Forensics & Incident Analysis

Kasi Viswanath Kethineni
Deputy Director (IT)/
Scientist C, NIC

Incident

An event is any observable occurrence in a system or network.

computer security incident

is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices → NIST

- Adversary Events are considered as Incidents

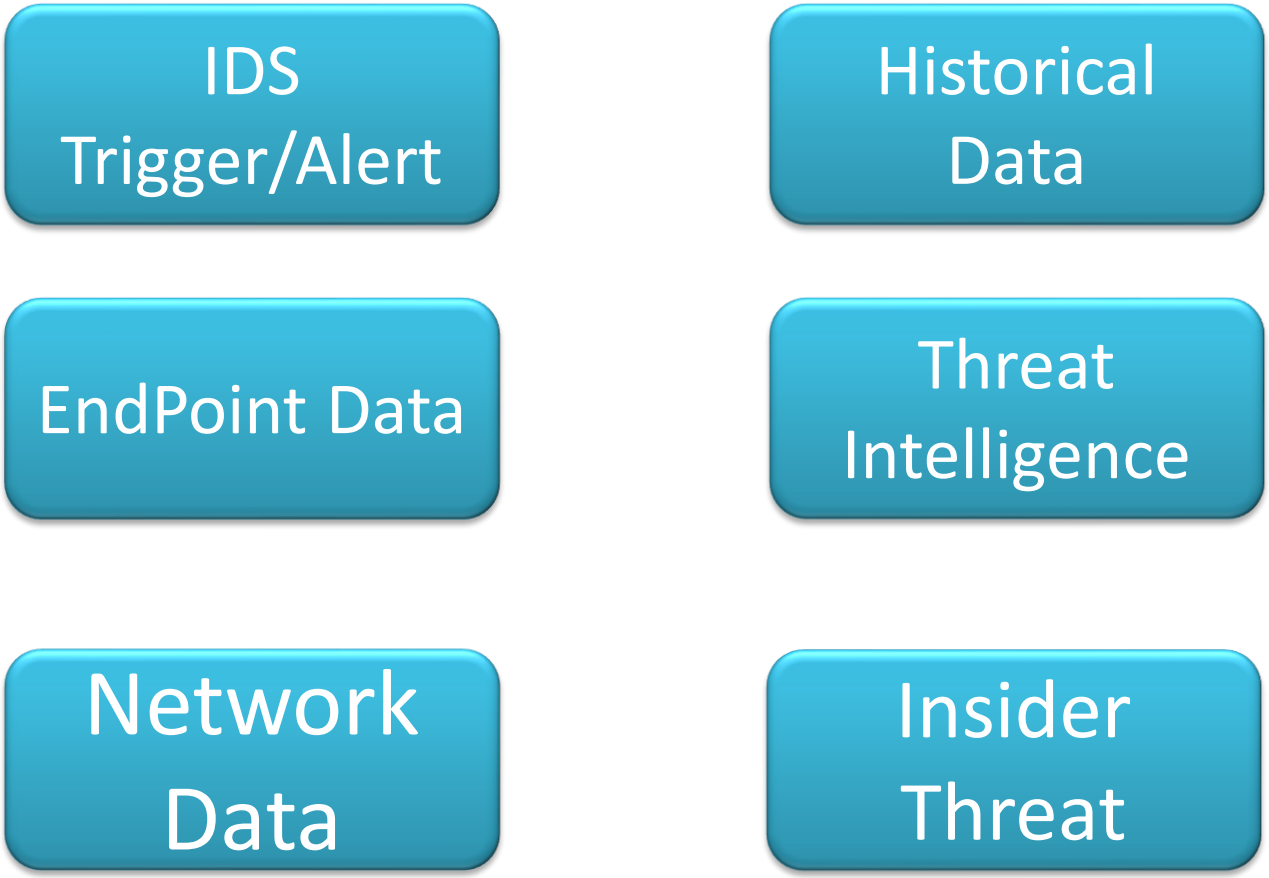
Eg: Defacing website.

Unauthorized stealing/inserting the data into database

Adverse Events – Incidents

- Website Defacement
- Denial of Service (DoS) or Distributed Denial of Service (DDoS)
- Unauthorized access or modification of Data or network or systems or services or programs
- Violation of organization policies, processes, guidelines..etc.
- Violation of Legal statutes and regulations (like IT Act, Aadhaar Act…etc)
- Loss or Theft of equipment on which data is stored (Ex: Hard Disk, Removable Media, Servers….etc)
- Social Engineering (Ex: Phishing, Spam, spoofing tele-calls…etc)
- Advanced Persistent Threats
- Ransomware Infection
- Malware/Virus/Trojan/Worm – Outbreak
- Data Exfiltration (Unauthorized Copying/Transferring, of data to external network/internet)
- Hacking/Intrusion
- Disclosure of sensitive data in public domain (Ex: display of personal information of citizens like bank records, date of birth….etc., in public domain)
- Unauthorized Scanning (both horizontal and vertical) of network

Input locations



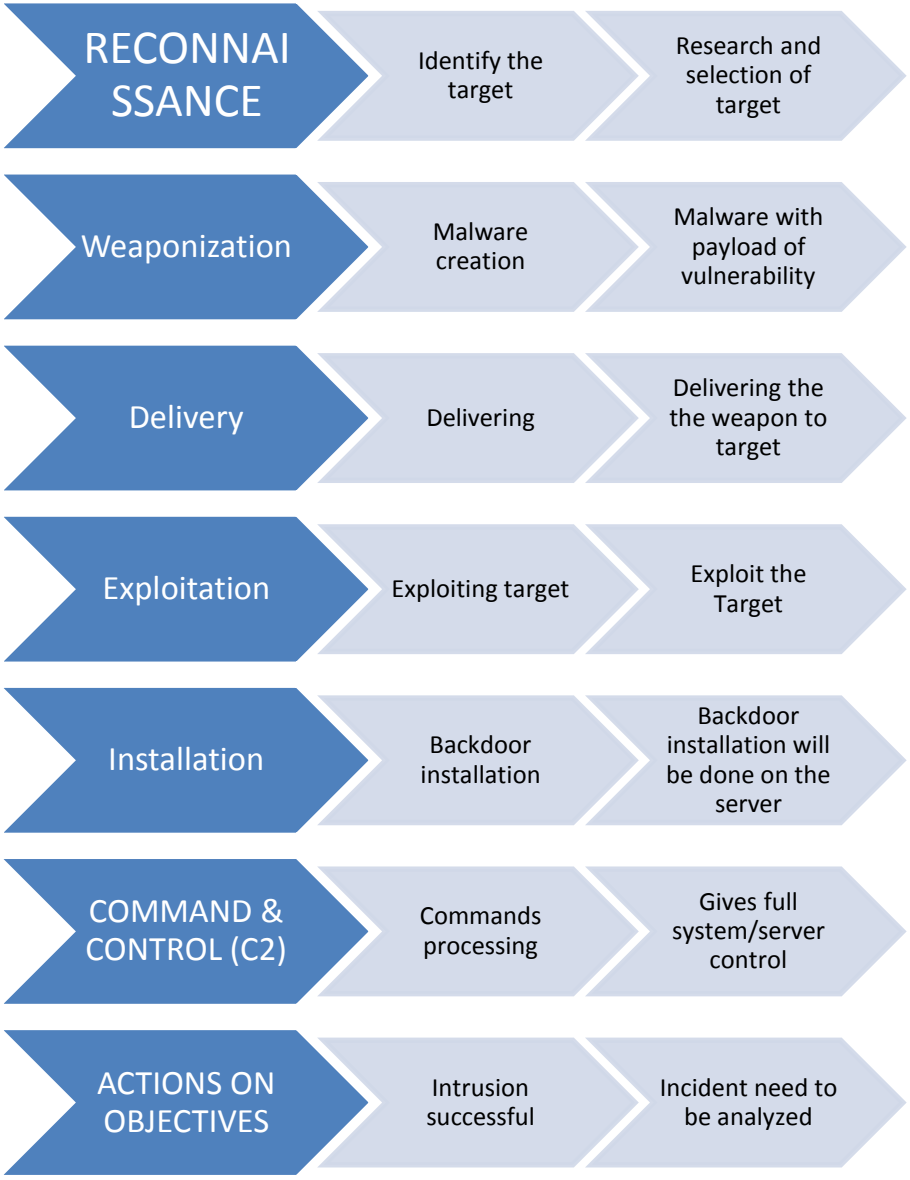
What Is *Computer* Forensics?

- The discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible in a court of law.
- AKA Cyber Forensics
- Goal
  - Identify, collect, preserve, and analyze data in a way that preserves the integrity of the evidence collected so it can be used effectively in a legal setting.
  - Ultimately, the goal is to present a plausible and believable chronicle of events to encourage a specific result While all along following all relevant laws, practices, and procedures

Forensics Vs Incident Response

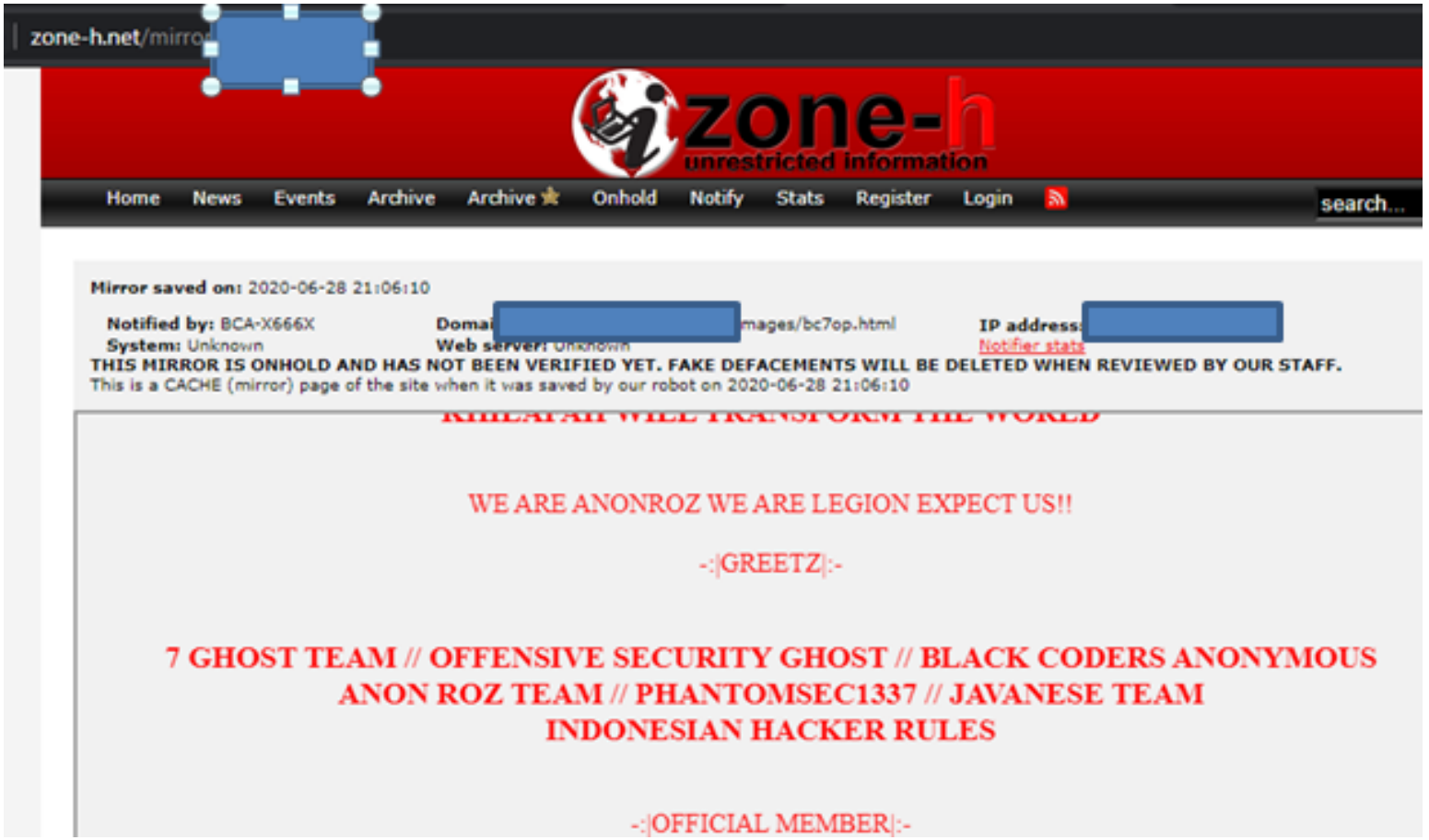
- How are incident response and forensics processes different?
- Goal
  - Incident Response – Stop the intruder(s)
  - Forensics – Reconstruct event(s)
- Time
  - Incident Response – more time pressures (the race is on)
  - Forensics – less time pressures (the race is over but there's
- Both impact how assets are acquired and analyzed
- Best practice in both cases

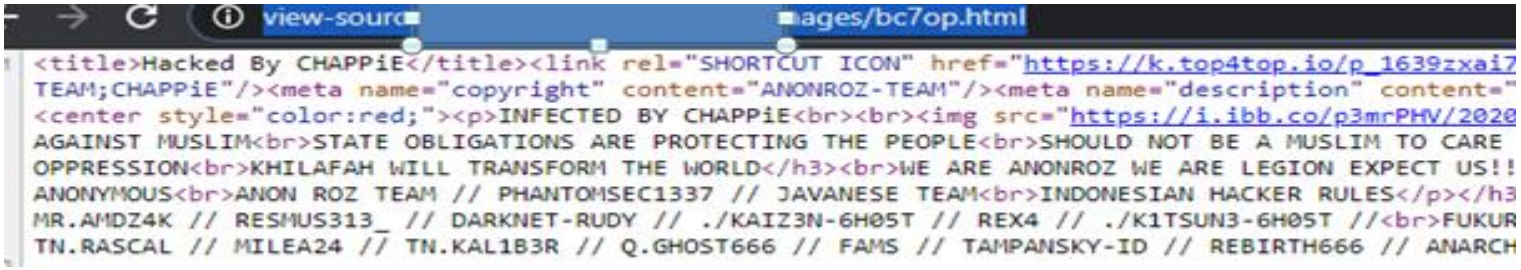
Lockheedmartin - Cyber Kill chain



Adversaries are intent on the compromise and extraction of data for economic, political and national security advancement.

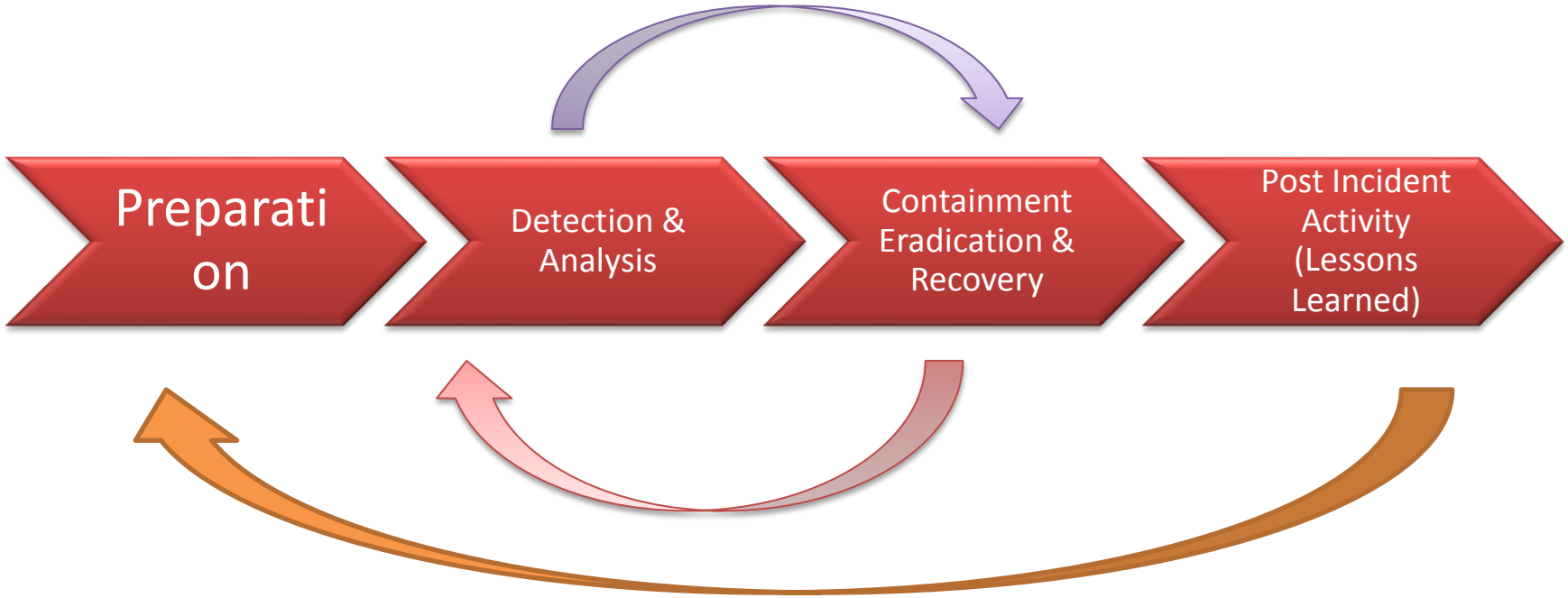
Even worse, adversaries have demonstrated their willingness to conduct destructive attacks. Their tools and techniques have the ability to defeat most common computer network defense mechanisms.


zone-h.net/mirror
zone-h
unrestricted information
Home News Events Archive Archive Onhold Notify Stats Register Login
search...
Mirror saved on: 2020-06-28 21:06:10
Notified by: BCA-X666X
System: Unknown
Domai mages/bc7op.html
Web server: Unknown
IP address:
Notifier stats
THIS MIRROR IS ONHOLD AND HAS NOT BEEN VERIFIED YET. FAKE DEFACEMENTS WILL BE DELETED WHEN REVIEWED BY OUR STAFF.
This is a CACHE (mirror) page of the site when it was saved by our robot on 2020-06-28 21:06:10
WE ARE ANONROZ WE ARE LEGION EXPECT US!!
-:|GREETZ|:-
7 GHOST TEAM // OFFENSIVE SECURITY GHOST // BLACK CODERS ANONYMOUS
ANON ROZ TEAM // PHANTOMSEC1337 // JAVANESE TEAM
INDONESIAN HACKER RULES
-:|OFFICIAL MEMBER|:-


view-sourc ages/bc7op.html
<title>Hacked By CHAPPiE</title><link rel="SHORTCUT ICON" href="https://k.top4top.io/p_1639zxai7
TEAM;CHAPPiE"/><meta name="copyright" content="ANONROZ-TEAM"/><meta name="description" content="
INFECTED BY CHAPPiE

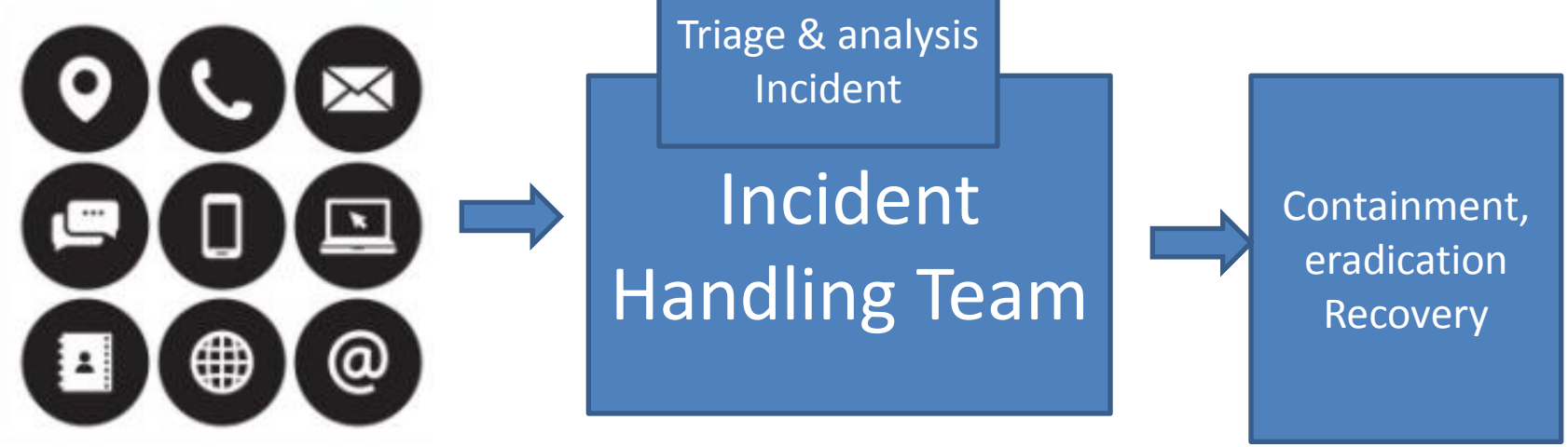
<img src="https://i.ibb.co/p3mrPHV/2020
AGAINST MUSLIM
STATE OBLIGATIONS ARE PROTECTING THE PEOPLE
SHOULD NOT BE A MUSLIM TO CARE
OPPRESSION
KHILAFAH WILL TRANSFORM THE WORLD</h3>
WE ARE ANONROZ WE ARE LEGION EXPECT US!!
ANONYMOUS
ANON ROZ TEAM // PHANTOMSEC1337 // JAVANESE TEAM
INDONESIAN HACKER RULES </h3
MR.AMDZ4K // RESMUS313_ // DARKNET-RUDY // ./KAIZ3N-6H05T // REX4 // ./K1TSUN3-6H05T //
FUKUR
TN.RASCAL // MILEA24 // TN.KAL1B3R // Q.GHOST666 // FAMS // TAMPANSKY-ID // REBIRTH666 // ANARCH

Incident Handling Methodology



NIST Incident Handling Framework reference Model:

Incident Process



Signs of an Incident

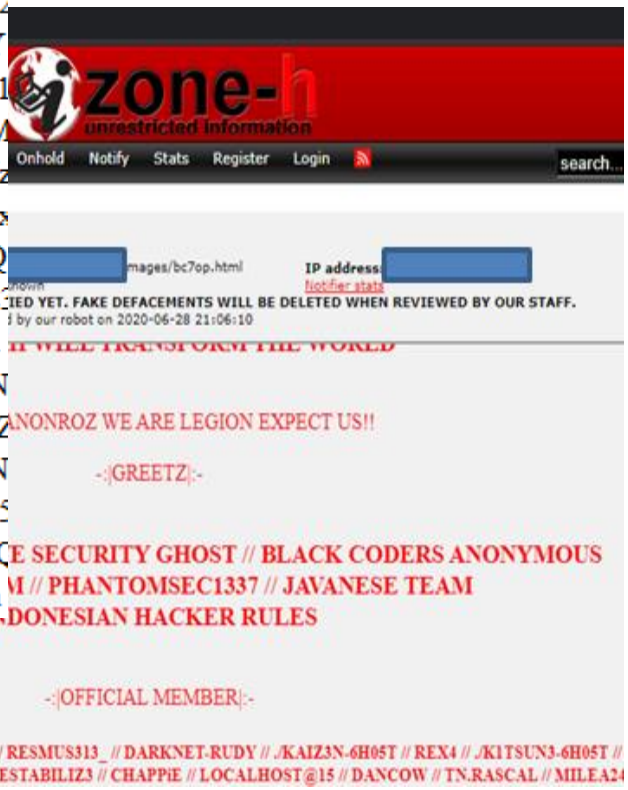
- the most challenging part of the incident response process is accurately detecting and assessing possible incidents—determining whether an incident has occurred and, if so, the type, extent, and magnitude of the problem
- Automated detection capabilities include network-based and HIPS, **antivirus software, and log analyzers**. Incidents may also be detected through manual means, such as problems reported by **users.** Some incidents have overt signs that can be easily detected, whereas others are almost impossible to detect.
- A system administrator sees a filename with unusual characters.
- The volume of potential signs of incidents is typically high – DdoS
- Deep, specialized technical knowledge and extensive experience are necessary for proper and efficient analysis of incident-related data
- Web server log entries that show the usage of a vulnerability scanner
- An announcement of a new exploit that targets a vulnerability of the organization's mail server
- A threat from a group stating that the group will attack the organization.
- Antivirus software alerts when it detects that a host is infected with malware.

Incident Analysis

160.206.114 - - [29/Jun/2020:02:29:52 +0530] "GET
lerysub.php?type=v&id=Ljc4IFVuaW9uIFNlbGVjdCAweDNjNzQ2OTc0NmM2
NlNDg2MTYzNmI2NTY0MjA0Mjc5MjA0MzQ4NDE1MDUwNjk0NTNjMmY
DY5NzQ2YzY1M2UzYzZjNjk2ZTZiMjA3MjY1NmMzZDIyNTM0ODRmNTI1
QzNTU1NDIwNDk0MzRmNGUyMjIwNjg3MjY1NjYzZDIyNjg3NDc0NzA3M
iMmYyZjZiMmU3NDZmNzAzNDc0NmY3MDJlNjk2ZjJmNzA1ZjMxMzYzMz
N2E3ODYxNjkzNzMxMmU3MDZlNjcyMjIwNzQ3OTcwNjUzZDIyNjk2ZDYx
2NTJmNjc2OTY2MjIzZTNjNmQ2NTc0NjEyMDYzNjg2MTcyNzM2NTc0M2Q
jU1NTQ0NjJkMzgyMjN1M2M2ZDY1NzQ2MTIwNmU2MTZkNjUzZDIyNDE
c0Njg2ZjcyMjIyMDYzNmY2ZTc0NjU2ZTc0M2QyMjQxNGU0ZjR1NTI0ZjVh
TEAM"/><m
Space"/><scr
style="color:
src="https://i.
OPPOSE CA
MUSLIM<b
PEOPLE<br
WHO ARE SUCKED
ENOUGH TO BE A HUMAN TO CARE ABOUT
OPPRESSION
KHILAFAH WILL TRANSFORM THE WORLD</h3><b
ARE ANONROZ WE ARE LEGION EXPECT US!!

-:|GREETZ|:-

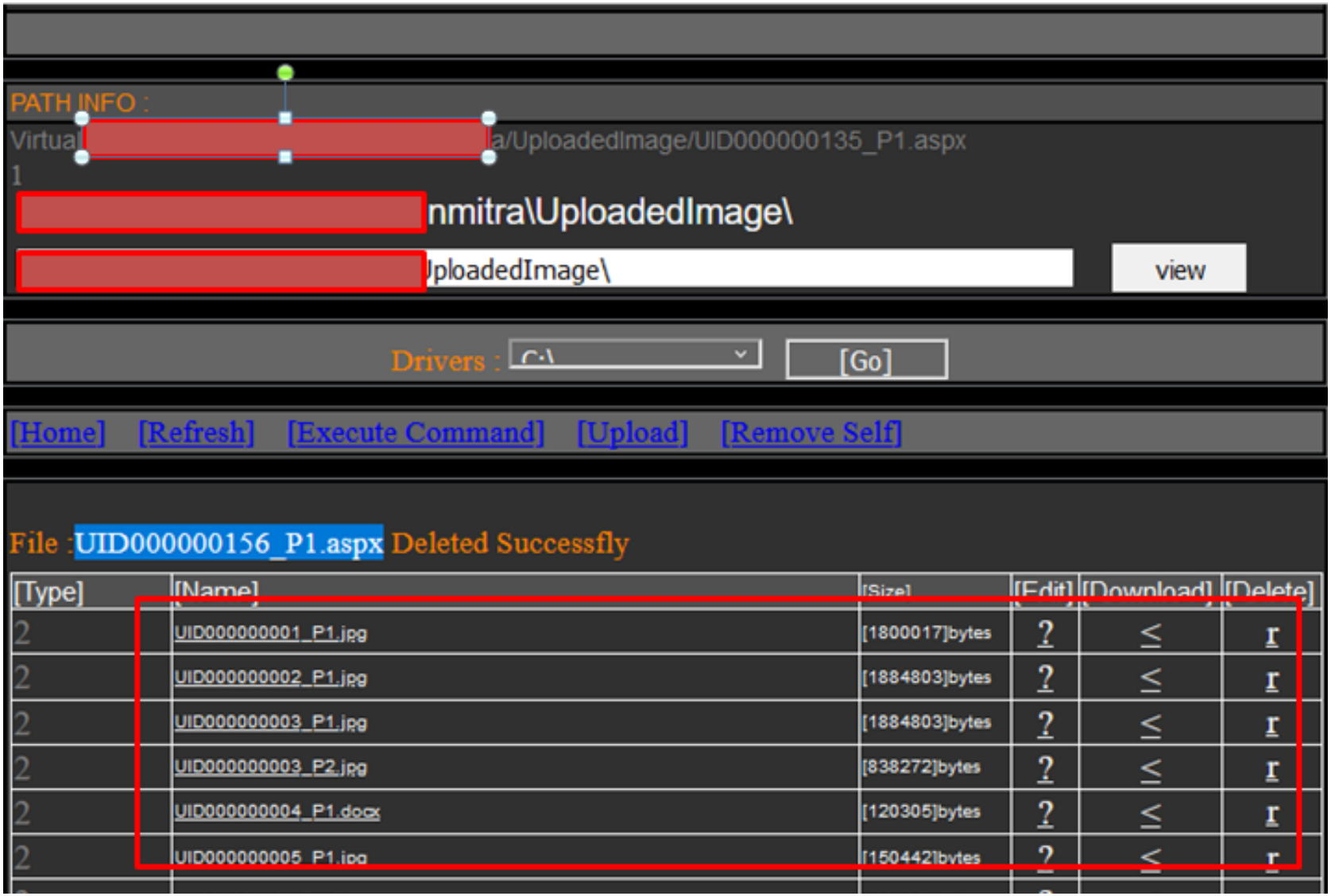
<h3>7 GHOST TEAM // OFFENSIVE SECURITY GHOST // BLAC
CODERS ANONYMOUS
ANON ROZ TEAM // PHANTOMSEC1337 //
JAVANESE TEAM
INDONESIAN HACKER RULES</p></h3>
-
:|OFFICIAL MEMBER|:-
<h5 style="text-align:center;">MR-X666X // SEA-
GHOST // MR.AMDZ4K // RESMUS313_ // DARKNET-RUDY // ./KAIZ3N-



Web Access log

- 12-07-2021 13:24:30 10.133.0.9 GET /ImgHandler.aspx SlNo=162 443 - 46.2.129.216 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/91.0.4472.124+Safari/537.36 https://mirror-h.org/ 200 0 0 225

Webshell


PATH INFO :
a/UploadedImage/UID000000135_P1.aspx
nmitra\UploadedImage\
UploadedImage\
view
Drivers :
C:\
[Go]
[Home] [Refresh] [Execute Command] [Upload] [Remove Self]
File :UID000000156_P1.aspx Deleted Successfly
[Type] [Name] [Size] [Edit] [Download] [Delete]
2 UID000000001_P1.jpg [1800017]bytes
2 UID000000002_P1.jpg [1884803]bytes
2 UID000000003_P1.jpg [1884803]bytes
2 UID000000003_P2.jpg [838272]bytes
2 UID000000004_P1.docx [120305]bytes
2 UID000000005_P1.jpg [150442]bytes

Incident Containment

- Containment is important before an incident overwhelms resources or increases damage.
- Containment provides time for developing a tailored remediation strategy. An essential part of containment is decision-making
- Containment strategies vary based on the type of incident.
- the strategy for containing an email-borne malware infection is quite different from that of a network-based DDoS attack.
- Organizations should create separate containment strategies for each major incident type, with criteria documented clearly to facilitate decision-making.

Incident Eradication

- deleting malware and disabling breached user accounts
- Fixing the vulnerable issues
- During eradication, it is important to identify all affected hosts within the organization so that they can be remediated.

Recovery

- In recovery, administrators restore systems to normal operation, confirm that the systems are functioning normally, and (if applicable) remediate vulnerabilities to prevent similar incidents.
  - Firewall rules
  - Antivirus
  - Restore/ reinstall entire systems
  - Vulnerabilities patching

Post Incident Activity (Lessons learned)

- Learning & improvement
- Meeting
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?
- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?

Forensics

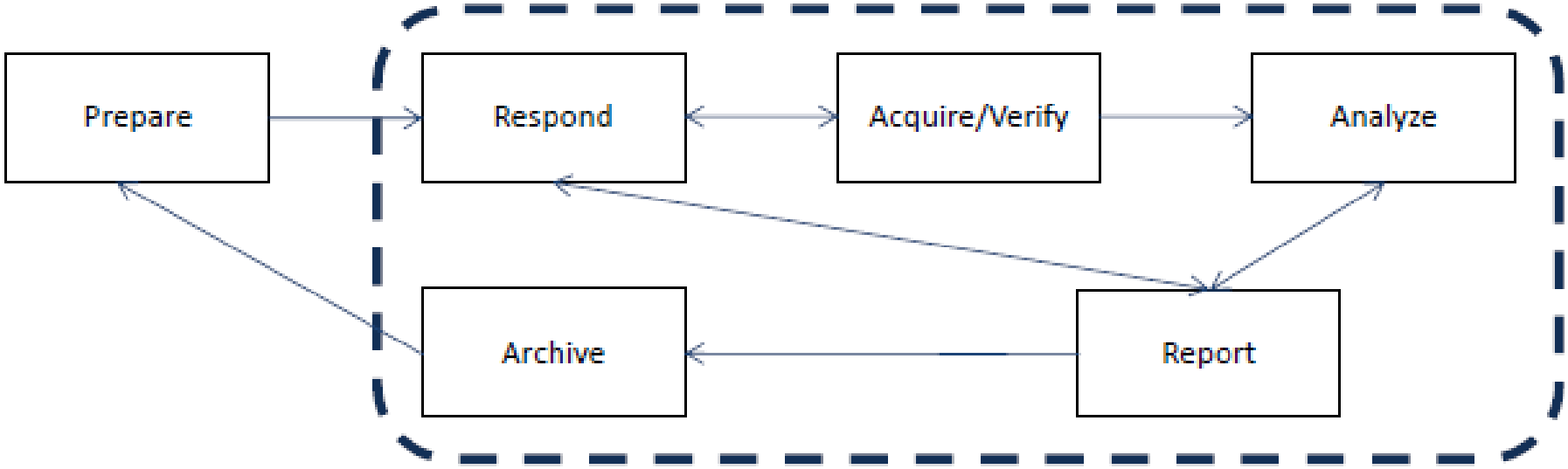
What Is *Computer* Forensics?

- The discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible in a court of law.
- AKA Cyber Forensics
- Goal
  - Identify, collect, preserve, and analyze data in a way that preserves the integrity of the evidence collected so it can be used effectively in a legal setting.
  - Ultimately, the goal is to present a plausible and believable chronicle of events to encourage a specific result While all along following all relevant laws, practices, and procedures

Cyber Forensic: Investigation Process

Identification	• Identify the purpose of Investigation • Identify the resources required
Seizure	• Data is isolate, Secure and preserve
Acquistion	• Imaging-security & Integrity
Analysis	• Identify tool and technique to use • process data • Interpret analysis results
Documentation	• Documentation of the crime scene along with photographing, sketchnig, and crime-scene mapping

Methodology contd..

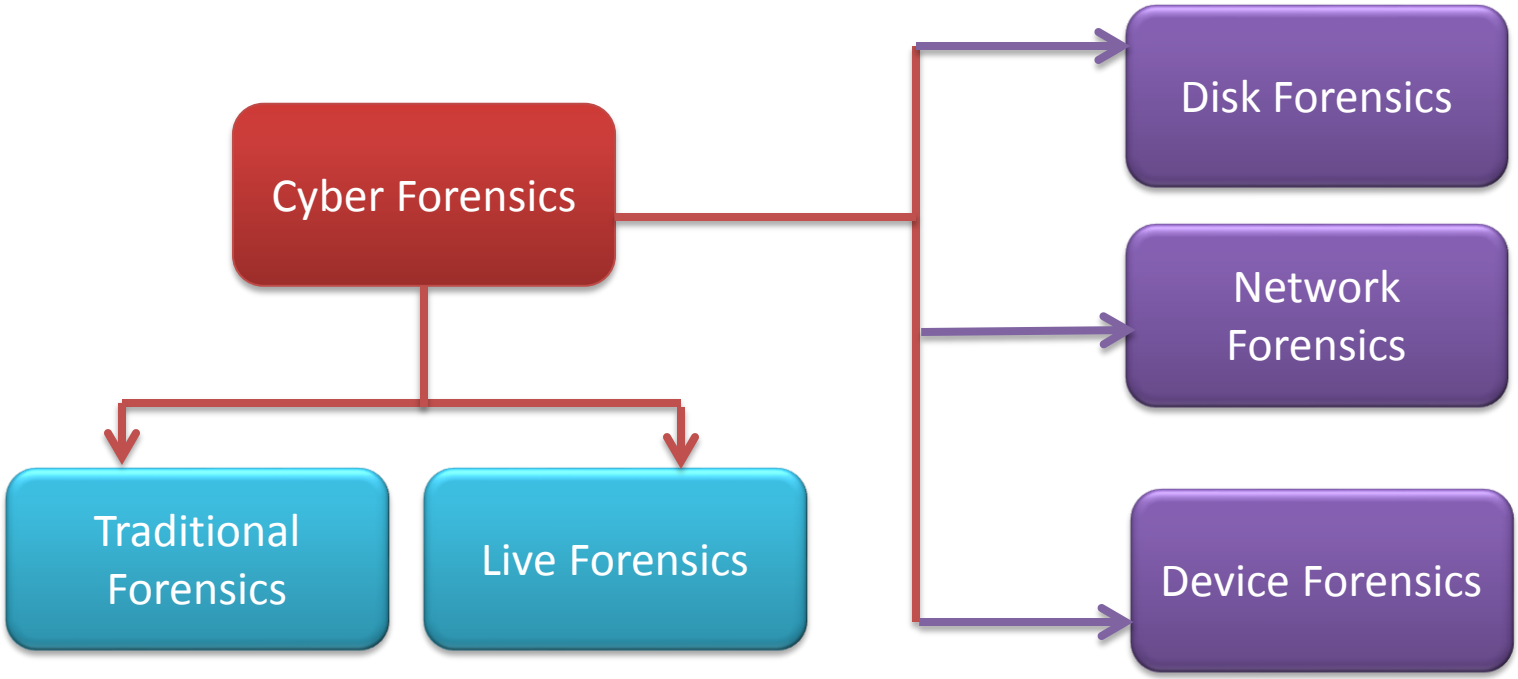


PRAVARA

Issues in Digital Evidence

- Digital evidence is volatile
- Extremely fragile
- Easily tampered

Cyber forensics



Seizure

- Seizure is the process of capturing suspect computer or storage media for evidence collection and generating a hash value corresponding to the evidence.

Seizure principles

Actions taken by investigating officer should not change data held on computer or storage media which may subsequently be relied upon in court

If a person finds it necessary to access original data held on computer or storage media. Person must be competent to do so and be able to give evidence explaining the relebance and implications of their applications

An audit trail or other record of all activities aplied to computer based evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

Investigating officer has overall responsibility in ensuring that thte law and these principles are adhered to

Investigative Principles
Evidence Preservation

- Investigative Principles
- Evidence Preservation
- AKA “Chain of Custody”
- All evidence must be accounted for at all times
- Evidence has not been altered
  - Digital evidence – checksums
- Party offering evidence has burden of proof as to its veracity
- Materials
- Evidence handling forms
  - Evidence containers
  - Safes/locked cabinets
  - Logs
  - Cameras or other photographic equipment
- Improperly preserved evidence: case could be tossed out

Prepare

- Build and maintain capabilities for all investigations
- • Reconnaissance capability
- - "*Know thy enemy*" (Sun Tzu)
- - Non-attribution
- • Imaging equipment
- - Hardware, software, tool building, Internet connectivity, reach back
- • Analysis environment
- • Physical storage
- • Workspace – classification issues?
- • Laws, Policies and procedures
- • Maintenance
  - - Equipment
  - - Personnel

Hash

- It is a one way function
- In real terms you simply cannot reverse engineer a password from a given hash value.
- In the forensic analysis community, if you provide a copy of a forensic image file set to another examiner, you also provide the hash value associated with it.
- The other examiner can compute the hash value for what they received and compare that to the provided hash value. If they match, we know that we are both looking at exactly the same thing.
- If the hash values don’t match, we know that something is different. The hash value provides no clues as to what is different.
- The hash value has nothing to do with the name of a file and different hash algorithms produce different hash values even when processing the same files. Just a hash value by itself is useless without identifying which hash algorithm was used to create it.

```
f5fbace98ed8829dc705191f18321d18 C:\TEMP\file-110738171218L001.pdf
935a569281046198ec9256da83b5fcd4 C:\TEMP\file-110739171218L001.pdf
d852a07c1a3065d42be9b119fd92091e C:\TEMP\file-110751171218L002.pdf
eac04333af784bc2094d55bd0b233173 C:\TEMP\file-110766171218L001.pdf
76f5af6dc1a97facc1f830d7a66cfd35 C:\TEMP\file-144727171111L001 (1).pdf
76f5af6dc1a97facc1f830d7a66cfd35 C:\TEMP\file-144727171111L001 (2).pdf
76f5af6dc1a97facc1f830d7a66cfd35 C:\TEMP\file-144727171111L001.pdf
```

MD5 Hash

```
a23e46b2e341d2b9f9bf291a67c9e207c70d796d70d0c6973cf46b0c2156f5ee C:\temp\file-110738171218L001.pdf
285aea0e4e4605f28c89ea20253456e98c5fb999d3988084b8ad1ed82f36fb2e C:\temp\file-110739171218L001.pdf
62e0c4e16b9ed0d23354a9973783958bb93fd3d93524fa5f49ee88663d086ba2 C:\temp\file-110751171218L002.pdf
4985619b30c4ef8dd100cc76810d50dbed9e2ee568281a843b49f75812730420 C:\temp\file-110766171218L001.pdf
95df48581de075511e44aceb2417a0cc125c593dfbc904fcb9ceaa3fefbd30c5 C:\temp\file-144727171111L001 (1).pdf
95df48581de075511e44aceb2417a0cc125c593dfbc904fcb9ceaa3fefbd30c5 C:\temp\file-144727171111L001 (2).pdf
95df48581de075511e44aceb2417a0cc125c593dfbc904fcb9ceaa3fefbd30c5 C:\temp\file-144727171111L001.pdf
```

SHA256 Hash

Forensic Toolkit

- CyberCheckSuite (C-DAC) : Commercial
- EnCase(Guidance) : Commercial
- FTK (AccessData) : Commercial
- Helix : Freeware
- Cellebrite : commercial
- Oxygen Forensic Suite : commercial
- Autopsy (GUI) + Sleuth Kit : Freeware
- TCT (The Coroner's Toolkit) : Freeware
- KnoppixSTD : Freeware
- ProDiscoverForensics: Commercial
- X-Ways Forensics: Commercial
- F-Response: Commercial

Tool Kit

- Log Book – To record all actions /events with date & time chronologically
- Safe Boot / Forensic Live CD – (e.g. Helix)
- Digital camera
- S/w Tools for – Volatile data collection – Imaging of the hard disk(s), etc – System H/w & S/w configuration details
- Laptop (Forensic Workstation)
- RJ-45 Crossed LAN cable
- Tools to open CPU Cabinet, detach Hard Disk (multi screw driver set, etc)
- Multi-purpose mechanical toolset
- Anti-static covers
- Air bubbled PVC covers
- Marking labels

Digital Evidence - Types

- Volatile (Non-persistent) Memory that loses its contents, if power is turned off; e.g. Data stored in RAM (semiconductor storage) (System BIOS: CMOS RAM - battery powered)
- Non-volatile (Persistent) No change in contents, even if power is turned off; e.g. Data stored in a tape / floppy disk / hard disk (magnetic storage), CD / DVD (optical storage), ROM (semiconductor storage; USB Thumb Drives – Flash Memory).

Digital evidence types contd..

- Volatile data:
  - Can disappear quickly, easily, asynchronously, automatically
  - Does not survive a reboot or power cycle
- Physical memory, which contains
  - Processes
  - Connections
  - Credentials
  - Clear text passwords
  - Decrypted file systems/containers
  - Network traffic
- Non-volatile data:
  - Usually does not disappear quickly
  - Does survive reboot or power cycle
  - Disks, CDs, DVDs, USB devices

What software is installed at the crime scene?

Write blockers

- Prevent writing of data to the suspected original hard disk / other popular data storage media
- Ensure the integrity of the suspected original hard disk / other popular data storage media
- Software Write Blockers v/s Hardware Write Blockers

Prepare: Policies and Procedures

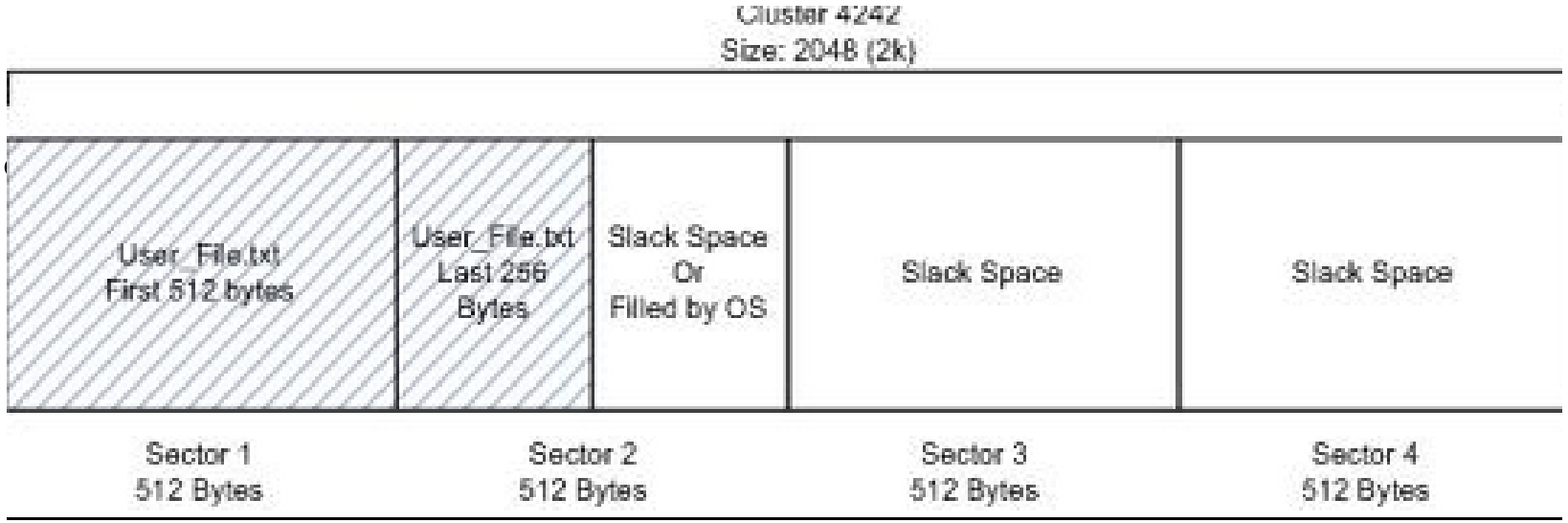
- Evidence and Handing
- • Storage
- • Chain of custody
- • Documentation
- Digital Forensic Lab Facilities
- • Access
- • Acceptable use
- Digital Forensic Lab Equipment
- • Acceptable use
- • Maintenance plans and inventory control

Direct Analysis of Org. Digital Evidence : Strictly Forbidden

- Will change MAC (last Modified, last Accessed, Created) details (date & time) of a file
- Analysing a live file system / original evidence also changes the state of the evidence (MAC details)
- Any analysis on the original digital evidence makes it a tampered digital evidence
- Digital evidence will not be accepted by court and render it useless
- Solution – analyse an image (also called clone) of the original digital evidence

Slack Space

- Hard Disk → File System→ Sectors→Clusters
- Slack space refers to portions of a hard drive that are not fully used by the current allocated file and which may contain data from a



Logical Copy v/s Physical Copy

- Logical copy In a logical copy, the active directories and files only of a logical volume are copied. It does not capture other data that may be present on the media such as deleted files or residual data stored in the slack space.
- Physical copy (generally called forensic imaging, imaging, cloning or mirror image) Generate a bit for bit copy of the original media; include free space and slack space.

Cloud

- Identifying the machines connecting to remote cloud machines.
- Tools supporting to connect and download the images.

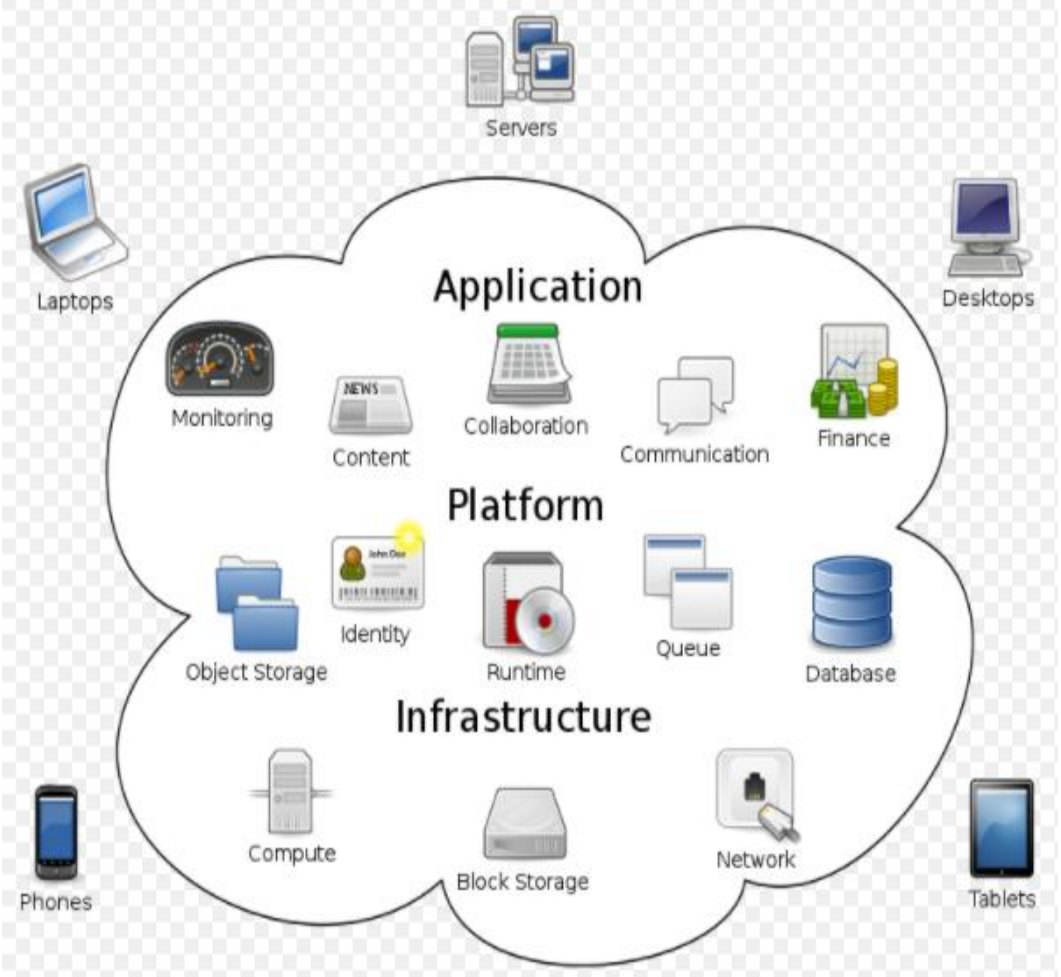


Image: https://en.wikipedia.org/wiki/Cloud_computing

VPN

- **Stream from anywhere**
- **Access blocked websites**
- **Avoid censorship**
- **Beat price discrimination**
- **Don’t be tracked**

Advantage of having the image of org. Digital Evidence

- Analyzing the image of the digital evidence will
  - Preserve the original evidence
  - Prevent any inadvertent alteration of original evidence during examination
  - Image (Clone) may be made again if required

Computer Forensic Toolkits: imaging s/w with GUI

- TrueBack (C-DAC) - Freeware
- FTK Imager (AccessData) – Freeware
- Built-in feature of most of the computer forensic toolkits

Respond

- Typically performed by victim organization
- • Detect or suspect unauthorized activity
- - Does the organization know what normal is
- • Report activity
- • Validate incident
- • Assess damage
- • Development strategy (containment, eradication, recovery, and investigation)
- • Coordinate (management, human, legal, external/press)

Reconnaissance

- Use reconnaissance capabilities to profile on-site environment if allowed
    - Non-attribution network?

Gather:

- IP address ranges
- IP addresses of technology of interest
- OSes, applications, and versions of technology of interest
- Network topology
- Open Source Intelligence
    - Social Media
    - Blogs and mailing lists
    - Google is your friend

Respond Phase
On-Site Survey

What's *really* at the crime scene?

You did recon, but now you're there

Goal:

- Understand sophistication of persons of interest
  - How?
- Understand and document all:
  - Hardware (devices)
  - Software (OS plus applications)
  - Infrastructure (wired, wireless, cable, fiber, etc.)
  - Remote access?
- Determine what needs to be acquired (confiscated and/or imaged)

Seizure

- Store the seized org. evidence in a protected storage (Air bubbled PVC, antistatic bag)
- Transfer the Computer System to a secure location

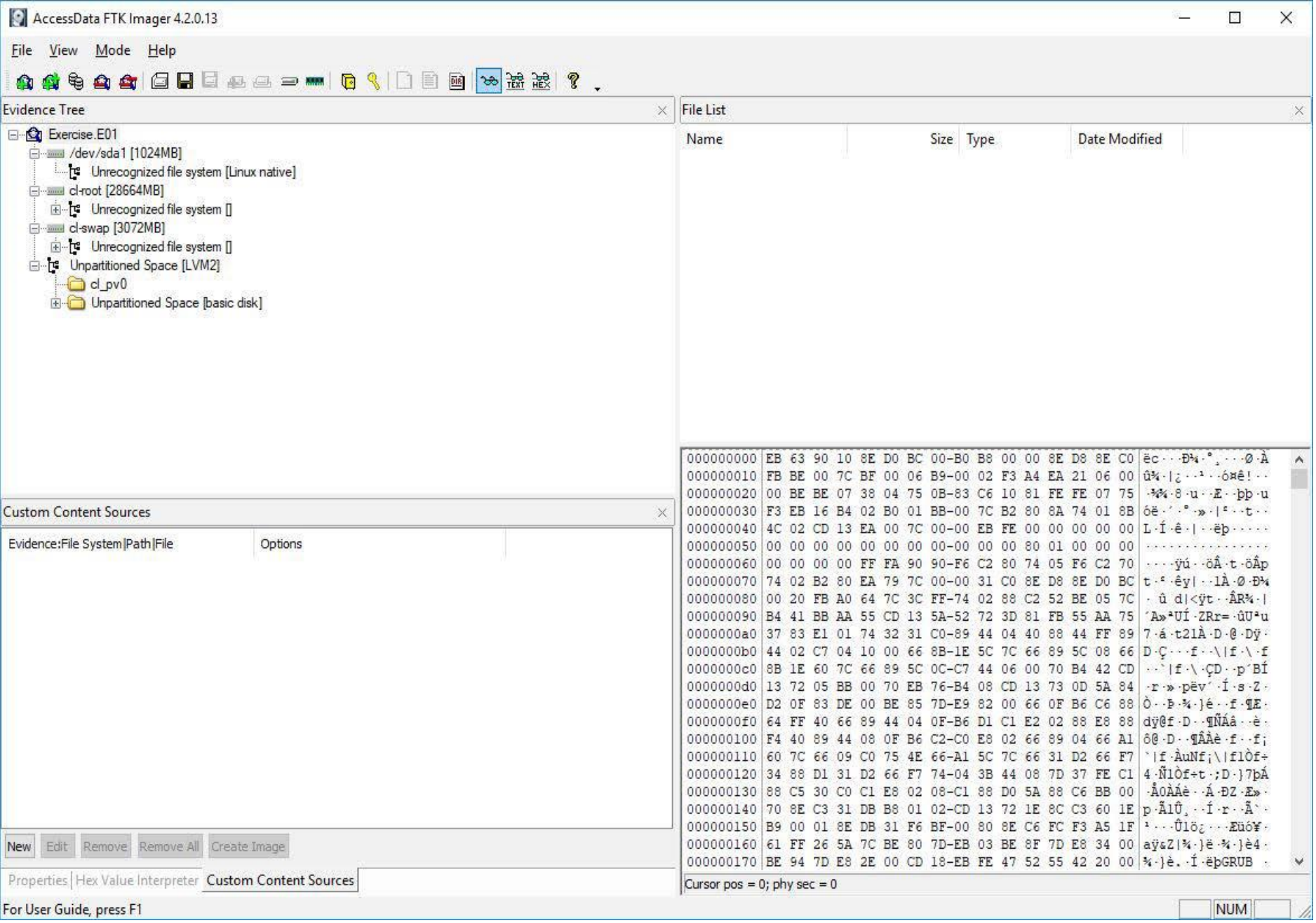
Acquire

- Host-based assets
- Network-based assets
- Removable media assets
- Mobile assets
- Verify all assets
- Likely one chance to acquire assets
- Evidence Handling
- Integrity
- Package, transport, and store assets

Acquire

Image with:

- Windows
  - FTK and EnCase
  - **win32dd** and **winen** from Helix, **mdd** from ManTech
- Unix/Linux
  - Need extensions (**fmem** and **LiMe**)
  - Example of needing to compile something after on-site (reachback)
- Process with:
  - Volatility Framework
  - Open source memory analysis software tools


AccessData FTK Imager 4.2.0.13
File View Mode Help
Evidence Tree
Exercise.E01
/dev/sda1 [1024MB]
Unrecognized file system [Linux native]
cl-root [28664MB]
Unrecognized file system []
cl-swap [3072MB]
Unrecognized file system []
Unpartitioned Space [LVM2]
cl_pv0
Unpartitioned Space [basic disk]
File List
Name
Size
Type
Date Modified
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value Interpreter
Custom Content Sources
000000000 EB 63 90 10 8E D0 BC 00-B0 B8 00 00 8E D8 8E C0
000000010 FB BE 00 7C BF 00 06 B9-00 02 F3 A4 EA 21 06 00
000000020 00 BE BE 07 38 04 75 0B-83 C6 10 81 FE FE 07 75
000000030 F3 EB 16 B4 02 B0 01 BB-00 7C B2 80 8A 74 01 8B
000000040 4C 02 CD 13 EA 00 7C 00-00 EB FE 00 00 00 00 00
000000050 00 00 00 00 00 00 00 00-00 00 00 80 01 00 00 00
000000060 00 00 00 00 FF FA 90 90-F6 C2 80 74 05 F6 C2 70
000000070 74 02 B2 80 EA 79 7C 00-00 31 C0 8E D8 8E D0 BC
000000080 00 20 FB A0 64 7C 3C FF-74 02 88 C2 52 BE 05 7C
000000090 B4 41 BB AA 55 CD 13 5A-52 72 3D 81 FB 55 AA 75
0000000a0 37 83 E1 01 74 32 31 C0-89 44 04 40 88 44 FF 89
0000000b0 44 02 C7 04 10 00 66 8B-1E 5C 7C 66 89 5C 08 66
0000000c0 8B 1E 60 7C 66 89 5C 0C-C7 44 06 00 70 B4 42 CD
0000000d0 13 72 05 BB 00 70 EB 76-B4 08 CD 13 73 0D 5A 84
0000000e0 D2 0F 83 DE 00 BE 85 7D-E9 82 00 66 0F B6 C6 88
0000000f0 64 FF 40 66 89 44 04 0F-B6 D1 C1 E2 02 88 E8 88
000000100 F4 40 89 44 08 0F B6 C2-C0 E8 02 66 89 04 66 A1
000000110 60 7C 66 09 C0 75 4E 66-A1 5C 7C 66 31 D2 66 F7
000000120 34 88 D1 31 D2 66 F7 74-04 3B 44 08 7D 37 FE C1
000000130 88 C5 30 C0 C1 E8 02 08-C1 88 D0 5A 88 C6 BB 00
000000140 70 8E C3 31 DB B8 01 02-CD 13 72 1E 8C C3 60 1E
000000150 B9 00 01 8E DB 31 F6 BF-00 80 8E C6 FC F3 A5 1F
000000160 61 FF 26 5A 7C BE 80 7D-EB 03 BE 8F 7D E8 34 00
000000170 BE 94 7D E8 2E 00 CD 18-EB FE 47 52 55 42 20 00
Cursor pos = 0; phy sec = 0
For User Guide, press F1
NUM

Analysis

- Confirmatory analysis
- Confirm or refute allegations of suspicious activity
- Transform data collected into more manageable size and form
- Initial survey of collected data
- Extract relevant data
- Examine, analyze, and reconstruct events

Analysis

- Goal: Search for evidence requested in analysis request
- Key point: Knowing the imaged device
- • Computer System
  - Disk specifics
- Bad blocks, host protected area, ???
  - File system specifics (FAT, NTFS, ext2, ext3, etc.)
- Arrangement, file allocation/deletion, free space, slack space
- - Operating system specifics
- Where information resides
- Configuration information
- Application-specific data (email, browser history, chat logs)
- Mobile Phones

The Analyze Contd..

Analysis Methodology – Goal 1

Goal: Construct a time line of events – event reconstruction

What is a timeline?

- An ordered list of changes on the device
- What was changed and when
- If file system, use file system metadata

- Modified, accessed, created/changed (MAC)
- Only last MAC time saved – intermediate changes lost
- Can zero in on a specific period
- File system independent (NTFS, FAT, ext{2,3})

Analysis contd..

- Search for evidence cited in original forensic request
- Analyze imaged information
  - What are you looking for?
  - How will you recognize it when you find it?
  - Where might you find it?
  - What does it mean once you've found it?

  Construct a time line of findings
  - How did you find what you found (repeatability)?

  Tools
  - Commercial and Open Source/Public Domain
  - Watch for counter forensics tools
- TAKE NOTES WHILE DOING DATA ANALYSIS!

Anti-Forensics

- Tools on RAM
- Diskless PC (RAM only)
- Disk Sanitisers-Wipe
- Compressed files (with password)
- Encrypted files (with password)
  - PGP
  - Digital Signature
- Steganography

Anti forensics contd..

Encryption

- Obfuscate information
- Examples:
  - Truecrypt
  - Bit Locker
  - File Vault
  - PGP – Pretty Good Privacy

Virtual Machines

- A system on top of another system
- Examples:
  - VMware
  - Virtual Box
  - Hyper-V

Reporting

- Present findings, findings, findings!
  - Communicate relevant findings to audiences
  - • Management
  - • Technical personnel
  - • Legal personal
  - • Law enforcement
  - Concise, clear, and concise
- May be report, but could be oral presentation, or both
- Establish timeline
- Tell a story

Archive

Data Preservation -1

Be prepared for a case to be reopened

Can you accommodate:

- Updates to analysis software
- Changes to analysis infrastructure
- Changes in personnel

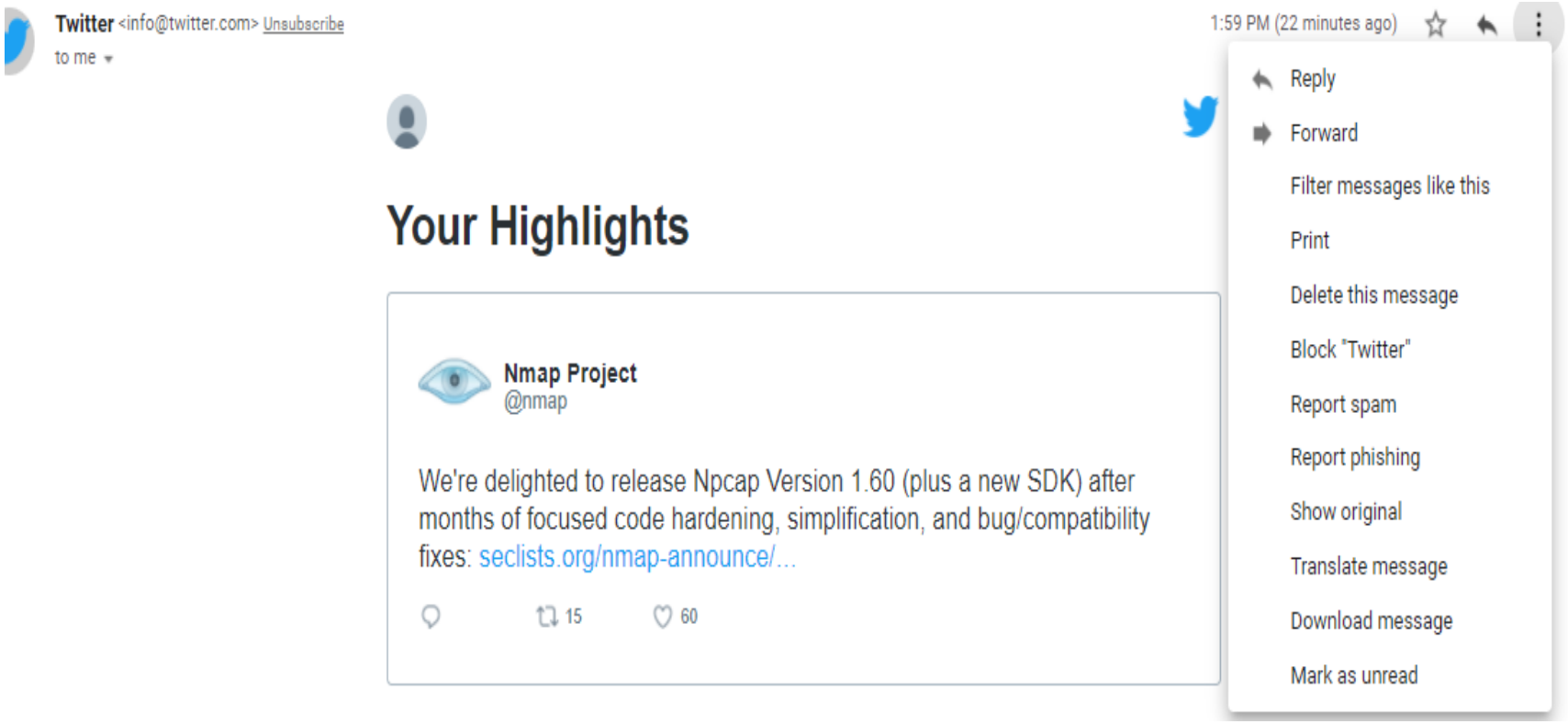
Goal:

  - Case should be “resurrected” to the same state as when it was Retired
- Secure location:
  - Safe
  - Locked cabinet
- Well-defined and understood storage procedures
- Records showing that procedures were followed
- Evidence custodian – who is this in your world?

Email

- Many compromises start with E-mail.
- Understanding how E-mails are crafted to fool people is an
- important step in investigating crimes.
- Looking at the URLs and files used by threat actors can help reveal
- other leads to investigate.
- Looking at E-mail in text format can help reveal data that was
- intended to be hidden.
- You MUST always be careful in handling suspect E-mail as it can
- contain viruses and other items that can infect your systems and
- alert the sender that someone viewed the E-mail.

Email Full details



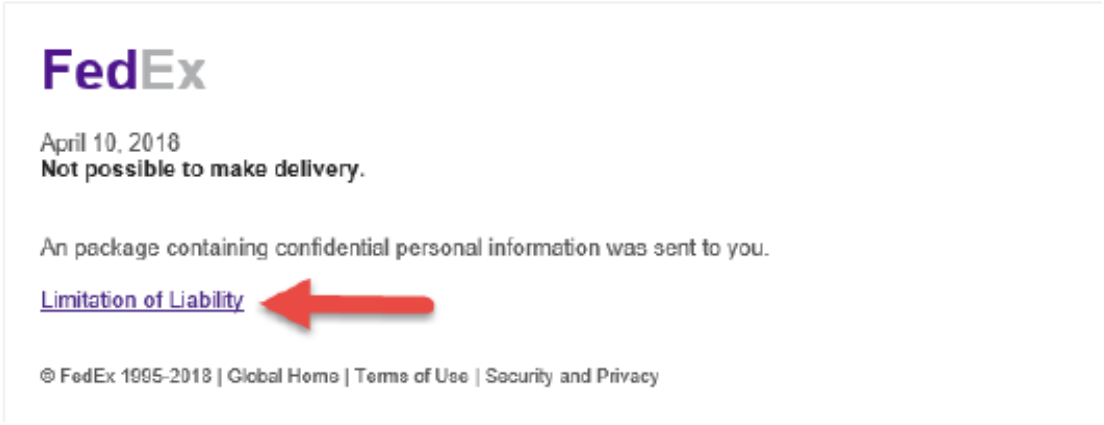
Email Analysis

```
Delivered-To:
Received: by 2002:a4a:c54b:0:0:0:0:0 with SMTP id j11csp133560ooq;
        Thu, 9 Dec 2021 00:29:47 -0800 (PST)
X-Google-Smtp-Source: ABdhPJwGA4TDWp9TdXuRnDj7paN/YEPcHC6vb1zponzDtKePFWCa0sWbFfJ+dol+ekii+qZD32KP
X-Received: by 2002:a05:6214:20ab:: with SMTP id 11mr14832608qvd.31.1639038587456;
        Thu, 09 Dec 2021 00:29:47 -0800 (PST)
ARC-Seal: i=1; a=rsa-sha256; t=1639038587; cv=none;
        d=google.com; s=arc-20160816;
        b=TIsSVRP5j8xOIQP3zjYg0FK1r96qbvWe5Rg0iJIcjIPElQB0HPjWQmoq64ZyMC+KNa
         OkPZc/upk13zJ9gPWW4LsbhcIRZM9vYFErXkSt/+8PrEPO10y8+TBAyqYSuPwg78UeJB
         RgtwVUZCWHmsyq3i7Q8YDRIjbBmacmsulWT0fR7nLn+FOpM0dKk/+WzX1qeokDAfUy/1
         fnhQqrFITA4PQvvRy9FlQ+1wPNYVgoO76gyI0yNAM4Em3iEqgNVF6qHSq+incITeYqnA
         20gcKTPGDrzBTkm6S88qaxTZshPuAQuqw+t0foAvHjNMoDSRi2JcFu/ASFDL2+fYQNsm
         N+8Q==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=feedback-id:message-id:precedence:list-unsubscribe:mime-version
         :subject:to:from:date:dkim-signature;
        bh=CB5X3V6nrEoUiDJJC78Zv/wceWJIwnwbEZL9cq3yMO8=;
        b=lQGX0K1/M3r4e6GG5/kDOxS8iG6xz7OohD0tIVYQgEYgoUvaPWdYZaPwZh5dOu5euk
         bY9qz4WxWu06UKOqajFiWmBHGF/X2sxjKRQAq3YXBljPK5kwgMWrV0SPGrk56b/W1LHj
         OViGSio+LldOTy0oRsaMwswzPUeaQSKQWmpfJsJY+PgQ9b8cV6/SarMvAM5C0mxmP801
         DaIF0J58whV88OpCZXcCslxfs4gToWnm5oz4olRq4hLJd2SA7CPhFrH6mc8OZ6xpffUN
         51soPPekKMqZOfyh77maCz0n5FEU8FWVrogjMt+LZABnYli/hs/IbAxc13YrQ+IKKBf/
         d+qg==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@twitter.com header.s=dkim-201406 header.b=AoCAWW47;
       spf=pass (google.com: domain of n0970b13a44-128db9ee5f824400-                ===gmail.com@bounce.twitter.com designates 199.59.150.93 as permitted sender)
smtp.mailfrom="n0970b13a44-128db9ee5f824400                gmail.com@bounce.twitter.com";
       dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=twitter.com
Return-Path: <n0970b13a44-128db9ee5f824400-                ===gmail.com@bounce.twitter.com>
Received: from spruce-goose-ax.twitter.com (spruce-goose-ax.twitter.com. [199.59.150.93])
        by mx.google.com with ESMTPS id m3si6472575qtk.534.2021.12.09.00.29.47
        for <                >
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Thu, 09 Dec 2021 00:29:47 -0800 (PST)
Received-SPF: pass (google.com: domain of n0970b13a44-128db9ee5f824400-                ===gmail.com@bounce.twitter.com designates 199.59.150.93 as permitted sender)
client-ip=199.59.150.93;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@twitter.com header.s=dkim-201406 header.b=AoCAWW47;
       spf=pass (google.com: domain of n0970b13a44-128db9ee5f824400-                ==gmail.com@bounce.twitter.com designates 199.59.150.93 as permitted sender)
smtp.mailfrom="n0970b13a44-128db9ee5f824400                ===gmail.com@bounce.twitter.com";
       dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=twitter.com
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=twitter.com; s=dkim-201406; t=1639038586; bh=CB5X3V6nrEoUiDJJC78Zv/wceWJIwnwbEZL9cq3yMO8=;
h=Date:From:To:Subject:MIME-Version:Content-Type:List-Unsubscribe:
        Message-ID; b=AoCAWW47vGGoFLcXjfnEbWAXiOSgf6U1FpL1vC2ExcIv8EQa/MNrmMEpsAJjcxKCG
        ZimqodTQRqoQ5oHakDiKO9lh795c8CqbC53glgonz4O/JGbjQ/2cxvv0kPoq40GGvy
        5PYi8o0LHvOnnp1q+/aF096fsGLP6tjlECO8pMDEITCfZ9zyDi9fC41T1b78gLVADv
        XD8SpXTcFMMQ5K0ONVNMjEJvU2wDqWzTk8p0qtUIN5+sDY1ldbEyuirfD3t2jd/Km7
```

- How email works
- Components of an Email
- URL Analysis
- File Attachment Analysis

Phishing ex

URL's can be masked when viewing in HTML format.



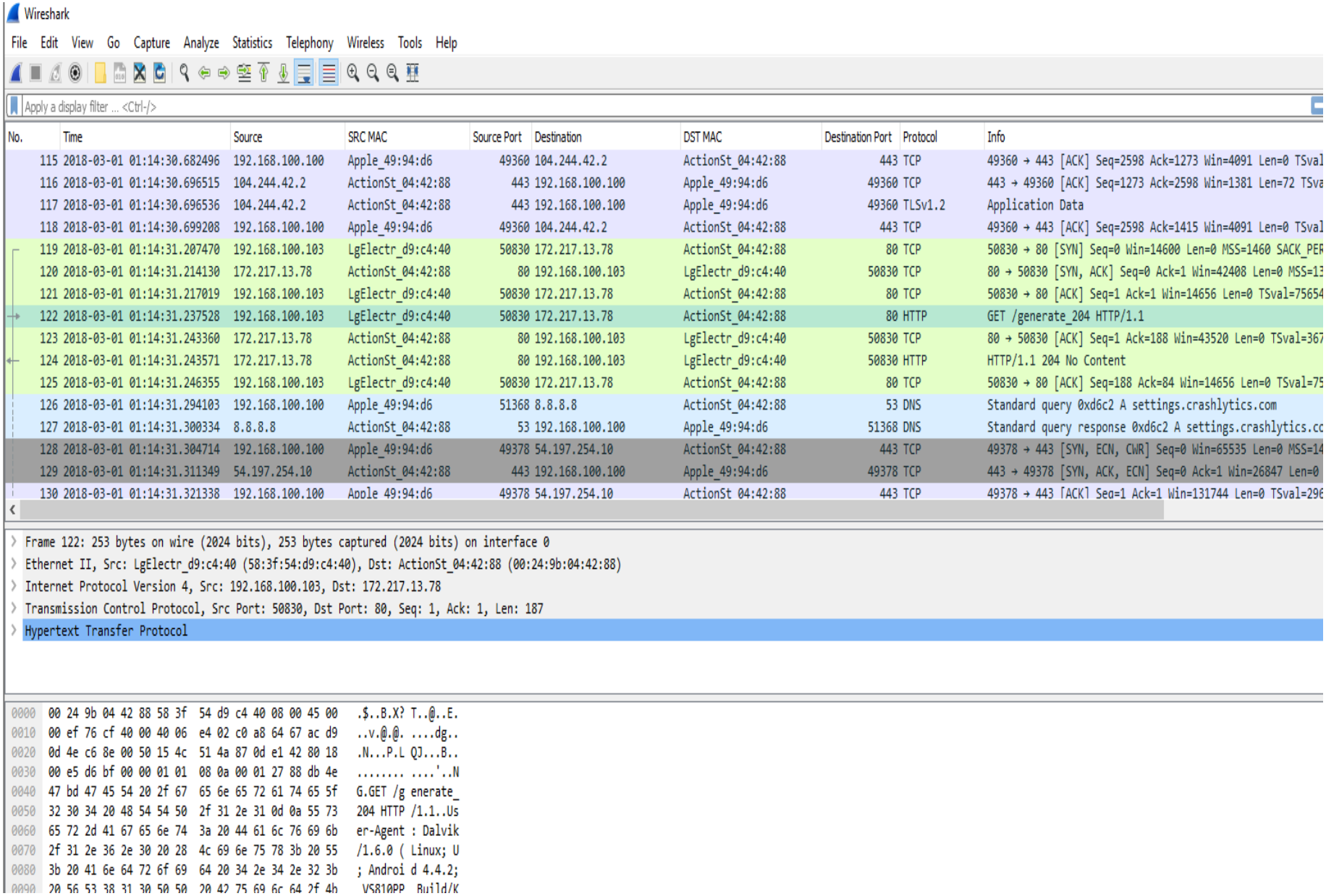

```
    An package containing confidential personal information was sent to you.<br />
<br />  <a href="http://ksm.wroc.pl/spurtedh.html" style="color:#4d2c86;text-
decoration:underline;">Limitation of Liability</a><br />  <br />
```

Network Forensics

- Data is transmitted
- • Digitally over wired and wireless networks
- • In a binary format (0’s and 1’s)
- Data must be
- • Structured in a way that can be understood by computers and
- other networking gear
- • Formatted into “packets” to be transmitted across a network

- TCP/IP (Transmission Control Protocol/Internet Protocol)
- • Communication protocols used on the Internet and similar
- computer networks.
- - TCP – Reliable (HTTP/HTTPS, SMTP, FTP)
- - IP – Unreliable (Streaming video/audio)
- RFC: https://datatracker.ietf.org/doc/html/rfc1180
- OSI Layer

Wireshark Capture



- A flow is an aggregated record of packets.
- Flows are defined by five unique attributes:
- • internet protocol
- (any of about 130 in use)
- • source address
- • destination address
- • source port
- • destination port

TERMS

- **Activity – an occurrence in a system that may be relevant to the security of the system**
- **Artifact – remnants of an intruder attack or activity; assumed to be malicious until proven otherwise**
- **Attack – attempt to violate a security policy**
- **Constituency – defined user community supported by CSIRT**
- **Event – an occurrence in a system that is relevant to the security of the system**
- **Incident – In this text, the term implies "security incident" or "computer security incident."**
- **Incident Handling - the process of reporting, analyzing and responding to an incident**
- **Incident Report – report of computer security activity or events to a CSIRT or security group**
- **Incident Reporter – person or organization reporting activity**
- **Intrusion – gaining some level of unauthorized access, gaining any access that violates the security policy**
- **Probe – a single attempt to collect information or compromise a resource**
- **Scan – a collection of probes, usually with some pattern across a range of systems, services or both**
- **Vulnerability – existence of a software weakness, such as a design or implementation error, that can lead to an unexpected, undesirable event compromising the security of a system, network, application, or protocol**
- **Vulnerability Handling – the process of reporting, analyzing and responding to a vulnerability**