



# جرم یابی دیجیتال و راهکارهای جمع آوری و حفظ ادله دیجیتال

---

حسین مومنی  
رییس مرکز آپا دانشگاه گلستان

# Outline

- **Computer Crime**
- **Digital Forensic**
- **Digital Evidence**
- **Preservation of Digital Evidence**
- **Computer Forensic Steps**
- **SysAdmin and Network Admin roles as First Responder**



# Type of Computer Crimes

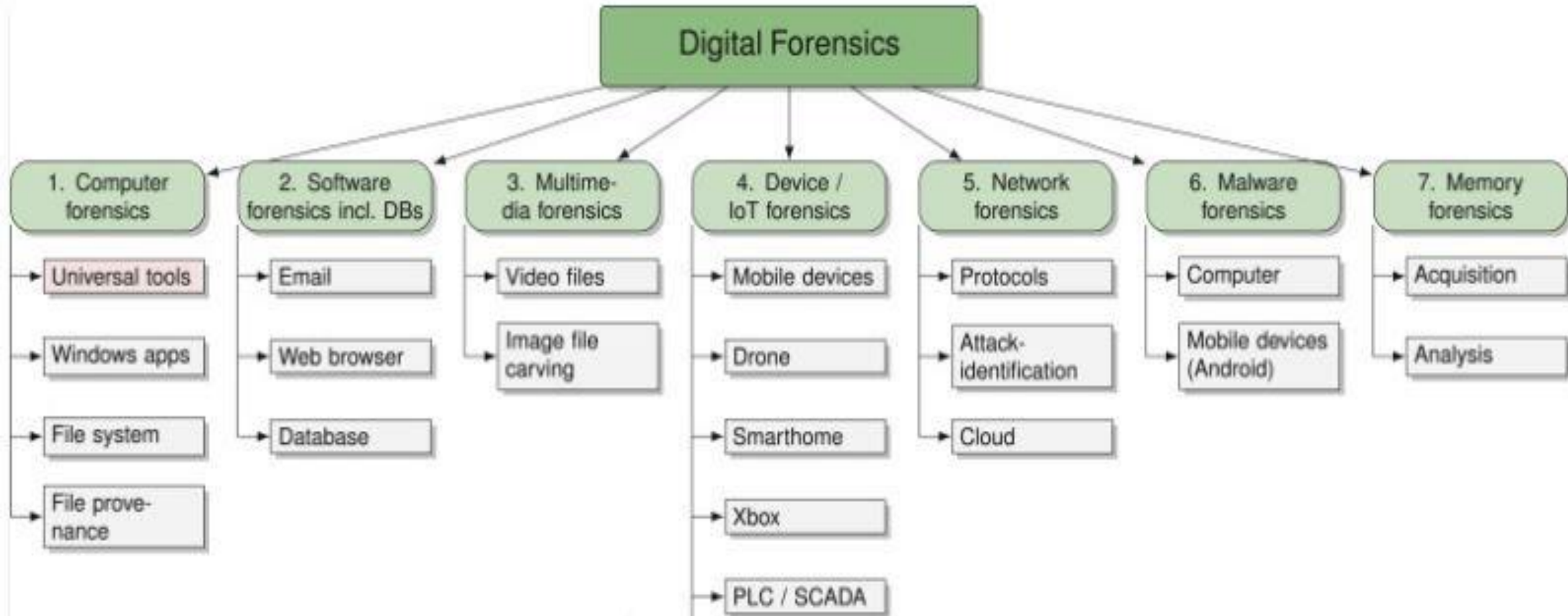
Identity Theft	Credit Card Fraud	Internet Extortion
Hacking	On-Line Auction Fraud	Investment Fraud
Computer Viruses	Email Bombing and SPAM	Escrow Services Fraud
Cyber Stalking	Theft of Intellectual Property	Cyber Defamation
Drug Trafficking	Denial of Service Attack	Software Piracy
Phishing/Spoofing	Debt Elimination	Counterfeit Cashier's Check
Wrongful Programming	Web Jacking	Embezzlement

# Computer Forensics in Today's World

- **Forensic Computing:** the science of capturing, processing, and investigating data from computers using a methodology whereby any evidence discovered is acceptable in the court of law.
- **Cyber Crime:** cybercrime is a term used to describe criminal activity in which a computer or network is a tool, a target, or a place of criminal activity.

**Computer as tools Vs. Computer as target**

# Digital Forensic Types



# Digital Evidence

- Digital evidence is any information of **probative value** that is either stored or transmitted in a digital form.
- Digital evidence is found in:
  - Network traffic
  - OS system files (event, task, process ...)
  - Server logs
  - Emails
  - Internet browser histories (Caches, Cookies)
  - DB files
  - Memory and Storage
  - Graphic, Audio and video files



# Characteristics of Digital Evidence

- **Characteristics of Digital Evidence**
  - Believable**
  - Admissible**
  - Authentic**
  - Reliable**
  - Complete**
  - Innocence**

# Digital Evidence

- **Type of digital Evidence**
  - ❑ **Volatile** (running processes)
  - ❑ **Transient** (open network connection)
  - ❑ **Fragile** (last file access)
  - ❑ **Archival**
  - ❑ **Backup**



## INCIDENT RESPONSE STEPS

### **NIST Framework**

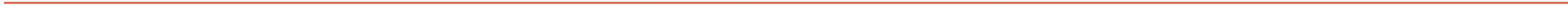
1. Preparation
2. Detection and Analysis
3. Containment, Eradication and Recovery
4. Post-Incident Activity

### **SANS Framework**

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

# First Responder

- First responder is a person who **arrives first at the crime scene** and accesses the victim's computer system after the incident
- System or network administrator
- Responsible for protecting, integrating, and preserving the evidence obtained from the crime scene



# First Responder

- **Roles of First Responder**
    - ❑ Identifying the crime scene
    - ❑ Protecting the crime scene
    - ❑ Preserving temporary evidence
    - ❑ Collecting the complete information
    - ❑ Documenting all finding
- 



# Pre-Incident Preparation

- Incident response is **reactive** in nature.
- The pre-incident preparation phase is the **proactive** and is establishing policies, and procedures to manage and respond to security incidents **BEFORE** you need them.
- Administrator of an organization consider the following strategies:
  - ❑ Organizing the networks and assets
  - ❑ Deploying sensors to data gathering
  - ❑ Training end users
  - ❑ Employing an IDS
  - ❑ Creating strong access control
  - ❑ Ensuring backups are performed on a regular basis

## Policy vs. Mechanism

# Common indicators of a computer security incident

- **IDS Detection of Remote Attacks**
- **Numerous Failed Logon Attempts**
- **Login into Dormant or Default Accounts**
- **System Crash**
- **New Accounts not Created by SysAdmin**
- **Gaps in Log files**
- **Alter Pages on Webservers**
- **Slower System Performance**
- **Receipt of emails extorting your Organizations**
- **Unfamiliar files or executable programs**
- **Activity during non-working Hours**

# First Responder Common Mistakes

- **Shutting down or rebooting the victim's computer:** In this case, the system loses the complete **volatile data**, such as MAC time and log files, shuts down processes running when shutting down and rebooting.
- **Assuming that some components of the victim's computer may be reliable and usable:** In this case, using some commands on the victim's computer may activate Trojans, malware, and time bombs to delete vital volatile data.



# Volatile Information

- **The system date and time**
- **The applications currently running on the system**
- **The currently established network connections**
- **The currently open sockets (ports)**
- **The applications listening on the open sockets**
- **The state of the network interface (promiscuous or not)**

**This information can be collected when a computer system is still powered on and running**

# First Step-Preparation

## Initial response checklist

- **Initial response checklist to make sure you record the pertinent facts.**
  - Current time and date
  - Who/what reported the incident
  - The nature of the incident
  - When the incident occurred
  - Hardware/software involved
  - Points of contact for involved personnel

Incident #: \_\_\_\_\_

Date: \_\_\_\_\_

Initial Response Checklist

**Contact Information**

<b>Your Contact Information</b>	
Name:	
Department:	
Telephone	
Other Telephone:	
Email:	

<b>Individual Reporting Incident*</b>	
Name:	
Department:	
Telephone:	
Other Telephone:	
Email:	

\* If the Contact Information is the same as the individual above, please leave blank.

## Incident Detection

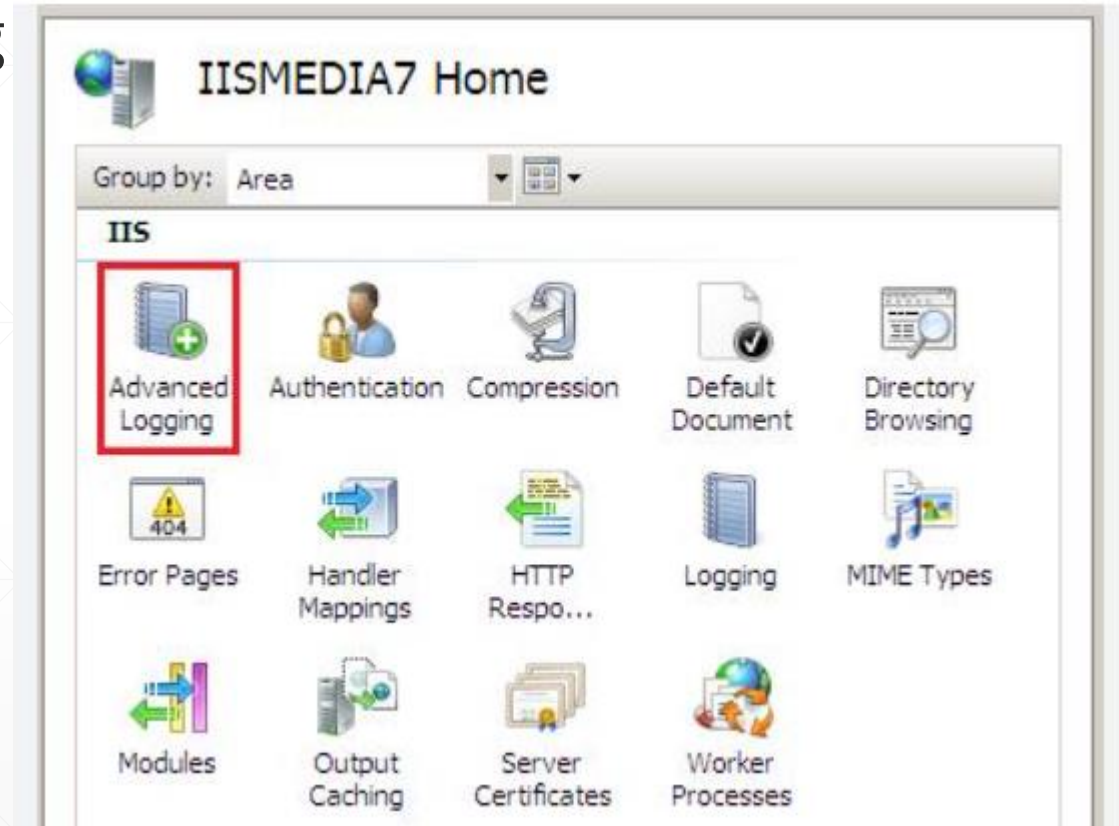
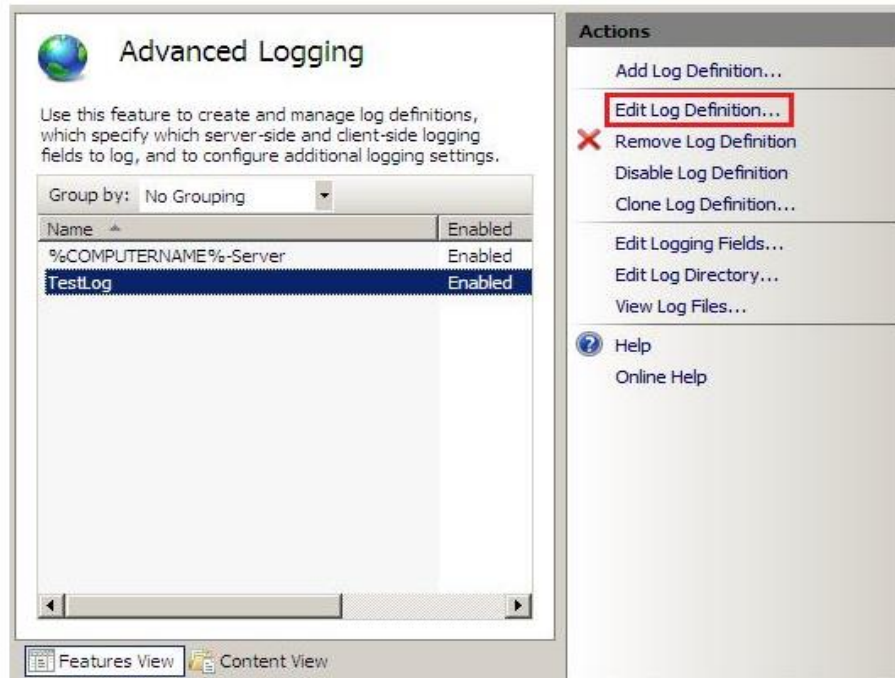
Type of Incident:	<input type="checkbox"/> Denial of Service <input type="checkbox"/> Virus <input type="checkbox"/> Hoax <input type="checkbox"/> Unauthorized Access <input type="checkbox"/> Unauthorized Use of Computer Resources <input type="checkbox"/> Theft of Intellectual Property <input type="checkbox"/> Other:
Location of Incident:	Address:  Building:  Room Number:
Describe the Physical Security At the Site:  Are there locks? Alarm systems? Who is in charge of the physical security at the site?	
How the Incident was Detected:	
Is the information concerning the incident stored in a protected, tamper-proof manner?	

# First Step-Preparation

- **Increasing or Enabling Secure Audit Logging**
- **Expand the default logging capabilities so that you'll have plenty of data to review in the event of an incident.**
- **Unix-like OS:**
  - **Syslog: auth.info /var/log/syslog or \*.\* /var/log/syslog**
- **Window OS: C:\WINDOWS\system32\config\
  - **Enabling Security Auditing**
  - **Auditing File and Directory Actions**
  - **Setting Up Remote Logging****

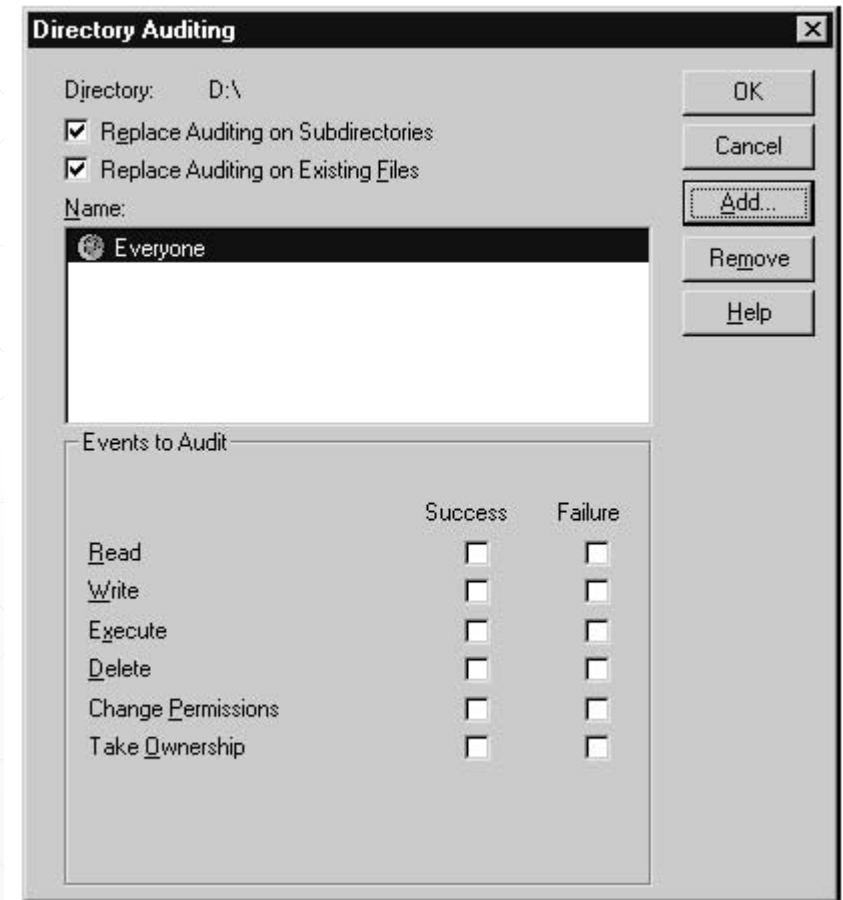
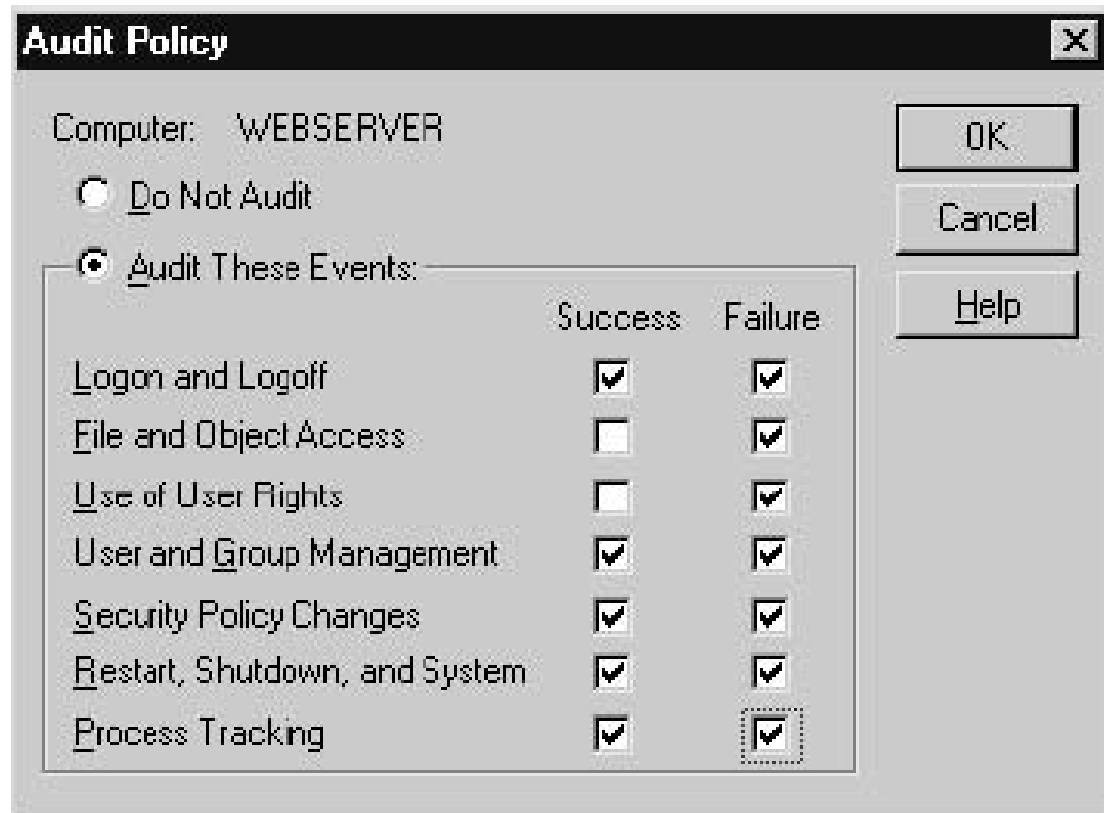
# First Step-Preparation

- **Configuring Application Logging**
  - ❑ **Advanced Logging IIS**
  - ❑ **Advanced Logging Apache**
    - `var/log/httpd/`



# First Step-Preparation

- **Audit Policy Setting**



# Second Step-Data Collection

## What Data to Collect?

- System time
- Logged-on user(s)
- Open files, Ports
- Detect Backdoors
- Network information
- Network connections
- Running Process information
- Process-to-port mapping
- Running program information
- Network status
- Service/driver information
- Command history
- Script
- Autoruns
- Modification, creation and access time of all files



# Second Step-Data Collection

`~/.local/share/recently-used.xbel`

## Data Collection

### Network-Based Evidence

- Obtain IDS Logs
- Obtain Existing Router Logs
- Obtain Relevant Firewall Logs
- Obtain Remote Logs from a Centralized Host (SYSLOG)
- Perform Network Monitoring
- Obtain Backups

### Host-Based Evidence

- Obtain the Volatile Data during a Live Response
- Obtain the System Time
- Obtain the Time/Date Stamps for Every File on the Victim System
- Obtain all Relevant Files that Confirm or Dispel Allegation
- Obtain Backups

### Other Evidence

- Obtain Oral Testimony from Witnesses

## Analysis

1. Review the Volatile Data.
  - Review the Network Connections.
  - Identify Any Rogue Processes (Backdoors, Sniffers).
2. Analyze the Relevant Time/Date Stamps.
  - Identify Files Uploaded to the System by an Attacker.
  - Identify Files Downloaded or Taken from the System.
3. Review the Log Files.
4. Identify Unauthorized User Accounts.
5. Look for Unusual or Hidden Files.
6. Examine Jobs Run by the Scheduler Service.
7. Review the Registry.
8. Perform Keyword Searches.

```

MS-A:\cmd.exe
A:\>netstat -an

Active Connections

Proto Local Address           Foreign Address         State
TCP   0.0.0.0:25               0.0.0.0:*               LISTENING
TCP   0.0.0.0:80               0.0.0.0:*               LISTENING
TCP   0.0.0.0:135              0.0.0.0:*               LISTENING
TCP   0.0.0.0:135              0.0.0.0:*               LISTENING
TCP   0.0.0.0:443              0.0.0.0:*               LISTENING
TCP   0.0.0.0:465              0.0.0.0:*               LISTENING
TCP   0.0.0.0:1026             0.0.0.0:*               LISTENING
TCP   0.0.0.0:1028             0.0.0.0:*               LISTENING
TCP   0.0.0.0:1029             0.0.0.0:*               LISTENING
TCP   0.0.0.0:1031             0.0.0.0:*               LISTENING
TCP   0.0.0.0:3970             0.0.0.0:*               LISTENING
TCP   127.0.0.1:1025           0.0.0.0:*               LISTENING
TCP   127.0.0.1:1025           127.0.0.1:1026         ESTABLISHED
TCP   127.0.0.1:1026           127.0.0.1:1025         ESTABLISHED
TCP   127.0.0.1:1027           0.0.0.0:*               LISTENING
TCP   127.0.0.1:1027           127.0.0.1:1027         ESTABLISHED
TCP   127.0.0.1:1029           0.0.0.0:*               LISTENING
TCP   127.0.0.1:1030           0.0.0.0:*               LISTENING
TCP   192.168.0.100:137        0.0.0.0:*               LISTENING
TCP   192.168.0.100:138        0.0.0.0:*               LISTENING
TCP   192.168.0.100:139        0.0.0.0:*               LISTENING
TCP   192.168.0.100:139        192.168.0.100:139     ESTABLISHED
TCP   192.168.0.100:1152       0.0.0.0:*               LISTENING
TCP   192.168.0.100:1152       192.168.0.100:1152    ESTABLISHED
UDP   0.0.0.0:135              *:.*                    LISTENING
UDP   192.168.0.100:137        *:.*                    LISTENING
UDP   192.168.0.100:138        *:.*                    LISTENING
A:\>

```

```

[root@conan /root]# netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      176 66.192.0.66:22          66.192.0.26:20819     ESTABLISHED
tcp        0      0 0.0.0.0:80              0.0.0.0:*              LISTEN
tcp        0      0 0.0.0.0:21              0.0.0.0:*              LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*              LISTEN
udp        0      0 0.0.0.0:69              0.0.0.0:*

```

```

MS A:\cmd.exe
A:\>fport
FPort v1.31 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com
Securing the dot com world
Pid      Process          Port  Proto Path
2        System          -> 25   TCP   D:\WINNT\System32\inetsrv\inetinfo.exe
160     inetinfo        -> 25   TCP
2        System          -> 80   TCP   D:\WINNT\System32\inetsrv\inetinfo.exe
160     inetinfo        -> 80   TCP
79      RpcSs           -> 135  TCP   D:\WINNT\system32\RpcSs.exe
2        System          -> 135  TCP
2        System          -> 139  TCP
2        System          -> 443  TCP
160     inetinfo        -> 443  TCP   D:\WINNT\System32\inetsrv\inetinfo.exe
2        System          -> 465  TCP
160     inetinfo        -> 465  TCP
79      RpcSs           -> 1025 TCP
2        System          -> 1025 TCP
79      RpcSs           -> 1026 TCP
2        System          -> 1026 TCP
2        System          -> 1027 TCP
91      msdtc           -> 1027 TCP
2        System          -> 1028 TCP
91      msdtc           -> 1028 TCP
2        System          -> 1029 TCP
91      msdtc           -> 1029 TCP
2        System          -> 1030 TCP
160     inetinfo        -> 1030 TCP
2        System          -> 1031 TCP
160     inetinfo        -> 1031 TCP
2        System          -> 1151 TCP
2        System          -> 3970 TCP
160     inetinfo        -> 3970 TCP

79      RpcSs           -> 135  UDP
2        System          -> 135  UDP
2        System          -> 137  UDP
2        System          -> 138  UDP

A:\>

```

```

[root@conan /root]# netstat -anp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State
PID/Program name
1) tcp 0 0 0.0.0.0:143 0.0.0.0:* LISTEN 385/inetd
2) tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN 395/sshd
3) tcp 0 0 0.0.0.0:512 0.0.0.0:* LISTEN 385/inetd
4) tcp 0 0 0.0.0.0:513 0.0.0.0:* LISTEN 385/inetd
5) tcp 0 0 0.0.0.0:514 0.0.0.0:* LISTEN 385/inetd
6) tcp 0 0 0.0.0.0:23 0.0.0.0:* LISTEN 385/inetd
7) tcp 0 0 0.0.0.0:21 0.0.0.0:* LISTEN 385/inetd
8) udp 0 0 0.0.0.0:69 0.0.0.0:* 385/inetd
9) raw 0 0 0.0.0.0:1 0.0.0.0:* 7
-
10) raw 0 0 0.0.0.0:6 0.0.0.0:* 7
-

```

```

MS A:\cmd.exe
A:\>pslist

PsList v1.12 - Process Information Lister
Copyright (C) 1999-2000 Mark Russinovich
Systems Internals - http://www.sysinternals.com

Process information for WEBTARGET:

Name           Pid Pri Thd  Hnd   Mem   User Time   Kernel Time   Elapsed Time
Idle           0   0   1    0    16    0:00:00.000  10:33:22.424  0:00:00.000
System        2   8   33   476   200    0:00:00.000  0:00:25.666  0:00:00.000
smss          26  11   6    30    36    0:00:00.070  0:00:00.020  10:35:10.149
CSRSS         34  13   7    274   968    0:00:00.260  0:00:02.263  10:34:53.625
WINLOGON     40  13   2    41    60    0:00:00.020  0:00:00.170  10:34:51.072
SERVICES     46   9  20   261  3164    0:00:00.180  0:00:01.001  10:34:48.258
LSASS        49   9  11   100  2032    0:00:00.060  0:00:00.110  10:34:47.226
SPOOLSS      73   8   6    55   496    0:00:00.000  0:00:00.000  0:00:00.000
RPCSS        79   8   8   131   820    0:00:00.000  0:00:00.000  0:00:00.000
msdtc       91   8  16   103  1664    0:00:00.000  0:00:00.000  0:00:00.000
ati2plab    109   8   2    20   712    0:00:00.000  0:00:00.000  0:00:00.000
CARDPWR     112   8   2    20    36    0:00:00.000  0:00:00.000  0:00:00.000
cisvc       115   8   9   169  4800    0:00:00.000  0:00:00.000  0:00:00.000
PwrApp      117   8   1    14    28    0:00:00.000  0:00:00.000  0:00:00.000
LLSSRU      122   9   9    72   464    0:00:00.000  0:00:00.000  0:00:00.000
PSTORES     52   8   5    53    72    0:00:00.000  0:00:00.000  0:00:00.000
certsrv     143   8   9    68  1340    0:00:00.000  0:00:00.000  0:00:00.000
inetinfo    160   8  31   366  2364    0:00:00.000  0:00:00.000  0:00:00.000
cidaemon    45   4   1    60    72    0:00:00.000  0:00:00.000  0:00:00.000
NDDEAGNT    203   8   1    16    48    0:00:00.000  0:00:00.000  0:00:00.000
EXPLORER     48   8   4    57  3300    0:00:00.000  0:00:00.000  0:00:00.000
pemapp      210   8   2    34    72    0:00:00.000  0:00:00.000  0:00:00.000
atiptaab    224   8   1    28    56    0:00:00.000  0:00:00.000  0:00:00.000
LOADWC      226   8   2    28   996    0:00:00.000  0:00:00.000  0:00:00.000
NIUDM       233   8   3    64   648    0:00:00.000  0:00:00.000  0:00:00.000
EVENTUWR    222   8   1    27   200    0:00:00.000  0:00:00.000  0:00:00.000
USRMGR       214   8   1    25   228    0:00:00.000  0:00:00.000  0:00:00.000
cmd          65   8   1    22  1780    0:00:00.000  0:00:00.000  0:00:00.000
PSLIST      50   8   1    56  1976    0:00:00.000  0:00:00.000  0:00:00.000

A:\>

```

```

[root@conan]# ps -aux
USER      PID %CPU %MEM  VSZ   RSS TTY      STAT START TIME COMMAND
root         1  0.1  0.7 1060   480 ?        S    17:52 0:03  init [3]
root         2  0.0  0.0    0     0 ?        SW   17:52 0:00  [kflushd]
root         3  0.0  0.0    0     0 ?        SW   17:52 0:00  [kupdate]
root         4  0.0  0.0    0     0 ?        SW   17:52 0:00  [kpiod]
root         5  0.0  0.0    0     0 ?        SW   17:52 0:00  [kswapd]
root         6  0.0  0.0    0     0 ?        SW<  17:52 0:00  [mdrecoveryd]
root       259  0.0  0.2   348  136 ?        S    17:52 0:00  /sbin/dhccpd eth0
root       316  0.0  0.8  1112  556 ?        S    17:52 0:00  syslogd -m 0
root       326  0.0  1.1  1360  756 ?        S    17:52 0:00  klogd
daemon     341  0.0  0.7  1084  492 ?        S    17:52 0:00  /usr/sbin/atd
root       356  0.0  0.9  1272  608 ?        S    17:53 0:00  crond

```

# Logs in Windows

- Event viewer *C:|WINDOWS|system32|config*
  - **Security** - Logs related to various authentication requests, failed and successful logins.
  - **Application** - System components logs and other logs related to drivers.
  - **System** - Logs created by the operating system, status change of the various services, and uptime.
  - **Setup** - Logs regarding updates and installs on your Windows system.
- Useful commands: cmd.exe, Netstat, Arp, ipconfig

# Logs in Linux

- **/var/log/auth.log** or **/var/log/secure**: Keep authentication logs for both successful or failed logins, and authentication processes.
- **/var/log/boot.log**: start-up messages and boot info.
- **/var/log/maillog** or **var/log/mail.log**: is for mail server logs.
- **/var/log/kern**: keeps in Kernel logs and warning info.
- **/var/log/dmesg**: a repository for device driver messages.
- **/var/log/faillog**: records info on failed logins.

# Logs in Networks

- Network-based logs includes information obtained from the following sources:
  - IDS/IPS logs
  - Monitoring logs
  - Web Servers Logs(IIS, Apache, NginX)
  - Router&Switch logs
  - Firewall logs(Network Firewall, WAF, OS Firewall)
  - Authentication servers

# Other Important Logs

- Application Logs
- DB Log
- USB Log
- Email Log

# Common Tools to Digital Forensic

- [Wireshark](#) and [NetworkMiner](#) to Network Forensic
- [Network Mapper \(NMAP\)](#) is one of the digital forensics services for network scanning and auditing
- [The Sleuth Kit](#) extracts data from hard disk drives and other types of storage media.
- [Volatility](#) is a memory forensics framework that allows you to extract information directly from the processes that are running on the computer
- [Free Hex Editor Neo](#) is one of the top database forensic tools for handling large files

# Questions ?

Thanks for your Attention

