**B2-P3**

Filter by basic to pull up http request and tls handshakes. And remove the upnp

Follow tcp steam for the first http request

See it’s a windows nt 6.2 device. NT 6.1 is windows 7.  
Show slide for windows.

**B2-P4**

Follow tcp stream for the first HTTP request to [www.centerofportugual.com](http://www.centerofportugual.com) to show fedora.

**B2-P5**

Filter for basic

Follow TCP stream for either HTTP request to spoonplanet.com

See it is an android 7.1.2 LM-X210APM

Do a quick google search on make and model.

See its an LG-Phoenix 4 mobile phone device.

**B2-P6**

Filter basic

Tcp steram for http request to bostonlybyfoot.org

Iphone running os12-04

**B2-P7**

**Kerberos**

Here are the most basic steps taken to authenticate in a Kerberized environment.

1. Client requests an authentication ticket (TGT) from the Key Distribution Center (KDC)
2. The KDC verifies the credentials and sends back an encrypted TGT and session key
3. The TGT is encrypted using the Ticket Granting Service (TGS) secret key
4. The client stores the TGT and when it expires the local session manager will request another TGT (this process is transparent to the user)

If the Client is requesting access to a service or other resource on the network, this is the process:

1. The client sends the current TGT to the TGS with the Service Principal Name (SPN) of the resource the client wants to access
2. The KDC verifies the TGT of the user and that the user has access to the service
3. TGS sends a valid session key for the service to the client
4. Client forwards the session key to the service to prove the user has access, and the service grants access.

**B3 – P1  
EMAIL!**

Filter for SMTP

Follow TCP stream

Most legitimate email today. Uses some sort of encryption between the mail client and the mail server.

You will see startTTLS and then everything else in encrypted.

**B3-P3**

**Filter for DNS**

**Scroll to Bottom**

**There are corresponding dns queries for the same strings as the HTTP head requests.**

Most often you will only see the DNS queries andnot the HTTP Head requests

Use basic filter and find HTTP hostnames ending with .gvt1.com this is chrome update traffic

Google chrome also generates SSDP traffic. Which is excluded from our basic web filter.

Follow UDP Stream

**B4-P1**

**LOKIBOT**

Filter by basic

See the first POST from manrp.com

Open the tcp steam.

Charon is a discontinued web browser for the inferno operating system.

See the user name of Sarah Rutherford and the hostname of the PC. Rutherford-pc

----------

**B4-P2**

**Formbook**

**Filter by basic**

**SECOND GET REQUEST SPKABO.EXE**

Any url that ends in .exe is suspicious

**Follow tcp stream**

User agent string. MSIE 7.0 is antiquated. (old version of IE)

Executables show up as MZ first two characters are ascii MZ.

As well as this program must be run under win32.

File export >> http objects

Application / x-msdownload. Spkabo.exe

Go back to slide show!

**B4-P5**

Filter by basic.

Follow tcp stream for the first segment with a tcp port 21

Were starting to see some information about the ftp session. STOR hawkeye key logger. Sarah.rutherford.

**FILTER FOR BASIC PLUS AGAIN**

**Follow tcp stream for tcp port 30964**

We can all the user information the keylogger stored.

**FILTER FOR FTP-DATA**

Shows all the items being stored for the ftp data streams.

**GO BACK TO SLIDES to show the STOR**

**LOAD B4-P6**

**FILTER** for ftp-data

Show the info all the requests. And stor.

Filter for [FTP.REQUEST.COMMAND](ftp://FTP.REQUEST.COMMAND)

Show all the requests

Filter for ftp-data

Follow tcp stream for FTP data: 556 bytes.

See the username and the password to his online banking default page.

Follow ftp-stream again and go to the one above it

Show data from ascii to raw.

Save it as a jpg and open it up

Show picture.  
it’s a capture of the infected hosts desktop