HIVE

a covert communication platform of CIA

스노든 "美, 中 국가기관·기업 등 수백곳 해킹"

입력 : | 수정 : 2013-06-14 00:28

스노든 "美, 中 국가기관·기업 등 수백곳 해킹"

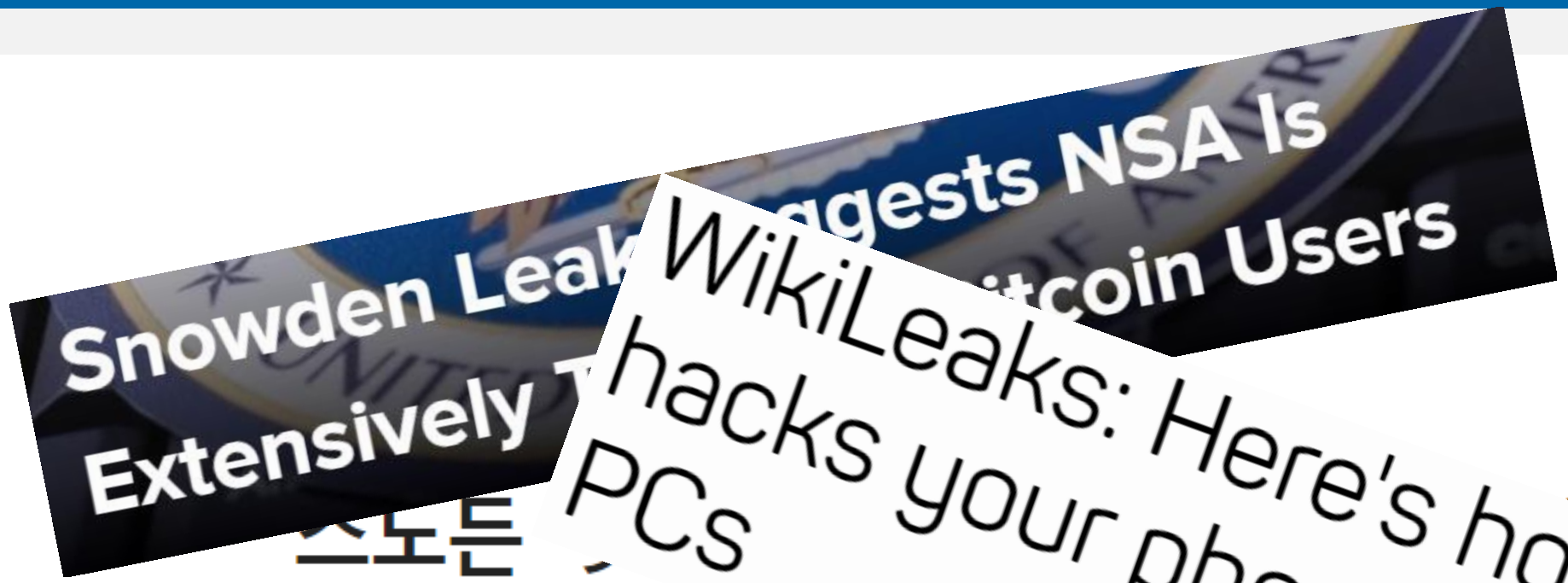
입력 : | 수정 : 2013-06-14 00:28

스노든 "美, 中 국가기관·기업 등 수백곳 해킹"

입력 : | 수정 : 2013-06-14 00:28

Hacking group auctions 'cyber weapons' stolen from NSA

Guardian



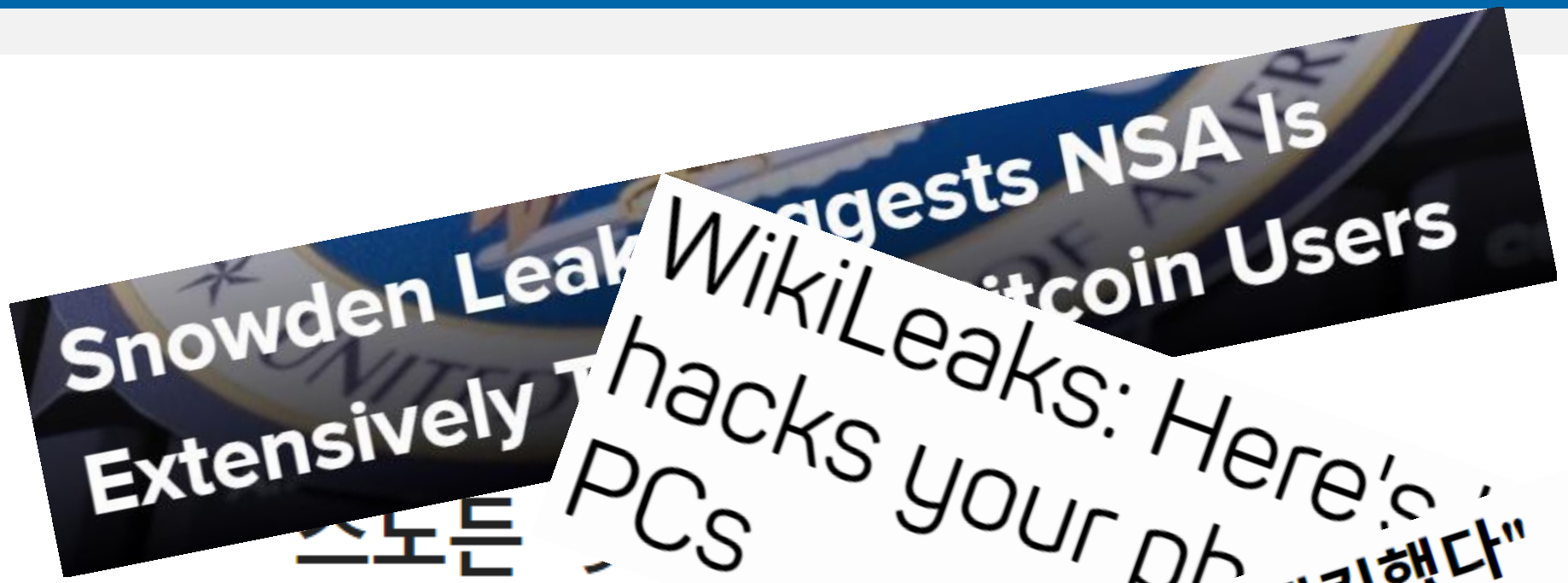
WikiLeaks: Here's how the CIA hacks your phones, TVs and PCs

해킹"

입력 : | 수정 : 2013-06-14 00:28

Hacking group auctions 'cyber weapons' stolen from NSA

Guardian



스노든

입력 : | 수정 : 2013-06-14 00:28

WikiLeaks: Here's
hacks your ph
PCs
해킹"
w the CIA
S, TVs and

위키리크스 "국정원, 변호사 해킹했다"

Hacking gro
stolen from NSA
tions 'cyber weapons'

Guardian

HIVE

- CIA가 사용한 다중 감시, 원격 제어 시스템

- Wikileaks에 의하여 대중에게 공개됨
  - 2017년 3월: 존재가 밝혀짐 (Vault 7)
  - 2017년 11월: 소스 코드 공개 (Vault 8)

HIVE가 하는 일

- 악성코드로 감염시킨 대상
  - 지속적인 정보 습득
  - 명령어 실행

HIVE가 하는 일

- 예) 시리아 IS의 컴퓨터를 해킹하는 데 성공했다. 어떻게 할까?

HIVE가 하는 일

- 예) 시리아 IS의 컴퓨터를 해킹하는 데 성공했다. 어떻게 할까?

1. 컴퓨터에 있는 데이터를 다 지워버리고 고장내 버린다

HIVE가 하는 일

- 예) 시리아 IS의 컴퓨터를 해킹하는 데 성공했다. 어떻게 할까?

1. 컴퓨터에 있는 데이터를 다 지워버리고 고장내 버린다

→ 단기적으로 테러를 막을 수는 있으나
→ 새로 사서 복구하면 그만
→ 이후에 해킹 대책을 세울 수도 있다

HIVE가 하는 일

- 예) 시리아 IS의 컴퓨터를 해킹하는 데 성공했다. 어떻게 할까?

2. HIVE를 이용해서 지속적인 감시를 하자

HIVE가 하는 일

- 예) 시리아 IS의 컴퓨터를 해킹하는 데 성공했다. 어떻게 할까?

2. HIVE를 이용해서 지속적인 감시를 하자

→ IS가 어디서 어떤 테러를 꾸미고 있는지 지속적인 정찰
→ 가장 핵심적인 타이밍에 데이터 파괴

멀웨어 소모임에서는 무엇을 했나요?

- 11월 ~ 2월 HIVE 분석
  - CIA 내부 HIVE 문건 읽기
  - HIVE 코드 분석
  - HIVE 테스트 환경 구축 (네트워크 구축, 코드 수정)
  - 테스트

목차

- HIVE structure overview
- HIVE 동작 방식
  - Beacon Structure
  - Client-Server Connection
- HIVE 코드 살펴보기

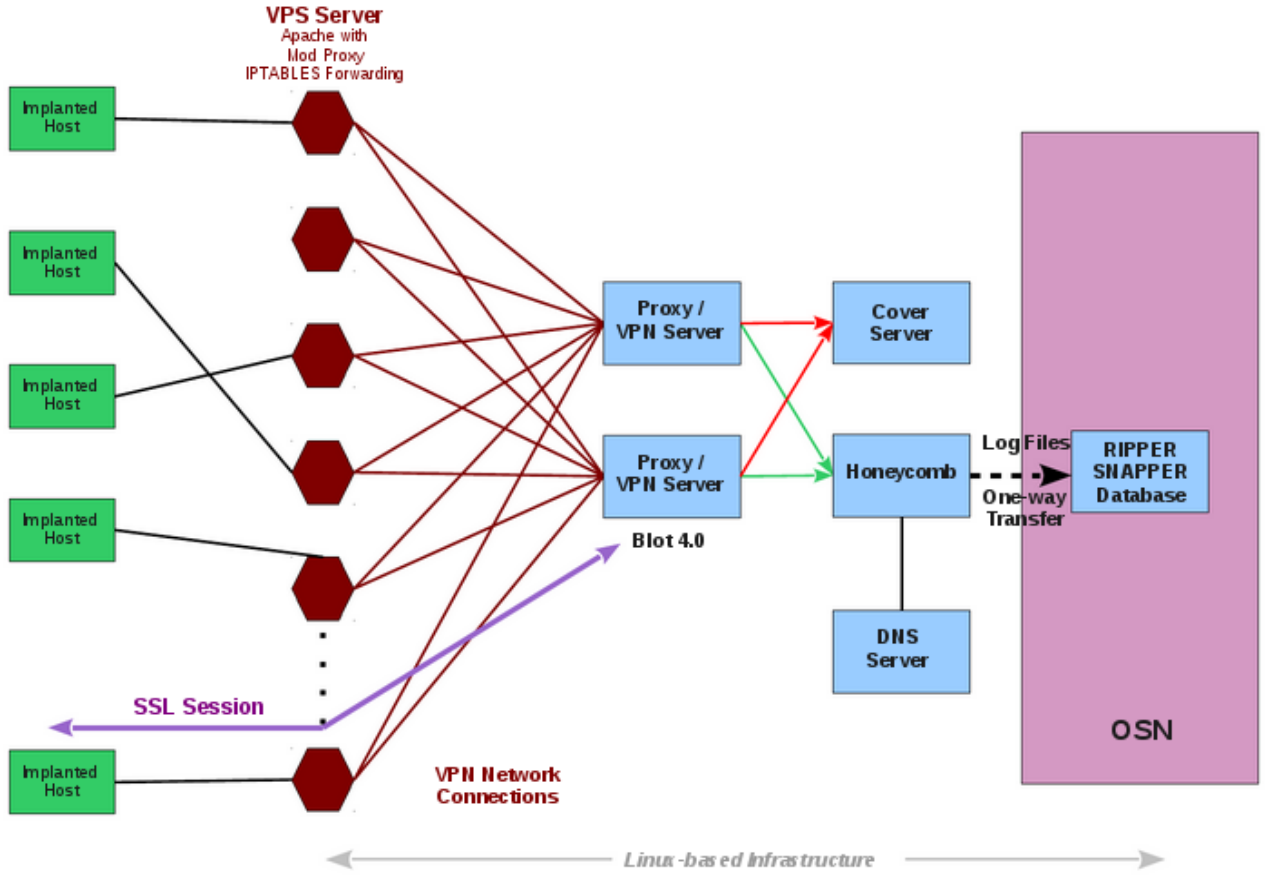
HIVE structure overview

1. Victim으로부터 지속적인 정보를 얻는다

2. Victim에게 직접적인 명령을 내린다

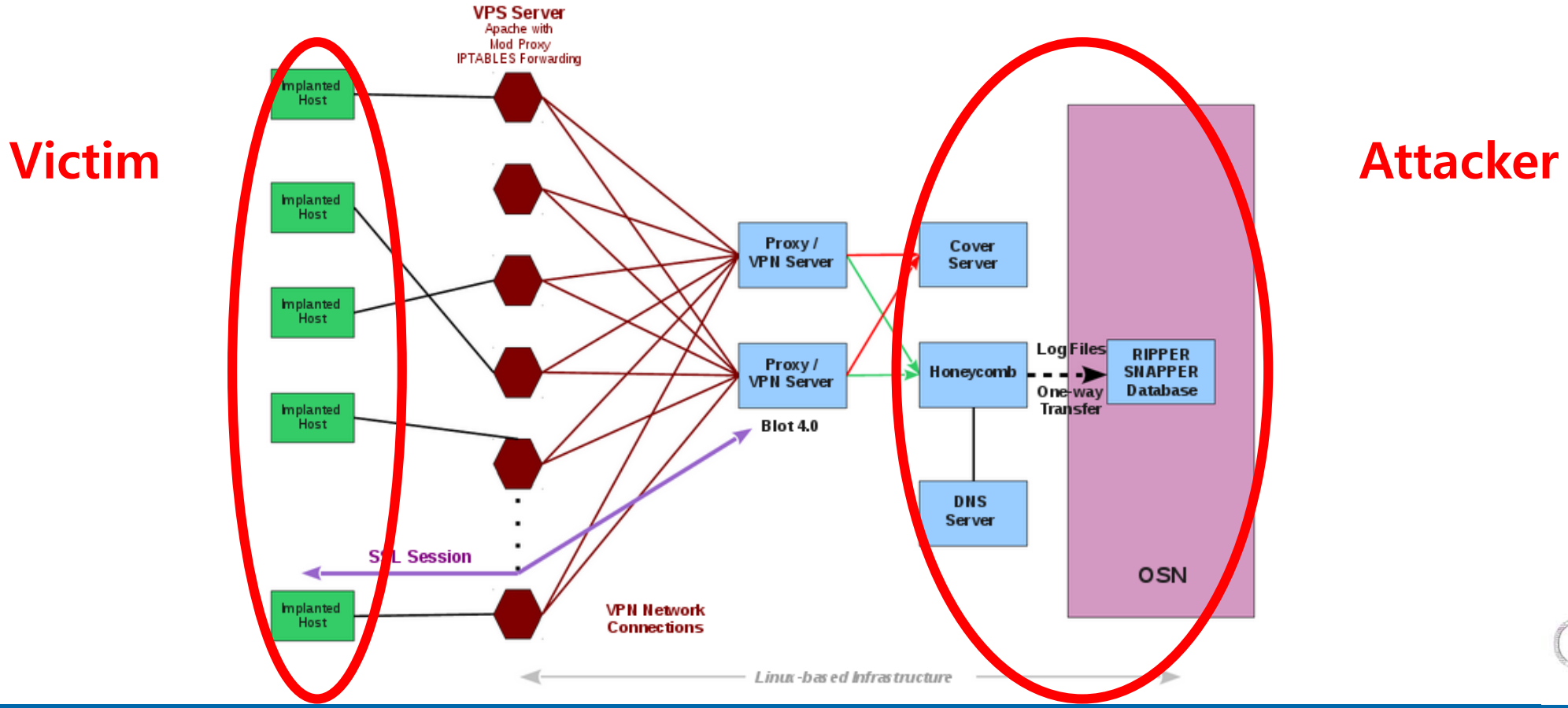
HIVE structure overview

1. Victim으로부터 지속적인 정보를 얻는다



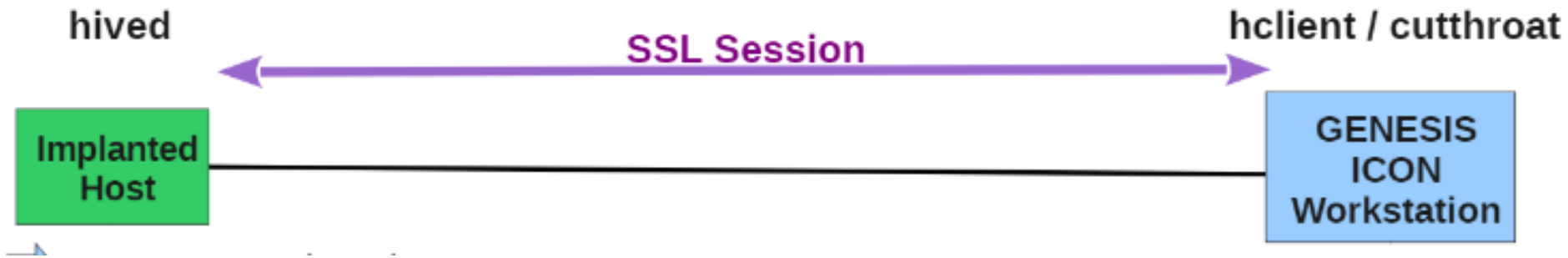
HIVE structure overview

1. Victim으로부터 지속적인 정보를 얻는다



HIVE structure overview

2. Victim에게 직접적인 명령을 내린다



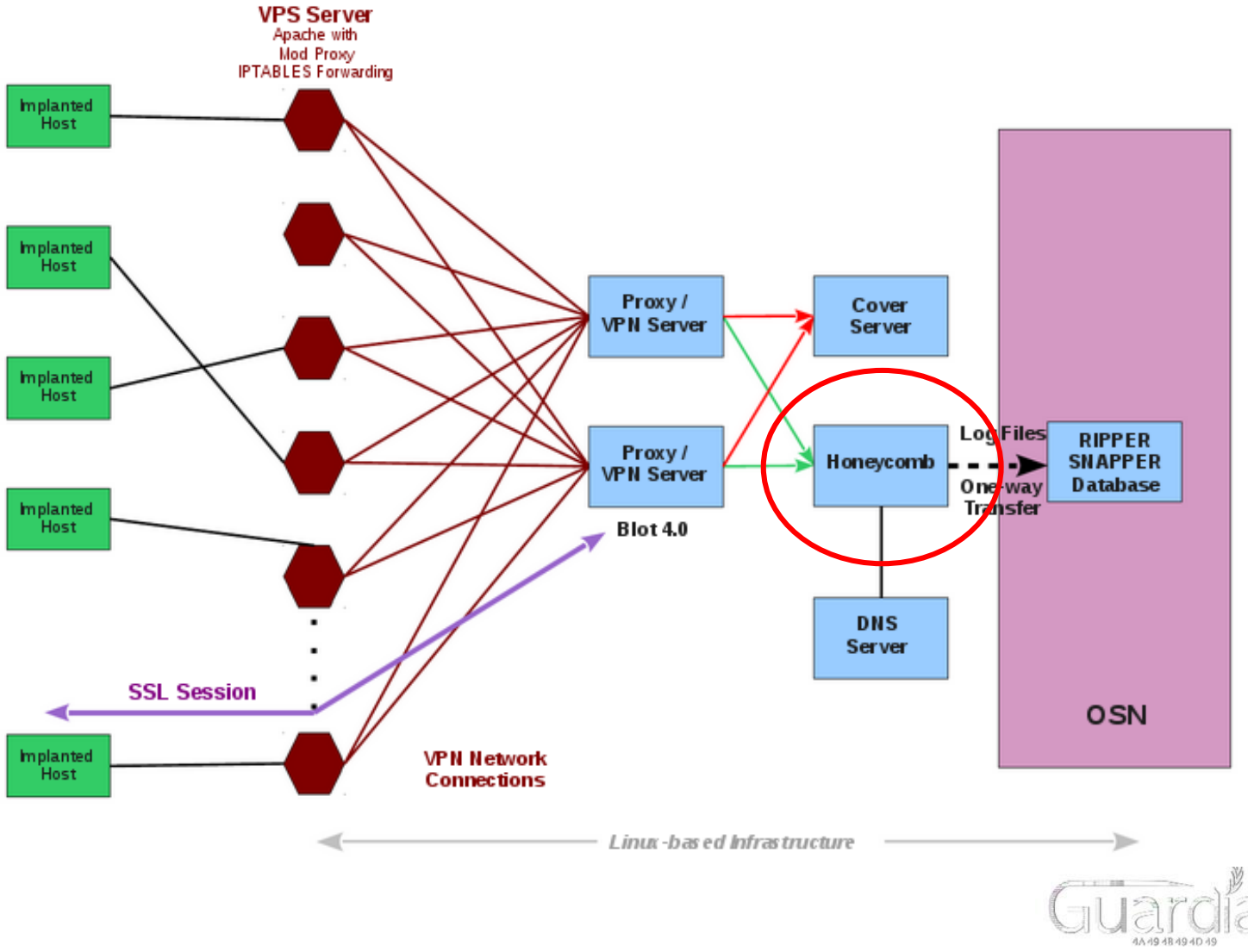
Honeycomb

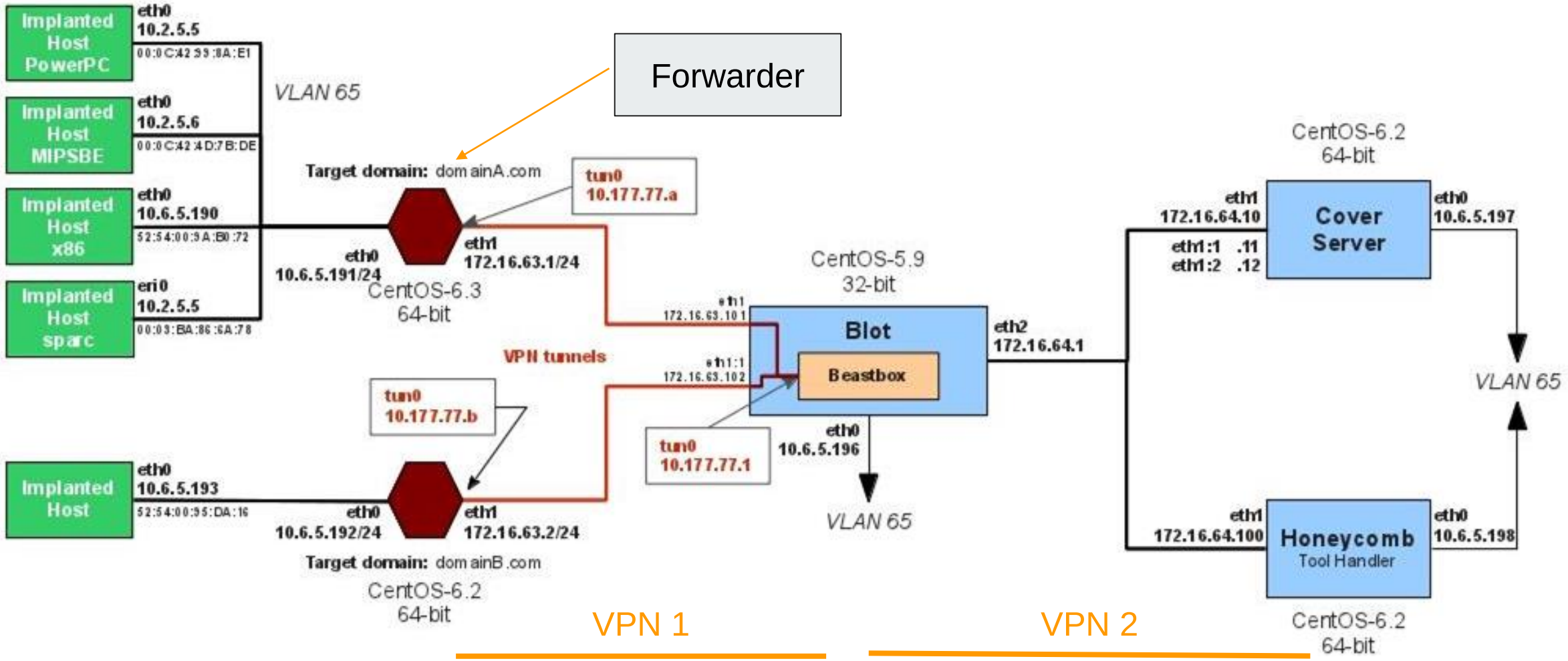
Honeycomb

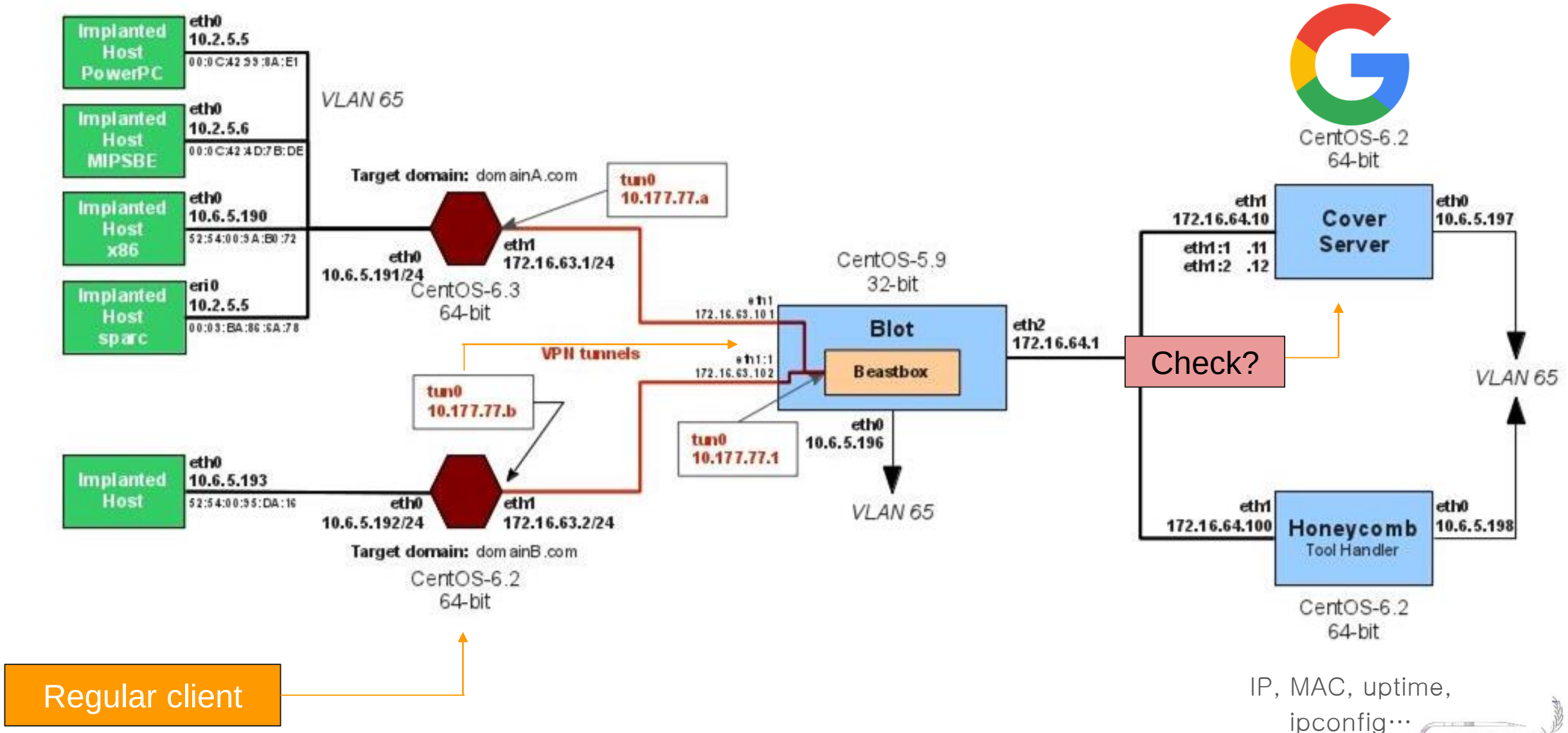
Victim이 보낸 정보를 기록하는 코드.

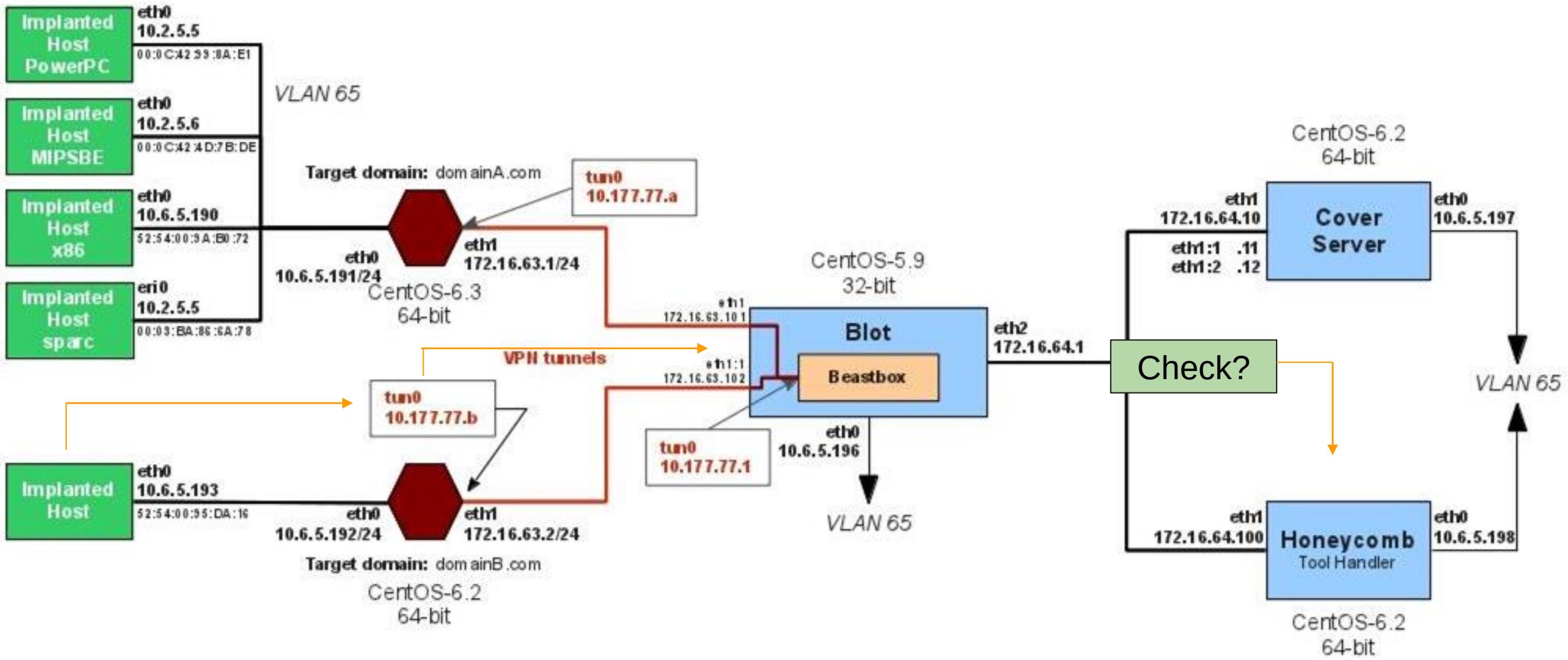
honeycomb.py	Linux executable. Tool handler for Hive beacons. HTTPS beacons validated by Swindle are passed to Honeycomb. Honeycomb receives and logs the beacons.

Honeycomb


VPS Server
Apache with
Mod Proxy
IPTABLES Forwarding
Implanted Host
Implanted Host
Implanted Host
Implanted Host
Implanted Host
Proxy / VPN Server
Proxy / VPN Server
Blot 4.0
Cover Server
Honeycomb
DNS Server
Log Files
One-way Transfer
RIPPER SNAPPER Database
OSN
SSL Session
VPN Network Connections
Linux-based Infrastructure


Implanted Host PowerPC
eth0
10.2.5.5
00:0C:42:33:8A:E1
Implanted Host MIPSBE
eth0
10.2.5.6
00:0C:42:4D:7B:DE
Implanted Host x86
eth0
10.6.5.190
52:54:00:5A:B0:72
Implanted Host sparc
eri0
10.2.5.5
00:03:BA:86:6A:78
VLAN 65
Forwarder
Target domain: domainA.com
tun0
10.177.77.a
eth0
10.6.5.191/24
eth1
172.16.63.1/24
CentOS-6.3
64-bit
VPN tunnels
tun0
10.177.77.b
Implanted Host
eth0
10.6.5.193
52:54:00:35:DA:16
eth0
10.6.5.192/24
eth1
172.16.63.2/24
Target domain: domainB.com
CentOS-6.2
64-bit
CentOS-5.9
32-bit
eth1
172.16.63.101
Blot
eth1:1
172.16.63.102
Beastbox
tun0
10.177.77.1
eth0
10.6.5.196
VLAN 65
eth2
172.16.64.1
CentOS-6.2
64-bit
eth1
172.16.64.10
eth1:1 .11
eth1:2 .12
Cover Server
eth0
10.6.5.197
VLAN 65
eth1
172.16.64.100
Honeycomb
Tool Handler
eth0
10.6.5.198
CentOS-6.2
64-bit
VPN 1
VPN 2
SSL


Implanted Host PowerPC
eth0
10.2.5.5
00:0C:42:99:8A:E1
Implanted Host MIPSBE
eth0
10.2.5.6
00:0C:42:4D:7B:DE
Implanted Host x86
eth0
10.6.5.190
52:54:00:9A:B0:72
Implanted Host sparc
eri0
10.2.5.5
00:03:BA:86:6A:78
VLAN 65
Target domain: domainA.com
tun0
10.177.77.a
eth0
10.6.5.191/24
eth1
172.16.63.1/24
CentOS-6.3
64-bit
VPN tunnels
tun0
10.177.77.b
Implanted Host
eth0
10.6.5.193
52:54:00:95:DA:16
eth0
10.6.5.192/24
eth1
172.16.63.2/24
Target domain: domainB.com
CentOS-6.2
64-bit
CentOS-5.9
32-bit
eth1
172.16.63.101
Blot
Beastbox
eth1:1
172.16.63.102
tun0
10.177.77.1
eth0
10.6.5.196
VLAN 65
eth2
172.16.64.1
Check?
CentOS-6.2
64-bit
eth1
172.16.64.10
eth1:1 .11
eth1:2 .12
Cover Server
eth0
10.6.5.197
VLAN 65
eth1
172.16.64.100
Honeycomb
Tool Handler
eth0
10.6.5.198
CentOS-6.2
64-bit
Regular client
IP, MAC, uptime,
ipconfig…



IP, MAC, uptime,
ipconfig…

Honeycomb

어떤 정보를 빼낼까?

- IP 주소, MAC 주소
- OS type (Linux, Solaris, PowerPC, etc...)
- uptime: 얼마동안 컴퓨터가 켜져있었는지
- process list: 현재 돌아가고 있는 프로그램 리스트
- ipconfig/ifconfig: 네트워크 설정
- netstat -rn: 라우팅 테이블
- netstat -an: 현재 열려있는 connection들

이걸로 뭘 알아낼 수 있을까?

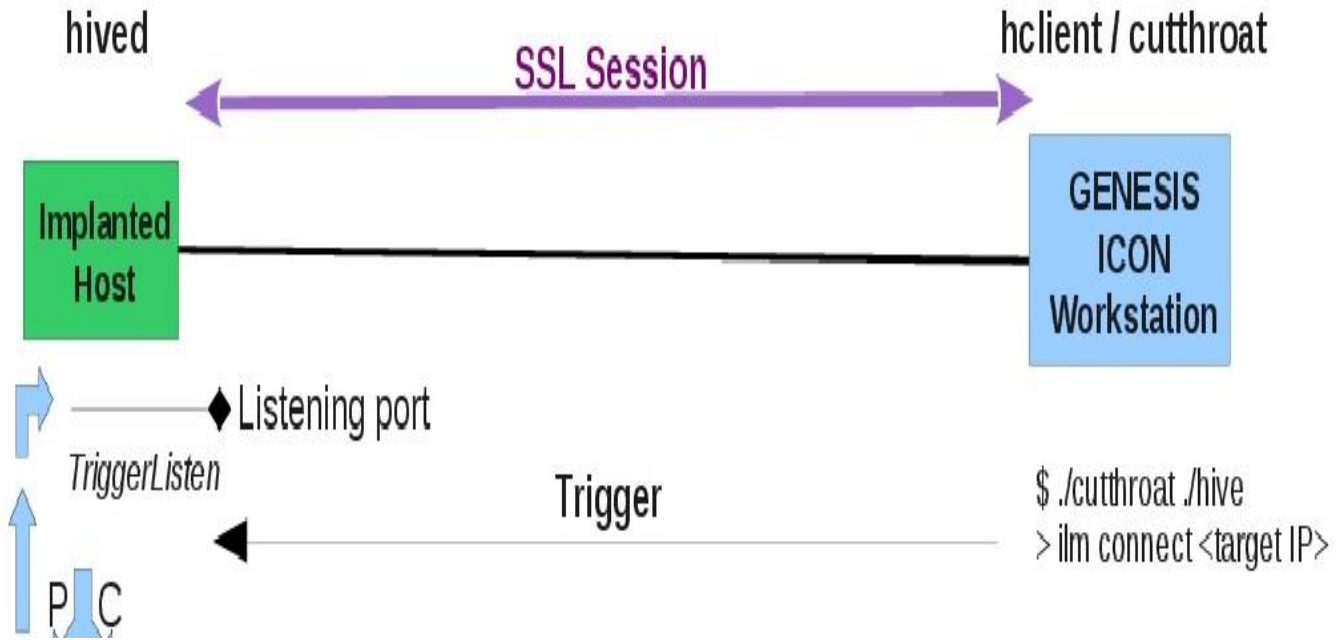
- 누가
- 어디서
- 얼마동안
- 뭘
- 누구랑
- 어떻게

Attacker

어떻게 명령을 전달할 수 있을까?

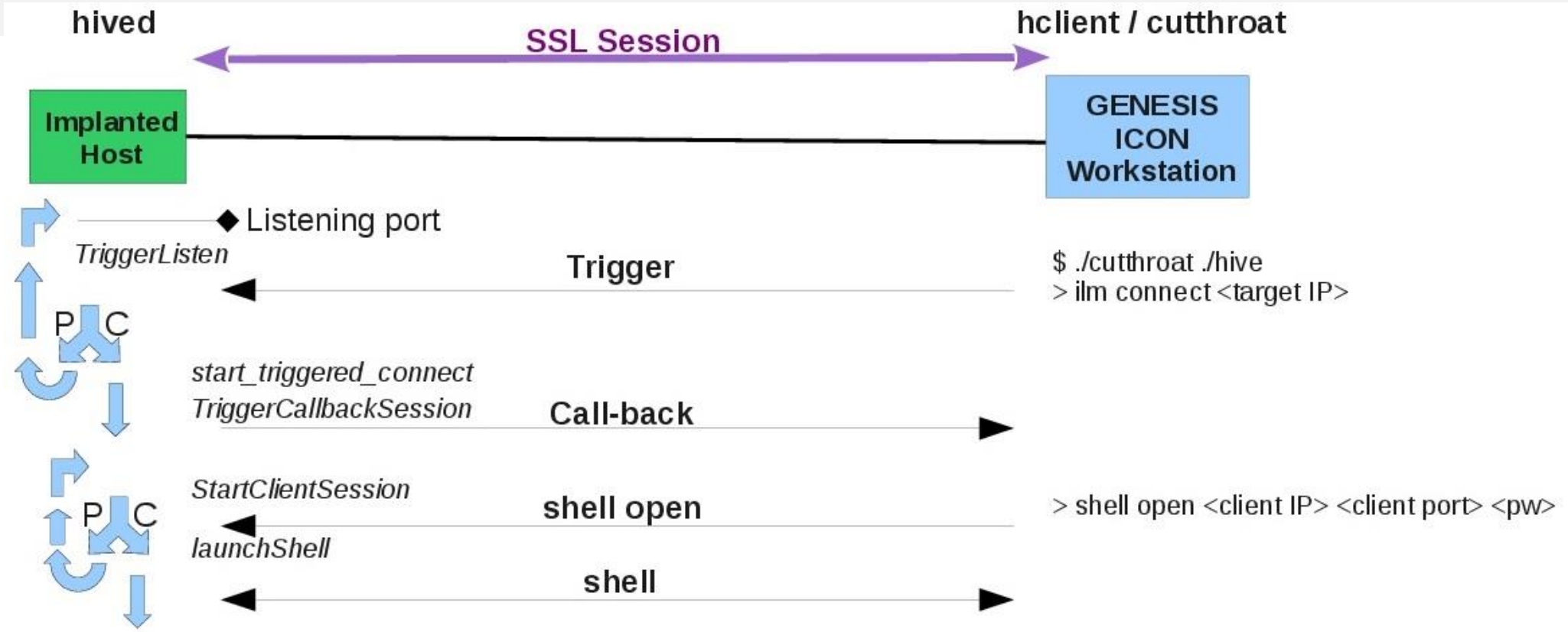
Trigger

- 다른 사람의 신호와 Attacker의 신호를 어떻게 구별할 수 있을까?
- 어떤 정보를 보내야 서로 통신할 수 있을까?



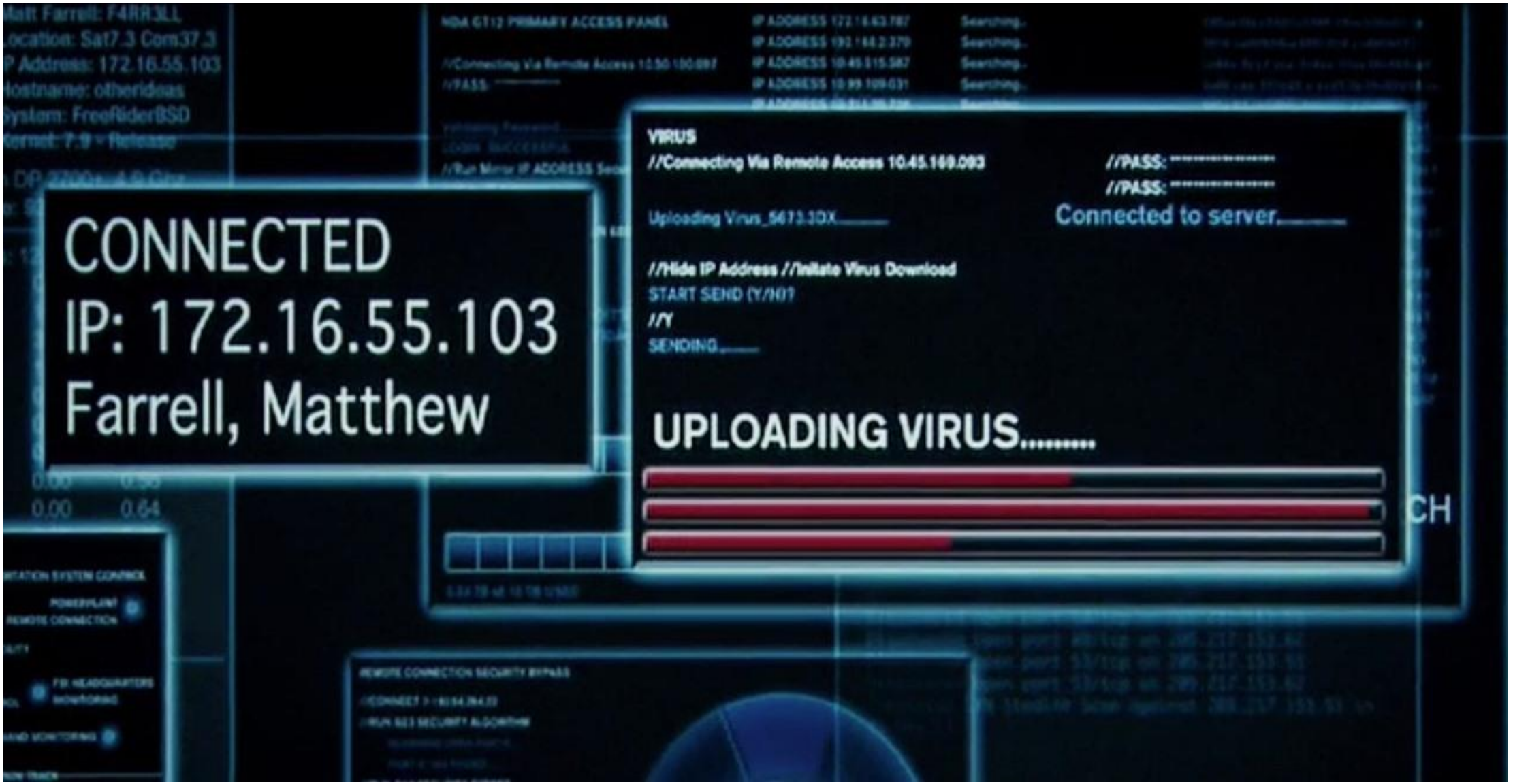

hived
SSL Session
hclient / cutthroat
Implanted Host
GENESIS ICON Workstation
Listening port
TriggerListen
Trigger
$ ./cutthroat ./hive
> ilm connect <target IP>
P
C
start_triggered_connect
TriggerCallbackSession
Call-back

Callback



Shell

통신하자! Window처럼!

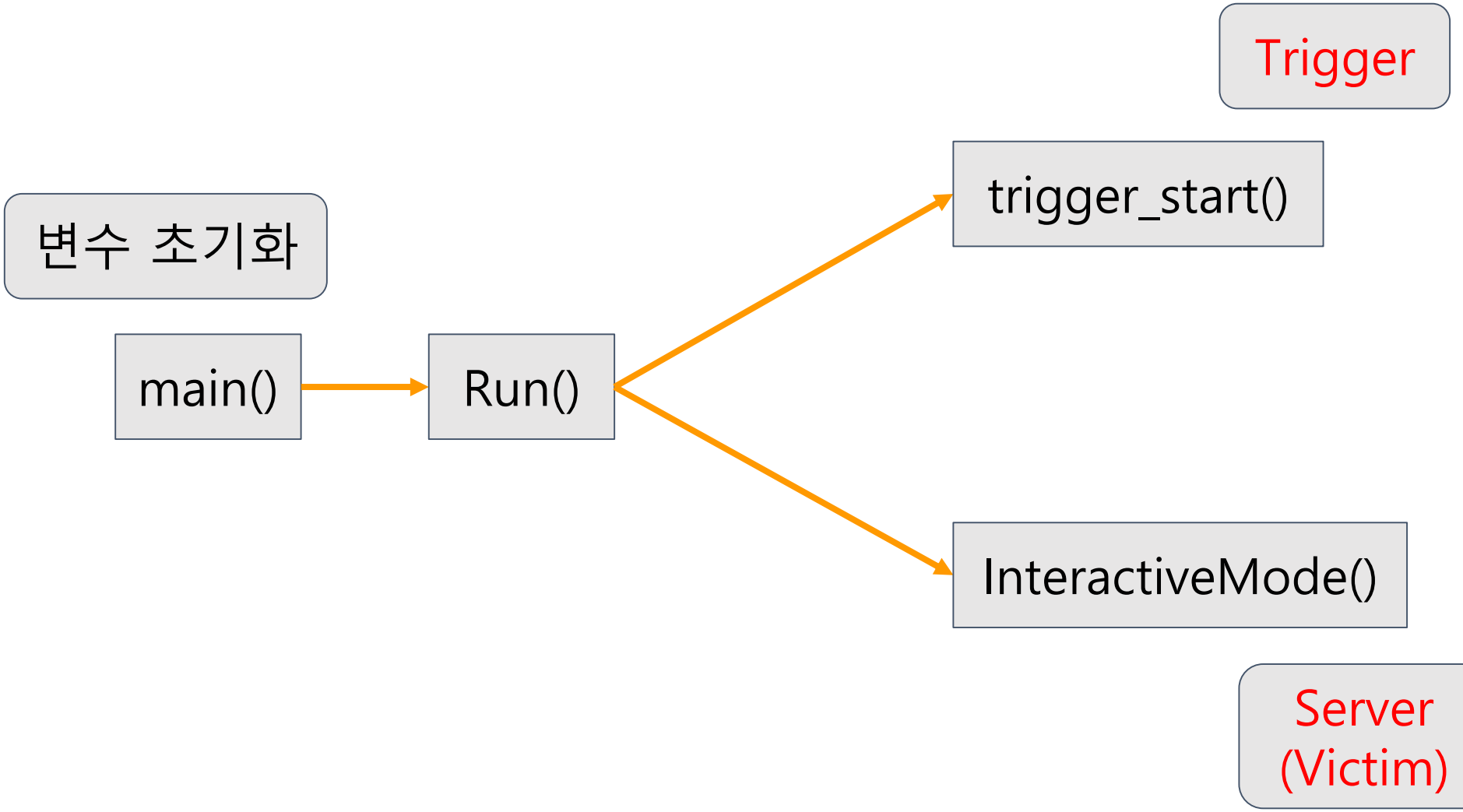

CONNECTED
IP: 172.16.55.103
Farrell, Matthew
VIRUS
//Connecting Via Remote Access 10.45.169.093
//PASS:
//PASS:
Uploading Virus_5673.3DX
Connected to server
//Hide IP Address //Initate Virus Download
START SEND (Y/N)?
/Y
SENDING
UPLOADING VIRUS.....

Client

- Trigger packet을 보내 Victim(Server)과 연결 시도

- 연결된 경우, Server에게 특정 작업을 수행시키기 위한 Command 전달

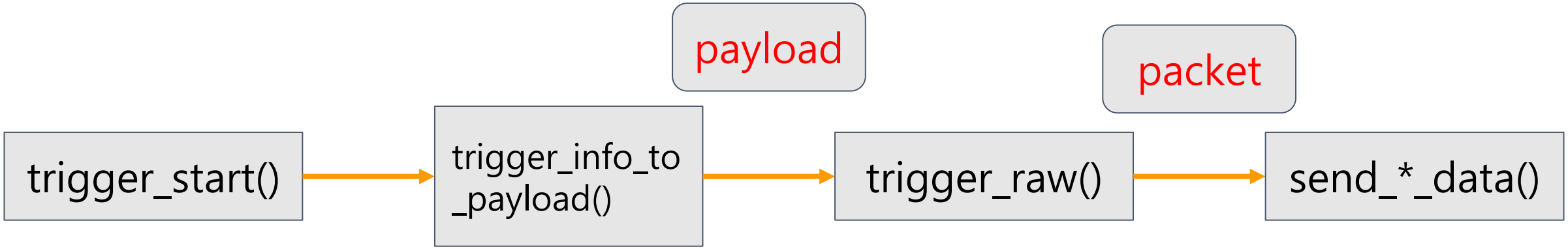
main()


Trigger
trigger_start()
변수 초기화
main()
Run()
InteractiveMode()
Server
(Victim)

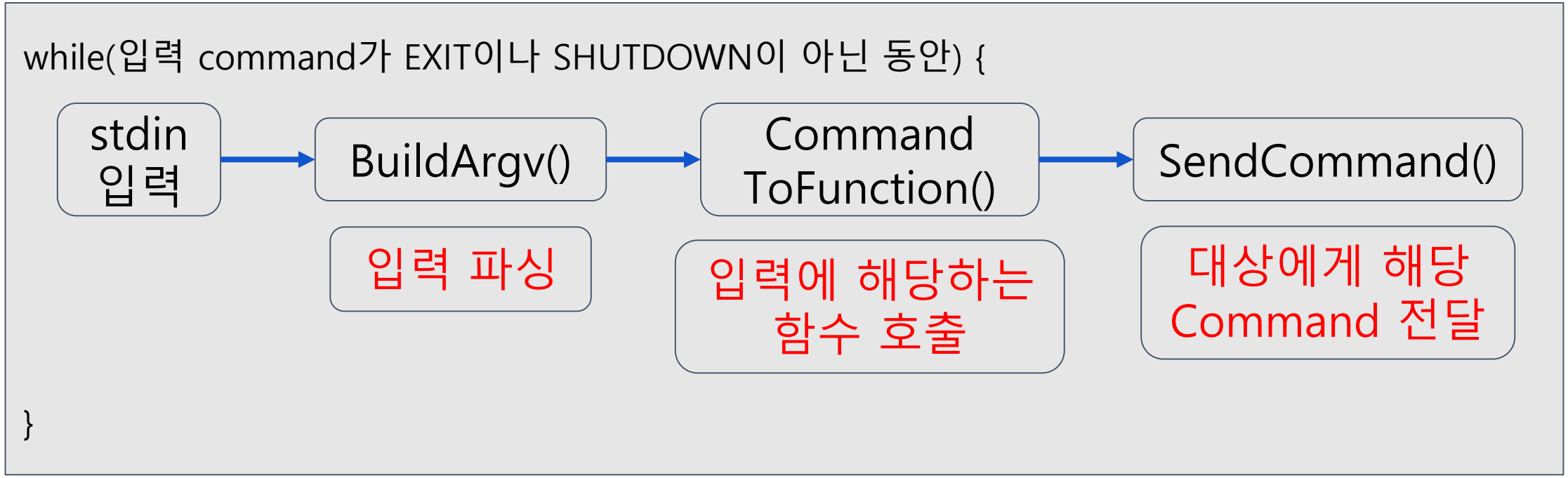
trigger_start()

- trigger_info_to_payload() 함수를 통해 trigger를 담은 payload를 만든 뒤, trigger_raw() 호출

- trigger_raw() 함수는 받은 payload를 포함한 실제 packet을 만들어 프로토콜 상태에 따라 send_TCP_data() / send_UDP_data() 호출



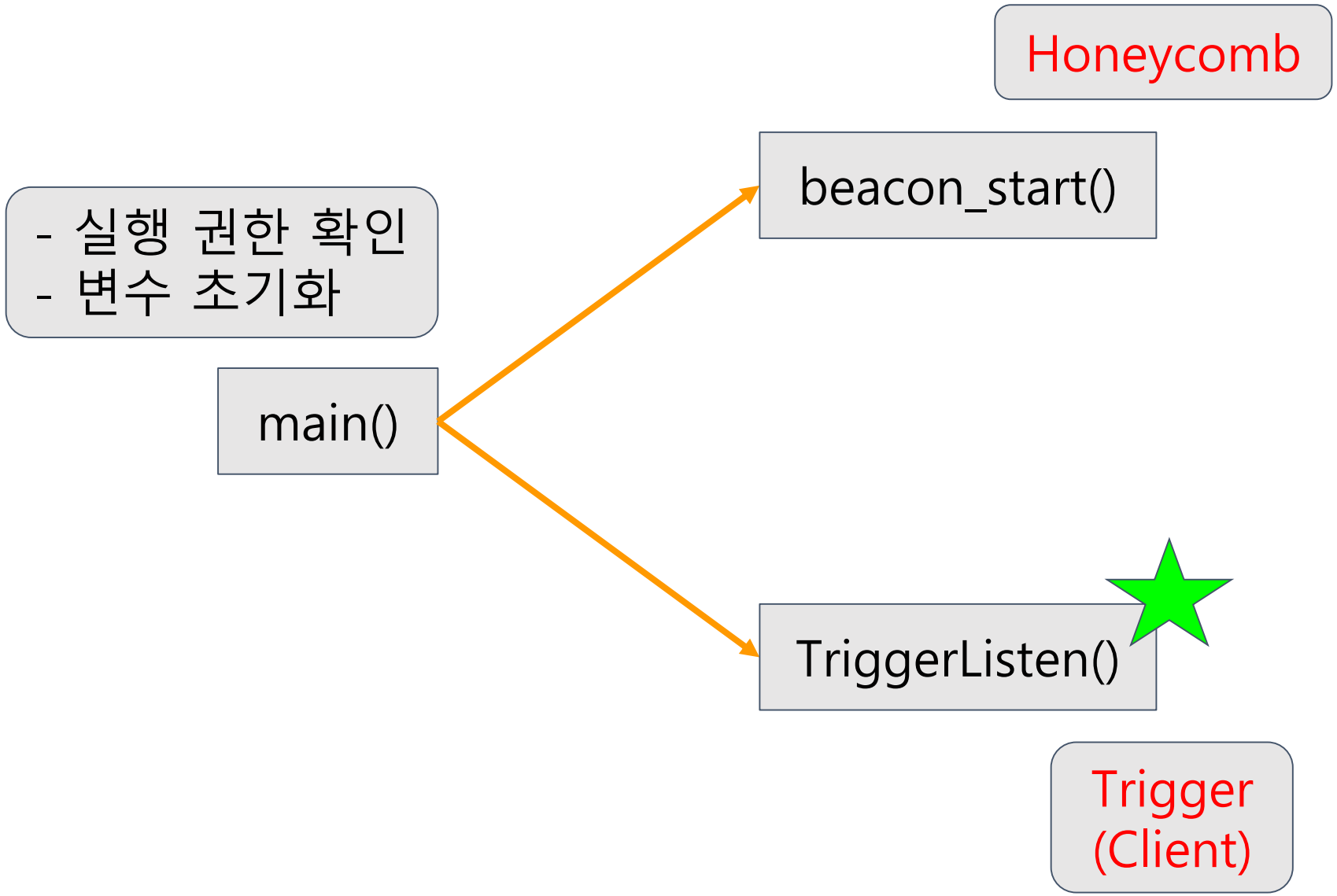
InteractiveMode()



Server

- 지속적으로 beacon에게 데이터 전달
- Trigger packet을 받아 해당 Client와 연결, Command를 받아 해당 작업 수행

main()

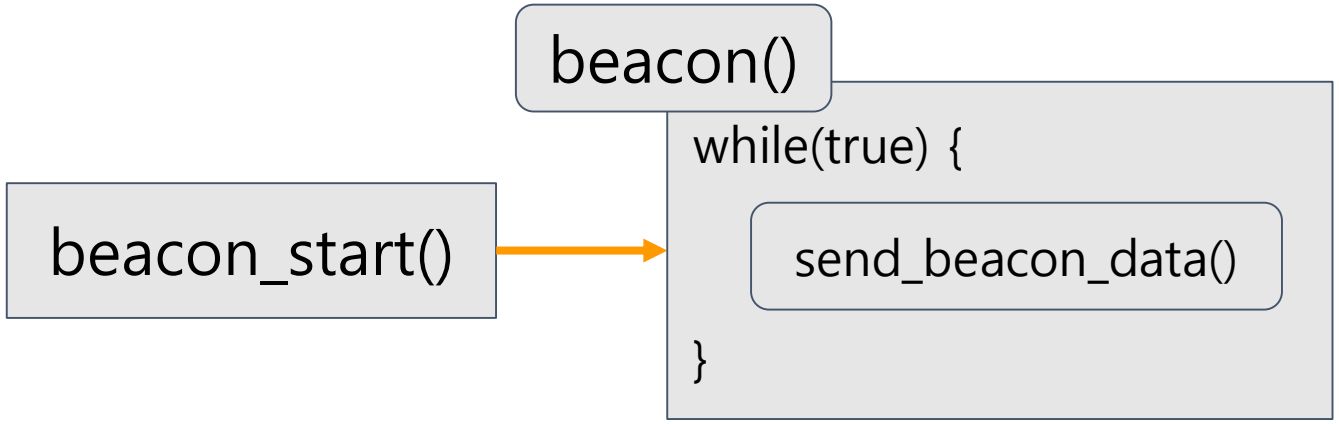

Honeycomb
beacon_start()
- 실행 권한 확인
- 변수 초기화
main()
TriggerListen()
Trigger
(Client)

beacon_start()

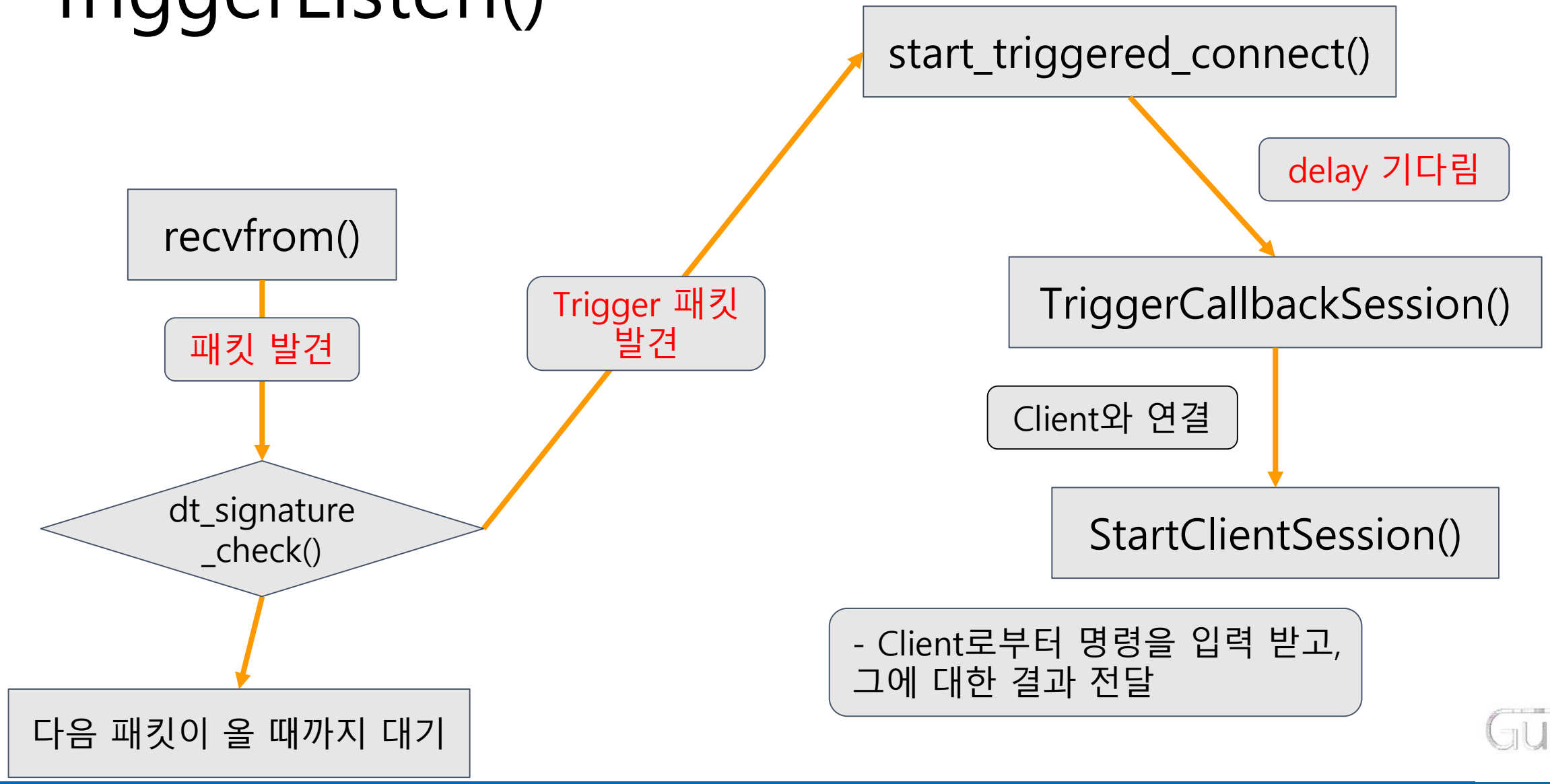
- pthread_create() 함수로 beacon() 함수를 실행하는 쓰레드 생성

- beacon() 함수는 무한 루프를 돌면서 데이터 전달을 위한 변수들 체크 후 send_beacon_data() 호출

- send_beacon_data() 에서는 beacon 타겟과 연결한 후 데이터를 보냄

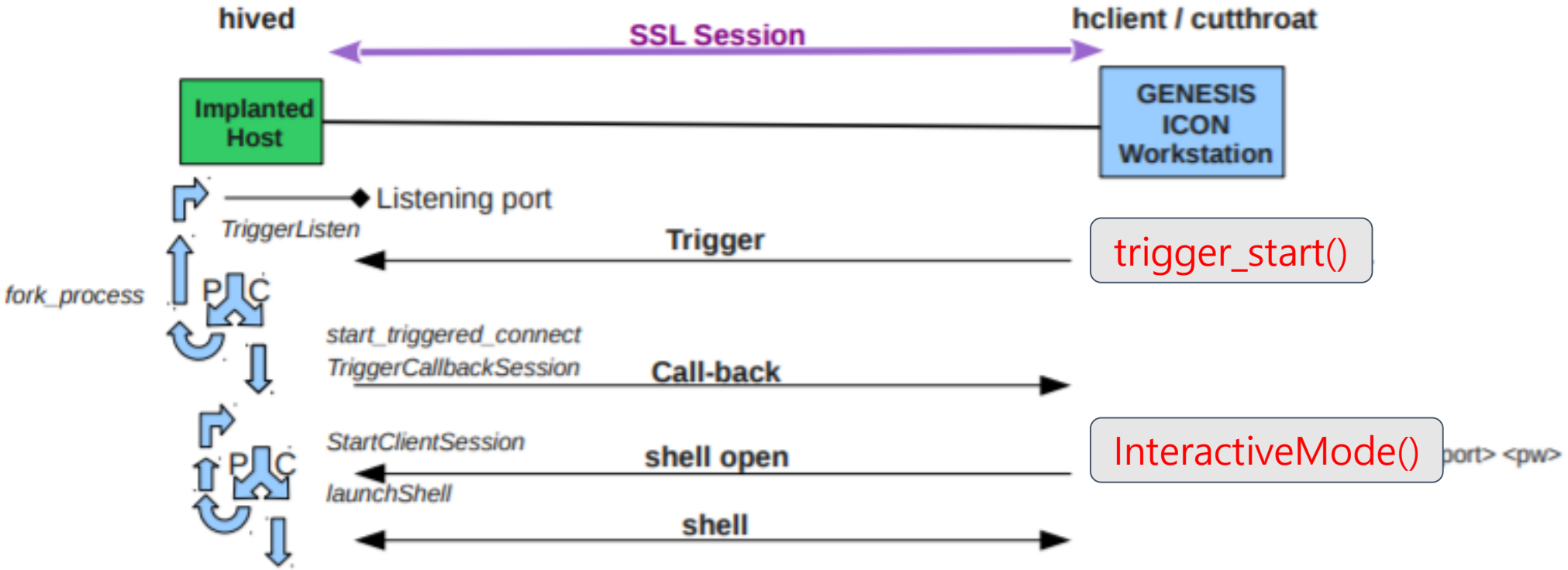


TriggerListen()

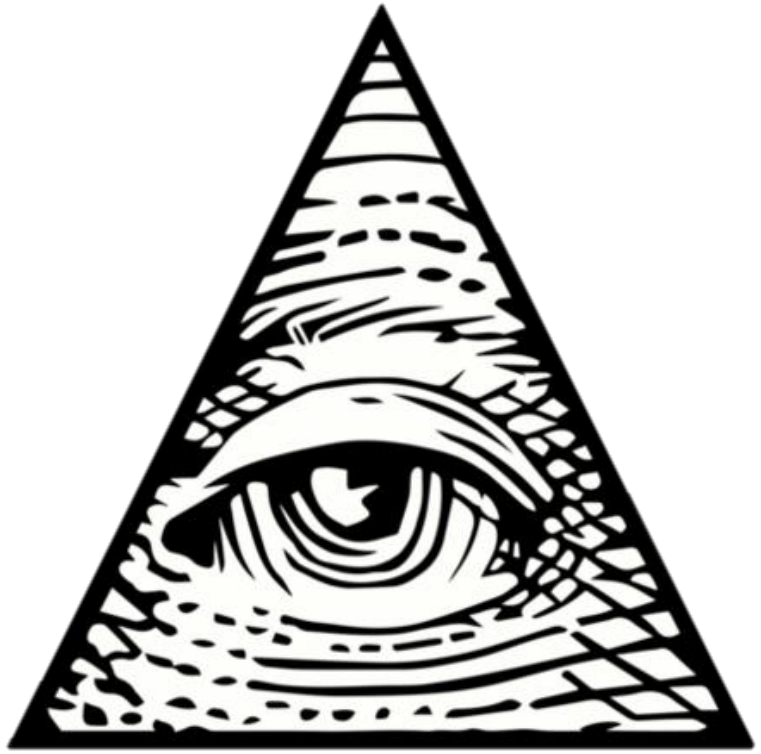


SECRET//NOFORN

Hive Operation



Demonstration



지금 이 순간
당신의 스마트폰도
알 수 없는 데이터를
전송하고 있지는 않나요?

멀웨어 분석 소모임에 관심이 있다면?

- 매주 목요일 오후 6시
- 가입 조건 : X
- 원하는 인재
  - 다양한 침투 방식과 취약점 악용을 분석하는 데 관심있는 사람
  - 동아리비로 맛있는 걸 먹으러 다닐 사람

매주 (목) 오후 6시 302동 식당!
혹은 가디언 회장에게 알려주세요!