

网络取证与网络取证分析技术

北京大学 刘欣



议题

□ 计算机取证与网络取证

□ 网络取证概述

□ 网络取证相关研究

□ 网络取证分析技术

计算机取证的发展历史

□ 计算机取证(Computer Forensics)

- 单机取证：媒质分析（Media analysis）指检查单机系统以便发现犯罪案件中的数字证据的过程。
- 网络取证(Network forensics)：此类的取证过程以抓取网络流量并对之进行分析为特征
- 取证计算（Forensic Computing）：此阶段所涉及的数字证据来源不再局限于计算机，还包括DC，DV，PDA等多种电子设备。

网络取证的定义

- 网络取证即是从多样化、动态传输中的数据源里以科学可证实的技术来获取、融合、识别、检查、关联、分析及归档数字证据，其目标是发现与案情相关企图关联的事实或恶意非授权行为及为重构事件提供信息与依据。

不同观点下的网络取证



Application Viewpoint

Internet Browser forensics
Email forensics
Register File forensics
Application software forensics
Virus forensics
Worm forensics
File slack, Erased files and Swap files

System Viewpoint

UNIX File System forensics
Windows File System forensics
Log system forensics
Audit system forensics

Hardware Viewpoint

PC forensic
PDA forensics
Printer forensics
Router forensics
Firewall forensics

Processing

Victim side forensics
Intermediate side forensics
Attacker side forensics

网络取证中证据源

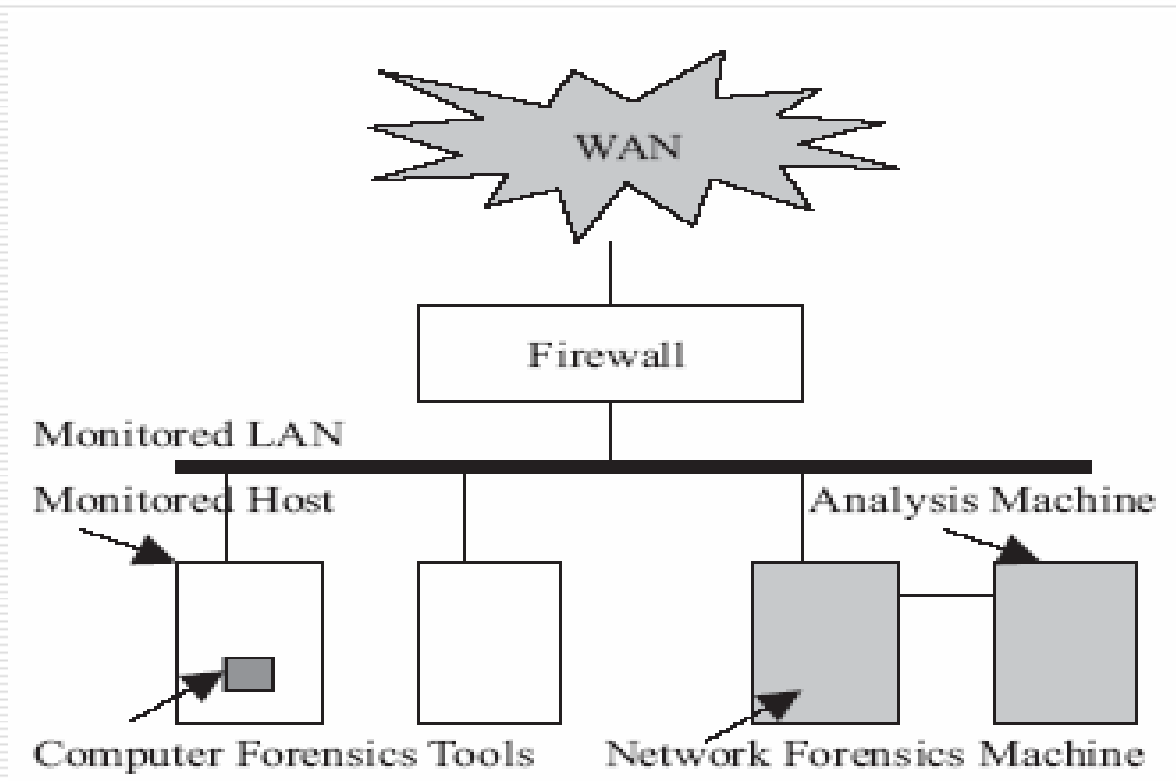
From End Sides (attacker side or victim side.)	Operation system audit trail System event log Application event log Alert log file File MAC (Modify/Access/Create) timestamp Recovery data File slack, Erased files and Swap files
From Intermediate Side	Network traffic data packets Firewall log IDS log Access control system log Router log Firewall log Internet Information

网络取证相关技术

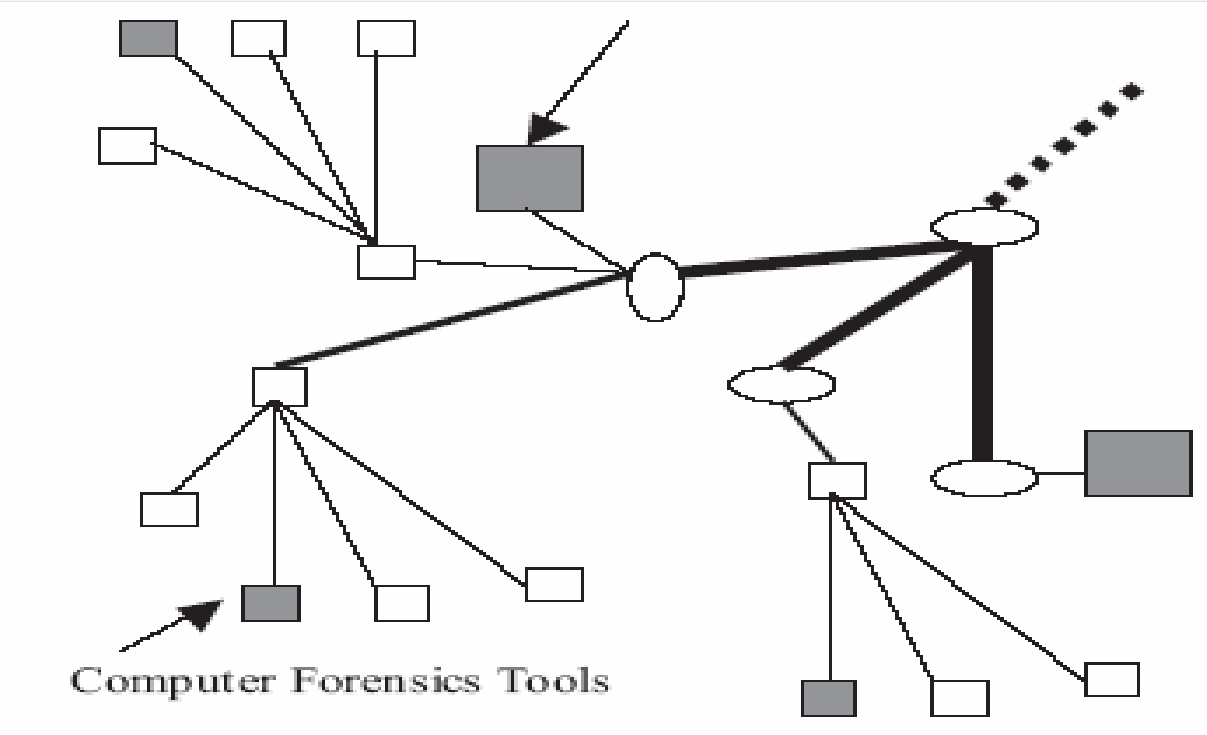
TABLE 3 Network Forensics Techniques

Capture	Copy	Transfer	Analysis	Investigation	Presentation
Access Control, Digital Signature, Digital Digest, Digital Timestamps, Encryption					
Audit System Data, Log System Data, Network Management Data, Traffic Monitor, Topdump/Windump, Honeypot/Honeynet, IDS Alert	Disk Image/Clone, MD5/SHA	SSL, VPN, GB LAN, High Speed Channel, S/N	FAT Analysis, Data Mining, Data Fusion, Data Recovery, Protocol Analysis, Data Hiding Discovery, Reverse Engineering, Decryption	IP Trace back, Mapping to Geographic Location, Scanning, Network Survey, OS Fingerprint, Remote Forensics	Visualization, Documentation, Human- Machine Interaction, Computer Graphics, Remote Access, Remote Management

内部网取证体系结构



InterNet取证体系结构



网络取证相关研究

- 网络取证平台研究
- 网络取证模型研究（以基于代理的结构为代表）
- 网络取证专用协议开发
- 网络取证分析技术研究

网络取证分析所面临的挑战

- 入侵证据源不能满足取证调查的需要，分析过程常被海量低质量数据淹没。
- 攻击过程复杂化。

网络取证分析系统应满足的特性

- 短暂的响应时间。
- 友好的界面：便于结合专家观点与带外信息进行取证分析。

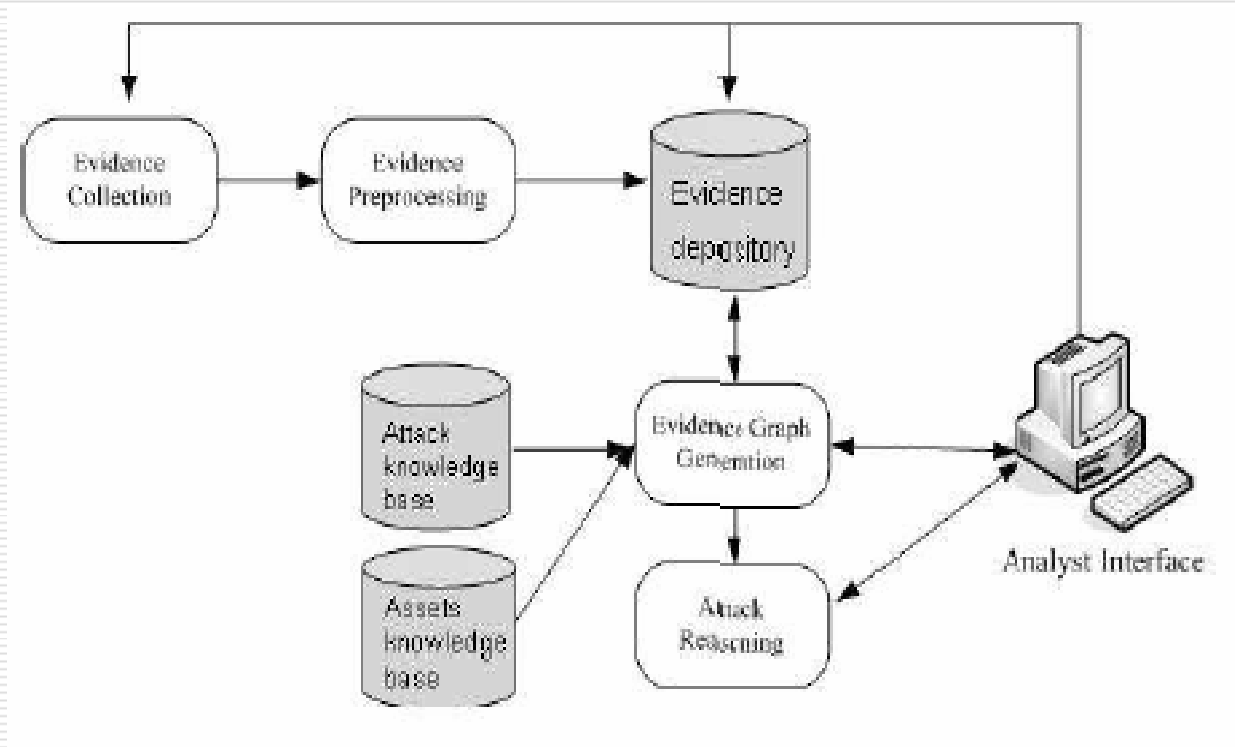
网络取证分析的目标

- 攻击源（单机/组）的确定
- 攻击场景的重构

攻击相关角色

- 攻击者 (Attackers)
- 受害者 (Victims)
- 跳板 (Stepping Stones)
- 背景攻击者 (Background Attackers)

网络取证分析体系结构



网络取证分析：证据处理

□ Leader-Follower报警聚合算法

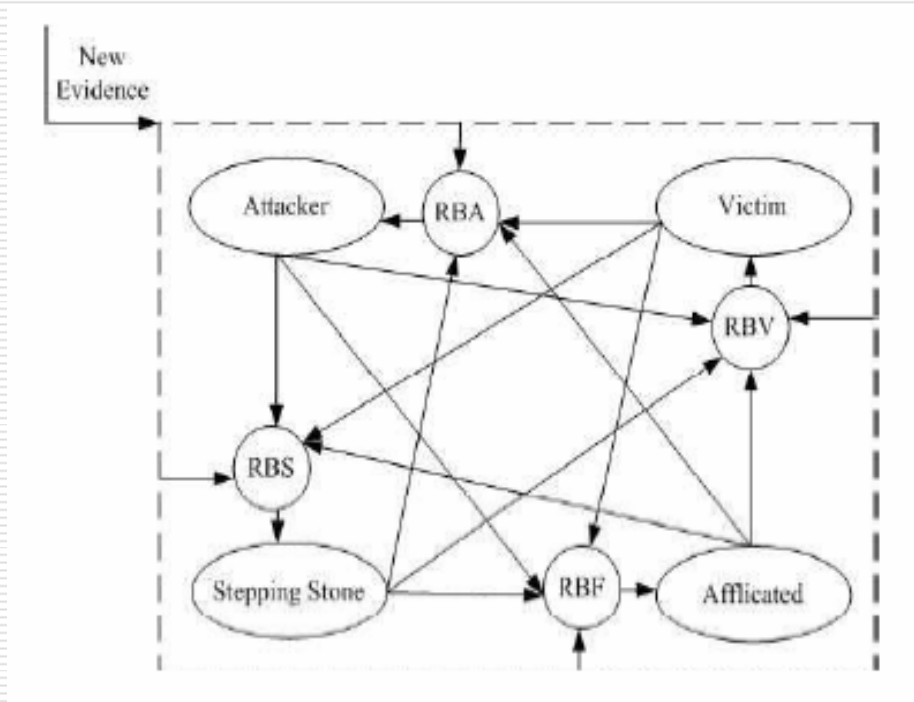
```
input : A set of raw alerts  $r_1 \dots r_n$ , time limit  $T$ 
output: A set of hyper alerts  $h_1 \dots h_m$ 
begin
   $h_1 \leftarrow r_1$ ;
   $m \leftarrow 1$ ;
  for  $i \leftarrow 2$  to  $n$  do
     $merged \leftarrow 0$ ;
    for  $j \leftarrow 1$  to  $m$  do
      if  $r_i.sourceaddr = h_j.sourceaddr \ \&\&$ 
         $h_j.destaddr = r_i.destaddr \ \&\&$ 
         $h_j.class = r_i.class \ \&\&$ 
         $h_j.starttime - T \leq r_i.detecttime \leq$ 
         $h_j.endtime + T$  then
         $h_j.starttime \leftarrow$ 
         $min(h_j.starttime, r_i.detecttime)$ ;
         $h_j.endtime \leftarrow$ 
         $max(h_j.endtime, r_i.detecttime)$ ;
         $r_i.hyperid \leftarrow h_j.id$ ;
         $h_j.count \leftarrow h_j.count + 1$ ;
         $merged \leftarrow 1$ ;
        break;
      end
    end
    if  $merged = 0$  then
       $m \leftarrow m + 1$ ;
       $h_m \leftarrow r_i$ ;
       $h_m.count \leftarrow 1, h_m.HyperID \leftarrow m$ ;
    end
  end
end
```

网络取证分析：证据图构建

```
input : Stream of evidence in time order
output: Evidence graph  $G$ 
begin
  foreach evidence  $E$  in stream do
    foreach host  $V$  affected by  $E$  do
      if  $V$  does not exist in  $G$  then
        CreateNode ( $G, V$ );
      end
    end
    CreateEdge ( $G, E$ );
    foreach host  $V$  affected by  $E$  do
      UpdateNode ( $E, V$ );
    end
  end
end
```

网络取证分析：本地推理

□ RBFCM模型



网络取证分析：本地推理

□ 规则集

If *BackOrifice* is detected
Then *Victim* state is activated highly.

If exploit of weight w initiates from *self*
Then *Attacker* state value is increased by w .

If *Victim* state is activated highly and
Attacker state is activated highly and
 $AT(T_{activate}) > VI(T_{activate})$
Then *Stepping Stone* state is activated highly.

If ftp connection to host n is detected and
 $Victim(n) = high$ and
 $T_{ftp} - T_{activate}(VI) < T_{limit}$
Then *Affiliated* state value is activated medium.

网络取证分析：全局推理

□ 两步骤：

■ 种子选择

- 基于结点状态及上下文选择种子
 - ✓ 选择受害者
 - ✓ 选择本地推理过程中信任域里处于攻击者状态的主机
- 基于图矩阵选择种子

■ 群组扩张

网络取证分析：全局推理

□ 攻击群组扩张算法

```
input : Evidence graph  $G$ , initial seed node  $v_0$  and  
        distance threshold  $d$   
output: The group of nodes  $group$   
begin  
     $group \leftarrow v_0$ ;  
     $neighbors \leftarrow \emptyset$ ;  
     $candidates \leftarrow \emptyset$ ;  
    repeat  
        foreach node  $v$  in the set  $group$  do  
             $neighbors \leftarrow \text{FindNeighbour}(G, v)$ ;  
             $candidates \leftarrow candidates \cup neighbors$ ;  
        end  
        foreach node  $v$  in the set  $candidates$  do  
             $v.distance \leftarrow \text{GetDistance}$   
                 $(v, group)$ ;  
        end  
         $new \leftarrow \text{RankCandidates}(candidates, d)$ ;  
         $group \leftarrow group \cup new$ ;  
    until no new member is found;  
end
```

网络取证分析相关实验

□ 实验场景角色分配

Attacker	192.168.21.3
Stepping Stone 1	192.168.25.3
Stepping Stone 2	192.168.22.4
Victim	192.168.23.4
FTP Relay	192.168.24.4

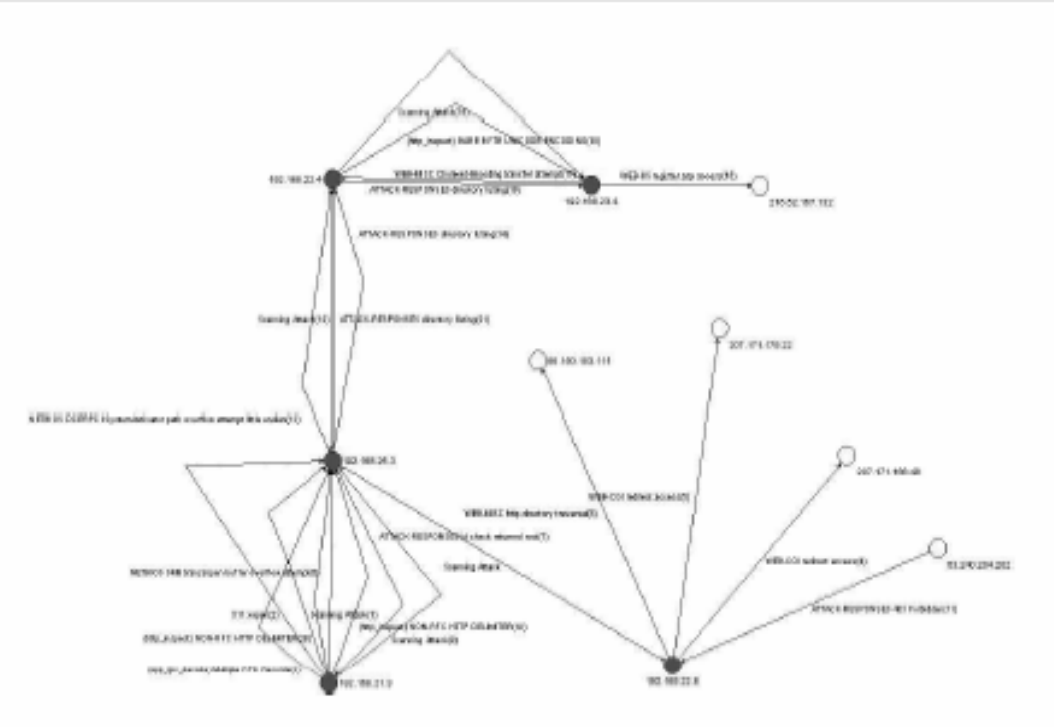
网络取证分析相关实验

□ 攻击场景

1. Samba remote buffer overflow attack against stepping stone 1 from attacker.
2. Download attack tools from ftp relay to stepping stone 1 and start an Netcat backdoor on stepping stone 1.
3. Windows DCOM remote buffer overflow attack against stepping stone 2 from stepping stone 1.
4. Download attack tools from ftp relay to stepping stone 2 and starts a backdoor on stepping stone 2.
5. Frontpage Server 2000 buffer overflow attack against the victim from stepping stone 2.
6. Download backdoor program from ftp relay to victim and starts backdoor on victim.
7. Transfer data from the victim to the ftp relay and close backdoor connections.

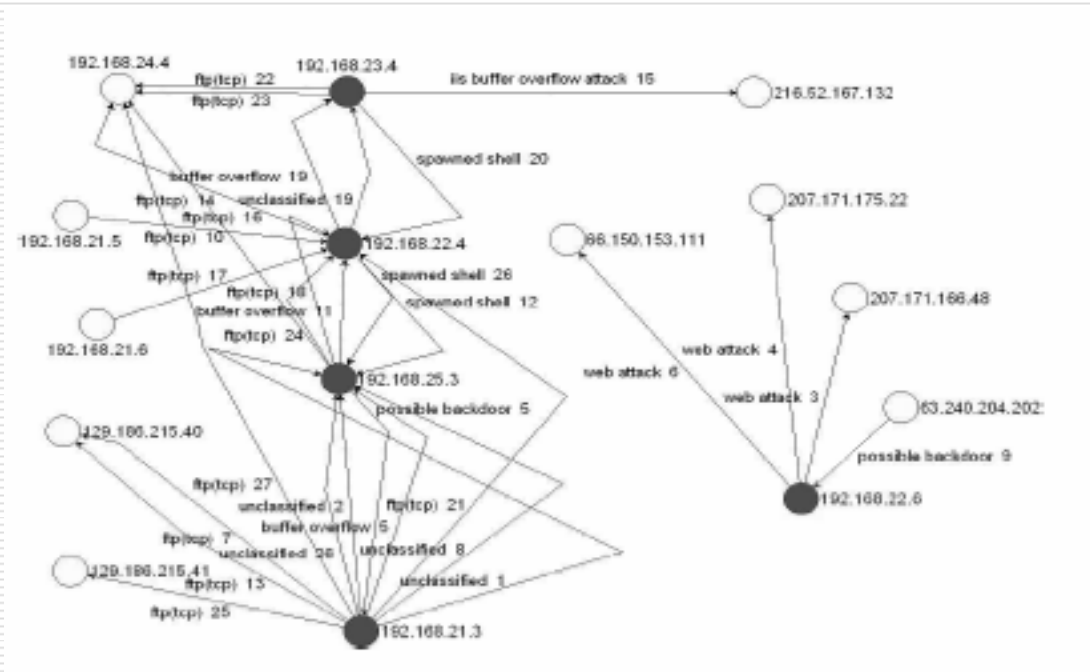
网络取证分析相关实验

□ 基于基本证据的证据图



网络取证分析相关实验

□ 基于二阶证据的更丰富证据图



网络取证分析相关实验

□ 本地推理结论

Host	degree	AT	VI	SS	AF
192.168.22.4	12	0.85	0.85	0.87	0.84
192.168.25.3	12	0.85	0.80	0.94	0.84
192.168.21.3	11	0.80	0	0	0.84
192.168.23.4	6	0.69	0.85	0	0.82
192.168.24.4	5	0	0	0	0.84
192.168.22.6	4	0.85	0.50	0	0
129.186.215.40	2	0	0	0	0.81
129.186.215.41	1	0	0	0	0.69
192.168.21.5	1	0	0	0	0.70
192.168.21.6	1	0	0	0	0.70
207.171.166.48	1	0	0.67	0	0
207.171.175.22	1	0	0.67	0	0
66.150.153.111	1	0	0.67	0	0
216.52.167.132	1	0	0.69	0	0
63.240.204.202	1	0	0.71	0	0

网络取证分析相关实验

□ 全局推理结论

Host 1	Host 2	Distance
192.168.25.3	192.168.22.4	0.23
192.168.21.3	192.168.25.3	0.24
192.168.23.4	192.168.22.4	0.43
192.168.23.4	192.168.24.4	0.59
192.168.21.3	129.186.215.40	0.67
63.240.204.202	192.168.22.6	1.11
192.168.21.3	192.168.22.4	1.18
192.168.21.6	192.168.22.4	1.19
192.168.22.4	192.168.24.4	1.19
192.168.21.5	192.168.22.4	1.19
192.168.21.3	192.168.24.4	1.25
192.168.23.4	216.52.167.132	1.25
192.168.21.3	129.186.215.41	1.27
192.168.25.3	192.168.24.4	1.27
192.168.22.6	207.171.175.22	1.43
192.168.22.6	207.171.166.48	1.43
192.168.22.6	66.150.153.111	1.43

谢 谢 !