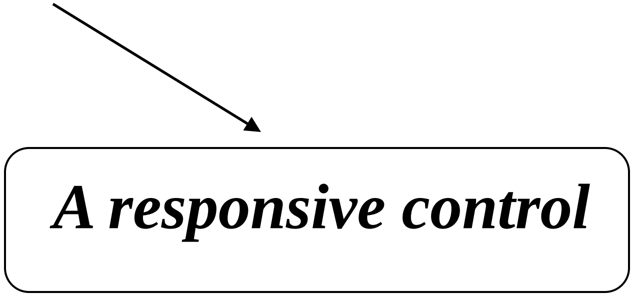
Computer Evidence Collection & Investigation Process

Definition:

Computer forensics *involves* ***obtaining*** *and* ***analyzing*** *digital information for use as evidence.*



A responsive control

Where is this digital information captured from?

Computer storage media;

Data in transit, etc

What is Possible with Computer Forensics?

Recovery of deleted data;

Discovery of when files were modified, created, deleted and organized;

What applications were installed;

Which websites have been visited

What is Not Possible

If the digital media is completely (physically) destroyed, recovery is impossible;

If digital media is securely overwritten, recovery is very complicated or impossible.

When is Computer Forensics Needed?

Insurance Fraud;

Illegal software uses;

Hacking;

Email misuse;

Money laundering;

Destruction/altering of data;

Intellectual property theft.

Purposes of Forensic Audit Process

Computer forensics is conducted for :three purposes

(a). Investigating and analyzing computer systems as related to violation of laws.

(b). Investigating and analyzing computer systems for compliance with an organization's policies.

(c). Investigating computer systems that have been remotely attacked.

Digital Evidence

- ✓*Digital evidence can be retrieved from computers, cell phones, pagers, PDAs, digital cameras, and any device that has memory or storage*

- ✓*Extremely susceptible to tampering*

Standards of Digital Evidence

- *If evidence will be used in court proceedings or actions that could be challenged legally, evidence must meet these three standards:*

  - ✓ ***Sufficiency:*** *The evidence must be convincing or measure up without question*

  - ✓ ***Competency:*** *The evidence must be legally qualified and reliable*

  - ✓ ***Relevancy:*** *The evidence must be material to the case or have a bearing on the matter at hand.*

Principles of Digital Evidence

- *Investigation/analysis performed on seized digital evidence should not change evidence in any form;*

- *Evidence should only be manipulated and analyzed on a* ***copy of original source;(cloning)***

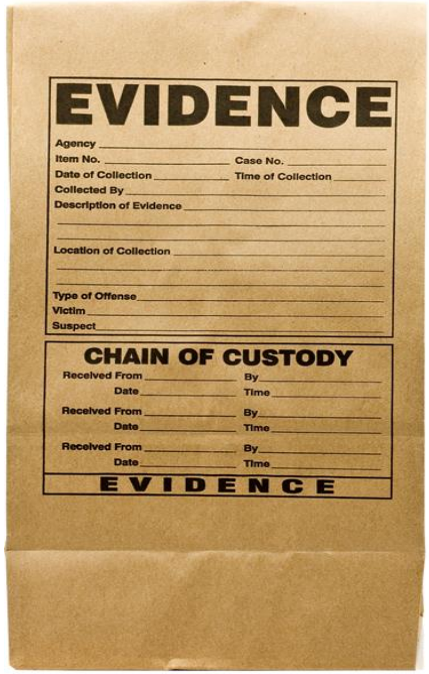
- *Individual must be forensically competent to be given permission to* ***access original*** *digital evidence;*

- *Activity relating to* ***seizure, access, storage, or transfer of digital*** *evidence must be fully* ***documented****, preserved, and available for review*

Identify & Labelling Evidence

- Mark evidence properly as it is collected so that it can be identified as the particular piece of evidence gathered at the scene.
  - ❑ Label and store evidence properly.
  - ❑ Ensure that the labels cannot be removed easily.
  - ❑ Keep a logbook.
  - ❑ Identify each piece of evidence (in case the label is removed).

Identify & Labelling Evidence



EVIDENCE

Agency ____________

Item No. ______ Case No. ______

Date of Collection ______ Time of Collection ______

Collected By ____________

Description of Evidence ____________

Location of Collection ____________

Type of Offense ____________

Victim ____________

Suspect ____________

CHAIN OF CUSTODY

Received From ______ By ______

Date ______ Time ______

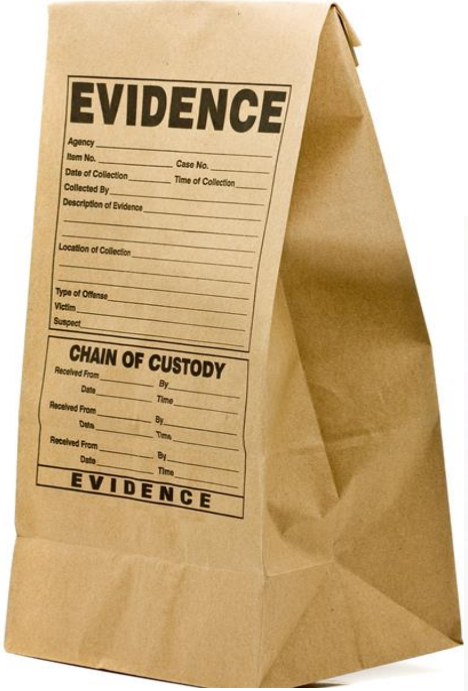
Received From ______ By ______

Date ______ Time ______

Received From ______ By ______

Date ______ Time ______

EVIDENCE



EVIDENCE

Agency ____________

Item No. ______ Case No. ______

Date of Collection ______ Time of Collection ______

Collected By ____________

Description of Evidence ____________

Location of Collection ____________

Type of Offense ____________

Victim ____________

Suspect ____________

CHAIN OF CUSTODY

Received From ______ By ______

Date ______ Time ______

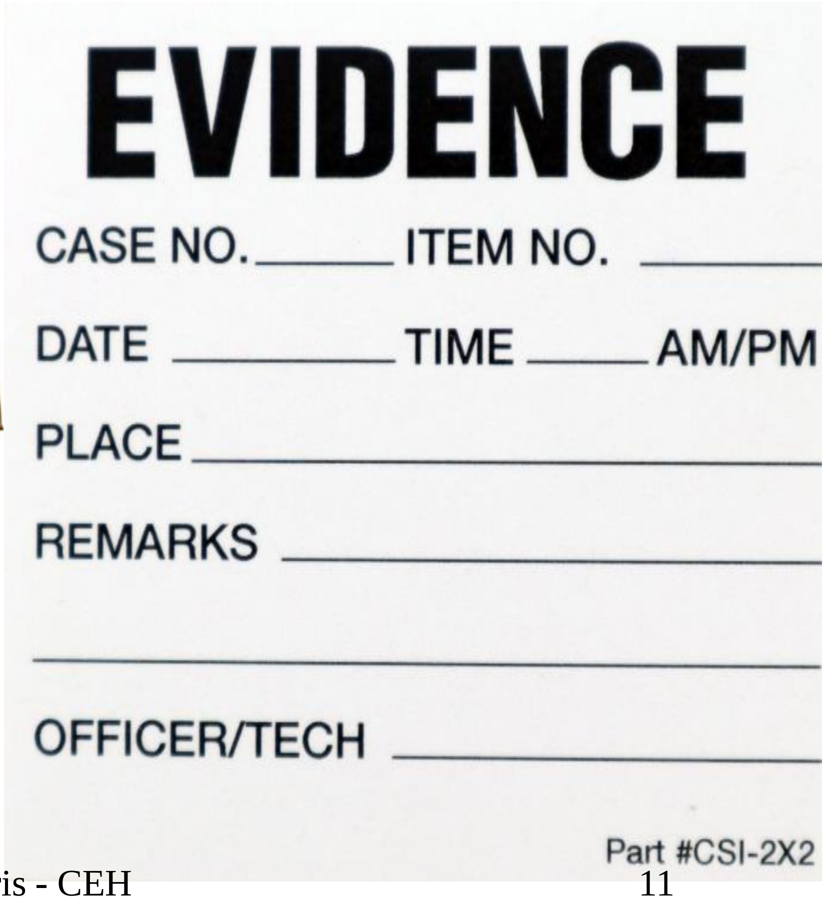
Received From ______ By ______

Date ______ Time ______

Received From ______ By ______

Date ______ Time ______

EVIDENCE



EVIDENCE

CASE NO. ______ ITEM NO. ______

DATE ______ TIME ______ AM/PM

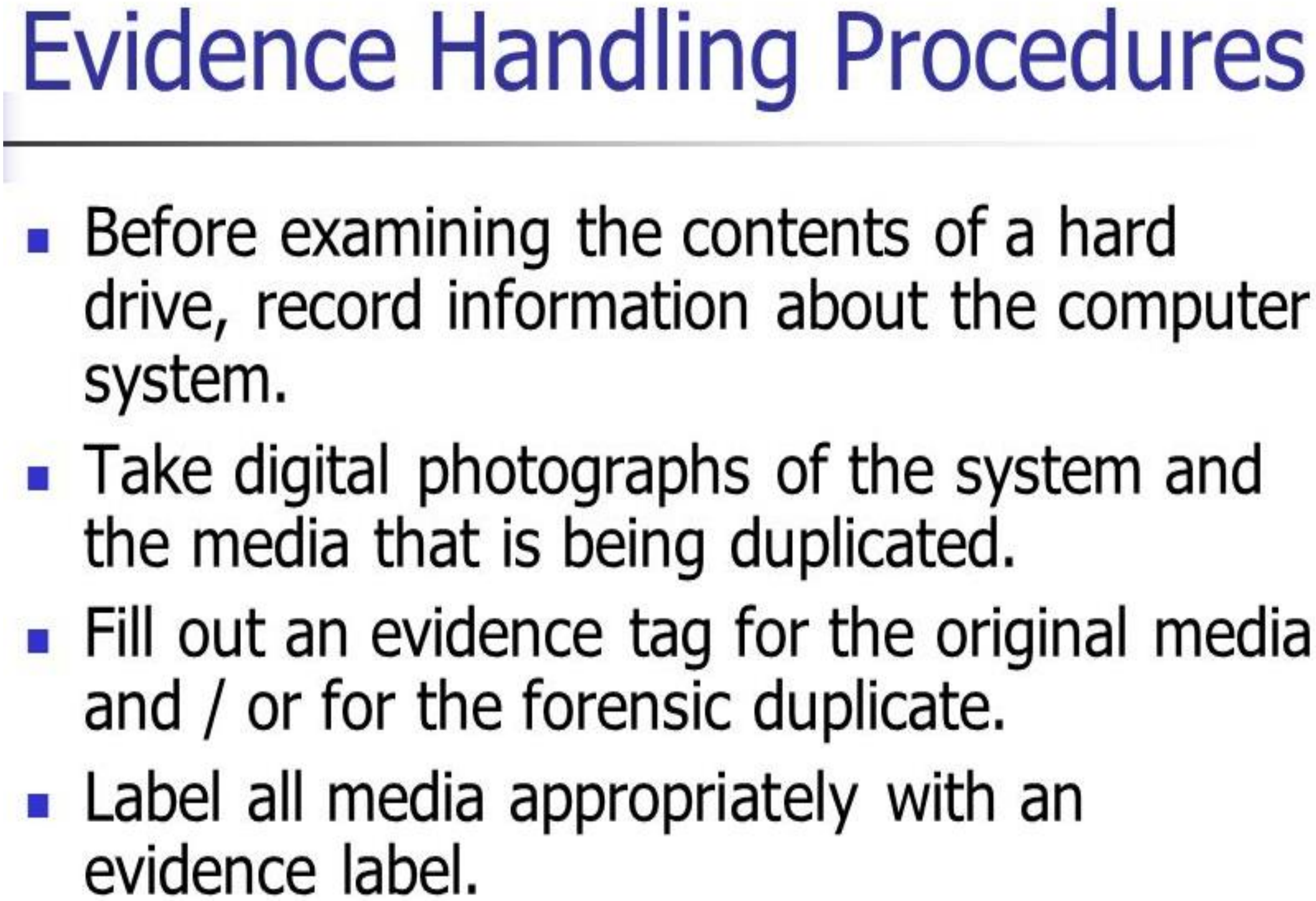
PLACE ____________

REMARKS ____________

____

OFFICER/TECH ____________

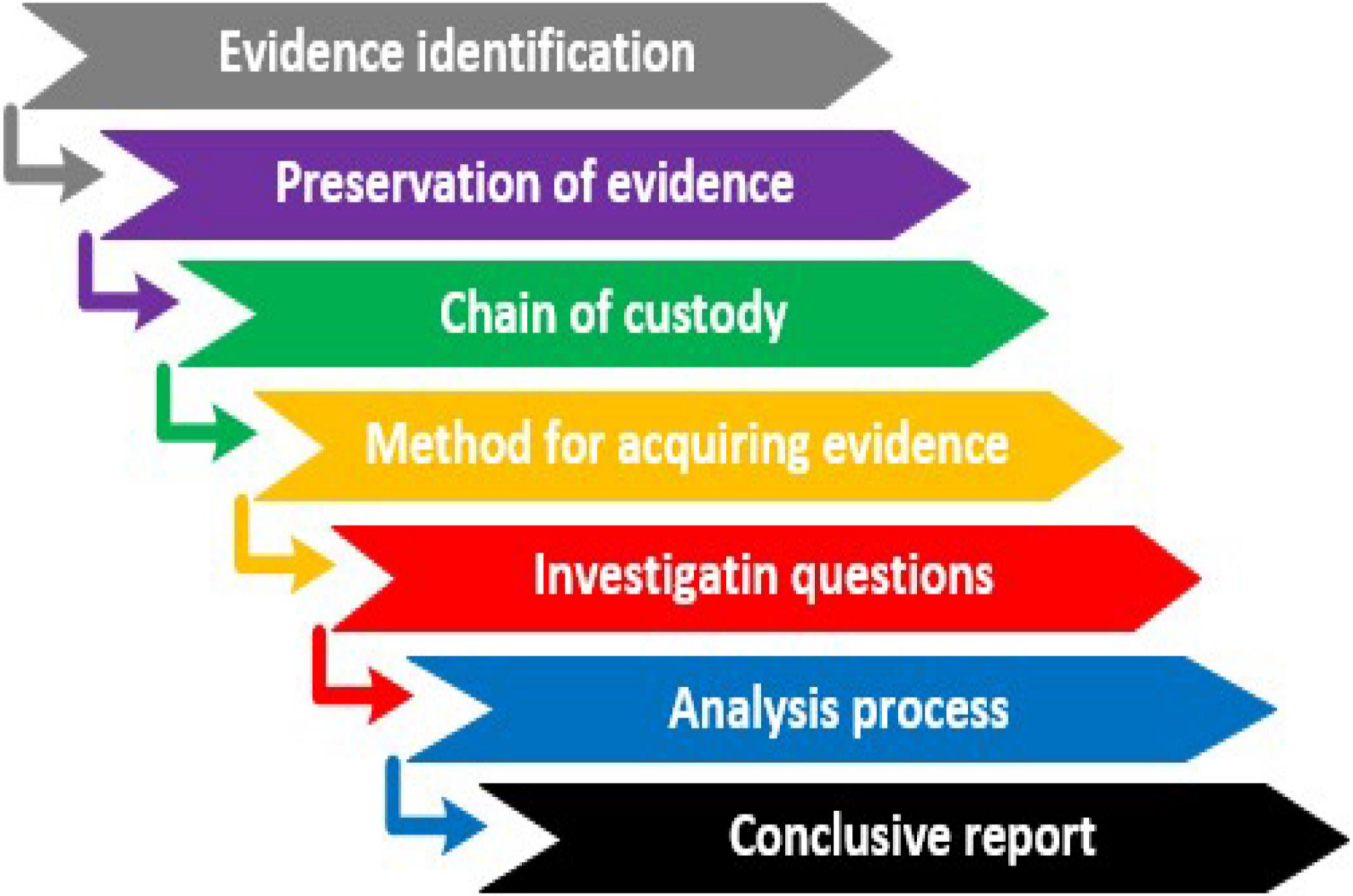
Part #CSI-2X2



Evidence Handling Procedures

- Before examining the contents of a hard drive, record information about the computer system.
- Take digital photographs of the system and the media that is being duplicated.
- Fill out an evidence tag for the original media and / or for the forensic duplicate.
- Label all media appropriately with an evidence label.

Evidence handling Procedure



Evidence identification

Preservation of evidence

Chain of custody

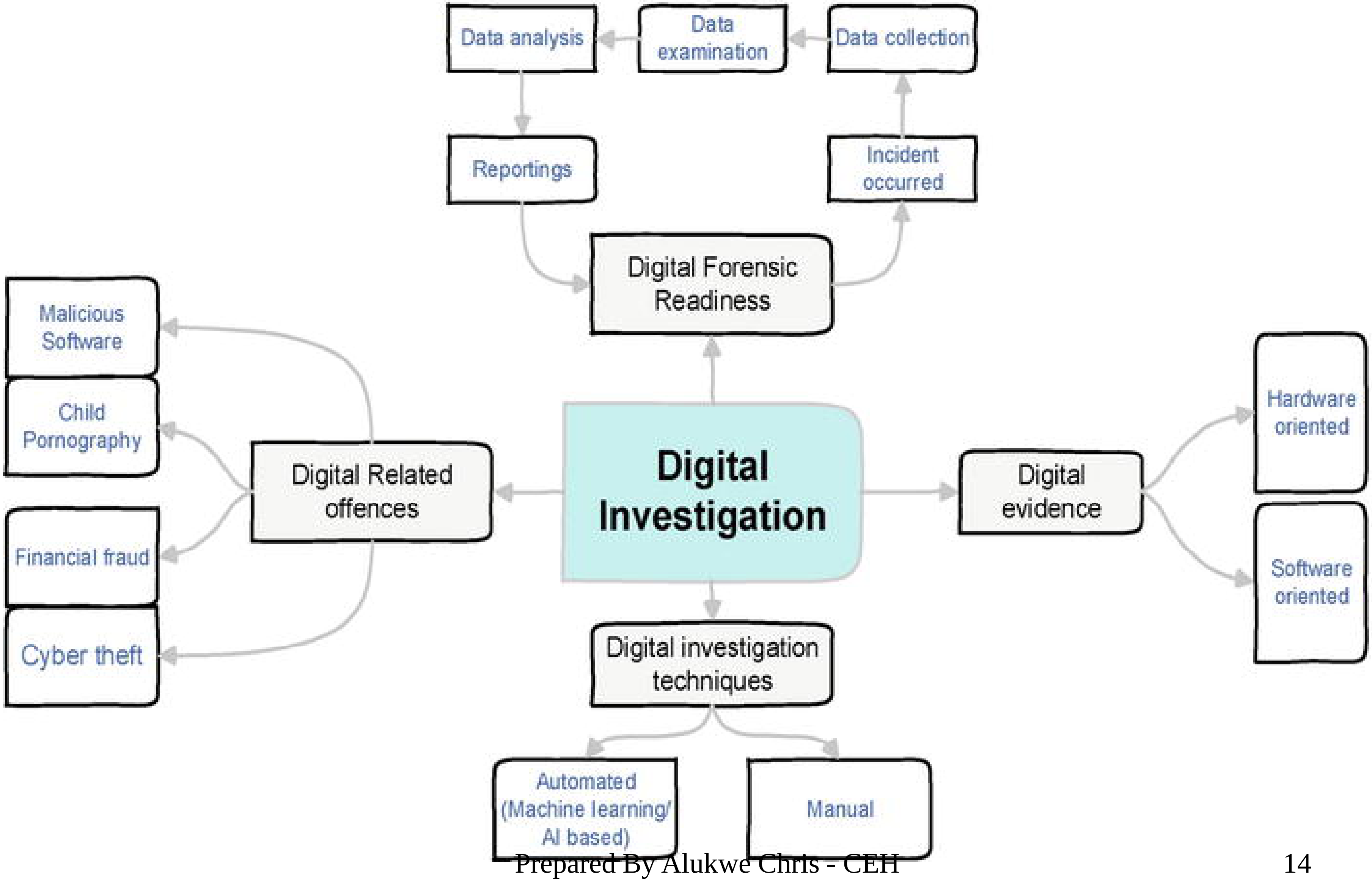
Method for acquiring evidence

Investigatin questions

Analysis process

Conclusive report

Forensic Investigation Using Machin Learning Approach



Identify Evidence (cont'd)

- The information should be **specific enough for Presentation later in the court.**

  - ❑ *Log other identifying marks, such as **device make, model, serial number, and cable configuration or type**.*
  - ❑ *Note any type of damage to the piece of evidence.*

- It is important to be methodical while identifying evidence.
  - ❑ ***Do not collect evidence by yourself—have a second person witness the actions.***

Identify Evidence (cont’d)

- ❑ Protect evidence from electromagnetic or mechanical damage (EMI, Radiations)
  - ❑ Ensure that the evidence is not tampered, damaged, or compromised by the procedures used during the investigation.
  - ❑ Do not damage evidence – Avoids liability problems later.
  - ❑ Protect evidence from extremes in heat and cold, humidity, water, magnetic fields, and vibration.
  - ❑ Use static-free evidence protection gloves, not standard latex gloves.
  - ❑ Seal the evidence in a proper container with evidence tape.

Static-free evidence protection gloves

Three rules of Evidence

- ***Best Evidence Rule***
  - *Courts prefer original evidence rather than a copy to ensure no alteration of the evidence has occurred.*
- ***Exclusionary Rule***
  - *The Fourth Amendment to the United States Constitution precludes illegal search and seizure and, therefore, any evidence collected in violation of the Fourth Amendment is not admissible as evidence.*
- ***Hearsay Rule***
  - *Hearsay is second-hand evidence—evidence not gathered from the personal knowledge of the witness.*

Guidelines for Collecting Evidence

- ❑ While conducting the investigation, analyze computer storage carefully.
- ❑ Analyze a copy of the system and not the original system – that is evidence.
- ❑ Conduct analysis in a controlled environment with:
  1. Strong physical security
  2. Minimal traffic
  3. Controlled access

Guidelines for Collecting Evidence

❑ Unless there are specific tools to take forensic images under Windows, DOS should be used for imaging process instead of standard Windows.

❑ Boot it from a floppy disk or a CD, and have only the minimal amount of software installed to preclude propagation of a virus or the inadvertent execution of a Trojan horse or other malicious program.

❑ Windows can then be used to examine copies of the system.

Collecting Evidence

- *Each investigation is different. Given below is an example of a comprehensive investigation.*

  - ❑ *Remove or image only one component at a time.*

  - ❑ *Remove the hard disk and label it – use an anti-static or static-dissipative wristband and mat before beginning the investigation.(grounding oneself)*

  - ❑ *Identify the disk type (Integrated Drive Electronics (IDE), Small Computer System Interface (SCSI)SATA, or other type).*

  - ❑ *Image the disk with a bit-level copy, sector by sector – this will retain deleted files, etc.*

Collection Steps

- ***Proceed from more volatile assets to less:***

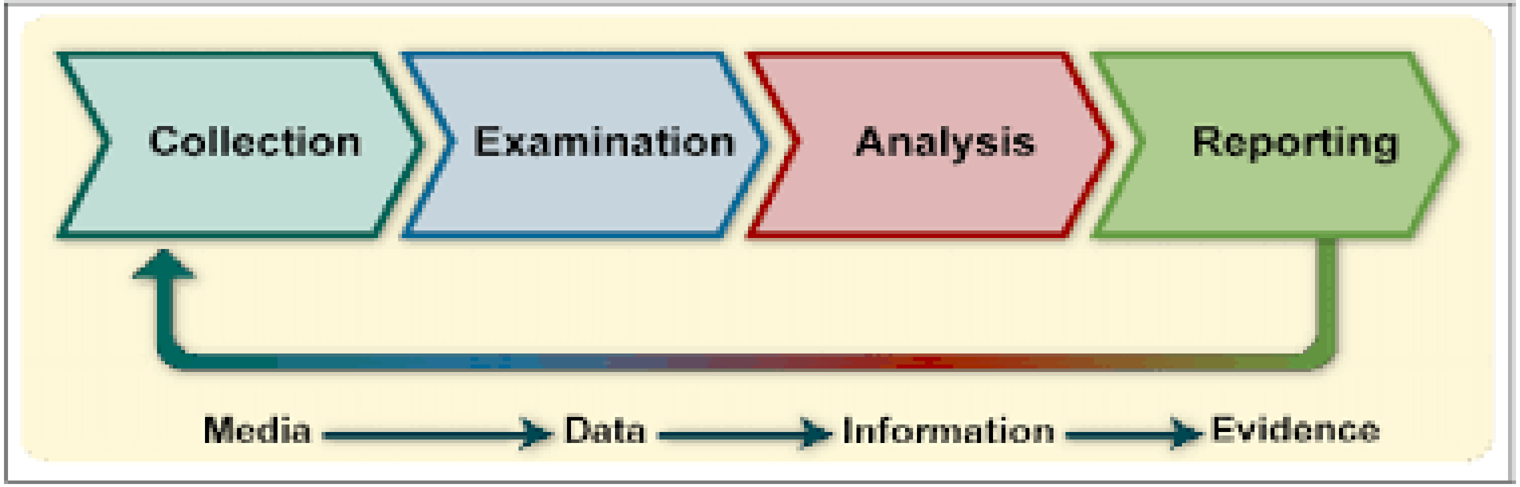
  - ❑ *Memory*
  - ❑ *Registry, routing table, arp cache, process cache*
  - ❑ *Network connections*
  - ❑ *Temporary files*
  - ❑ *Disk or storage device*

1. *Check processes running on the system*
2. *Copy arp cache, routing table, registry, status of network connections*
3. *Capture temporary files*
4. *Make byte-by-byte copy of entire media*
5. *Remove and store original media in a secure location*
6. *Do not run programs that modify files or their access times*
7. *Do not shutdown until the most volatile evidence has been collected*
8. *Do not trust programs on the system*
9. *Document the procedure*

Chain of Custody

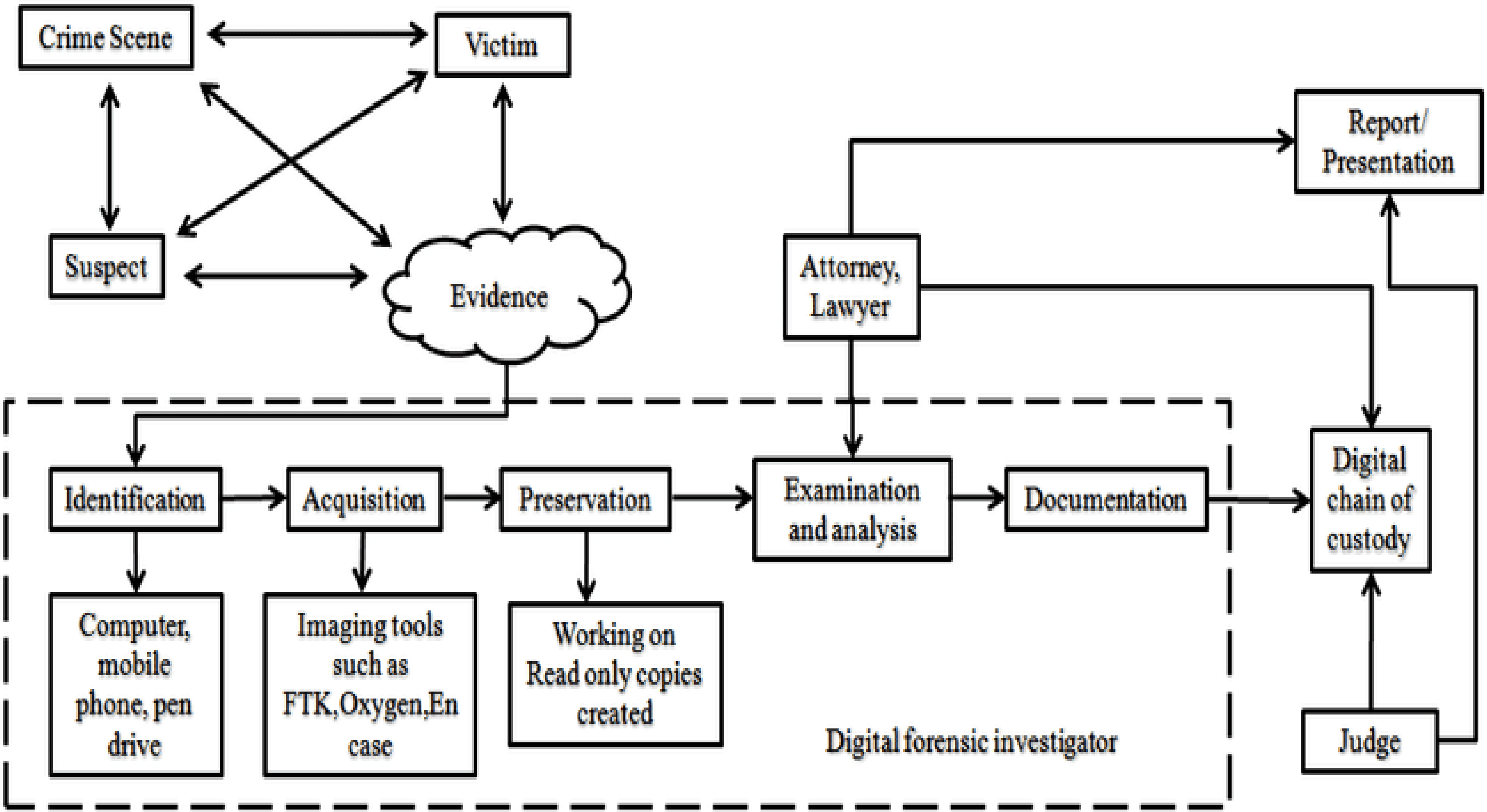
- ❑ *The chain of custody accounts for all persons who handled or had access to the evidence.*

- ❑ *It shows who obtained the evidence, when and where it was obtained, where it was stored, and who had control or possession of the evidence.*



Digital Forensic Chain of Custody

Relationship btwn Crime Scene & Chain of Custody



Chain of Custody (cont'd)

- ***Steps in the chain of custody are:***

  - ❑ *Record each item collected as evidence.*
  - ❑ *Record who collected the evidence along with the date and time.*
  - ❑ *Document a description of the evidence.*
  - ❑ *Put the evidence in containers and tag the containers with the case number the name of the person who collected it, and the date and time.*

Chain of Custody (cont'd)

- ***Steps in the chain of custody are (continued):***

❑ *Record all message digest (hash) values in the documentation.*

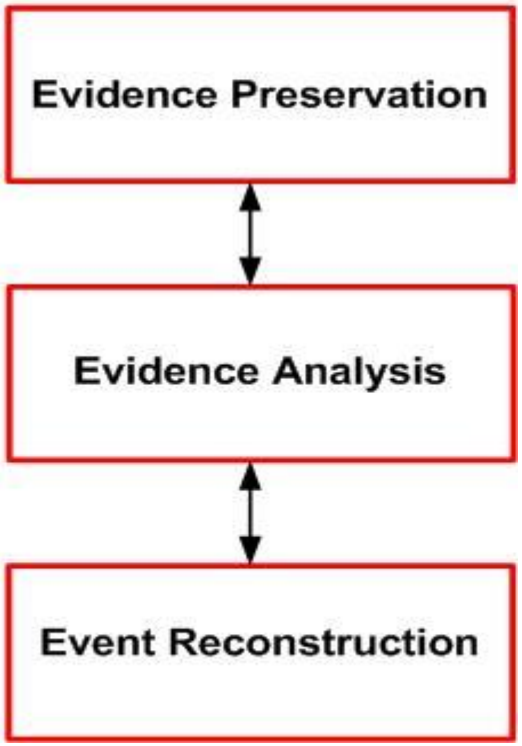
❑ *Securely transport the evidence to a protected storage facility.*

❑ *Obtain a signature from the person who accepts the evidence at this storage facility.*

❑ *Provide controls to prevent access to and compromise of the evidence while it is being stored.*

❑ *Securely transport it to the court for proceedings.*

Digital Investigation Process



Evidence Preservation

Evidence Analysis

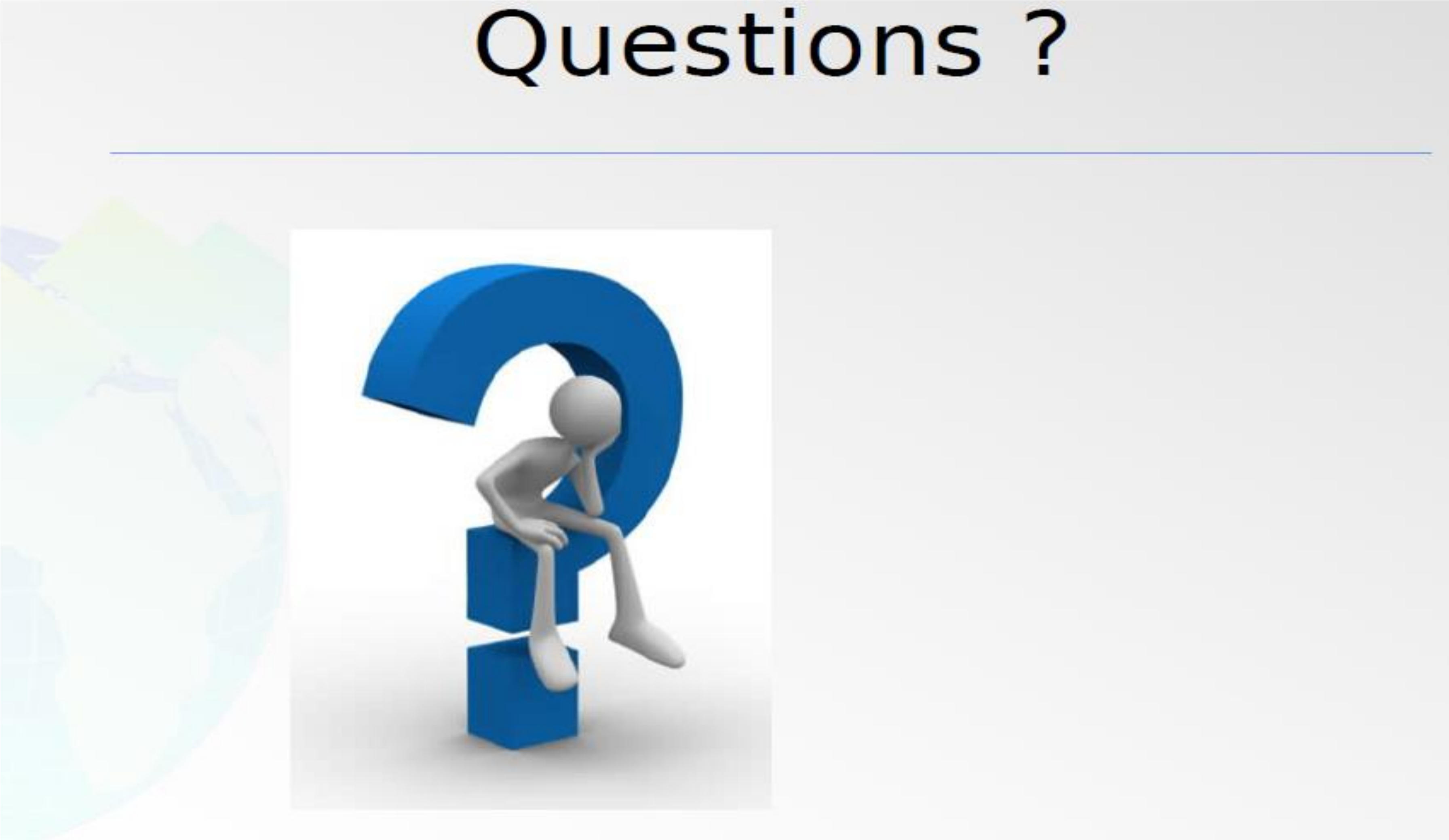
Event Reconstruction

-> Media Acquisition

-> Answer questions

-> Ensure answers are correct to the extent possible

Full process recommended in forensics but may take short-cuts in some investigations, eg skip directly to evidence analysis on live system



Questions ?

Extra Notes for Personal reading

Internet Forensics Analysis: Profiling the Cybercriminal – Internet Protocols

Internet Protocols

Internet *protocols* are those rules allowing different operating systems and machines to communicate with one another over the Internet.

The Internet

Transmission Control Protocol (TCP) divides electronic messages into "packets" of information and then reassembles these packets at the end.

Internet Protocol (IP) assigns a unique address to each computer on the Internet.

Transmission Control Protocol (TCP) and Internet Protocol (IP)

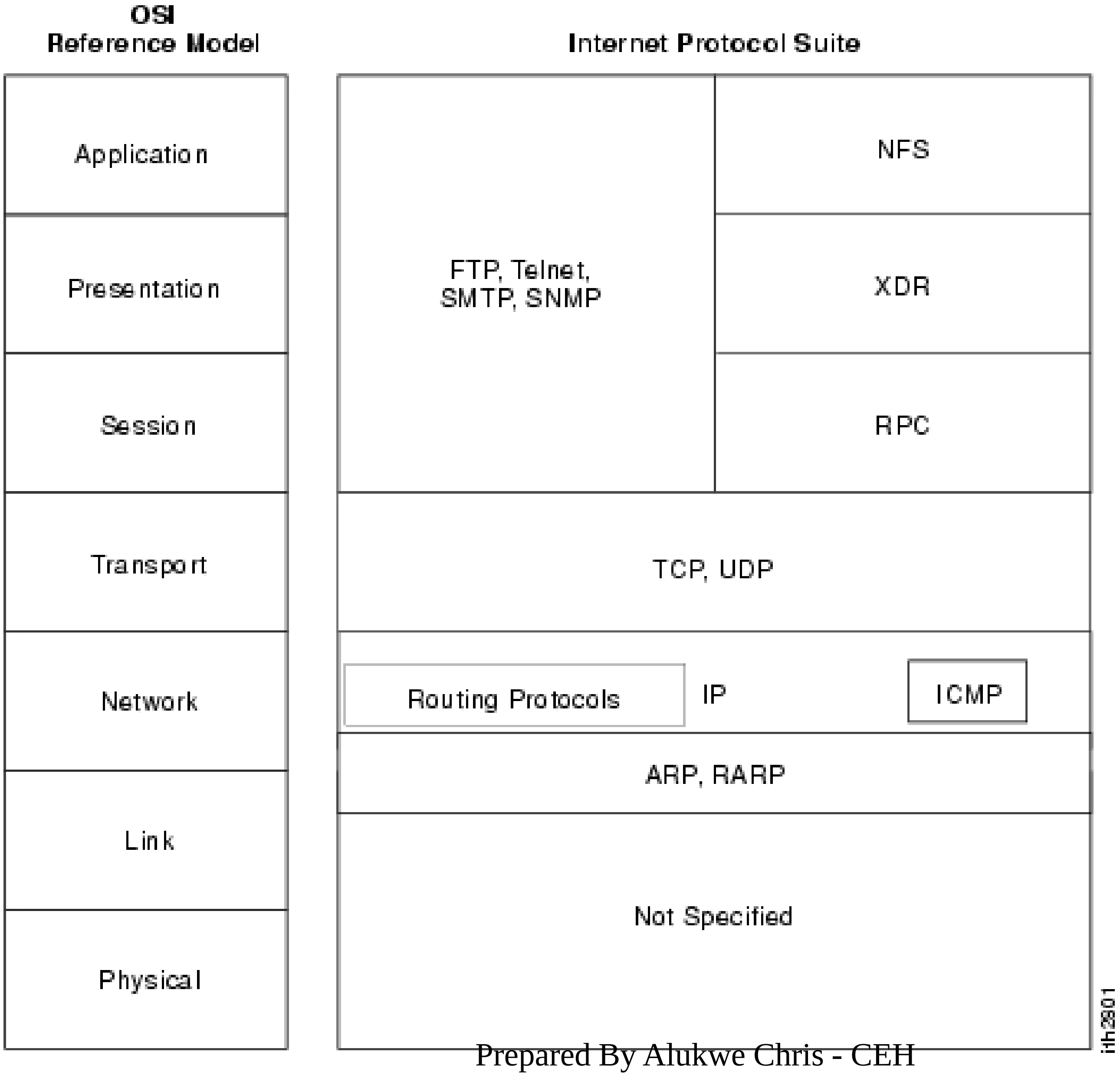
- TCP/IP protocols are the communication guidelines used and widely supported over the Internet.

- Almost every packet of information sent over the Internet uses the *datagrams* contained within a TCP/IP envelope. The datagrams consist of layers of information needed to verify the packet and get the information from the sender's to the receiver's location following traffic control guidelines.

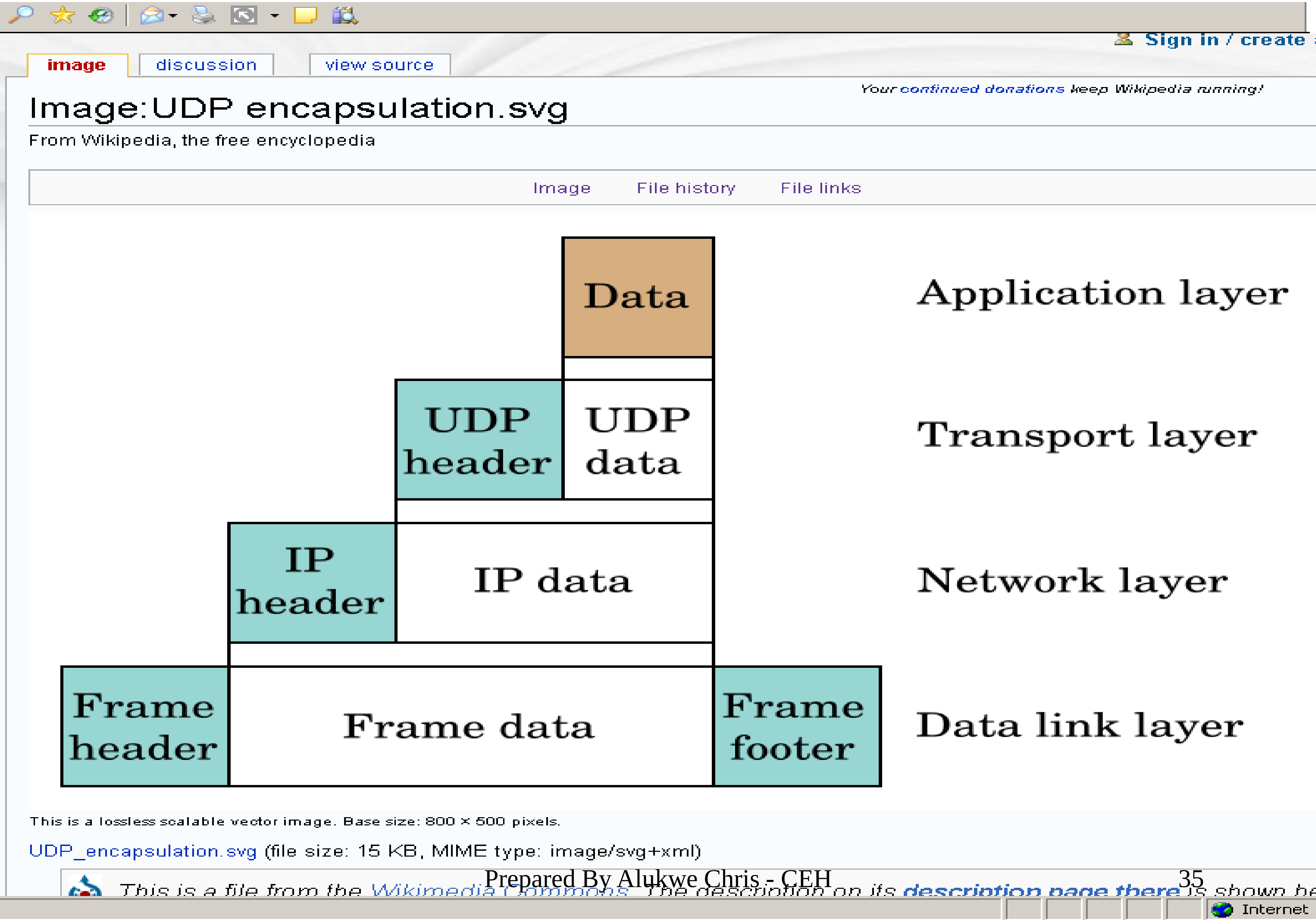
OSI Model

	Data unit	Layer	Function
Host layers	Data	Application	Network process to application
		Presentation	Data representation and encryption
		Session	Interhost communication
	Segments	Transport	End-to-end connections and reliability (TCP)
Media layers	Packets	Network	Path determination and logical addressing (IP)
	Frames	Data link	Physical addressing (MAC & LLC)
	Bits	Physical	Media, signal and binary transmission

Figure 30-1 Internet protocols span the complete range of OSI model layers.



Internet Protocol (IP)



Your continued donations keep Wikipedia running!

Image:UDP encapsulation.svg

From Wikipedia, the free encyclopedia

This is a lossless scalable vector image. Base size: 800 × 500 pixels.

UDP_encapsulation.svg (file size: 15 KB, MIME type: image/svg+xml)

This is a file from the Wikimedia Commons. The description on its description page there is shown be

TCP/IP Connections

- A three-way handshake synchronizes both ends of a connection by allowing both sides to agree upon initial sequence numbers. This mechanism also guarantees that both sides are ready to transmit data and know that the other side is ready to transmit as well.
- SYN → SYN/ACK → ACK → FIN

Popular Protocols

- *DNS:* The Domain Name System
- *Finger:* Used to determine the status of other hosts and/or users
- *FTP:* The File Transfer Protocol allows a user to transfer files between local and remote host computers
- *HTTP:* The Hypertext Transfer Protocol is the basis for exchange of information over the World Wide Web

Popular Protocols

- IMAP: The Internet Mail Access Protocol defines an alternative to POP as the interface between a user's mail client software and an e-mail server, used to download mail from the server to the client

- Ping: A utility that allows a user at one system to determine the status of other hosts and the latency in getting a message

- POP: The Post Office Protocol defines a simple interface between a user's mail client software and an e-mail server

Popular Protocols

- *SSH:* The Secure Shell is a protocol that allows remote logon to a host across the Internet

- *SMTP:* The Simple Mail Transfer Protocol is the standard protocol for the exchange of electronic mail over the Internet

- *SNMP:* The Simple Network Management Protocol defines procedures and management information databases for managing TCP/IP-based network devices

- *Telnet:* Short for *Telecommunication Network*, a virtual terminal protocol allowing a user logged on to one TCP/IP host to access other hosts

Web Log Entries

- One important method for finding the web trail of an attacker is in examining web logs.

- Recorded network logs provide information needed to trace all website usage.
- Web Log = Blog

- Also check transaction logs and server logs

Web Log Entries

- Information provided in a log includes the ***visitor's IP address, geographical location, the actions the visitor performs on the site, browser type, time on page, and the site the visitor used before arriving.***

- Logs should be stored on a separate computer from the web server hosting the site so they cannot be easily altered.

TCPDUMP

- *TCPDUMP is a form of network sniffer that can disclose most of the information contained in a TCP/IP packet.*
- *Windows uses WinDUMP*
- *A sniffer is a program used to secretly capture datagrams moving across a network and disclose the information contained in the datagram’s network protocols.*

Decoding Simple Mail Transfer Protocol (SMTP)

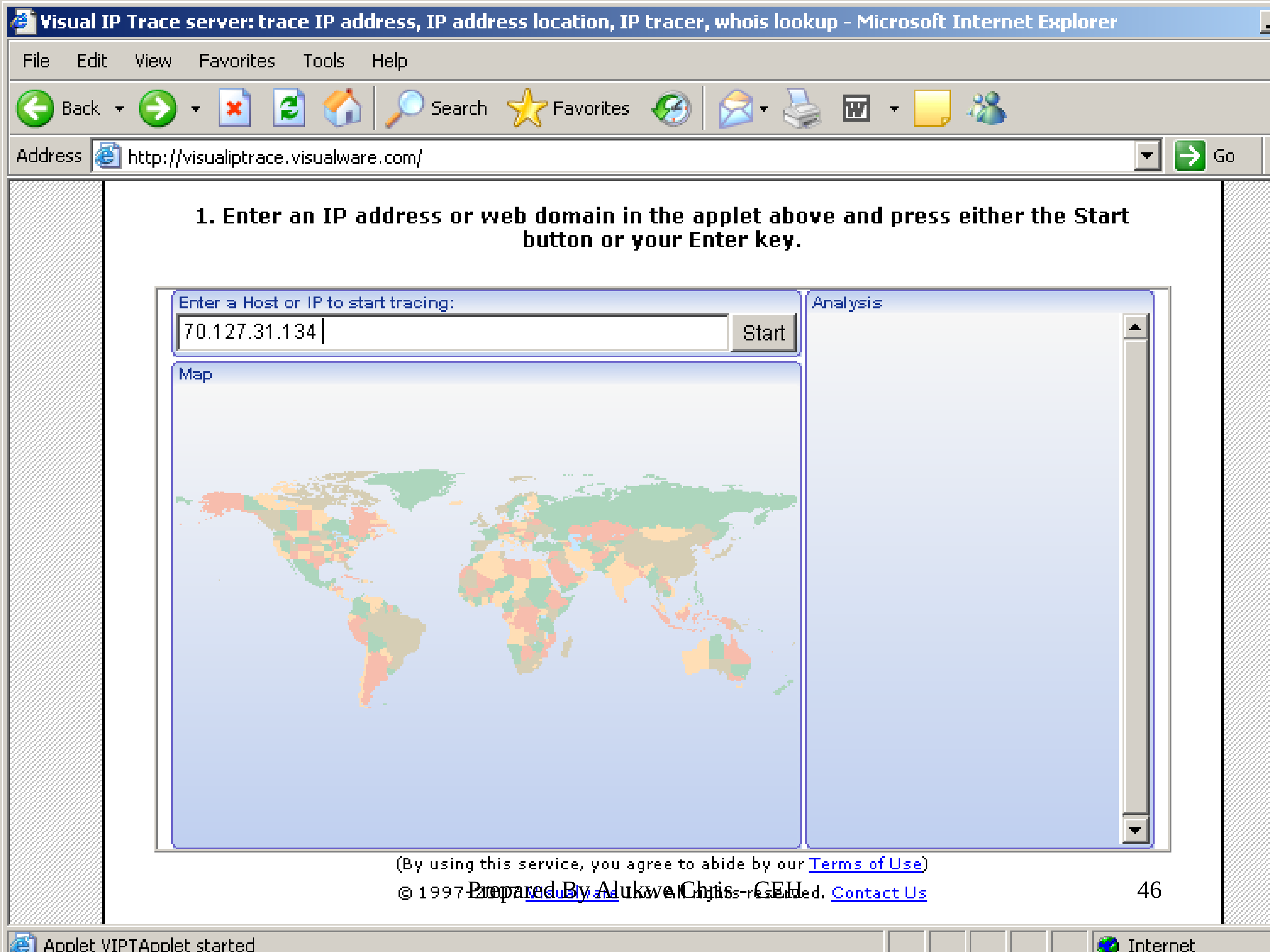
- SMTP is the protocol used to send e-mail over the Internet.
- SMTP server logs can be used to check the path of the e-mail from the sending host to the receiving host.

Decoding Simple Mail Transfer Protocol (SMTP)

Most of the important information about the origin of an e-mail message is in the long form of the header. The most important data for tracing purposes is the IP addresses and the message ID.

Tracing and Decoding IP Addresses

- *Traceroute*
- *Whois*
- *Ping*
- *Finger searches*



Visual IP Trace server: trace IP address, IP address location, IP tracer, whois lookup - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address
Go
Start
Map
Analysis
Applet VIPTApplet started
Internet

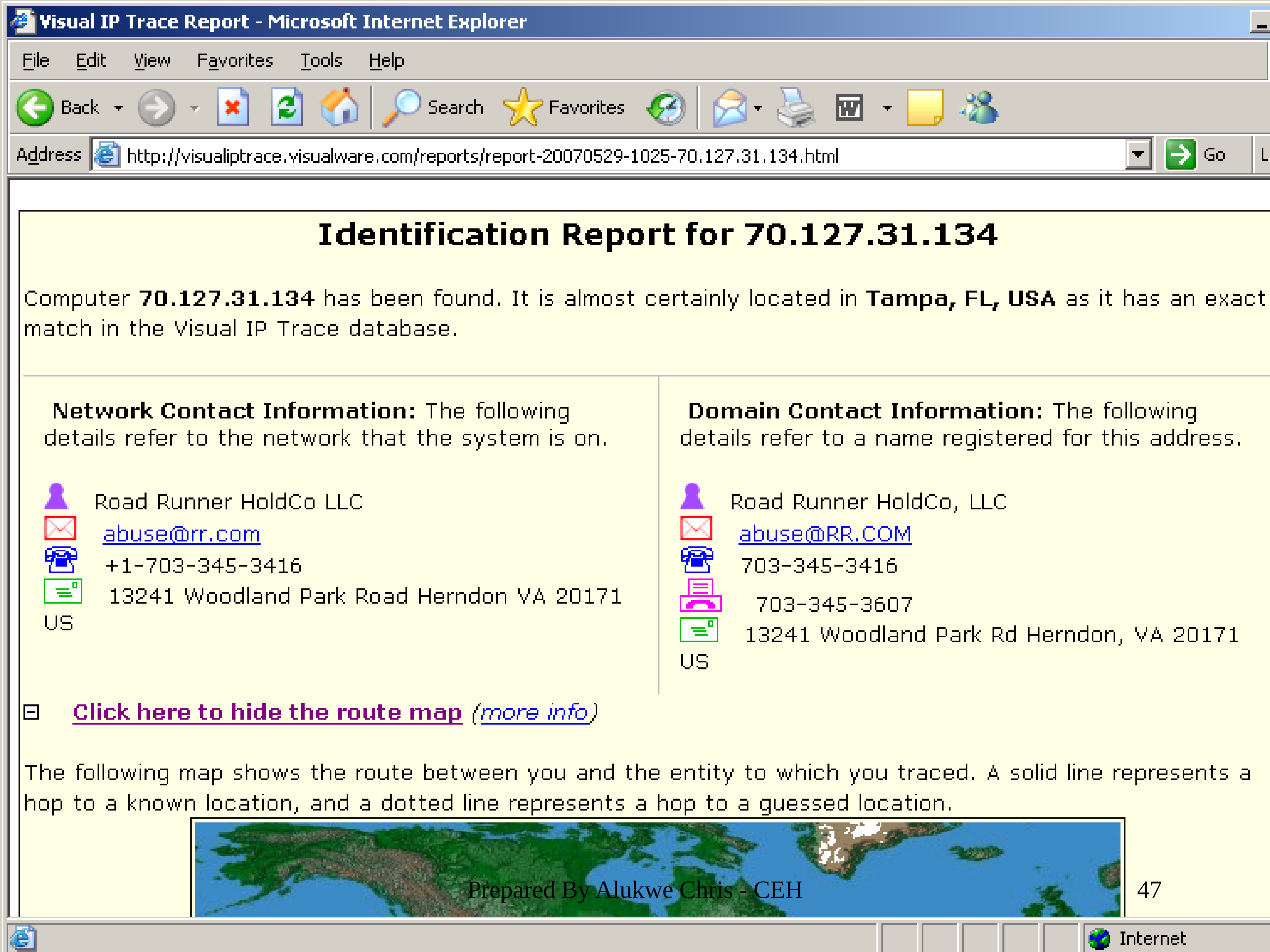
Address: http://visualiptrace.visualware.com/

1. Enter an IP address or web domain in the applet above and press either the Start button or your Enter key.

Enter a Host or IP to start tracing: 70.127.31.134

(By using this service, you agree to abide by our Terms of Use)

© 1997-2007 Visualware Inc. All rights reserved. Contact Us



http://visualiptrace.visualware.com/reports/report-20070529-1025-70.127.31.134.html

Identification Report for 70.127.31.134

Computer **70.127.31.134** has been found. It is almost certainly located in **Tampa, FL, USA** as it has an exact match in the Visual IP Trace database.

Network Contact Information: The following details refer to the network that the system is on.

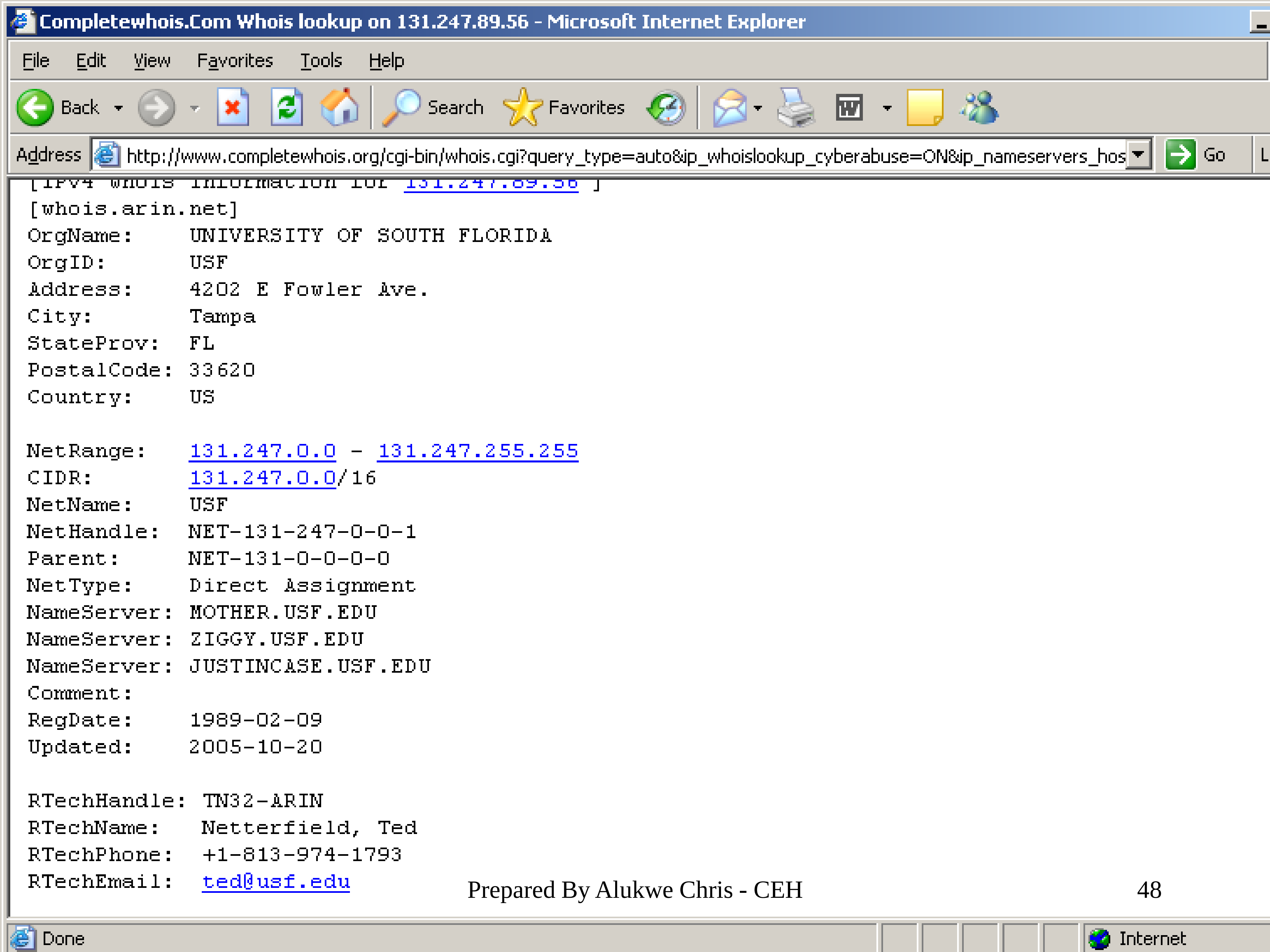
Road Runner HoldCo LLC
abuse@rr.com
+1-703-345-3416
13241 Woodland Park Road Herndon VA 20171
US

Domain Contact Information: The following details refer to a name registered for this address.

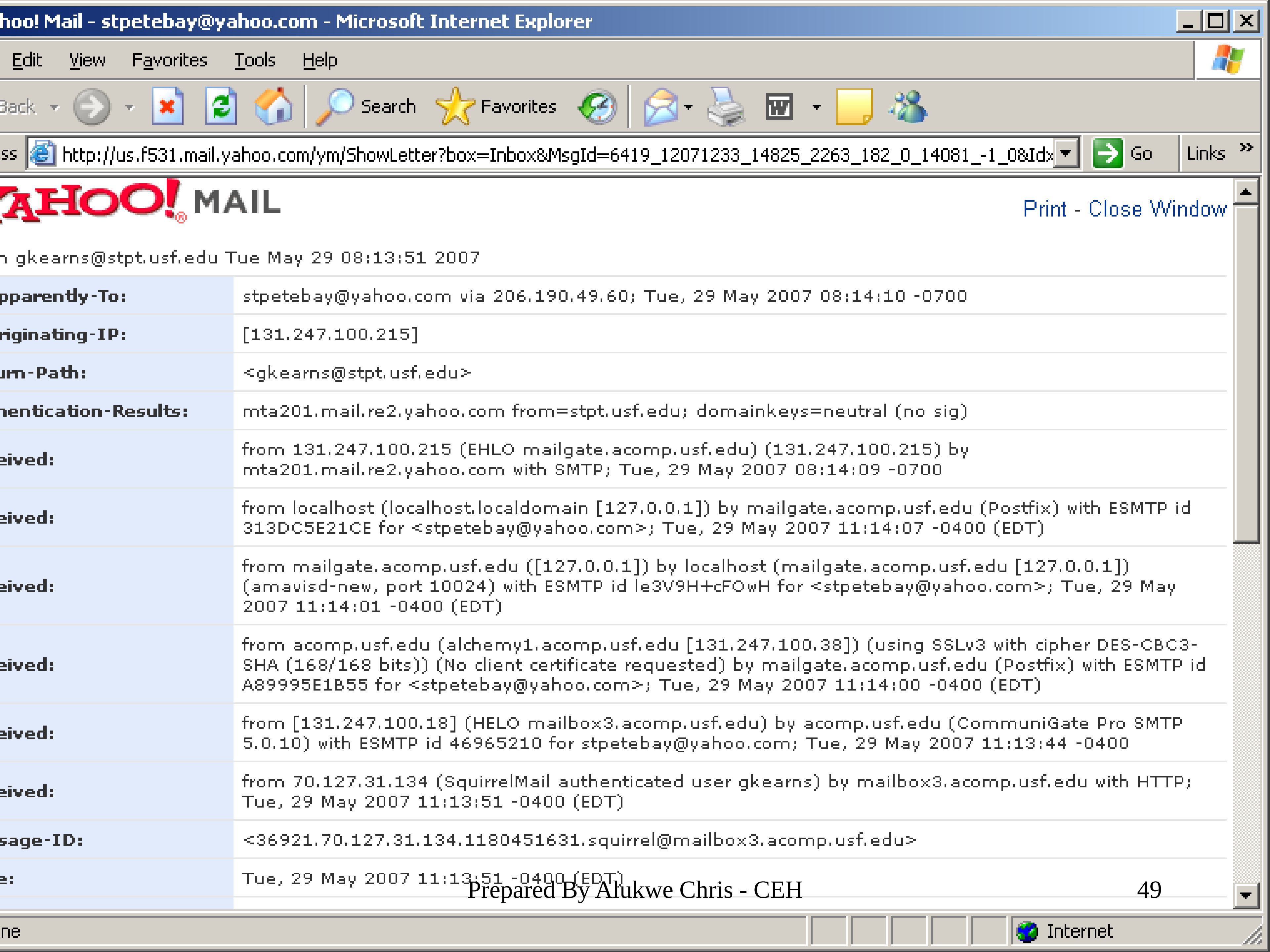
Road Runner HoldCo, LLC
abuse@RR.COM
703-345-3416
703-345-3607
13241 Woodland Park Rd Herndon, VA 20171
US

⊟ **Click here to hide the route map** (*more info*)

The following map shows the route between you and the entity to which you traced. A solid line represents a hop to a known location, and a dotted line represents a hop to a guessed location.

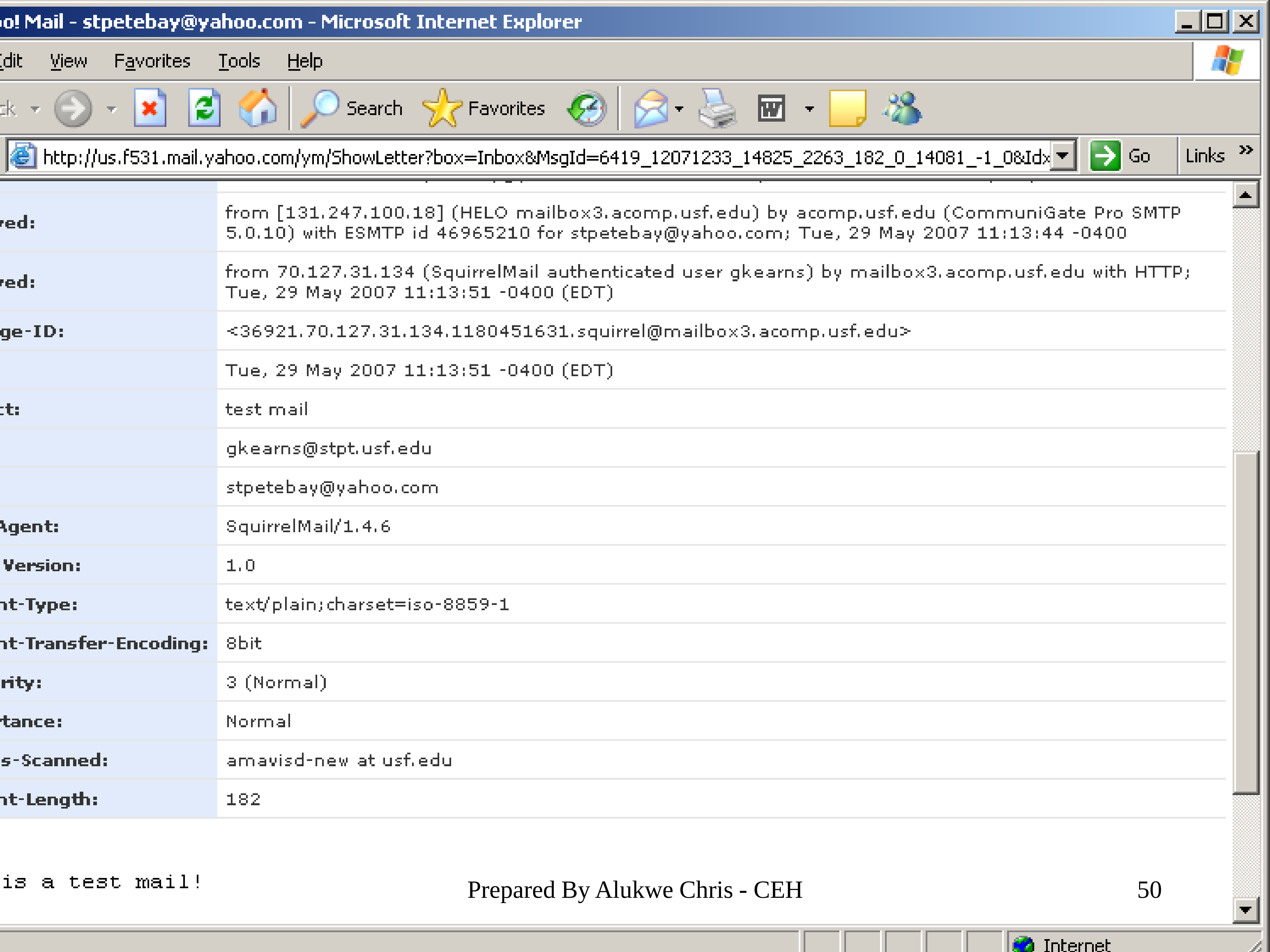

Completewhois.Com Whois lookup on 131.247.89.56 - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address
http://www.completewhois.org/cgi-bin/whois.cgi?query_type=auto&ip_whoislookup_cyberabuse=ON&ip_nameservers_hos
Go
Done
Internet

```
[IPv4 Whois Information for 131.247.89.56 ]
[whois.arin.net]
OrgName:    UNIVERSITY OF SOUTH FLORIDA
OrgID:      USF
Address:    4202 E Fowler Ave.
City:       Tampa
StateProv:  FL
PostalCode: 33620
Country:    US

NetRange:   131.247.0.0 - 131.247.255.255
CIDR:       131.247.0.0/16
NetName:    USF
NetHandle:  NET-131-247-0-0-1
Parent:     NET-131-0-0-0-0
NetType:    Direct Assignment
NameServer: MOTHER.USF.EDU
NameServer: ZIGGY.USF.EDU
NameServer: JUSTINCASE.USF.EDU
Comment:
RegDate:    1989-02-09
Updated:    2005-10-20

RTechHandle: TN32-ARIN
RTechName:   Netterfield, Ted
RTechPhone:  +1-813-974-1793
RTechEmail:  ted@usf.edu
```


hoo! Mail - stpetebay@yahoo.com - Microsoft Internet Explorer
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
ss
http://us.f531.mail.yahoo.com/ym/ShowLetter?box=Inbox&MsgId=6419_12071233_14825_2263_182_0_14081_-1_0&Idx
Go
Links
AHOO! MAIL
Print - Close Window
ne
Internet

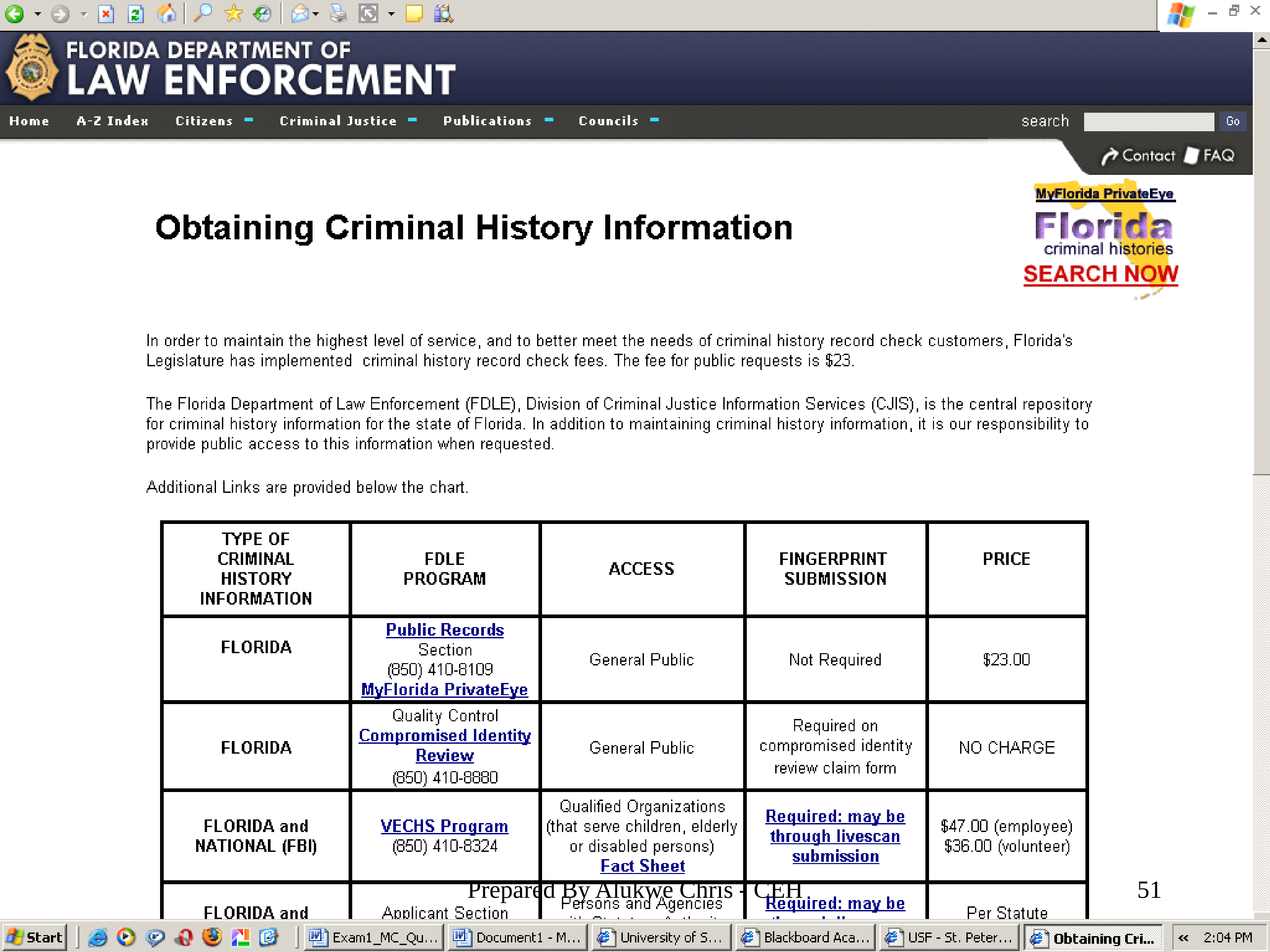
n gkearns@stpt.usf.edu Tue May 29 08:13:51 2007

pparently-To:	stpetebay@yahoo.com via 206.190.49.60; Tue, 29 May 2007 08:14:10 -0700
riginating-IP:	[131.247.100.215]
urn-Path:	<gkearns@stpt.usf.edu>
nentication-Results:	mta201.mail.re2.yahoo.com from=stpt.usf.edu; domainkeys=neutral (no sig)
eived:	from 131.247.100.215 (EHLO mailgate.acomp.usf.edu) (131.247.100.215) by mta201.mail.re2.yahoo.com with SMTP; Tue, 29 May 2007 08:14:09 -0700
eived:	from localhost (localhost.localdomain [127.0.0.1]) by mailgate.acomp.usf.edu (Postfix) with ESMTP id 313DC5E21CE for <stpetebay@yahoo.com>; Tue, 29 May 2007 11:14:07 -0400 (EDT)
eived:	from mailgate.acomp.usf.edu ([127.0.0.1]) by localhost (mailgate.acomp.usf.edu [127.0.0.1]) (amavisd-new, port 10024) with ESMTP id le3V9H+cFOwH for <stpetebay@yahoo.com>; Tue, 29 May 2007 11:14:01 -0400 (EDT)
eived:	from acomp.usf.edu (alchemy1.acomp.usf.edu [131.247.100.38]) (using SSLv3 with cipher DES-CBC3-SHA (168/168 bits)) (No client certificate requested) by mailgate.acomp.usf.edu (Postfix) with ESMTP id A89995E1B55 for <stpetebay@yahoo.com>; Tue, 29 May 2007 11:14:00 -0400 (EDT)
eived:	from [131.247.100.18] (HELO mailbox3.acomp.usf.edu) by acomp.usf.edu (CommuniGate Pro SMTP 5.0.10) with ESMTP id 46965210 for stpetebay@yahoo.com; Tue, 29 May 2007 11:13:44 -0400
eived:	from 70.127.31.134 (SquirrelMail authenticated user gkearns) by mailbox3.acomp.usf.edu with HTTP; Tue, 29 May 2007 11:13:51 -0400 (EDT)
sage-ID:	<36921.70.127.31.134.1180451631.squirrel@mailbox3.acomp.usf.edu>
e:	Tue, 29 May 2007 11:13:51 -0400 (EDT)


o! Mail - stpetebay@yahoo.com - Microsoft Internet Explorer
dit View Favorites Tools Help
ck Search Favorites
http://us.f531.mail.yahoo.com/ym/ShowLetter?box=Inbox&MsgId=6419_12071233_14825_2263_182_0_14081_-1_0&Idx
Go
Links »
Internet

ved:	from [131.247.100.18] (HELO mailbox3.acomp.usf.edu) by acomp.usf.edu (CommuniGate Pro SMTP 5.0.10) with ESMTP id 46965210 for stpetebay@yahoo.com; Tue, 29 May 2007 11:13:44 -0400
ved:	from 70.127.31.134 (SquirrelMail authenticated user gkearns) by mailbox3.acomp.usf.edu with HTTP; Tue, 29 May 2007 11:13:51 -0400 (EDT)
ge-ID:	<36921.70.127.31.134.1180451631.squirrel@mailbox3.acomp.usf.edu>
	Tue, 29 May 2007 11:13:51 -0400 (EDT)
t:	test mail
	gkearns@stpt.usf.edu
	stpetebay@yahoo.com
Agent:	SquirrelMail/1.4.6
Version:	1.0
nt-Type:	text/plain;charset=iso-8859-1
nt-Transfer-Encoding:	8bit
rity:	3 (Normal)
tance:	Normal
s-Scanned:	amavisd-new at usf.edu
nt-Length:	182

```
is a test mail!
```



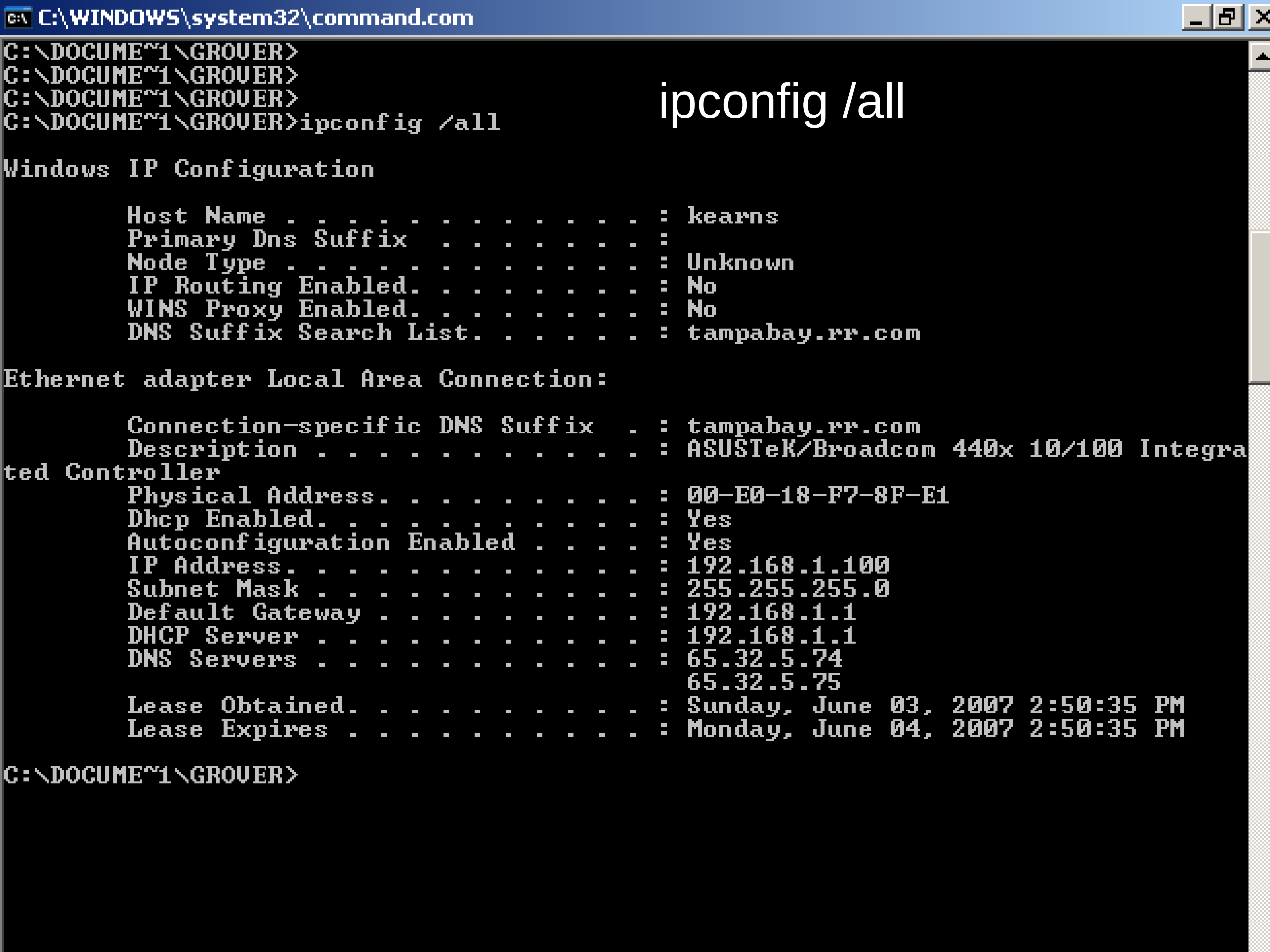
Obtaining Criminal History Information

In order to maintain the highest level of service, and to better meet the needs of criminal history record check customers, Florida's Legislature has implemented criminal history record check fees. The fee for public requests is $23.

The Florida Department of Law Enforcement (FDLE), Division of Criminal Justice Information Services (CJIS), is the central repository for criminal history information for the state of Florida. In addition to maintaining criminal history information, it is our responsibility to provide public access to this information when requested.

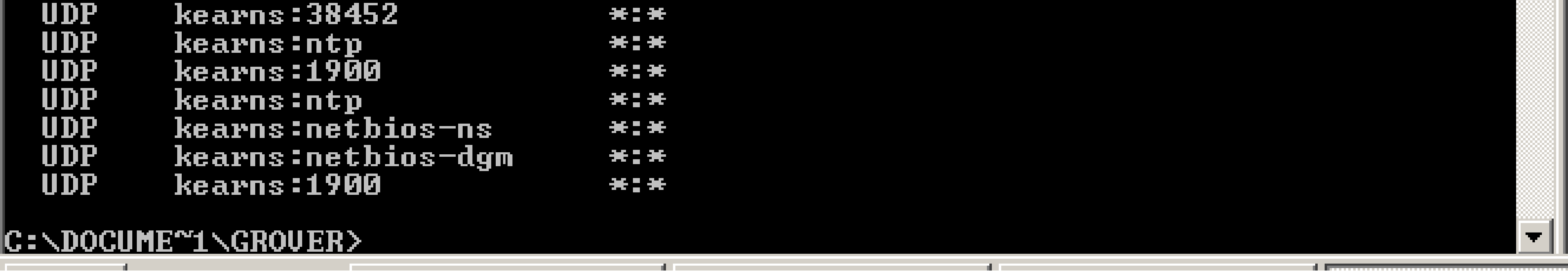
Additional Links are provided below the chart.

TYPE OF CRIMINAL HISTORY INFORMATION	FDLE PROGRAM	ACCESS	FINGERPRINT SUBMISSION	PRICE
FLORIDA	Public Records Section (850) 410-8109 MyFlorida PrivateEye	General Public	Not Required	$23.00
FLORIDA	Quality Control Compromised Identity Review (850) 410-8880	General Public	Required on compromised identity review claim form	NO CHARGE
FLORIDA and NATIONAL (FBI)	VECHS Program (850) 410-8324	Qualified Organizations (that serve children, elderly or disabled persons) Fact Sheet	Required: may be through livescan submission	$47.00 (employee) $36.00 (volunteer)
FLORIDA and	Applicant Section	Persons and Agencies	Required: may be	Per Statute



ipconfig /all

```
C:\DOCUME~1\GROVER>
C:\DOCUME~1\GROVER>
C:\DOCUME~1\GROVER>
C:\DOCUME~1\GROVER>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : kearns
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : tampabay.rr.com

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : tampabay.rr.com
        Description . . . . . . . . . . . : ASUSTeK/Broadcom 440x 10/100 Integra
ted Controller
        Physical Address. . . . . . . . . : 00-E0-18-F7-8F-E1
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.1.100
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1
        DHCP Server . . . . . . . . . . . : 192.168.1.1
        DNS Servers . . . . . . . . . . . : 65.32.5.74
                                            65.32.5.75
        Lease Obtained. . . . . . . . . . : Sunday, June 03, 2007 2:50:35 PM
        Lease Expires . . . . . . . . . . : Monday, June 04, 2007 2:50:35 PM

C:\DOCUME~1\GROVER>
```



```
  UDP    kearns:38452           *:*
  UDP    kearns:ntp             *:*
  UDP    kearns:1900            *:*
  UDP    kearns:ntp             *:*
  UDP    kearns:netbios-ns      *:*
  UDP    kearns:netbios-dgm     *:*
  UDP    kearns:1900            *:*

C:\DOCUME~1\GROVER>
```

Initial Response

Off-scene Response

- **Freeze** the Incident Scene
  - **Verbally contain the scene** with instructions such as:
    - “Take your hands off the keyboard and step away from the computer.”
    - “Physically disconnect the computer from the network.”
    - “What is your name, office and telephone number.”
    - “What is the hardware and operating system?”
    - “I’m going to fax you a set of instruction. What is your Fax number?”

□ Incident Response Checklist

□ Version 1.0

- □ Date:
- □ Time:
- □ Name:
- □ Telephone Number:

- □ Nature of Incident:
- □ Time of Incident:
- □ How was the incident detected:
- □ Current Impact of Incident:
- □ Future Impact of incident:
- □ Description of the incident:
  - □ Hardware/OS/Software involved:
  - □ IP and network addresses of compromised systems:
  - □ Network Type:
  - □ Modem:
  - □ Criticality of Information:
  - □ Physical location:
  - □ System Administrator Name and Number:
  - □ Current status of machine:
- □ Description of Hacker Actions
  - □ Ongoing activity:
  - □ Source Address:
  - □ Malicious program involved:
  - □ Denial of Service
  - □ Vandalism:
  - □ Indication of insider or outsider:

□ Incident Response Checklist Continued

□ Version 1.0

□ Client Actions

- □ Network disconnected:
- □ Remote access available:
- □ Local Access available:
- □ Audit logs available and examined:
- □ Any changes to firewall:
- □ Any changes to ACL:
- □ Who has been notified:
- □ Other actins taken:

□ Available Tools

- □ Third party host auditing:
- □ Network monitoring:
- □ Network Auditing:

□ Additional Contacts

- □ Users:
- □ System Administrators:
- □ Network Administrators:

□ Special Information

- □ Who should not know about this incident:

□ Response Team Member Signature/Date: ______________________

□

Incident Response Team Fax

□ Version 1.0

□ Date:_____________

□ Time:____________

□ Name:_______________________

□ Thank you for notifying the incident response team and agreeing to help. Please do not touch the affected computer(s) unless told to do so by a member of the Incident Response team. Please remain within sight of the computer until a member of the Incident Response Team arrives and assure that no one touches the computer.

□ Please help us by detailing as much information about the incident as possible. Please complete the following items. If additional space is required use a separate sheet of paper.

□ **Witnesses**:

□ 1.

□ 2.

□ 3.

□ What indicators lead you to notice and/or report the incident. Be as specific as possible.

□ Incident Indicators:

□ The next section is important so be as accurate as possible. From the time you noticed the incident to the time you took your hands from the computer, list every command you typed and any file you accessed.

□ **Commands typed and Files accessed:**

□ Response Team Member Signature:__________________________________-

On-scene Response

- **Physically contain the scene**
- Two personnel, if possible, should immediately respond to the scene
  - **Incident Scene Survey** (1st Member)
    - Use a portable tape recorder to:

      1. Record the scene
      2. Everyone present
         - » Order everyone to leave the scene who is not directly involved in the incident
      3. Interview the individual who reported the incident
      4. Record, intermittently, the actions of the 2nd individual
      5. Assist the 2nd Member

On-Scene Response Continued

- **Contain the System (2nd Member)**
  - Ask the System Administrator to assist.
  - Back up the system.
    - » Do this with forensic type tool that does bit-by-bit backup such as SafeBack at http://www.forensics-intl.com
    - » Alternatively, remove the drive and seal it in a plastic bag with your notes and the notes of the individual who reported the incident
  - Attempt to identify the changed files through:
    - » Tripwire http://www.tripwire.org/ or alternatively
    - » Expert Witness at http://www.asrdata.com.

Knowing Architecture and Policies

- Review Network Topology
  - *External connectivity*
    - *Internet*
    - *Extranet*
    - *Dial-up*
    - *Remote Sites*
  - *Network Devices: Routers, Firewall, IDS*
  - *Broadcast domains*
- Review the Corporate Policies with regard to
  - *Acceptable use policies*
  - *Network Monitoring*
  - *Computer Forensics*

Conducting Personnel Interviews

- **System administrator** selected questions include:
  - Unusual Activity?
  - Administrative Access to System?.
  - Remote Access to Systems?
  - Logging Capabilities?
  - Current Security Precautions?
- **Managers** selected questions include:
  - On-going Security tests?
  - Disgruntled employees?
  - Recently fired employee?
  - History of current employees?
  - Sensitive data or applications on the systems?
- **End users** selected questions include:
  - Anomalous Behavior or Suspicious activity?

Initial Assessment

- Assess the potential security Incident
  - What are the incident symptoms?
  - Is it a security incident?
  - A system problem?
    - Power outage
    - Faulty software
    - Communication problems
    - Procedural problem
    - Training Problem

Initial Evaluation

- Evaluate the severity & scope of incident
  - What specifically happened?
  - What was the entry point?
  - What local computers/networks were affected?
  - What remote computers/networks were affected?
  - What information was affected?
    - What was its value to the organization?
  - What further can possibly occur?
  - Who else knows about the incident?
  - What are the estimated time/resources required to handle the incident.

Incident Indications

- A new account
- Passwords were changed on existing accounts
- The protection changed on selected files/devices
- System programs have been added/modified
- An alias has been installed in the E-Mail system to run a program
- New features have been added to your news
- Password sniffer was found (Steal passwords to use **Crack**)
- File dates have been modified
- Login files have been modified
- The system has an unexplained crash
- Accounting discrepancies
- Denial of Service
- Unexplained poor system performance
- Suspicious probes/browsing

Incident Indications (cont'd)

- Undocumented changes or upgrades to programs
- Unexplained user account charges or changes
- Security Access compromise (passwords, etc)
- Unauthorized use of computer facilities
- Unexplained network/computer crashes
- Unexplained corrupted files or services
- Theft/missing computer/storage equipment
- Unexplained Performance/response problems
- Unexplained High utilization of equipment, storage or network resources
- Unexplained loss of critical/sensitive data
- Unexplained user account lockouts
- Unexplained Network traps/alarms
- Unexplained Firewall/IDS alerts/alarms

Initial Steps

- All systems/networks are suspect until the actual extent of the incident is known
  - Verify integrity of all site computers
  - Verify integrity of all site networks
  - Verify integrity of all files/directories (checksums)
  - Compare system files with backups or initial distributions
  - Compare software application with the baseline
- Analyze the documentation, files and security logs

Be careful not to contaminate the crime scene

Forensics Terminology

- **Evidence Media:** Original media that needs to be investigated
- **Target Media:** the media that the evidence media is duplicated onto
- **Restored Image:** Copy of the forensic image restored to bootable form
- **Native Operating System:** OS utilized when the evidence media or forensic duplicate is booted for analysis
- **Live Analysis:** A analysis conducted on the original evidence media
- **Off-line Analysis:** Analysis conducted on the forensic image
- **Trace Evidence:** Fragments of information from the free space, etc.

Common evidence mistakes

- These include include:
  - Altering time and date stamps
  - Killing rogue processes
  - Patching the system before the investigation
  - Not recording commands executed on the system
  - Using un-trusted commands and binaries
  - Writing over potential evidence:
    - Installing software on the evidence media
    - Running program that store output on evidence media.