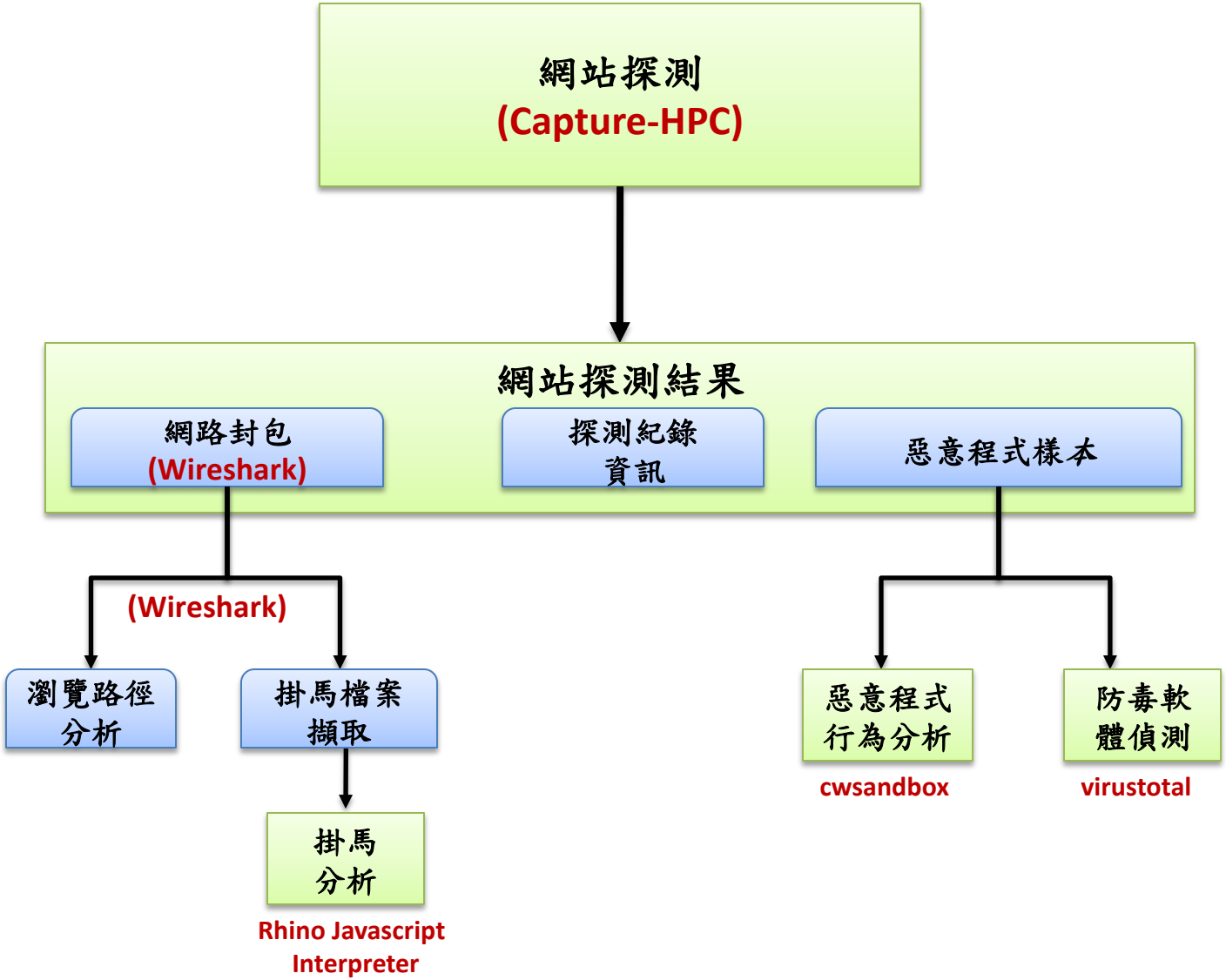
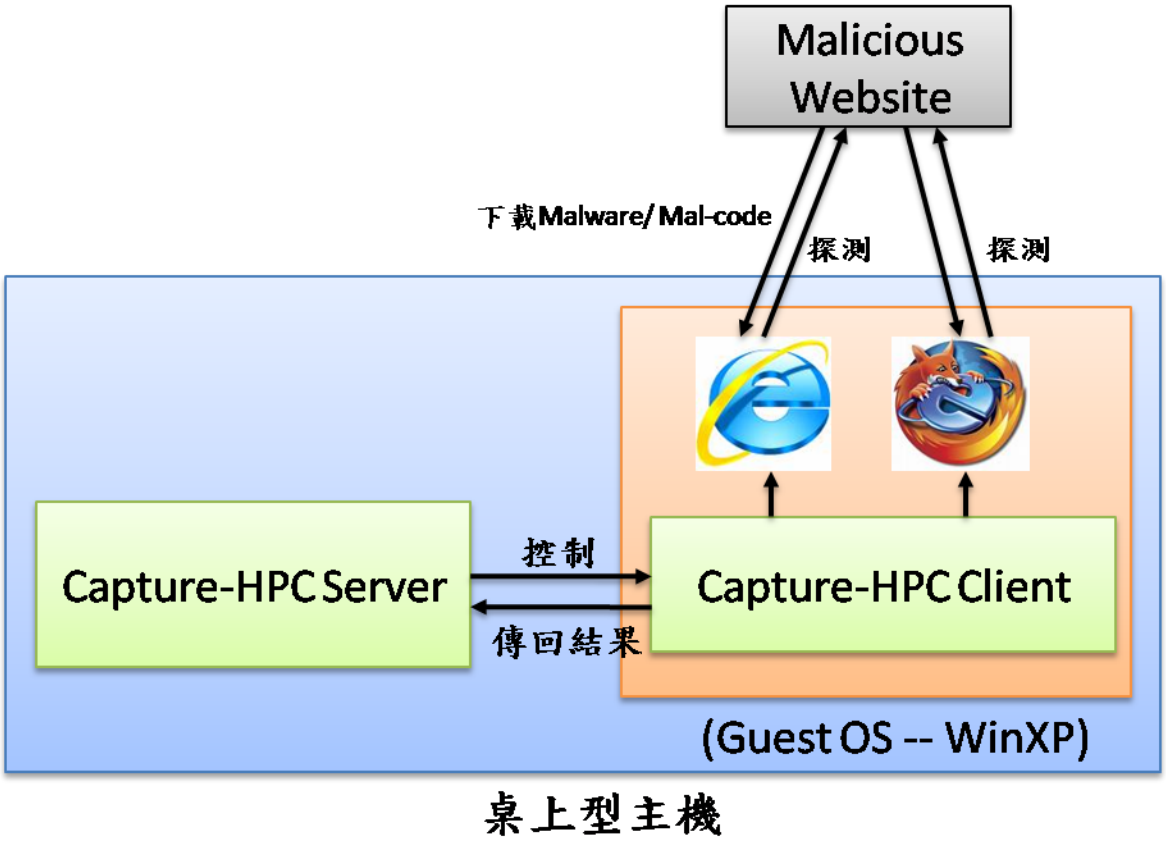
惡意網站與網頁掛馬實作課程

Taiwan Honeynet Project

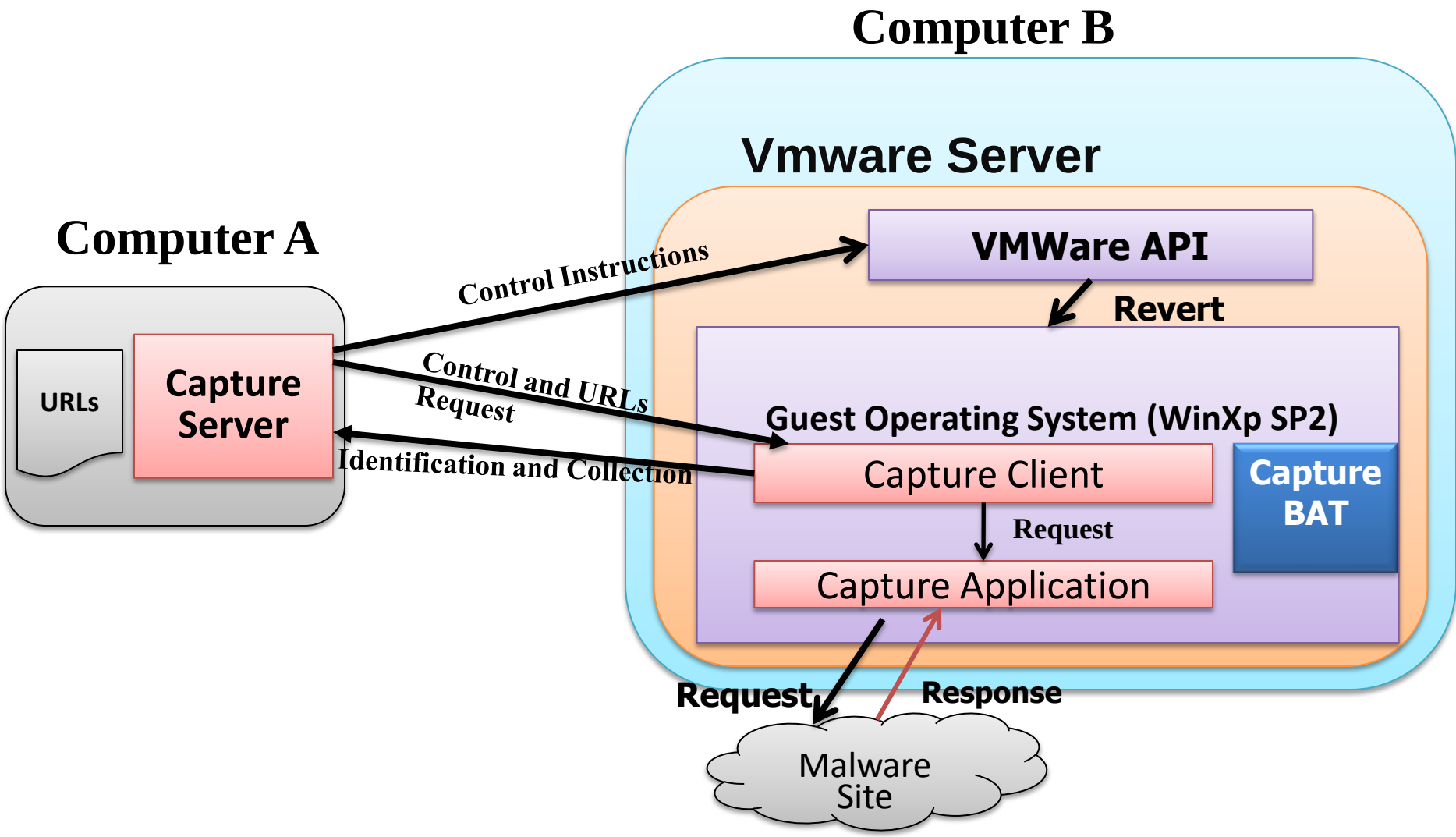
資安分析師 鄭毓芹


網站探測
(Capture-HPC)
網站探測結果
網路封包
(Wireshark)
探測紀錄
資訊
惡意程式樣本
(Wireshark)
瀏覽路徑
分析
掛馬檔案
擷取
惡意程式
行為分析
防毒軟
體偵測
cwsandbox
virustotal
掛馬
分析
Rhino Javascript
Interpreter

Phase 1: 惡意網站探測



Capture-HPC Architecture



Capture-BAT 介紹

- 系統行為分析工具
- 運行於Win 32 OS
- 使用API hooking 來監控Registry, Process與File狀態的變化。
- 提供exclusion lists來過濾正常的事件
- 提供系統行為監控的log，幫助後續分析

註: Capture-HPC 以Capture-BAT為基礎，進行發展，控制Client Application對Remote Server 探測，藉由Capture-BAT來對整體系統狀態改變進行監控:

Step 1: 安裝步驟: 桌上型主機

- **安裝Java執行環境**
- **安裝Capture-HPC Server**
- **安裝VMware-Server 1.0.6**
  - Step 1: 本機電腦(任何OS皆可)，安裝Vmware server，VMware-server-installer-1.0.6-91891.exe
- **開啟Firewall Port 902 (By Pass)**
  - Step 2: Vmware將會開啟Port 902接受Capture Server的命令進行探測，因此本機電腦防火牆須開啟Port 902
- **載入Guest OS (WinXP Sp2)**
  - Step 3: 安裝Guest OS於VMware Server上，Guest OS限定是Windows XP SP2，其他版本會有問題 (網路連接選擇Custom → VMnet8 (NAT))
- **停止防毒軟體**

安裝步驟: Guest OS (WinXP SP2)

- **Capture-HPC Client 運作於虛擬機器Guest OS中**
  - Step 1: 安裝Vmware Tools
  - Step 2: 安裝 Micosoft Visual C++ 2008 Redistributable Libraries (SP0) vcredist_x86.exe
  - Step 3: GuestOS(WinXP SP2)中，安裝 winpcap 4.0.2
  - Step 4: 安裝Capture-Client程式，CaptureClient-Setup.exe
  - Step 5: 安裝其他需要的程式，ex: Wireshark、Firefox
  - Step 6: 設定登入帳號密碼(開始→控制台→使用者帳戶→新增密碼)
  - Step 7:關閉Windows Update (控制台→自動更新→關閉自動更新)
  - Step 8: 瀏覽器功能與安全性設定
    - 安裝Adobe Flash Player
    - IE: 工具→快顯封鎖程式→關閉
    - IE: 網際網路選項→安全性→ 自訂等級→ 啟用功能
    - IE: 隱私權→接受所有的Cookies
    - 清除Cache 與暫存檔
  - Step 9:安裝完所有需要的工具與修改設定後，一定要做Take Snapshot **(千萬要記得!)**

Step 2: Capture-HPC Server 設定說明

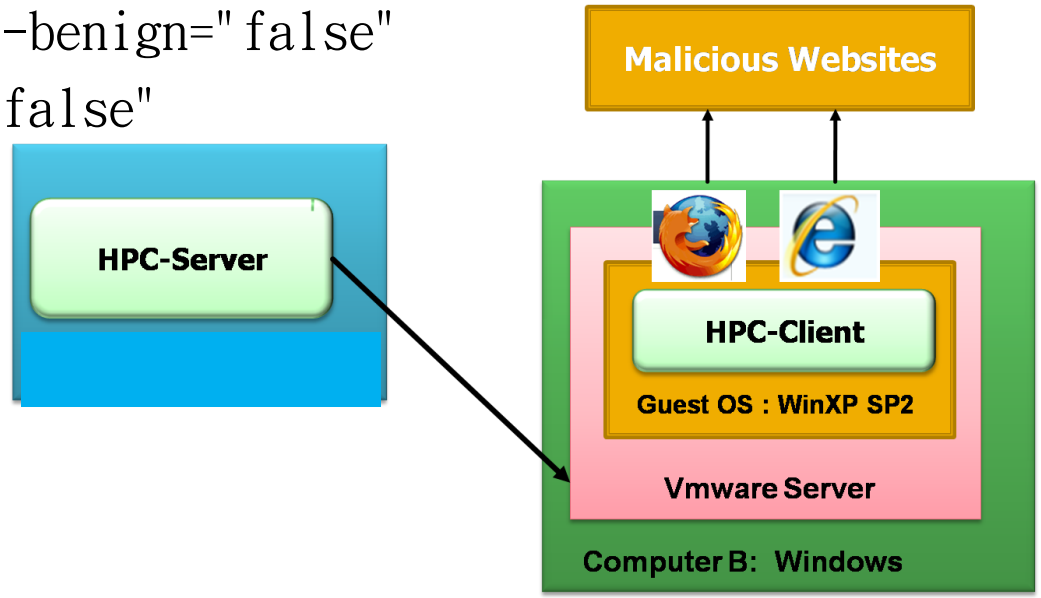
編輯: config.xml 檔案

- 分為兩大部分: Global options 與 Virtual Machine 資訊

Global options

< global collect-modified-files="true “

- client-default= “iexplore” iexplore bulk -> iexplore
- client-default-visit-time= “300”
- capture-network-packets-malicious="true"
- capture-network-packets-benign="false"
- send-exclusion-lists= “false"
- terminate= “false"
- group_size="10"



- vm_stalled_after_revert_timeout=“300” HPC Server送出vix api ，HPC-Client最長回應時間
- revert_timeout=“300” HPC Client執行revert時，最常多久之內要完成
- client_inactivity_timeout=“60” 送出Ping資訊，等待回應
- vm_stalled_during_operation_timeout=“300” HPC Server送出URL ，HPC-Client最長回應時間
- same_vm_revert_delay=“6” 送出revert 給同一台vmware上有多個HPC-Client時，delay時間
- different_vm_revert_delay=“24” 送出revert給不同vmare上的HPC-Client，delay時間

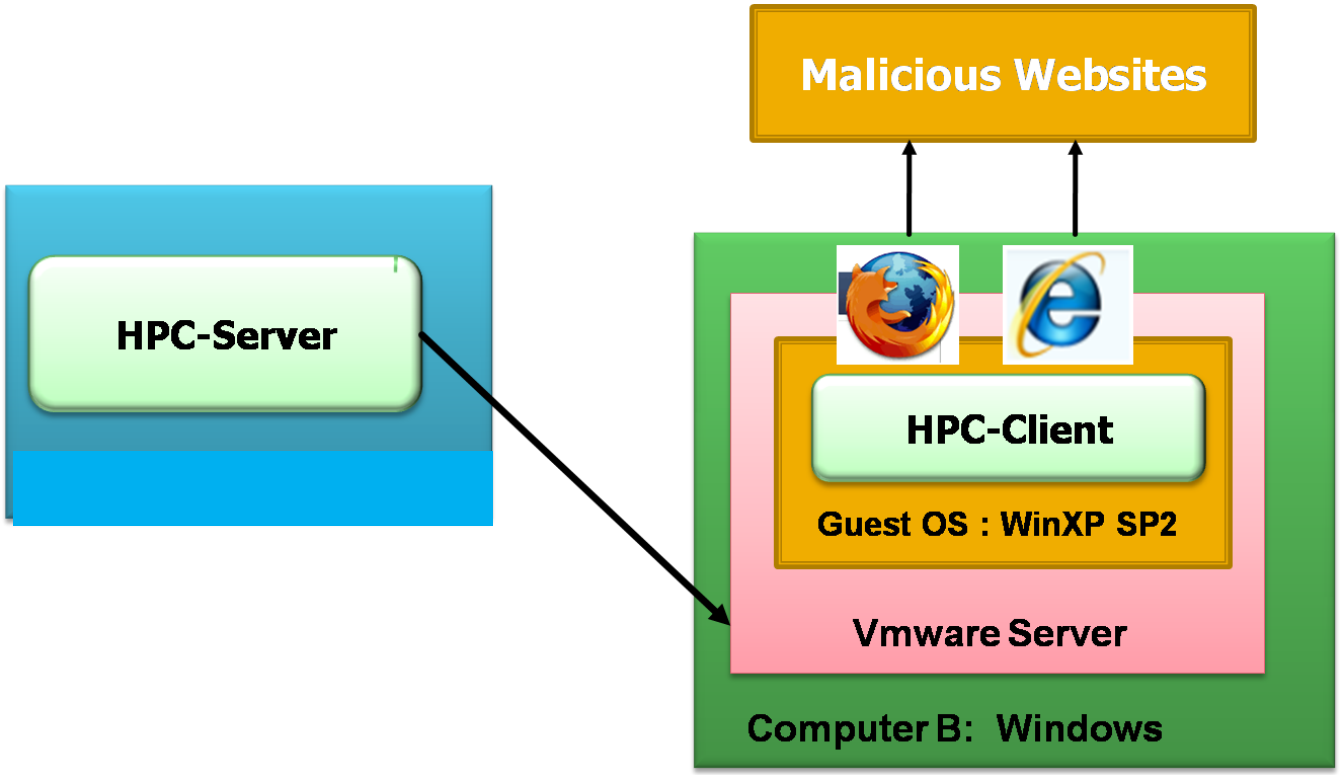
/>

Virtual Machine Server

```
<virtual-machine-server
 type= “vmware-server”
  address= “VMware Server 所在主機IP”  port= “902 (Listen Port) “
 username=”  VMware Server 所在主機登入帳號  ”
 password= “ VMware Server 所在主機登入密碼 ">
<virtual-machine
  vm-path= “Vmware上GuestOS 路徑
      C:\Virtual Machines\xxx\Windows XP Professional.vmx"
      client-path= “HPC-Client程式路徑
  C:\Progra~1\Capture\CaptureClient.bat"
      username= “GuestOS 登入帳號 HPC “
      password=”  GuestOS 登入密碼HPC@nchc “
 />
 </virtual-machine-server>
```

執行

- java -Djava.net.preferIPv4Stack=true –jar CaptureServer.jar
  -s <控制端IP Lisening address>:<IP Listening port>
  -f input_url.txt



Log Information on Capture-Server

- Safe.log : the clear and deemed benign URLs
- Process.log : visiting information for URLs
- Error.log : URLs that could not be visited
- States.log: the performance of the Capture-System
- Malicious.log : the list of deemed malicious URLs
- Server_timestamp.log : a list of state changes for visiting each URLs
- Server_timestamp.zip: the files with modified or deleted off on the client machine during the interaction with a malicious servers

參考文件列表

- Capture-Client Readme
- Capture-Server Readme
- Capture Communication Protocol
- Capture FAQ : https://projects.honeynet.org/capture-hpc/wiki/FAQ
- Preprocessor_README
- TroubleshootingGuide