CSI Maui: Forensics in the Case of the Attacked Browser

Share Session

Session 10393

Laura Knapp
WW Business Consultant
Laurak@aesclever.com

Background

Incident Evaluation

Trace Evaluation

What is Computer Forensics

- Computer forensics involves the preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/or root cause analysis

- Network or TCP/IP forensics involves the preservation, extraction, documentation and interpretation of TCP/IP data for evidentiary and/or root cause analysis

- Doesn't prevent computer crime

- After the fact investigation

- Forensics experts follow clear, well-defined mythologies and procedures

What is Network Forensics

- Network forensics entails monitoring network traffic and determining if there is an attack and if so, determine the nature of the attack
- Key tasks include traffic capture, analysis and visualization
- Network forensics systems can be one of two kinds:
  - *"Catch-it-as-you-can" systems*, in which all packets passing through a certain traffic point are captured and written to storage with analysis being done subsequently in batch mode
  - *"Stop, look and listen" systems*, in which each packet is analyzed in a rudimentary way in memory and only certain information saved for future analysis

Employee Trust

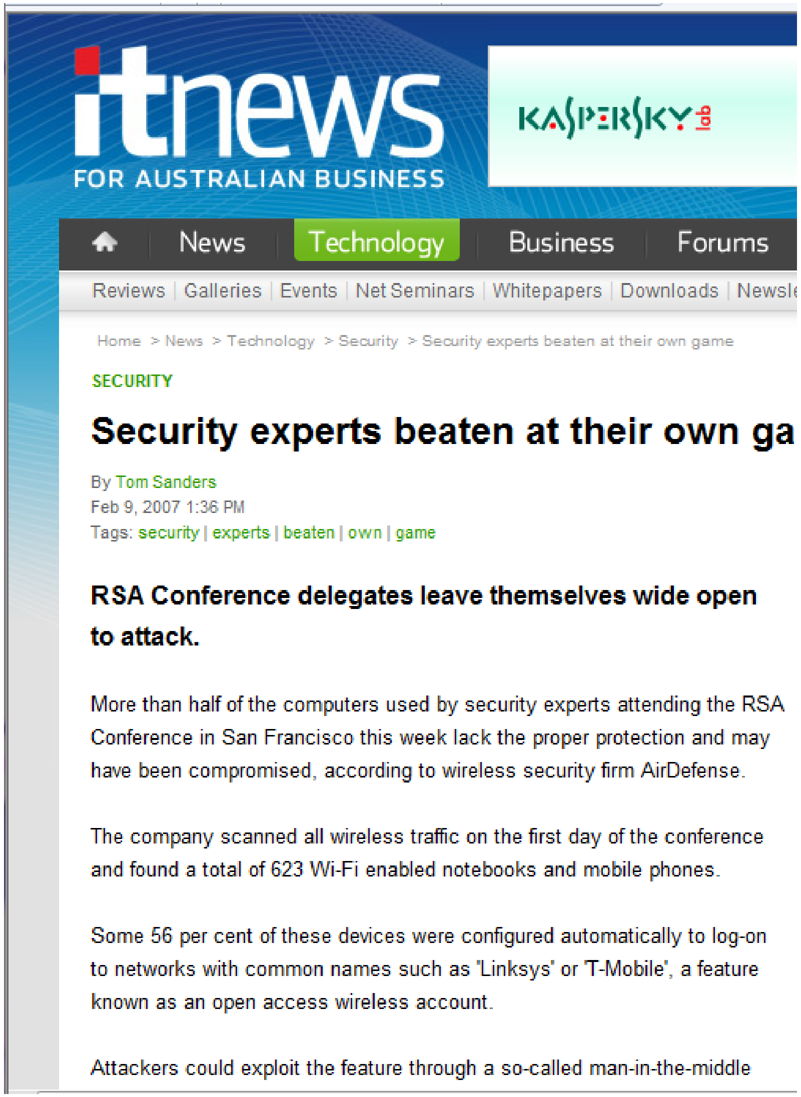
- Construction Company

- Senior IT person also in charge of security
- Used cost issue to convince upper management to let him store data at his home rather than pay for external off-site storage
- Conflict arose between the Employee and Employer
- Employee sent email's to clients of the construction company indicating he had personal information
- Took 6 months to shut down the rogue employee after the employee used the internet to threatened people at which time the FBI became involved
- Construction company was fundamentally out of business

http://www.cio.com/article/454614/IT_Security_Pros_Share_Horror_Stories

Process Vulnerability

•Security administrator asked to shut off web security monitoring system as it was interfering with marketing’s ability to access the corporate web site for creation and editing.
•Director said ‘switch off’ not….. find a work around…find a fix….just ‘switch it off’
•Users quickly found that out that all web controls were no longer active
•A report surfaced that a user had used a desktop to access porn
•Due to the use of generic accounts tracking activity to a user was not possible
•Took 3 months, CCTV, internal and external police to finally catch the culprit
•To make matters worse the company dropped any further work on a security framework and made the security positions obsolete


itnews
FOR AUSTRALIAN BUSINESS
KASPERSKY lab
News
Technology
Business
Forums
Reviews | Galleries | Events | Net Seminars | Whitepapers | Downloads | Newsle
Home > News > Technology > Security > Security experts beaten at their own game

SECURITY

Security experts beaten at their own ga

By Tom Sanders
Feb 9, 2007 1:36 PM
Tags: security | experts | beaten | own | game

RSA Conference delegates leave themselves wide open to attack.

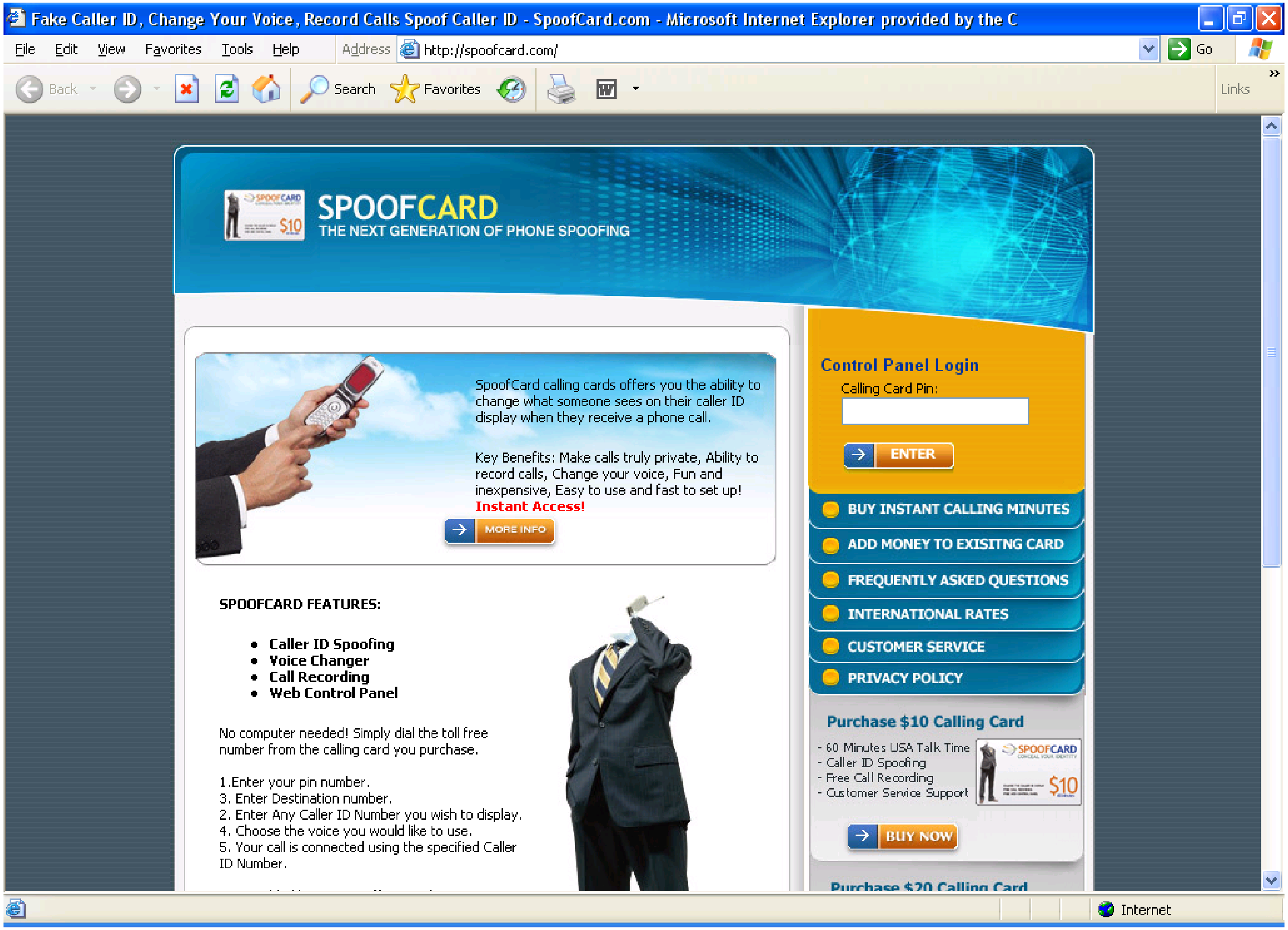
More than half of the computers used by security experts attending the RSA Conference in San Francisco this week lack the proper protection and may have been compromised, according to wireless security firm AirDefense.

The company scanned all wireless traffic on the first day of the conference and found a total of 623 Wi-Fi enabled notebooks and mobile phones.

Some 56 per cent of these devices were configured automatically to log-on to networks with common names such as 'Linksys' or 'T-Mobile', a feature known as an open access wireless account.

Attackers could exploit the feature through a so-called man-in-the-middle

- •RSA conference 2007
- •Over half the computers lacked proper protection
  - •Many configured to automatically log on to WiFI networks like ‘Linksys’ ‘T-Mobile’
- • Five rogue networks mimicked common hotspot names
  - •These could easily insert man in the middle routines and capture data
- •The RSA conference had a SAFE WIFI network but it was toooooo complex to use and the help desk line was long and slow


Fake Caller ID, Change Your Voice, Record Calls Spoof Caller ID - SpoofCard.com - Microsoft Internet Explorer provided by the C
File Edit View Favorites Tools Help
Address http://spoofcard.com/
Go
Back
Search
Favorites
Links
SPOOFCARD
THE NEXT GENERATION OF PHONE SPOOFING
MORE INFO
Control Panel Login
Calling Card Pin:
ENTER
BUY INSTANT CALLING MINUTES
ADD MONEY TO EXISITNG CARD
FREQUENTLY ASKED QUESTIONS
INTERNATIONAL RATES
CUSTOMER SERVICE
PRIVACY POLICY
BUY NOW
Internet

SpoofCard calling cards offers you the ability to change what someone sees on their caller ID display when they receive a phone call.

Key Benefits: Make calls truly private, Ability to record calls, Change your voice, Fun and inexpensive, Easy to use and fast to set up! **Instant Access!**

SPOOFCARD FEATURES:

- **Caller ID Spoofing**
- **Voice Changer**
- **Call Recording**
- **Web Control Panel**

No computer needed! Simply dial the toll free number from the calling card you purchase.

1.Enter your pin number.
3. Enter Destination number.
2. Enter Any Caller ID Number you wish to display.
4. Choose the voice you would like to use.
5. Your call is connected using the specified Caller ID Number.

Purchase $10 Calling Card

- 60 Minutes USA Talk Time
- Caller ID Spoofing
- Free Call Recording
- Customer Service Support

Purchase $20 Calling Card

2009 Litigation Highlights

Starwood v. Hilton (2009) - Complaint alleging that 2 former Starwood execs looted >100k Starwood computer files.

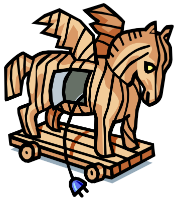
U.S. v. Chung (2009) – Boeing employee convicted at trial for passing trade secrets to Chinese government for 30 years. Co-defendant convicted and jailed for 24 years; Chung, 74 years old, received 15 years in prison.

-US v. Zhu (2009) – Indictment alleging Chinese national employed as engineer at US environmental company stole software from his employer and sold modified version to Chinese government.

US v. Lee (2009) – Former technical director of paint and coating company quit 2 weeks after return from business trip to China; discovered downloaded trade secrets, deleted files, one way ticket from Chicago to Shanghai.

Vistakon v. Bausch & Lomb (2009) – Subsidiary of J&J alleges that B&L misappropriated trade secrets in an effort to recruit sales force to bring new contact lens product to market quickly.

The Impact of a Digital Crime



- Disruption to organizational routines and processes
- Direct financial losses through information theft and fraud
- Decrease in shareholder value
- Loss of privacy
- Reputational damage causing brand devaluation
- Loss of confidence in IT
- Expenditure on information security assets and data damaged, stolen, corrupted or lost in incidents
- Loss of competitive advantage
- Reduced profitability
- Impaired growth due to inflexible infrastructure/system/application environments
- Injury or loss of life if safety-critical systems fail

- Theft of trade secrets exceeded $1 trillion in 2008 and continues to escalate
- Over 40% of U.S. businesses have reported intellectual property losses in 2008

Background

Incident Evaluation

Trace Evaluation

Incident Reporting

Law Enforcement report?

Regulatory agency report?

Insurance claim?

Disciplinary action?

Dismissal action?

Vendor report?

Update disaster recovery plan?

Update software to new versions?

Update employee training?

Public Affairs report?

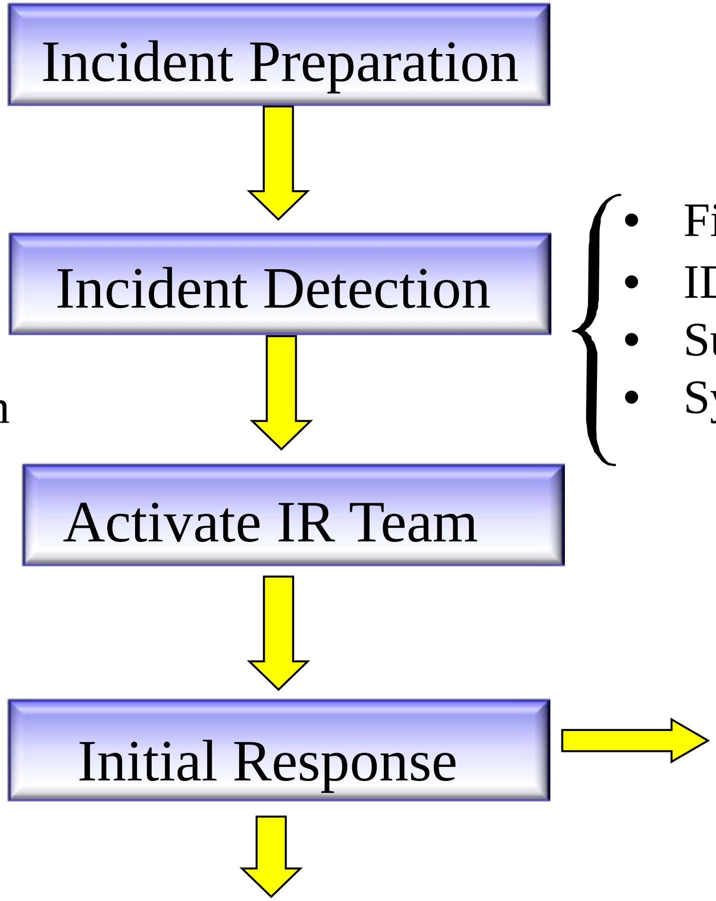
CEO report to employees?

Incident Response Process

- Define Roles
- Establish Policies
- Identify Tools
- Network Preparation

Complete IR Checklist

- Who/What/Where/When
- Incident Description
- Hardware/Software
- Personnel Involved
- Network



Incident Preparation

Incident Detection

Activate IR Team

Initial Response

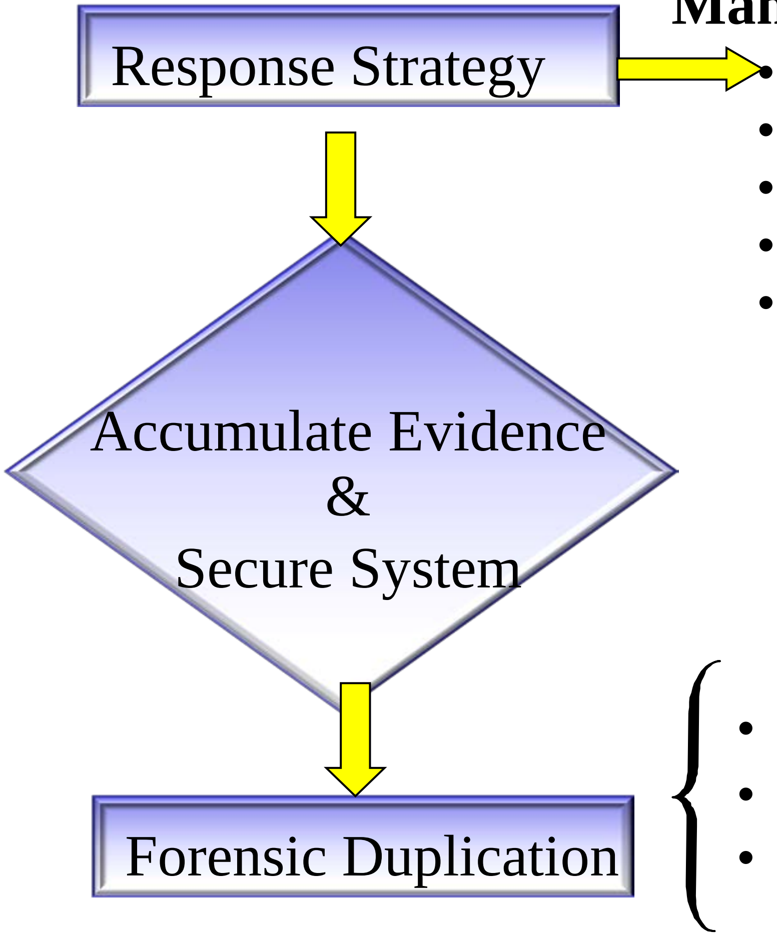
- Firewall Logs
- IDS Logs
- Suspicious User
- System Administrator

- Verify Incident
- Affected Systems
- Users Involved
- Business Impact

Completed IR Checklist.

Is it really and Incident?

Incident Response Process Response



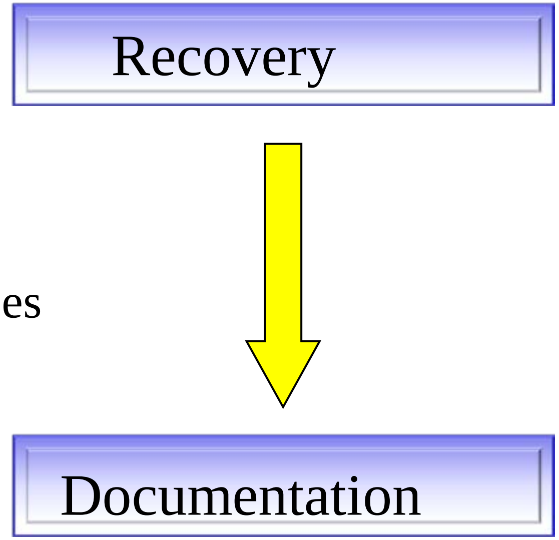
Management Approval

- Dollar Loss
- Downtime
- Legal Liability
- Publicity
- Intellectual Property

- System Criticality
- Information Sensitivity
- Perpetrators
- Publicity
- Skill of Attacker
- System Downtime
- Dollar Loss

- Best Evidence Rule
- Chain of custody
- Data Volatility

Incident Response Process Improvements



Recovery

- New Procedures
- Reinstall files
- Reinstall from CD-Rom
- Secure System
  - Turnoff unneeded services
  - Apply patches
  - Strong Passwords
  - Strong Administration

Documentation

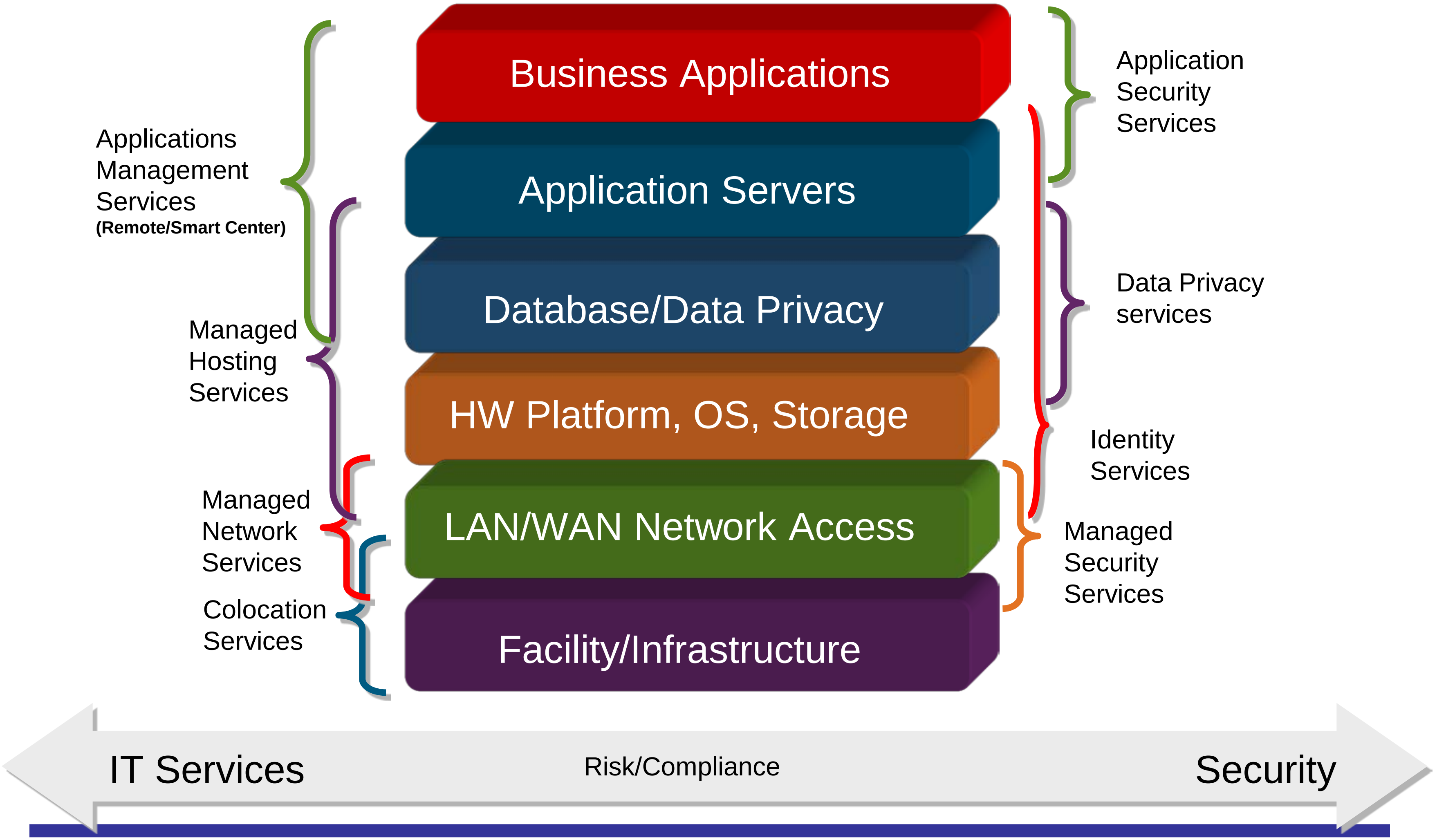
- Document everything as it occurs
- Support both criminal and civil prosecution
- Produce the final report
- Process improvement

Background

Incident Evaluation

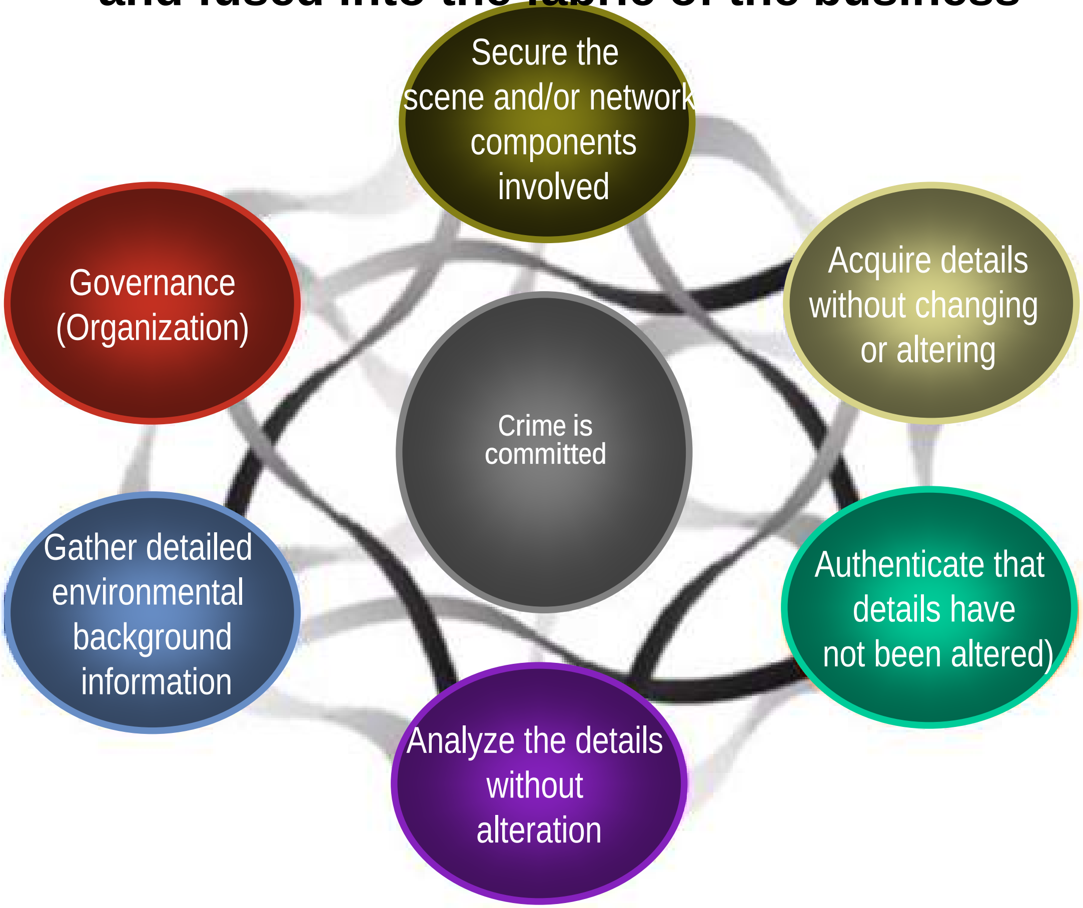
Trace Evaluation

Elements of Digital Forensics



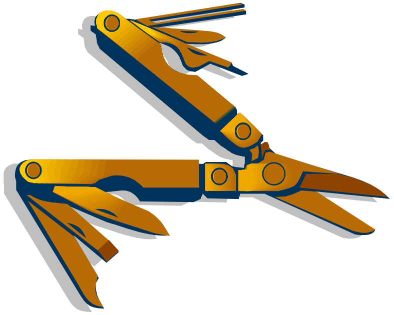
Network Forensics Elements

Security has to be applied within a business context and fused into the fabric of the business


Secure the scene and/or network components involved
Acquire details without changing or altering
Authenticate that details have not been altered)
Analyze the details without alteration
Gather detailed environmental background information
Governance (Organization)
Crime is committed

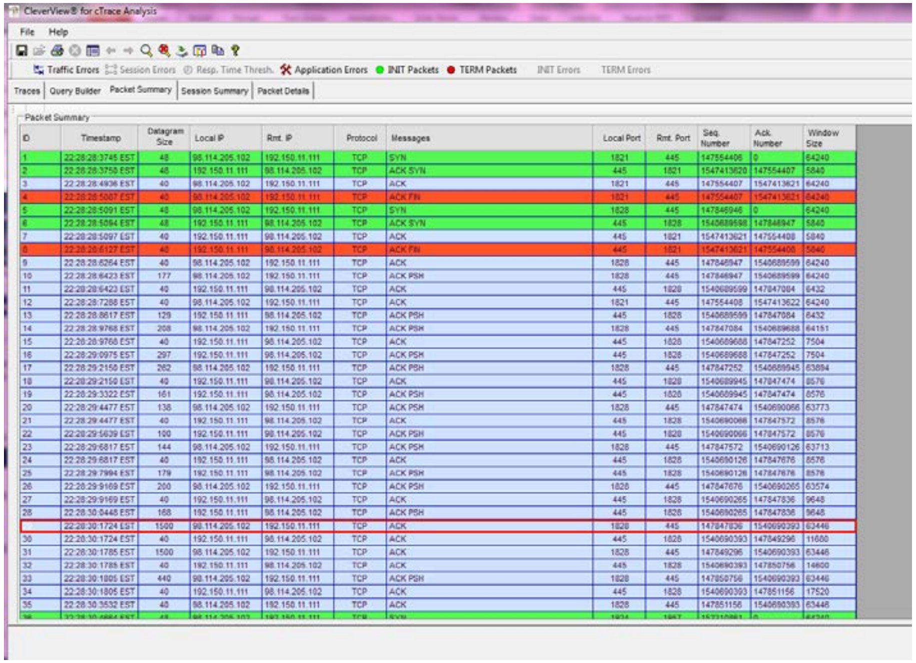
Forensic Tools

- IDS (Intrusion Detection System) attempts to detect activity that violates an organization's security policy
- Firewall allows or disallows traffic to or from specific networks, machine addresses and port numbers
- Network Forensic Analysis Tools (NFAT) synergizes with IDSs and Firewalls.
    - Preserves long term record of network traffic
    - Allows quick analysis of trouble spots identified by IDSs and Firewalls
        - NFATs must do the following:
            - Capture network traffic
            - Analyze network traffic according to user needs
            - Allow system users discover useful and interesting things about the analyzed traffic



NFAT Tasks

- Traffic Capture
  - What is the policy?
  - What is the traffic of interest?
  - Internal/External?
  - Collect packets
  - Traffic Analysis
  - Organize traffic by session
  - Protocol Parsing and analysis
  - Check for strings, use expert systems for analysis
- Interacting with NFAT
  - Appropriate user interfaces, reports, examine large quantities of information and make it manageable

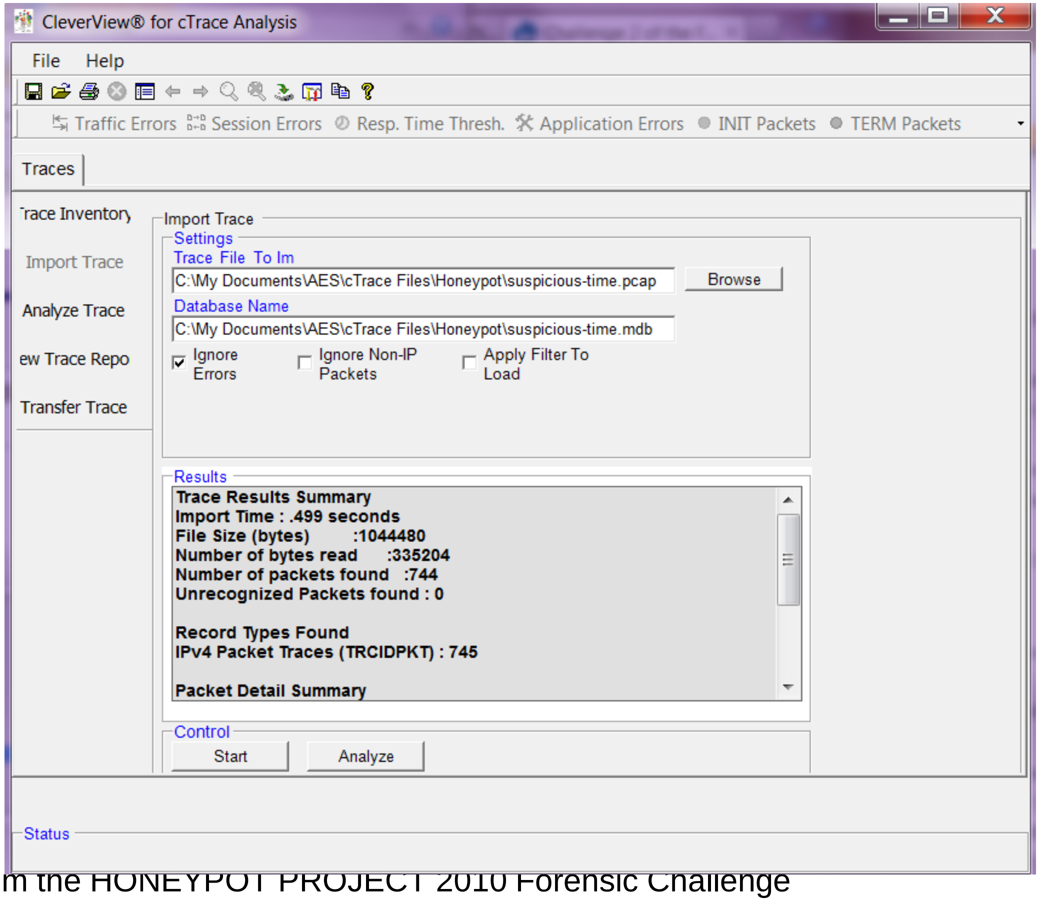


Packet Summary

ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Protocol	Messages	Local Port	Rmt. Port	Seq. Number	Ack. Number	Window Size
1	22:28:28:3745 EST	48	98.114.205.102	192.150.11.111	TCP	SYN	1821	445	147554406	0	64240
2	22:28:28:3758 EST	48	192.150.11.111	98.114.205.102	TCP	ACK SYN	445	1821	1547413620	147554407	5840
3	22:28:28:4936 EST	40	98.114.205.102	192.150.11.111	TCP	ACK	1821	445	147554407	1547413621	64240
4	22:28:28:5087 EST	40	98.114.205.102	192.150.11.111	TCP	ACK FIN	1821	445	147554407	1547413621	64240
5	22:28:28:5091 EST	48	98.114.205.102	192.150.11.111	TCP	SYN	1828	445	147846946	0	64240
6	22:28:28:5094 EST	48	192.150.11.111	98.114.205.102	TCP	ACK SYN	445	1828	1540689598	147846947	5840
7	22:28:28:5097 EST	40	192.150.11.111	98.114.205.102	TCP	ACK	445	1821	1547413621	147554408	5840
8	22:28:28:6127 EST	40	192.150.11.111	98.114.205.102	TCP	ACK FIN	445	1821	1547413621	147554408	5840
9	22:28:28:6264 EST	40	98.114.205.102	192.150.11.111	TCP	ACK	1828	445	147846947	1540689599	64240
10	22:28:28:6423 EST	177	98.114.205.102	192.150.11.111	TCP	ACK PSH	1828	445	147846947	1540689599	64240
11	22:28:28:6423 EST	40	192.150.11.111	98.114.205.102	TCP	ACK	445	1828	1540689599	147847084	6432
12	22:28:28:7288 EST	40	98.114.205.102	192.150.11.111	TCP	ACK	1821	445	147554408	1547413622	64240
13	22:28:28:8617 EST	129	192.150.11.111	98.114.205.102	TCP	ACK PSH	445	1828	1540689599	147847084	6432
14	22:28:28:9768 EST	208	98.114.205.102	192.150.11.111	TCP	ACK PSH	1828	445	147847084	1540689688	64151
15	22:28:28:9768 EST	40	192.150.11.111	98.114.205.102	TCP	ACK	445	1828	1540689688	147847252	7504
16	22:28:29:0975 EST	297	192.150.11.111	98.114.205.102	TCP	ACK PSH	445	1828	1540689688	147847252	7504
17	22:28:29:2150 EST	262	98.114.205.102	192.150.11.111	TCP	ACK PSH	1828	445	147847252	1540689945	63894
18	22:28:29:2150 EST	40	192.150.11.111	98.114.205.102	TCP	ACK	445	1828	1540689945	147847474	8576
19	22:28:29:3322 EST	161	192.150.11.111	98.114.205.102	TCP	ACK PSH	445	1828	1540689945	147847474	8576
20	22:28:29:4477 EST	138	98.114.205.102	192.150.11.111	TCP	ACK PSH	1828	445	147847474	1540690066	63773
21	22:28:29:4477 EST	40	192.150.11.111	98.114.205.102	TCP	ACK	445	1828	1540690066	147847572	8576
22	22:28:29:5639 EST	100	192.150.11.111	98.114.205.102	TCP	ACK PSH	445	1828	1540690066	147847572	8576
23	22:28:29:6817 EST	144	98.114.205.102	192.150.11.111	TCP	ACK PSH	1828	445	147847572	1540690126	63713
24	22:28:29:6817 EST	40	192.150.11.111	98.114.205.102	TCP	ACK	445	1828	1540690126	147847676	8576
25	22:28:29:7994 EST	179	192.150.11.111	98.114.205.102	TCP	ACK PSH	445	1828	1540690126	147847676	8576
26	22:28:29:9169 EST	200	98.114.205.102	192.150.11.111	TCP	ACK PSH	1828	445	147847676	1540690265	63574
27	22:28:29:9169 EST	40	192.150.11.111	98.114.205.102	TCP	ACK	445	1828	1540690265	147847836	9648
28	22:28:30:0448 EST	168	192.150.11.111	98.114.205.102	TCP	ACK PSH	445	1828	1540690265	147847836	9648
29	22:28:30:1724 EST	1500	98.114.205.102	192.150.11.111	TCP	ACK	1828	445	147847836	1540690393	63446
30	22:28:30:1724 EST	40	192.150.11.111	98.114.205.102	TCP	ACK	445	1828	1540690393	147849296	11680
31	22:28:30:1785 EST	1500	98.114.205.102	192.150.11.111	TCP	ACK	1828	445	147849296	1540690393	63446
32	22:28:30:1785 EST	40	192.150.11.111	98.114.205.102	TCP	ACK	445	1828	1540690393	147850756	14600
33	22:28:30:1805 EST	440	98.114.205.102	192.150.11.111	TCP	ACK PSH	1828	445	147850756	1540690393	63446
34	22:28:30:1805 EST	40	192.150.11.111	98.114.205.102	TCP	ACK	445	1828	1540690393	147851156	17520
35	22:28:30:3532 EST	40	98.114.205.102	192.150.11.111	TCP	ACK	1828	445	147851156	1540690393	63446
36	22:28:30:4984 EST	48	98.114.205.102	192.150.11.111	TCP	SYN	1834	1867	[illegible]	0	64240

PCAP Attack Situation*

A malware attack is suspected and you need to identify the malicious web pages.



Trace File To Im: C:\My Documents\AES\cTrace Files\Honeypot\suspicious-time.pcap

Database Name: C:\My Documents\AES\cTrace Files\Honeypot\suspicious-time.mdb

☑ Ignore Errors ☐ Ignore Non-IP Packets ☐ Apply Filter To Load

```
Trace Results Summary
Import Time : .499 seconds
File Size (bytes)        :1044480
Number of bytes read      :335204
Number of packets found   :744
Unrecognized Packets found : 0

Record Types Found
IPv4 Packet Traces (TRCIDPKT) : 745

Packet Detail Summary
```

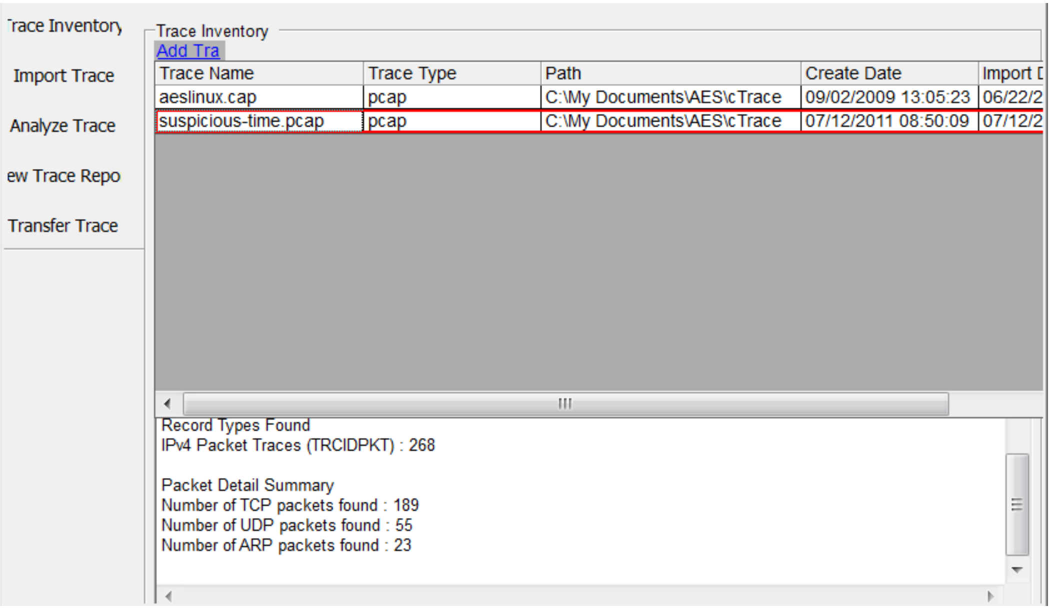
* Excerpts from the HONEYPOT PROJECT 2010 Forensic Challenge

What Can You Learn from the Trace?

- List the protocols found in the capture. What protocol do you think the attack is based on?
- List IPs, host names/domain names. What can you discern based on this information? Do you think it is a real situation?
- List all the visited web pages? Which ones might contain malicious javascript and who is connecting to them? Describe the nature of the malicious web pages.
- What are the overall actions performed by the attacker?
- What steps slow the analysis down?
- What Operating Systems, software, and vulnerabilities were involved?

What Can You Learn from the Trace?

List the protocols found in the capture. What protocol do you think the attack is based on? *Tools used: CleverView for cTrace Analysis*



Trace Name	Trace Type	Path	Create Date	Import D
aeslinux.cap	pcap	C:\My Documents\AES\cTrace	09/02/2009 13:05:23	06/22/2
suspicious-time.pcap	pcap	C:\My Documents\AES\cTrace	07/12/2011 08:50:09	07/12/2

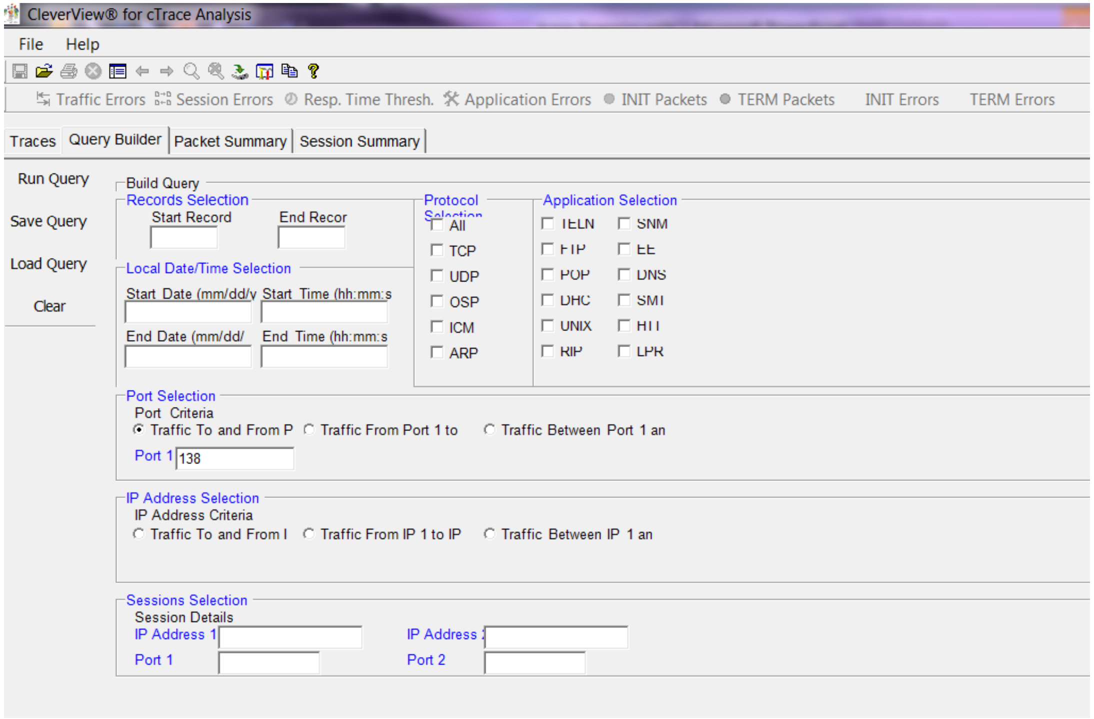
```
Record Types Found
IPv4 Packet Traces (TRCIDPKT) : 268

Packet Detail Summary
Number of TCP packets found : 189
Number of UDP packets found : 55
Number of ARP packets found : 23
```

ARP
DNS
DHCP
HTTP
NetBIOS

Use Query Builder function to view protocols in trace

How to Determine Protocols Runing in Trace?

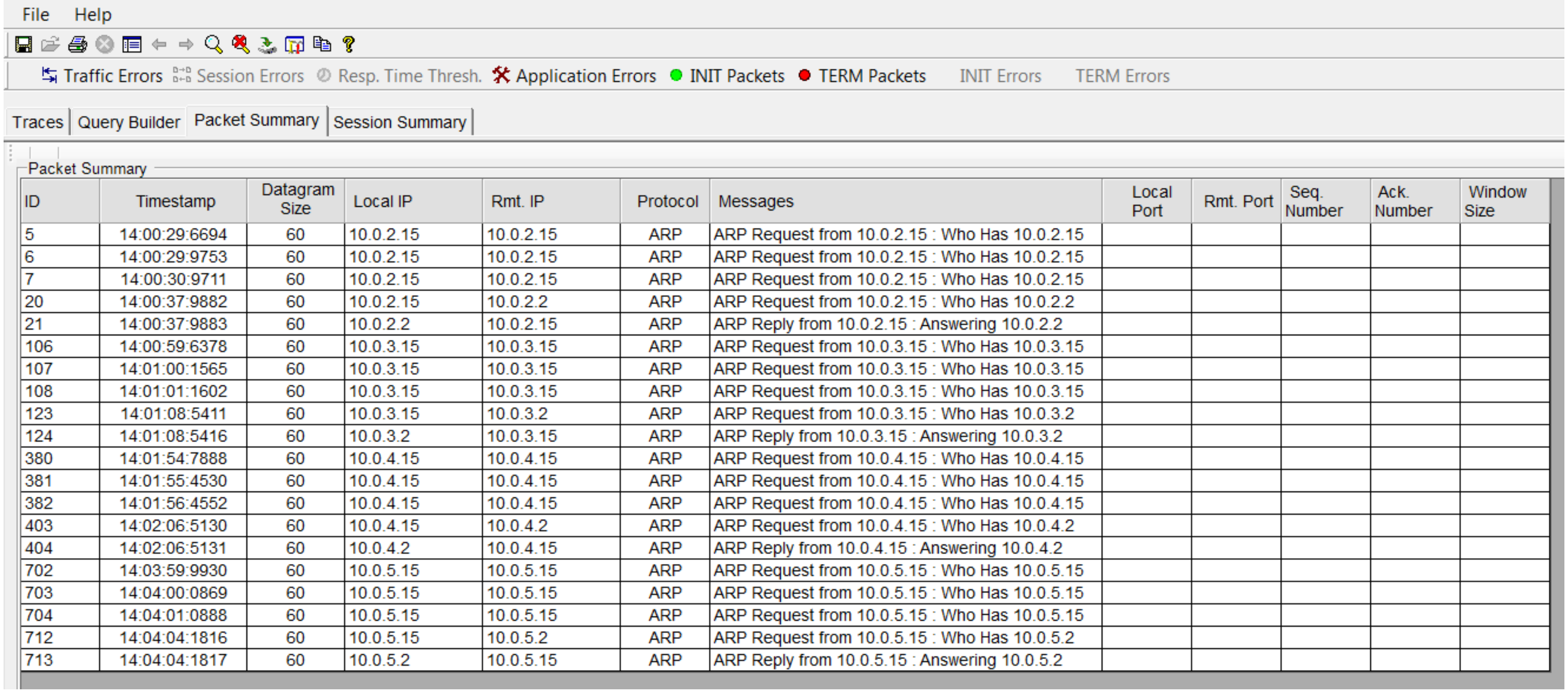


Port Criteria
● Traffic To and From P ○ Traffic From Port 1 to ○ Traffic Between Port 1 an

Port 1: 138

Query Builder allows viewing only specific common protocols/applications or ports

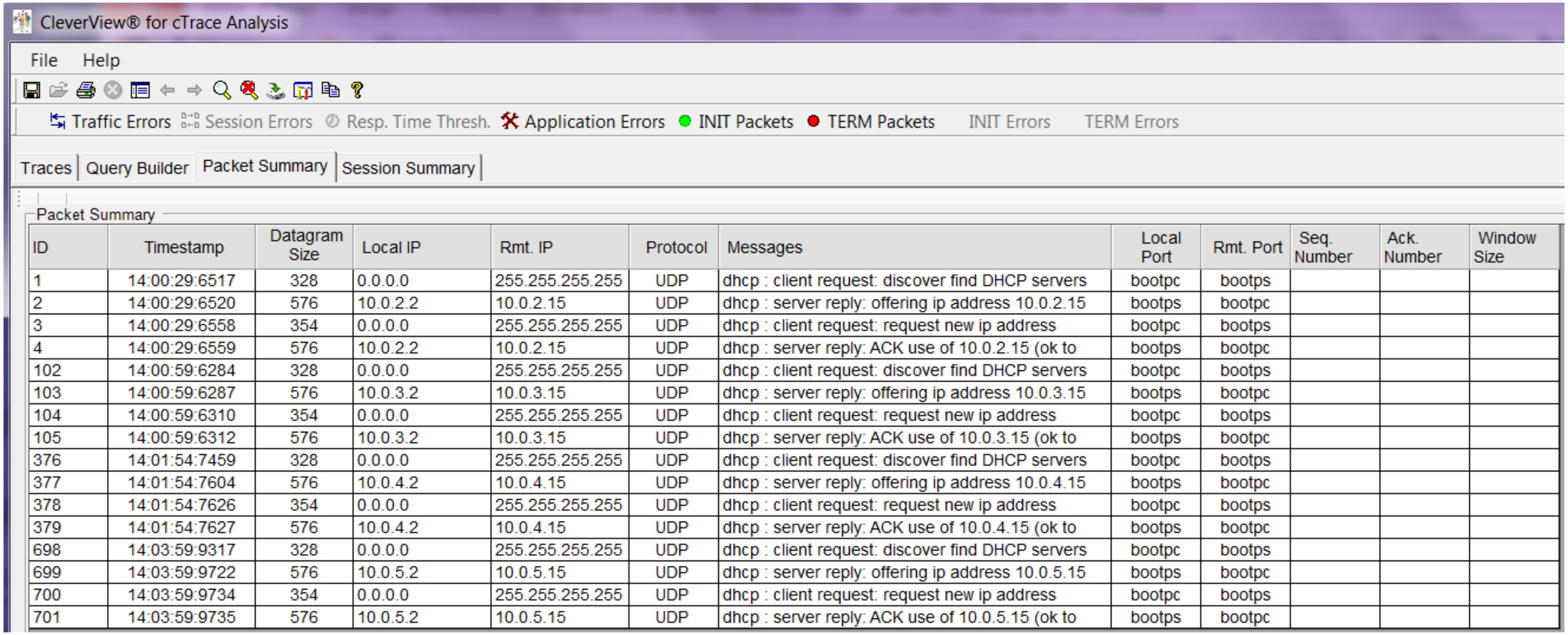
What Can You Learn from this Trace? ARP



ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Protocol	Messages	Local Port	Rmt. Port	Seq. Number	Ack. Number	Window Size
5	14:00:29:6694	60	10.0.2.15	10.0.2.15	ARP	ARP Request from 10.0.2.15 : Who Has 10.0.2.15					
6	14:00:29:9753	60	10.0.2.15	10.0.2.15	ARP	ARP Request from 10.0.2.15 : Who Has 10.0.2.15					
7	14:00:30:9711	60	10.0.2.15	10.0.2.15	ARP	ARP Request from 10.0.2.15 : Who Has 10.0.2.15					
20	14:00:37:9882	60	10.0.2.15	10.0.2.2	ARP	ARP Request from 10.0.2.15 : Who Has 10.0.2.2					
21	14:00:37:9883	60	10.0.2.2	10.0.2.15	ARP	ARP Reply from 10.0.2.15 : Answering 10.0.2.2					
106	14:00:59:6378	60	10.0.3.15	10.0.3.15	ARP	ARP Request from 10.0.3.15 : Who Has 10.0.3.15					
107	14:01:00:1565	60	10.0.3.15	10.0.3.15	ARP	ARP Request from 10.0.3.15 : Who Has 10.0.3.15					
108	14:01:01:1602	60	10.0.3.15	10.0.3.15	ARP	ARP Request from 10.0.3.15 : Who Has 10.0.3.15					
123	14:01:08:5411	60	10.0.3.15	10.0.3.2	ARP	ARP Request from 10.0.3.15 : Who Has 10.0.3.2					
124	14:01:08:5416	60	10.0.3.2	10.0.3.15	ARP	ARP Reply from 10.0.3.15 : Answering 10.0.3.2					
380	14:01:54:7888	60	10.0.4.15	10.0.4.15	ARP	ARP Request from 10.0.4.15 : Who Has 10.0.4.15					
381	14:01:55:4530	60	10.0.4.15	10.0.4.15	ARP	ARP Request from 10.0.4.15 : Who Has 10.0.4.15					
382	14:01:56:4552	60	10.0.4.15	10.0.4.15	ARP	ARP Request from 10.0.4.15 : Who Has 10.0.4.15					
403	14:02:06:5130	60	10.0.4.15	10.0.4.2	ARP	ARP Request from 10.0.4.15 : Who Has 10.0.4.2					
404	14:02:06:5131	60	10.0.4.2	10.0.4.15	ARP	ARP Reply from 10.0.4.15 : Answering 10.0.4.2					
702	14:03:59:9930	60	10.0.5.15	10.0.5.15	ARP	ARP Request from 10.0.5.15 : Who Has 10.0.5.15					
703	14:04:00:0869	60	10.0.5.15	10.0.5.15	ARP	ARP Request from 10.0.5.15 : Who Has 10.0.5.15					
704	14:04:01:0888	60	10.0.5.15	10.0.5.15	ARP	ARP Request from 10.0.5.15 : Who Has 10.0.5.15					
712	14:04:04:1816	60	10.0.5.15	10.0.5.2	ARP	ARP Request from 10.0.5.15 : Who Has 10.0.5.2					
713	14:04:04:1817	60	10.0.5.2	10.0.5.15	ARP	ARP Reply from 10.0.5.15 : Answering 10.0.5.2					

ARP was used once per client computer

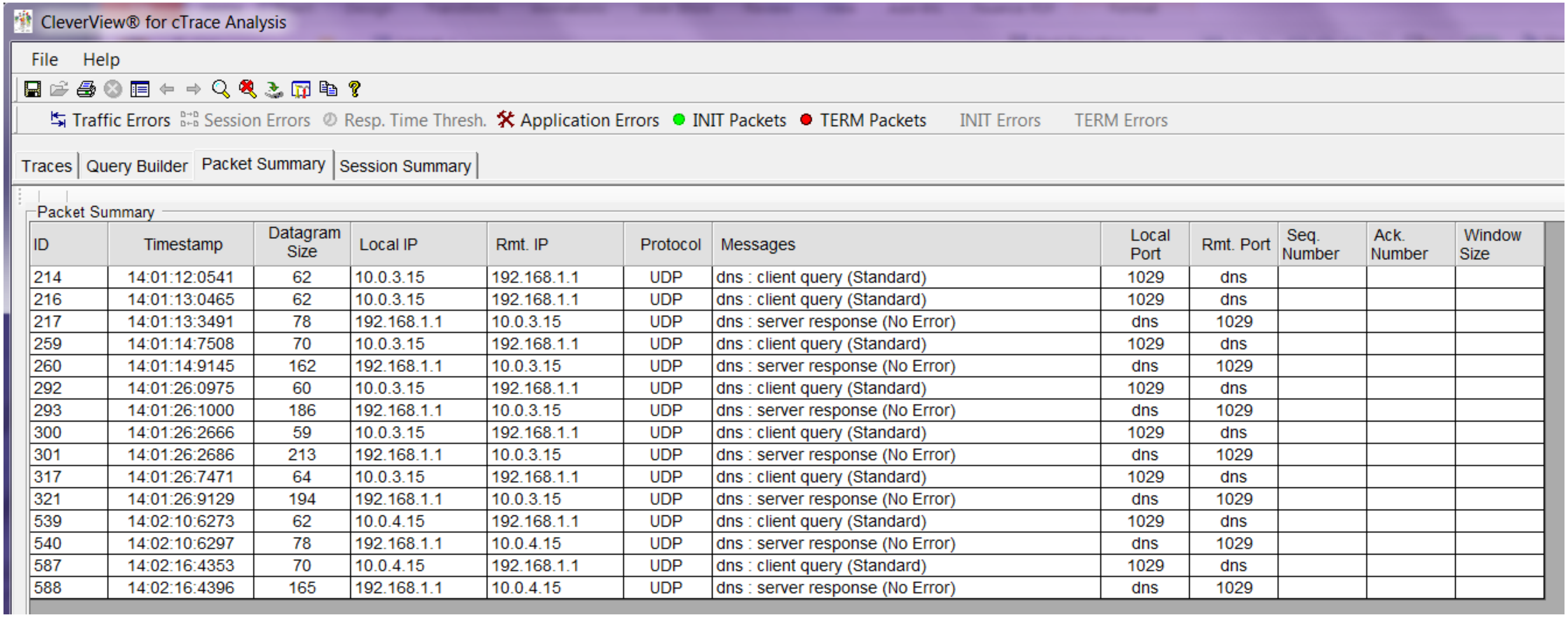
What Can You Learn from this Trace? DHCP



ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Protocol	Messages	Local Port	Rmt. Port	Seq. Number	Ack. Number	Window Size
1	14:00:29:6517	328	0.0.0.0	255.255.255.255	UDP	dhcp : client request: discover find DHCP servers	bootpc	bootps			
2	14:00:29:6520	576	10.0.2.2	10.0.2.15	UDP	dhcp : server reply: offering ip address 10.0.2.15	bootps	bootpc			
3	14:00:29:6558	354	0.0.0.0	255.255.255.255	UDP	dhcp : client request: request new ip address	bootpc	bootps			
4	14:00:29:6559	576	10.0.2.2	10.0.2.15	UDP	dhcp : server reply: ACK use of 10.0.2.15 (ok to	bootps	bootpc			
102	14:00:59:6284	328	0.0.0.0	255.255.255.255	UDP	dhcp : client request: discover find DHCP servers	bootpc	bootps			
103	14:00:59:6287	576	10.0.3.2	10.0.3.15	UDP	dhcp : server reply: offering ip address 10.0.3.15	bootps	bootpc			
104	14:00:59:6310	354	0.0.0.0	255.255.255.255	UDP	dhcp : client request: request new ip address	bootpc	bootps			
105	14:00:59:6312	576	10.0.3.2	10.0.3.15	UDP	dhcp : server reply: ACK use of 10.0.3.15 (ok to	bootps	bootpc			
376	14:01:54:7459	328	0.0.0.0	255.255.255.255	UDP	dhcp : client request: discover find DHCP servers	bootpc	bootps			
377	14:01:54:7604	576	10.0.4.2	10.0.4.15	UDP	dhcp : server reply: offering ip address 10.0.4.15	bootps	bootpc			
378	14:01:54:7626	354	0.0.0.0	255.255.255.255	UDP	dhcp : client request: request new ip address	bootpc	bootps			
379	14:01:54:7627	576	10.0.4.2	10.0.4.15	UDP	dhcp : server reply: ACK use of 10.0.4.15 (ok to	bootps	bootpc			
698	14:03:59:9317	328	0.0.0.0	255.255.255.255	UDP	dhcp : client request: discover find DHCP servers	bootpc	bootps			
699	14:03:59:9722	576	10.0.5.2	10.0.5.15	UDP	dhcp : server reply: offering ip address 10.0.5.15	bootps	bootpc			
700	14:03:59:9734	354	0.0.0.0	255.255.255.255	UDP	dhcp : client request: request new ip address	bootpc	bootps			
701	14:03:59:9735	576	10.0.5.2	10.0.5.15	UDP	dhcp : server reply: ACK use of 10.0.5.15 (ok to	bootps	bootpc			

DHCP was used once per client computer

What Can You Learn from this Trace? DNS

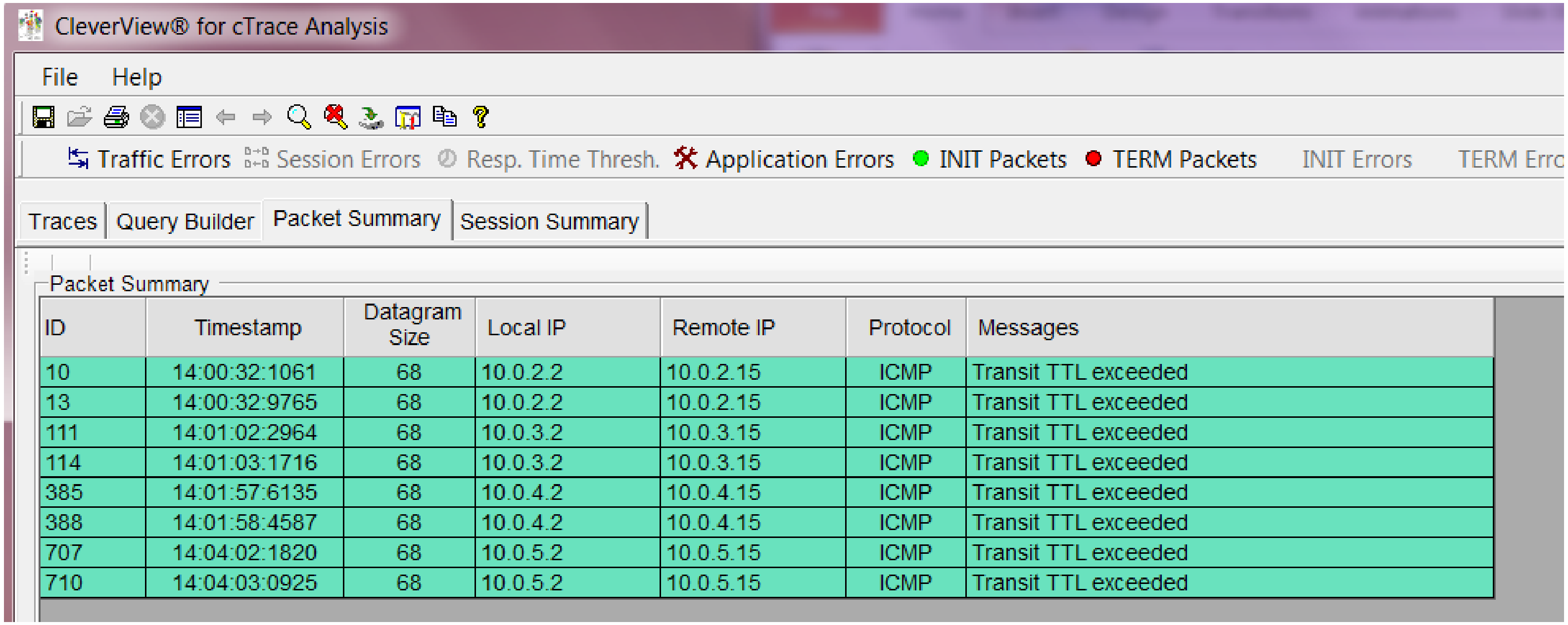


Packet Summary

ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Protocol	Messages	Local Port	Rmt. Port	Seq. Number	Ack. Number	Window Size
214	14:01:12:0541	62	10.0.3.15	192.168.1.1	UDP	dns : client query (Standard)	1029	dns			
216	14:01:13:0465	62	10.0.3.15	192.168.1.1	UDP	dns : client query (Standard)	1029	dns			
217	14:01:13:3491	78	192.168.1.1	10.0.3.15	UDP	dns : server response (No Error)	dns	1029			
259	14:01:14:7508	70	10.0.3.15	192.168.1.1	UDP	dns : client query (Standard)	1029	dns			
260	14:01:14:9145	162	192.168.1.1	10.0.3.15	UDP	dns : server response (No Error)	dns	1029			
292	14:01:26:0975	60	10.0.3.15	192.168.1.1	UDP	dns : client query (Standard)	1029	dns			
293	14:01:26:1000	186	192.168.1.1	10.0.3.15	UDP	dns : server response (No Error)	dns	1029			
300	14:01:26:2666	59	10.0.3.15	192.168.1.1	UDP	dns : client query (Standard)	1029	dns			
301	14:01:26:2686	213	192.168.1.1	10.0.3.15	UDP	dns : server response (No Error)	dns	1029			
317	14:01:26:7471	64	10.0.3.15	192.168.1.1	UDP	dns : client query (Standard)	1029	dns			
321	14:01:26:9129	194	192.168.1.1	10.0.3.15	UDP	dns : server response (No Error)	dns	1029			
539	14:02:10:6273	62	10.0.4.15	192.168.1.1	UDP	dns : client query (Standard)	1029	dns			
540	14:02:10:6297	78	192.168.1.1	10.0.4.15	UDP	dns : server response (No Error)	dns	1029			
587	14:02:16:4353	70	10.0.4.15	192.168.1.1	UDP	dns : client query (Standard)	1029	dns			
588	14:02:16:4396	165	192.168.1.1	10.0.4.15	UDP	dns : server response (No Error)	dns	1029			

DNS was used to resolve WEB Server Names

What Can You Learn from this Trace? ICMP

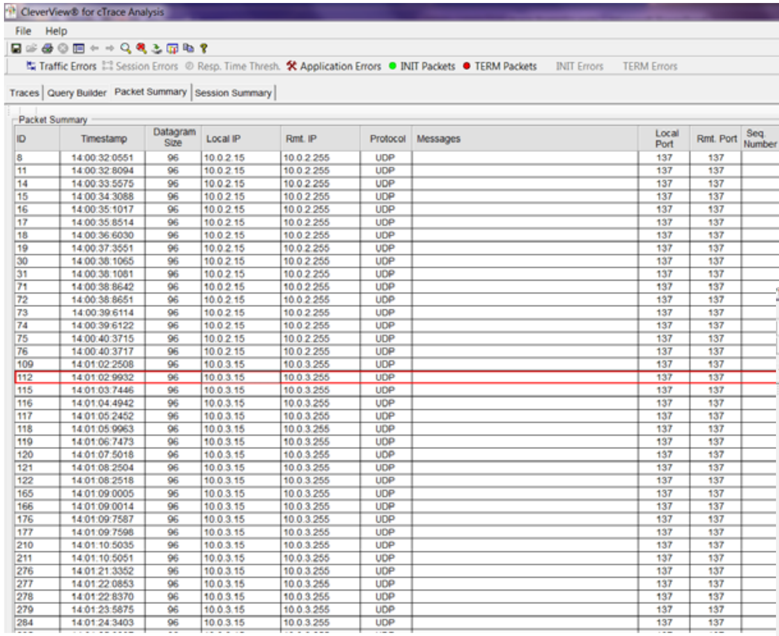


Packet Summary

ID	Timestamp	Datagram Size	Local IP	Remote IP	Protocol	Messages
10	14:00:32:1061	68	10.0.2.2	10.0.2.15	ICMP	Transit TTL exceeded
13	14:00:32:9765	68	10.0.2.2	10.0.2.15	ICMP	Transit TTL exceeded
111	14:01:02:2964	68	10.0.3.2	10.0.3.15	ICMP	Transit TTL exceeded
114	14:01:03:1716	68	10.0.3.2	10.0.3.15	ICMP	Transit TTL exceeded
385	14:01:57:6135	68	10.0.4.2	10.0.4.15	ICMP	Transit TTL exceeded
388	14:01:58:4587	68	10.0.4.2	10.0.4.15	ICMP	Transit TTL exceeded
707	14:04:02:1820	68	10.0.5.2	10.0.5.15	ICMP	Transit TTL exceeded
710	14:04:03:0925	68	10.0.5.2	10.0.5.15	ICMP	Transit TTL exceeded

ICMP reported Transit TTL exceptions

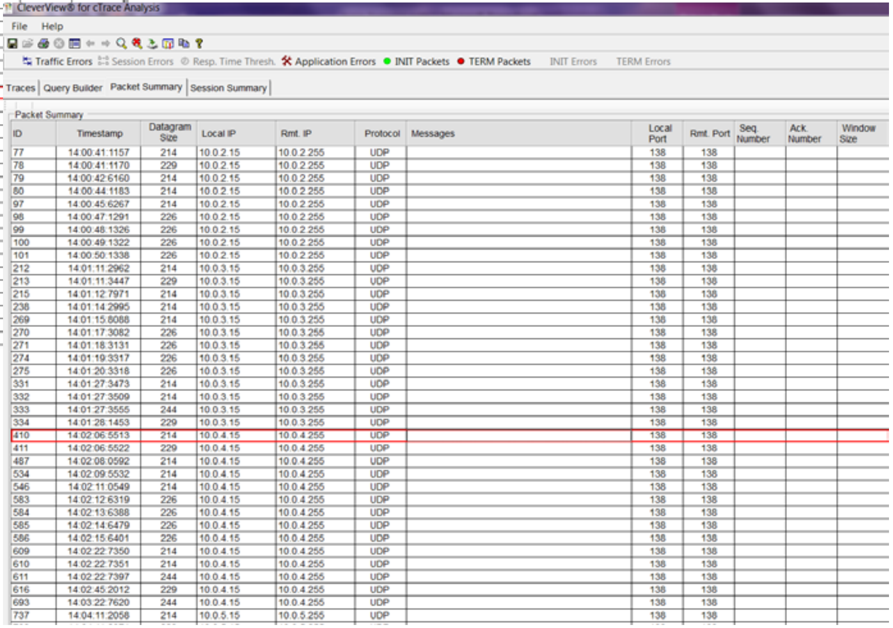
What Can You Learn from this Trace? NetBios



Packet Summary

ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Protocol	Messages	Local Port	Rmt. Port	Seq. Number	Ack. Number	Window Size
8	14:00:32:0551	96	10.0.2.15	10.0.2.255	UDP		137	137			
11	14:00:32:8094	96	10.0.2.15	10.0.2.255	UDP		137	137			
14	14:00:33:5575	96	10.0.2.15	10.0.2.255	UDP		137	137			
15	14:00:34:3088	96	10.0.2.15	10.0.2.255	UDP		137	137			
16	14:00:35:1017	96	10.0.2.15	10.0.2.255	UDP		137	137			
17	14:00:35:8514	96	10.0.2.15	10.0.2.255	UDP		137	137			
18	14:00:36:6030	96	10.0.2.15	10.0.2.255	UDP		137	137			
19	14:00:37:3551	96	10.0.2.15	10.0.2.255	UDP		137	137			
30	14:00:38:1065	96	10.0.2.15	10.0.2.255	UDP		137	137			
31	14:00:38:1081	96	10.0.2.15	10.0.2.255	UDP		137	137			
71	14:00:38:8642	96	10.0.2.15	10.0.2.255	UDP		137	137			
72	14:00:38:8651	96	10.0.2.15	10.0.2.255	UDP		137	137			
73	14:00:39:6114	96	10.0.2.15	10.0.2.255	UDP		137	137			
74	14:00:39:6122	96	10.0.2.15	10.0.2.255	UDP		137	137			
75	14:00:40:3715	96	10.0.2.15	10.0.2.255	UDP		137	137			
76	14:00:40:3717	96	10.0.2.15	10.0.2.255	UDP		137	137			
109	14:01:02:2508	96	10.0.3.15	10.0.3.255	UDP		137	137			
112	14:01:02:9932	96	10.0.3.15	10.0.3.255	UDP		137	137			
115	14:01:03:7446	96	10.0.3.15	10.0.3.255	UDP		137	137			
116	14:01:04:4942	96	10.0.3.15	10.0.3.255	UDP		137	137			
117	14:01:05:2452	96	10.0.3.15	10.0.3.255	UDP		137	137			
118	14:01:05:9963	96	10.0.3.15	10.0.3.255	UDP		137	137			
119	14:01:06:7473	96	10.0.3.15	10.0.3.255	UDP		137	137			
120	14:01:07:5018	96	10.0.3.15	10.0.3.255	UDP		137	137			
121	14:01:08:2504	96	10.0.3.15	10.0.3.255	UDP		137	137			
122	14:01:08:2518	96	10.0.3.15	10.0.3.255	UDP		137	137			
165	14:01:09:0005	96	10.0.3.15	10.0.3.255	UDP		137	137			
166	14:01:09:0014	96	10.0.3.15	10.0.3.255	UDP		137	137			
176	14:01:09:7587	96	10.0.3.15	10.0.3.255	UDP		137	137			
177	14:01:09:7598	96	10.0.3.15	10.0.3.255	UDP		137	137			
210	14:01:10:5035	96	10.0.3.15	10.0.3.255	UDP		137	137			
211	14:01:10:5051	96	10.0.3.15	10.0.3.255	UDP		137	137			
276	14:01:21:3352	96	10.0.3.15	10.0.3.255	UDP		137	137			
277	14:01:22:0853	96	10.0.3.15	10.0.3.255	UDP		137	137			
278	14:01:22:8370	96	10.0.3.15	10.0.3.255	UDP		137	137			
279	14:01:23:5875	96	10.0.3.15	10.0.3.255	UDP		137	137			
284	14:01:24:3403	96	10.0.3.15	10.0.3.255	UDP		137	137			

NetBios Uses ports 137, 138, 139

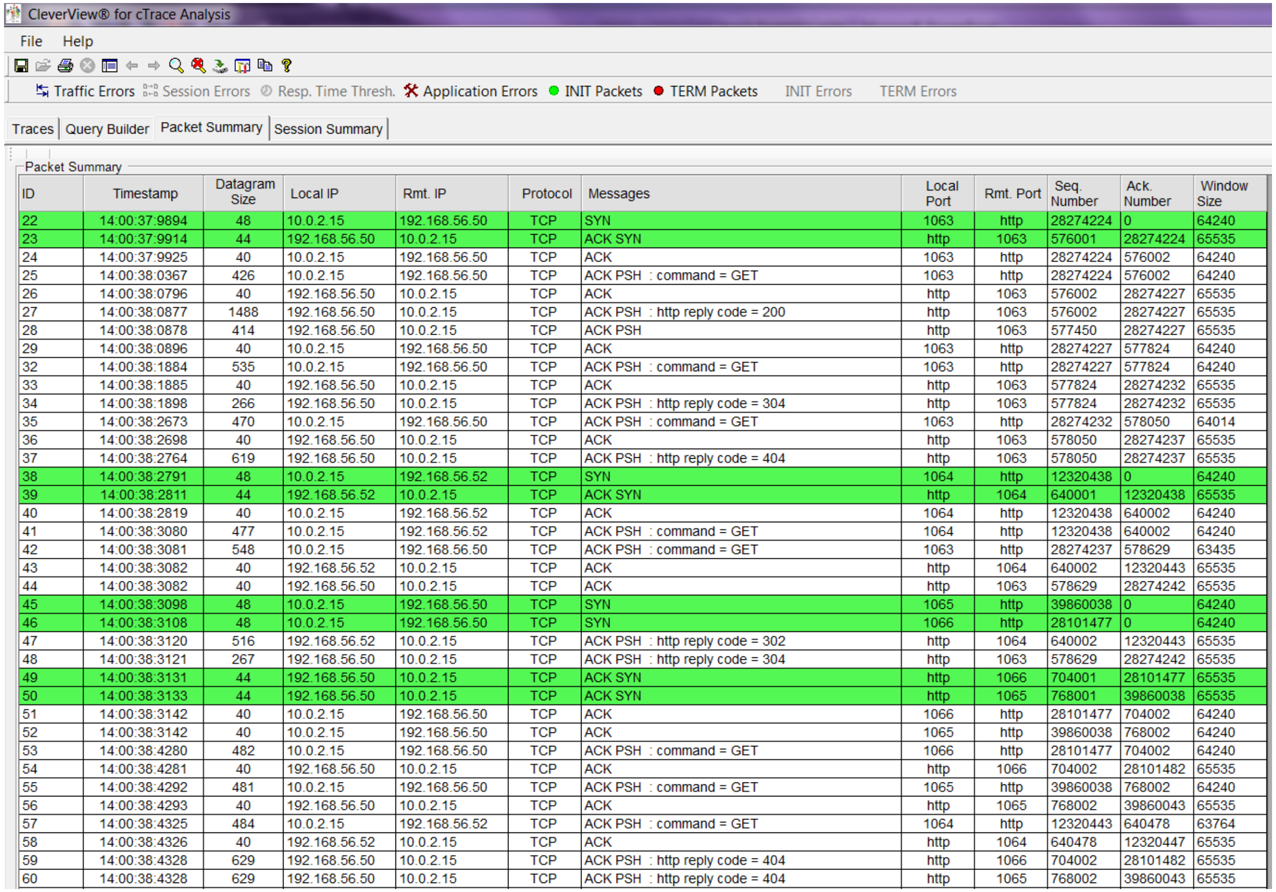


Packet Summary

ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Protocol	Messages	Local Port	Rmt. Port	Seq. Number	Ack. Number	Window Size
77	14:00:41:1157	214	10.0.2.15	10.0.2.255	UDP		138	138			
78	14:00:41:1170	229	10.0.2.15	10.0.2.255	UDP		138	138			
79	14:00:42:6160	214	10.0.2.15	10.0.2.255	UDP		138	138			
80	14:00:44:1183	214	10.0.2.15	10.0.2.255	UDP		138	138			
97	14:00:45:6267	214	10.0.2.15	10.0.2.255	UDP		138	138			
98	14:00:47:1291	226	10.0.2.15	10.0.2.255	UDP		138	138			
99	14:00:48:1326	226	10.0.2.15	10.0.2.255	UDP		138	138			
100	14:00:49:1322	226	10.0.2.15	10.0.2.255	UDP		138	138			
101	14:00:50:1338	226	10.0.2.15	10.0.2.255	UDP		138	138			
212	14:01:11:2962	214	10.0.3.15	10.0.3.255	UDP		138	138			
213	14:01:11:3447	229	10.0.3.15	10.0.3.255	UDP		138	138			
215	14:01:12:7971	214	10.0.3.15	10.0.3.255	UDP		138	138			
238	14:01:14:2995	214	10.0.3.15	10.0.3.255	UDP		138	138			
269	14:01:15:8088	214	10.0.3.15	10.0.3.255	UDP		138	138			
270	14:01:17:3082	226	10.0.3.15	10.0.3.255	UDP		138	138			
271	14:01:18:3131	226	10.0.3.15	10.0.3.255	UDP		138	138			
274	14:01:19:3317	226	10.0.3.15	10.0.3.255	UDP		138	138			
275	14:01:20:3318	226	10.0.3.15	10.0.3.255	UDP		138	138			
331	14:01:27:3473	214	10.0.3.15	10.0.3.255	UDP		138	138			
332	14:01:27:3509	214	10.0.3.15	10.0.3.255	UDP		138	138			
333	14:01:27:3555	244	10.0.3.15	10.0.3.255	UDP		138	138			
334	14:01:28:1453	229	10.0.3.15	10.0.3.255	UDP		138	138			
410	14:02:06:5513	214	10.0.4.15	10.0.4.255	UDP		138	138			
411	14:02:06:5522	229	10.0.4.15	10.0.4.255	UDP		138	138			
487	14:02:08:0592	214	10.0.4.15	10.0.4.255	UDP		138	138			
534	14:02:09:5532	214	10.0.4.15	10.0.4.255	UDP		138	138			
546	14:02:11:0549	214	10.0.4.15	10.0.4.255	UDP		138	138			
583	14:02:12:6319	226	10.0.4.15	10.0.4.255	UDP		138	138			
584	14:02:13:6388	226	10.0.4.15	10.0.4.255	UDP		138	138			
585	14:02:14:6479	226	10.0.4.15	10.0.4.255	UDP		138	138			
586	14:02:15:6401	226	10.0.4.15	10.0.4.255	UDP		138	138			
609	14:02:22:7350	214	10.0.4.15	10.0.4.255	UDP		138	138			
610	14:02:22:7351	214	10.0.4.15	10.0.4.255	UDP		138	138			
611	14:02:22:7397	244	10.0.4.15	10.0.4.255	UDP		138	138			
616	14:02:45:2012	229	10.0.4.15	10.0.4.255	UDP		138	138			
693	14:03:22:7620	244	10.0.4.15	10.0.4.255	UDP		138	138			
737	14:04:11:2058	214	10.0.5.15	10.0.5.255	UDP		138	138			

NetBios announcement queries being sent from the clients but no responses…..

What Can You Learn from this Trace? HTTP



ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Protocol	Messages	Local Port	Rmt. Port	Seq. Number	Ack. Number	Window Size
22	14:00:37:9894	48	10.0.2.15	192.168.56.50	TCP	SYN	1063	http	28274224	0	64240
23	14:00:37:9914	44	192.168.56.50	10.0.2.15	TCP	ACK SYN	http	1063	576001	28274224	65535
24	14:00:37:9925	40	10.0.2.15	192.168.56.50	TCP	ACK	1063	http	28274224	576002	64240
25	14:00:38:0367	426	10.0.2.15	192.168.56.50	TCP	ACK PSH : command = GET	1063	http	28274224	576002	64240
26	14:00:38:0796	40	192.168.56.50	10.0.2.15	TCP	ACK	http	1063	576002	28274227	65535
27	14:00:38:0877	1488	192.168.56.50	10.0.2.15	TCP	ACK PSH : http reply code = 200	http	1063	576002	28274227	65535
28	14:00:38:0878	414	192.168.56.50	10.0.2.15	TCP	ACK PSH	http	1063	577450	28274227	65535
29	14:00:38:0896	40	10.0.2.15	192.168.56.50	TCP	ACK	1063	http	28274227	577824	64240
32	14:00:38:1884	535	10.0.2.15	192.168.56.50	TCP	ACK PSH : command = GET	1063	http	28274227	577824	64240
33	14:00:38:1885	40	192.168.56.50	10.0.2.15	TCP	ACK	http	1063	577824	28274232	65535
34	14:00:38:1898	266	192.168.56.50	10.0.2.15	TCP	ACK PSH : http reply code = 304	http	1063	577824	28274232	65535
35	14:00:38:2673	470	10.0.2.15	192.168.56.50	TCP	ACK PSH : command = GET	1063	http	28274232	578050	64014
36	14:00:38:2698	40	192.168.56.50	10.0.2.15	TCP	ACK	http	1063	578050	28274237	65535
37	14:00:38:2764	619	192.168.56.50	10.0.2.15	TCP	ACK PSH : http reply code = 404	http	1063	578050	28274237	65535
38	14:00:38:2791	48	10.0.2.15	192.168.56.52	TCP	SYN	1064	http	12320438	0	64240
39	14:00:38:2811	44	192.168.56.52	10.0.2.15	TCP	ACK SYN	http	1064	640001	12320438	65535
40	14:00:38:2819	40	10.0.2.15	192.168.56.52	TCP	ACK	1064	http	12320438	640002	64240
41	14:00:38:3080	477	10.0.2.15	192.168.56.52	TCP	ACK PSH : command = GET	1064	http	12320438	640002	64240
42	14:00:38:3081	548	10.0.2.15	192.168.56.50	TCP	ACK PSH : command = GET	1063	http	28274237	578629	63435
43	14:00:38:3082	40	192.168.56.52	10.0.2.15	TCP	ACK	http	1064	640002	12320443	65535
44	14:00:38:3082	40	192.168.56.50	10.0.2.15	TCP	ACK	http	1063	578629	28274242	65535
45	14:00:38:3098	48	10.0.2.15	192.168.56.50	TCP	SYN	1065	http	39860038	0	64240
46	14:00:38:3108	48	10.0.2.15	192.168.56.50	TCP	SYN	1066	http	28101477	0	64240
47	14:00:38:3120	516	192.168.56.52	10.0.2.15	TCP	ACK PSH : http reply code = 302	http	1064	640002	12320443	65535
48	14:00:38:3121	267	192.168.56.50	10.0.2.15	TCP	ACK PSH : http reply code = 304	http	1063	578629	28274242	65535
49	14:00:38:3131	44	192.168.56.50	10.0.2.15	TCP	ACK SYN	http	1066	704001	28101477	65535
50	14:00:38:3133	44	192.168.56.50	10.0.2.15	TCP	ACK SYN	http	1065	768001	39860038	65535
51	14:00:38:3142	40	10.0.2.15	192.168.56.50	TCP	ACK	1066	http	28101477	704002	64240
52	14:00:38:3142	40	10.0.2.15	192.168.56.50	TCP	ACK	1065	http	39860038	768002	64240
53	14:00:38:4280	482	10.0.2.15	192.168.56.50	TCP	ACK PSH : command = GET	1066	http	28101477	704002	64240
54	14:00:38:4281	40	192.168.56.50	10.0.2.15	TCP	ACK	http	1066	704002	28101482	65535
55	14:00:38:4292	481	10.0.2.15	192.168.56.50	TCP	ACK PSH : command = GET	1065	http	39860038	768002	64240
56	14:00:38:4293	40	192.168.56.50	10.0.2.15	TCP	ACK	http	1065	768002	39860043	65535
57	14:00:38:4325	484	10.0.2.15	192.168.56.52	TCP	ACK PSH : command = GET	1064	http	12320443	640478	63764
58	14:00:38:4326	40	192.168.56.52	10.0.2.15	TCP	ACK	http	1064	640478	12320447	65535
59	14:00:38:4328	629	192.168.56.50	10.0.2.15	TCP	ACK PSH : http reply code = 404	http	1066	704002	28101482	65535
60	14:00:38:4328	629	192.168.56.50	10.0.2.15	TCP	ACK PSH : http reply code = 404	http	1065	768002	39860043	65535

HTTP represents the majority of traffic in the trace

List Key IP Addresses in this Trace - 192.168.56.52

Tools used: CleverView for cTrace Analysis, WHOIS

Clients:
10.0.2.15, 10.0.3.15, 10.0.4.15, 10.0.5.15…all use 8fd12edd2dc1462

Attacker:
192.168.56.52 (hostname: sploitme.com.cn)

Services:
10.0.2.2, 10.0.3.2, 10.0.4.2, 10.0.5.2 (DHCP servers and gateways)
192.168.1.1 (DNS)

Simulated hacked hosts:
192.168.56.51 (hostname: shop.honeynet.sg)
192.168.56.50 (hostname: rapidshare.com.eyu32.ru)

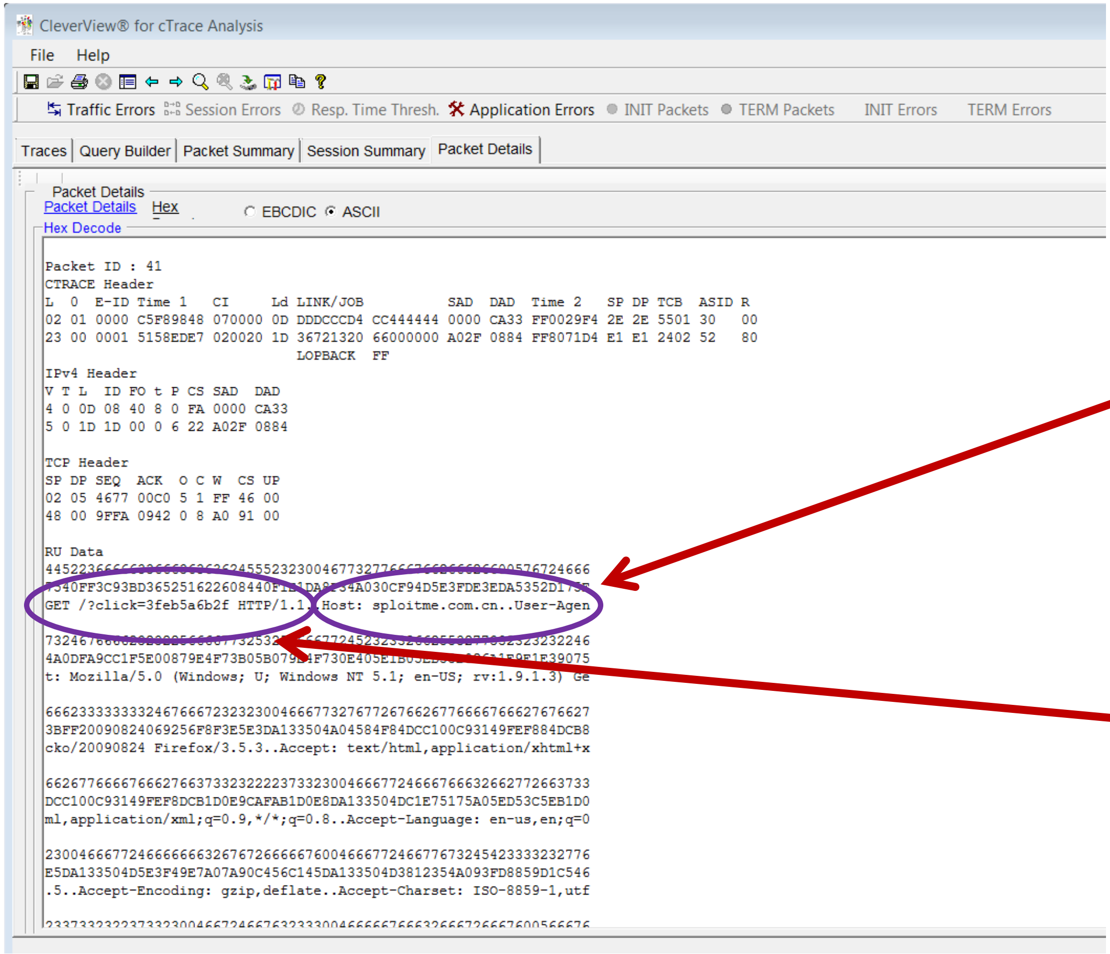
External hosts:
www.honeynet.org, www.google.com www.google.fr, www.google-analytics.com

The clients are most likely VMs, as each has its own subnet, but they share an ethernet adapter, a DNS server (single MAC address, multiple IPs per subnet) and a DHCP server (on a different subnet).

Attacker and hacked hosts reside in the same private subnet. (Not a real-world scenario.)

Hacked Site #1 is probably a ripoff of the well-known rapidshare.com. Hacked Site #2 is an e-commerce site, either innocent (but exploited to serve malicious JS) or malevolent.

List Key IP Addresses in this Trace –
Devil in the Details



```
Packet ID : 41
CTRACE Header
L  0  E-ID Time 1   CI     Ld LINK/JOB          SAD  DAD  Time 2   SP DP TCB  ASID R
02 01 0000 C5F89848 070000 0D DDDCCCD4 CC444444 0000 CA33 FF0029F4 2E 2E 5501 30   00
23 00 0001 5158EDE7 020020 1D 36721320 66000000 A02F 0884 FF8071D4 E1 E1 2402 52   80
                              LOPBACK  FF
IPv4 Header
V T L  ID FO t P CS SAD  DAD
4 0 0D 08 40 8 0 FA 0000 CA33
5 0 1D 1D 00 0 6 22 A02F 0884

TCP Header
SP DP SEQ  ACK  O C W  CS UP
02 05 4677 00C0 5 1 FF 46 00
48 00 9FFA 0942 0 8 A0 91 00

RU Data
445223666663366636362624555232300467732776667666266626600576724666
7540FF3C93BD365251622608440F1E1DA8F34A030CF94D5E3FDE3EDA5352D175E
GET /?click=3feb5a6b2f HTTP/1.1..Host: sploitme.com.cn..User-Agen

73246766662323225666677325325666677245232332662553277332323232246
4A0DFA9CC1F5E00879E4F73B05B079E4F730E405E1B05ED53B026A1E9E1E39075
t: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.3) Ge

66623333333324676667232323004666773276772676626776666766627676627
3BFF20090824069256F8F3E5E3DA133504A04584F84DCC100C93149FEF884DCB8
cko/20090824 Firefox/3.5.3..Accept: text/html,application/xhtml+x

66267766667666276637332322223733230046667724666766632662772663733
DCC100C93149FEF8DCB1D0E9CAFAB1D0E8DA133504DC1E75175A05ED53C5EB1D0
ml,application/xml;q=0.9,*/*;q=0.8..Accept-Language: en-us,en;q=0

23004666772466666663267672666667600466677246677673245423333232776
E5DA133504D5E3F49E7A07A90C456C145DA133504D3812354A093FD8859D1C546
.5..Accept-Encoding: gzip,deflate..Accept-Charset: ISO-8859-1,utf

23373323223733230046672466763233300466666766632666726667600566676
```

Host Details

MAC Address

List the WEB Sites involved and the Malicious Sites?

Tools Used: CleverView for cTrace Analysis: Microsoft Security Bulletins

URL	Comments
http://rapidshare.com.eyu32.ru/login.php Connected to by 10.0.2.15 and 10.0.3.15	Contains an encrypted iframe to page http://sploitme.com.cn/?click=3feb5a6b2f Decryption is done easily by replacing eval() and document.write() with alert()
http://sploitme.com.cn/?click=3feb5a6b2f Connected to by 10.0.2.15 and 10.0.3.15	Sends a redirect to http://sploitme.com.cn/fg/show.php?s=3feb5a6b2f Probably this is a traffic distribution system
http://sploitme.com.cn/fg/show.php?s=3feb5a6b2f Connected to by 10.0.2.15 with User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3	Contains a 404-disguising page with an encrypted javascript, also easily decoded by replacing eval() with alert() The javascript doesn't contain any malicious behaviour, perhaps because the exploit pack doesn't contain an exploit for sent User-Agent (Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3), which corresponds to Firefox v3.5.3

http://www.microsoft.com/technet/security/current.aspx

List the WEB Sites involved and the Malicious Sites?

Tools Used: CleverView for cTrace Analysis: Microsoft Security Bulletins

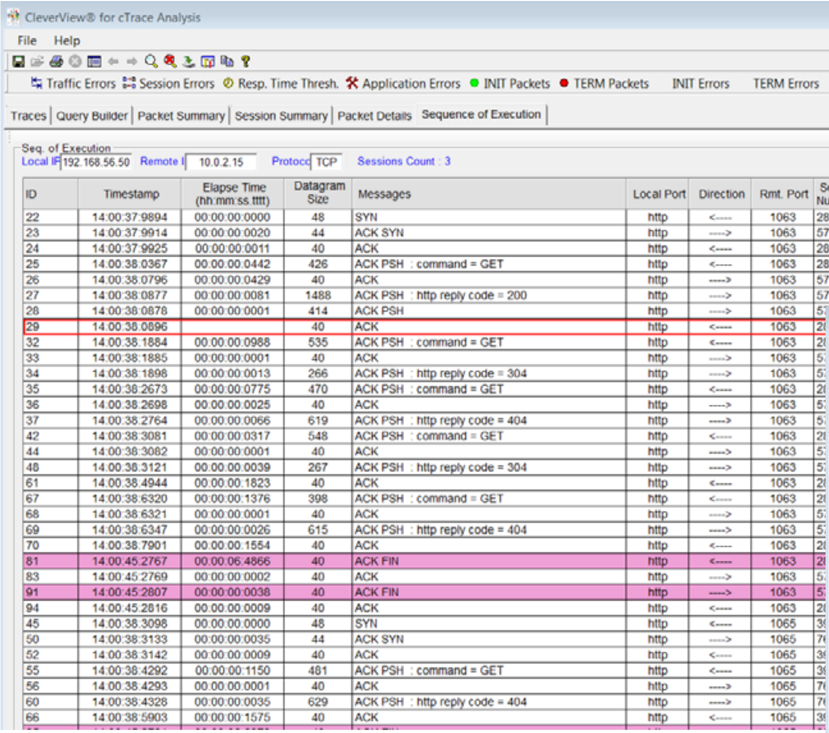
http://sploitme.com.cn/fg/show.php?s=3feb5a6b2f **First request by 10.0.3.15** **with User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)**	The decoded javascript contains an MDAC exploit (MS06-014) which has its effect (download&execute a binary) on the browser. The version of the browser is Internet Explorer v6 accordingly to the User-Agent
http://www.honeynet.org/	Contains no malicious content
http://www.google.com/	Sends a redirect to http://www.google.fr/
http://www.google.fr/	Although it contains a cryptic javascript, it's no malicious
http://sploitme.com.cn/fg/show.php?s=3feb5a6b2f **Second request by 10.0.3.15**	The 404-alike page now doesn't contain any javascript, probably because of an IP ban given by the exploit pack to prevent multiple infections of the same victim

List the WEB Sites involved and the Malicious Sites?

Tools Used: CleverView for cTrace Analysis: Microsoft Security Bulletins

http://shop.honeynet.sg/catalog/ **Requested by 10.0.4.15**	Contains a differently encrypted and inserted iframe to http://sploitme.com.cn/?click=84c090bd86 Decryption: replace document.write() with alert()
http://sploitme.com.cn/?click=84c090bd86 **Requested by 10.0.4.15**	Redirect to http://sploitme.com.cn/fg/show.php?s=84c090bd86
http://sploitme.com.cn/fg/show.php?s=84c090bd86 **Requested by 10.0.4.15** **User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)**	Malicious javascript contains following exploits: 1. MDAC exploit (MS06-014) 2. IWinAmpActiveX exploit (I think it's not gonna work because of an incorrect "classid") 3. DirectShow exploit (MS09-032) 4. MS Access Snapshot Viewer exploit (MS08-041) 5. Msdds.dll COM exploit (MS05-052) 6. Office Web Components exploit (MS09-043) The exploits are being executed in a chain, one after another. All exploits are targeted to perform a download&exec of the same binary.
http://sploitme.com.cn/fg/show.php **Requested by 10.0.5.15** **User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.6) Gecko/20040614 Firefox/0.8**	The page doesn't contain malicious content for the same reason as http://sploitme.com.cn/fg/show.php?s=3feb5a6b2f by 10.0.2.15 or because no 's' variable is specified

How did I get the Detailed Information on Web Sites?

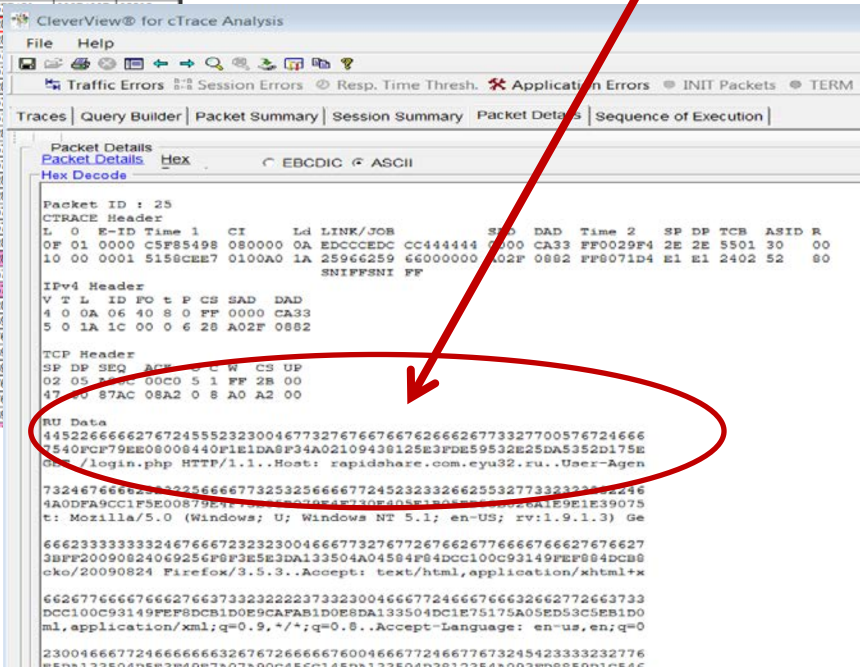


Seq. of Execution

Local IP 192.168.56.50 Remote I 10.0.2.15 Protocol TCP Sessions Count : 3

ID	Timestamp	Elapse Time (hh:mm:ss.tttt)	Datagram Size	Messages	Local Port	Direction	Rmt. Port	Seq. Number	Ack. Number	Window Size
22	14:00:37:9894	00:00:00:0000	48	SYN	http	<----	1063	28274224	0	64240
23	14:00:37:9914	00:00:00:0020	44	ACK SYN	http	---->	1063	576001	28274224	65535
24	14:00:37:9925	00:00:00:0011	40	ACK	http	<----	1063	28274224	576002	64240
25	14:00:38:0367	00:00:00:0442	426	ACK PSH : command = GET	http	<----	1063	28274224	576002	64240
26	14:00:38:0796	00:00:00:0429	40	ACK	http	---->	1063	576002	28274227	65535
27	14:00:38:0877	00:00:00:0081	1488	ACK PSH : http reply code = 200	http	---->	1063	576002	28274227	65535
28	14:00:38:0878	00:00:00:0001	414	ACK PSH	http	---->	1063	57		
29	14:00:38:0896		40	ACK	http	<----	1063	2		
32	14:00:38:1884	00:00:00:0988	535	ACK PSH : command = GET	http	<----	1063	28		
33	14:00:38:1885	00:00:00:0001	40	ACK	http	---->	1063	57		
34	14:00:38:1898	00:00:00:0013	266	ACK PSH : http reply code = 304	http	---->	1063	57		
35	14:00:38:2673	00:00:00:0775	470	ACK PSH : command = GET	http	<----	1063	28		
36	14:00:38:2698	00:00:00:0025	40	ACK	http	---->	1063	57		
37	14:00:38:2764	00:00:00:0066	619	ACK PSH : http reply code = 404	http	---->	1063	57		
42	14:00:38:3081	00:00:00:0317	548	ACK PSH : command = GET	http	<----	1063	28		
44	14:00:38:3082	00:00:00:0001	40	ACK	http	---->	1063	57		
48	14:00:38:3121	00:00:00:0039	267	ACK PSH : http reply code = 304	http	---->	1063	57		
61	14:00:38:4944	00:00:00:1823	40	ACK	http	<----	1063	28		
67	14:00:38:6320	00:00:00:1376	398	ACK PSH : command = GET	http	<----	1063	28		
68	14:00:38:6321	00:00:00:0001	40	ACK	http	---->	1063	57		
69	14:00:38:6347	00:00:00:0026	615	ACK PSH : http reply code = 404	http	---->	1063	57		
70	14:00:38:7901	00:00:00:1554	40	ACK	http	<----	1063	28		
81	14:00:45:2767	00:00:06:4866	40	ACK FIN	http	<----	1063	28		
83	14:00:45:2769	00:00:00:0002	40	ACK	http	---->	1063	57		
91	14:00:45:2807	00:00:00:0038	40	ACK FIN	http	---->	1063	57		
94	14:00:45:2816	00:00:00:0009	40	ACK	http	<----	1063	28		
45	14:00:38:3098	00:00:00:0000	48	SYN	http	<----	1065	39		
50	14:00:38:3133	00:00:00:0035	44	ACK SYN	http	---->	1065	76		
52	14:00:38:3142	00:00:00:0009	40	ACK	http	<----	1065	39		
55	14:00:38:4292	00:00:00:1150	481	ACK PSH : command = GET	http	<----	1065	39		
56	14:00:38:4293	00:00:00:0001	40	ACK	http	---->	1065	76		
60	14:00:38:4328	00:00:00:0035	629	ACK PSH : http reply code = 404	http	---->	1065	76		
66	14:00:38:5903	00:00:00:1575	40	ACK	http	<----	1065	39		

Shows Login to rapidshare.com/eyu32.ru



```
Packet ID : 25
CTRACE Header
L  O  E-ID Time 1   CI     Ld LINK/JOB          SAD  DAD  Time 2   SP DP TCB  ASID R
0F 01 0000 C5F85498 080000 0A EDCCCEDC CC444444 0000 CA33 FF0029F4 2E 2E 5501 30   00
10 00 0001 5158CEE7 0100A0 1A 25966259 66000000 A02F 0882 FF8071D4 E1 E1 2402 52   80
                              SNIFFSNI FF
IPv4 Header
V T L  ID FO t P CS SAD  DAD
4 0 0A 06 40 8 0 FF 0000 CA33
5 0 1A 1C 00 0 6 28 A02F 0882

TCP Header
SP DP SEQ  ACK  O C W  CS UP
02 05 [illegible] 00C0 5 1 FF 2B 00
47 [illegible] 87AC 08A2 0 8 A0 A2 00

RU Data
44522666662767245552323004677327676676676266626773327700576724666
7540FCF79EE08008440F1E1DA8F34A02109438125E3FDE59532E25DA5352D175E
G[illegible] /login.php HTTP/1.1..Host: rapidshare.com.eyu32.ru..User-Agen

7324676666[illegible]2256666773253256666772452323326625532773323[illegible]2246
4A0DFA9CC1F5E00879E[illegible]26A1E9E1E39075
t: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.3) Ge

66623333333324676667232323004666773276772676626776666766627676627
3BFF20090824069256F8F3E5E3DA133504A04584F84DCC100C93149FEF884DCB8
cko/20090824 Firefox/3.5.3..Accept: text/html,application/xhtml+x

66267766667666276637332322223733230046667724666766632662772663733
DCC100C93149FEF8DCB1D0E9CAFAB1D0E8DA133504DC1E75175A05ED53C5EB1D0
ml,application/xml;q=0.9,*/*;q=0.8..Accept-Language: en-us,en;q=0

230046667724666666663267672666667600466677246677673245423333232776
```

Used ‘Sequence of Execution’ to see the communication between the involved sites, then looked at the packet details

What are the Overall Actions Performed by the Hacker?

1. Hacked sites are initialized with javascript code that adds a hidden iframe pointing to sploitme.com/cn?click=x using SQL injections or XSS techniques
2. A client surfs to a hacked site and his browser requests sploitme.com.cn/?click=x which is redirected to sploitme.com.cn/fg/show.php?s=X
3. A 404 page is displayed which is intended to confuse the client
4. The browser executes the javascript which goes through a series of exploits to see if one is successful. (DirectShow is an example)
5. If an exploit is successful it executes a file at sploitme.com.cn/fg/load.php?e=X.
6. Some of the items performed by this malware:
   1. Client computer is a BOT for sending spa,

What Steps Slow Down the Analysis Process?

Iframe’s are difficult for human’s to understand

Malicious page is disguised to look like a 404 page

Javascript is coded using a polymorphic javascript

The sent exploit set depends on what browser the victim is using

Victim’s IP address is ‘banned’ by the exploit pack. In packet 366 the victim tries to access the show.php file again but gets a ‘clean’ 404 page

What Operating Systems, software, and Vulnerabilities were involved?

Exploit	Vulnerable Component	Published	Reference	Remedy
I	MDAC RDS.Dataspace ActiveX control	Apr 2006	CVE-2006-0003	MSB-MS06-014
II	AOL IWinAmpActiveX control (AmpX.dll)	May 2009	OSVDB-54706	(none)
III	DirectShow ActiveX control (msvidctl.dll)	Jul 2009	CVE-2008-0015	MSB-MS09-032
IV	Office Snapshot Viewer ActiveX control	Jul 2008	CVE-2008-2463	MSB-MS08-041
V	COM Object Instantiation (msdds.dll)	Aug 2005	CVE-2005-2127	MSB-MS05-052
VI	Office Web Components ActiveX control	Jul 2009	CVE-2009-1136	MSB-MS09-043

Summary

- Forensic science is application of science to questions of interest to the legal profession
- Several unique opportunities give computer forensics the ability to uncover evidence that would be extremely difficult to find using a manual process
- Computer forensics also has a unique set of challenges that are not found in standard evidence gathering, including volume of electronic evidence, how it is scattered in numerous locations, and its dynamic content
- Searching for digital evidence includes looking at "obvious" files and e-mail messages
- Need for information security workers will continue to grow, especially in computer forensics
- Skills needed in these areas include knowledge of TCP/IP, packets, firewalls, routers, IDS, and penetration testing

AES Sessions at Share

Mar 12, 2012: 1:30-2:30 10715: Keeping Your Network at Peak Performance as You Virtualize the Data Center
Mar 14, 2012: 8:00-9:00 10397: IPv6 Basics
Mar 14 2012: 1:30-2:30 10395: IPv6 Tunneling Technologies
Mar 14, 2011: 1:30-2:30 10720: **Network Problem Diagnosis with OSA Examples**
Mar 15, 2012: 3:00-4:00 10401: IPv6 Transitioning
Mar 16, 2012 9:30-10:30 10393: CSI Maui: The Case of the Compromised Server
Mar 16 2012 11:00-12:00 10414 IPv6 Deep Dive

Vielen Dank

QUESTIONS?

Köszönettel

Obi

Спасибо

ขอบคุณ

شكراً

Bedankt

Gracias

Ευχαριστώ

شكرا

धन्यवाद

THANK YOU

Merci

Díky

Grazie

Danke

Hvala

תודה

ありがとうございました

Merci

ขอบคุณ

Teşekkürler

धन्यवाद
Hindi

Gracias

laurak@aesclever.com

www.aesclever.com

감사합니다

நன்றி
Tamil

650-617-2400

Obrigado