیزه شده (غیر صفر) با در نظر گرفتن تابع چگالی پارامتریک اصلاح می‌شود.

این فرآیند علاوه بر تطبیق مدل با هر هیستوگرام با تعیین پارامترهای مدل مربوطه، به هیستوگرام با دقت پایین هر کانال فرکانس نیاز دارد.

روش‌های استگنوگرافی آماری در برابر حملات برش، چرخش و مقیاس‌بندی، همراه با هر حمله‌ای که برخلاف تکنیک واترمارک عمل می‌کند، آسیب‌پذیر هستند.





- تکنیک‌های تحریف (Distortion Techniques) :

- تکنیک‌های اعوجاج مستلزم دانش تصویر جلد اصلی در طول فرآیند رمزگشایی است
- رمزگذار، دنباله‌ای از تغییرات را به تصویر جلد اضافه می‌کند.
- با استفاده از این تکنیک، یک stego-object با اعمال دنباله‌ای از تغییرات در تصویر جلد ایجاد میشود
- پیام در پیکسل‌های شبه تصادفی کدگذاری می‌شود.
- اگر تصویر استگو با تصویر جلد در پیکسل پیام داده شده متفاوت باشد، بیت پیام "1" است. در غیر این صورت، بیت پیام "0" است.
- اکثر تکنیک‌های پنهان سازی مبتنی بر متن از نوع اعوجاج هستند.



- تکنیک تولید تصویر (Image Generation Technique) :
- Big Play Maker با تبدیل پیام متنی مخفی به یک قالب متنی بزرگتر و کمی دستکاری شده، اطلاعات را پنهان می‌کند.
- همین اصل را می‌توان در ایجاد تصویر به کار برد، که در آن یک پیام به عناصر تصویر تبدیل می‌شود و سپس به یک تصویر استگو کامل جمع آوری می‌شود
- به طور کلی، این تکنیک از تصاویر شبه تصادفی استفاده می‌کند، زیرا اگر یک شخص ثالث مخرب گروهی از تصاویر را بدون هیچ دلیلی برای حضور آنها در یک شبکه (یعنی تصاویر تصادفی) شناسایی کند که ممکن است مشکوک شود که تصاویر حاوی اطلاعات مخفی هستند و انتقال آنها را مسدود میکند.
- تکنیک‌های اصلاح عنصر تصویر (Image Element Modification Techniques) :
- برخی از تکنیک‌های استگانوگرافی سعی نمی‌کنند اطلاعات را با استفاده از عناصر واقعی تصویر پنهان کنند. در عوض، آنها عناصر تصویر را به روش‌های کاملاً غیرقابل شناسایی تنظیم می‌کنند، مثلاً با تغییر رنگ چشم یا رنگ موی یک فرد در یک عکس
- علاوه بر این، این اطلاعات از چرخش، پوسته پوسته شدن و فشرده سازی با اتلاف جان سالم به در خواهند برد. امکان اصلاح اشیاء درون تصاویر به عنوان تاکتیکی برای پنهان کردن اطلاعات مورد بحث قرار گرفته است. توجه به این نکته ضروری است که هنگام استفاده از این روش، از همان تصویر جلد نباید بیش از یک بار استفاده شود، زیرا عناصر استفاده شده آشکار می‌شوند. این تکنیک به صورت دستی با هر نرم افزار ویرایش عکس قابل دستیابی است. با ظهور سیستم‌های بینایی رایانه‌ای که اشیاء درون تصاویر را شناسایی می‌کنند، این روش‌ها عملی‌تر شده‌اند.

- استگانوگرافی تطبیقی (Adaptive Steganography) :
- استگانوگرافی تطبیقی یک مورد خاص از تکنیک‌های فضایی و تبدیلی است. علاوه بر این، به عنوان جاسازی و پوشاندن آگاه از آمار معرفی شده است. ویژگی‌های آماری کلی تصویر اساساً قبل از هر تلاشی برای مقابله با ضرایب تبدیل فرکانس آن استفاده می‌شود. این آمار تعیین می‌کند که چه تغییراتی می‌تواند ایجاد شود. یک انتخاب تطبیقی تصادفی از پیکسل‌ها در واقع این روش را مشخص می‌کند، با تکیه بر تصویر جلد و انتخاب پیکسل‌ها در یک بلوک با انحراف استاندارد بزرگ (STD). هدف دوم برای جلوگیری از مناطقی با رنگ یکنواخت، مانند مناطق صاف است. این تکنیک برای بهره‌برداری از تصاویر با نویز موجود یا عمداً اضافه شده و با تصاویری که پیچیدگی رنگ را نشان می‌دهند شناخته شده است.
- یک تکنیک تطبیقی که برای روش جایگزینی LSB اعمال می‌شود، پیشنهاد شده است. ایده پشت این روش استفاده از همبستگی بین پیکسل‌های همسایه برای محاسبه درجه صافی است. محققان گزینه‌های داشتن مسابقات دو، سه و چهار وجه را روشن کردند. محموله (ظرفیت جاسازی) که آنها توانستند به دست آورند بالا بود.
- تکنیکی به نام تکنیک «تطبیق بیشتر پیکسل‌های اطراف با استفاده از (A-MSPU)» ، که مشکلات نامحسوس بودن سیستم‌های نمادگذاری پایه چندگانه (MBNS) را بهبود می‌بخشد، در مورد بحث قرار گرفته است. این تکنیک به نواحی لبه یک تصویر جلد توجه می‌کند در حالی که بیت‌های مخفی را در سیستم‌های نمادی پایه چندگانه بیان می‌کند. رویکرد پیشنهادی از همان پارامتر احتمال برای پراکندگی بیت‌های مخفی استفاده می‌کند و همچنین از پیکسل‌های اطراف با حداکثر تعداد برای تعیین ظرفیت هر پیکسل هدف استفاده می‌کند. بیشتر تکنیک‌های استگانوگرافی از سه یا چهار پیکسل مجاور یک پیکسل هدف استفاده می‌کنند. روش پیشنهادی قادر به استفاده از هر هشت همسایه مجاور است که مقدار نامحسوس بودن را بهبود می‌بخشد.
- 
-

