Medsync

Topic 3
Data Acquisition and Duplication III

Learning Outcome

Explain the techniques and technologies in acquisition and duplication of evidence data from various sources, media and devices

Explain the use of write blocker in cyber forensic data acquisition

Apply the techniques and technologies in acquisition and duplication of evidence data from hard disk and network

Explain the techniques and technologies in acquisition and duplication of evidence data from mobile devices and social media

Explain the techniques and technologies in live response and triage

Road Map

Network Data Acquisition

Social Media Data Acquisition

Live Response and Triage

What will be your approach?

It was reported that an employee used online chat at his laptop to disclose the secret recipe of a company product to a person who is working for the competitor.

The employee later set fire on his laptop and data cannot be acquired from the laptop.

You are asked to acquire evidence data related to this case.

Data Acquisition and Duplication

Identify possible sources of data

- Network traffic
- Online chat - social media

Develop a plan to acquire the data

- Likely Value – The network traffic and online chat contains the disclosed secret recipe
- Volatility – Network traffic is volatile but messages in social media is not
- Amount of Effort Required – Physical acquisition of network traffic and logical acquisition of social media data

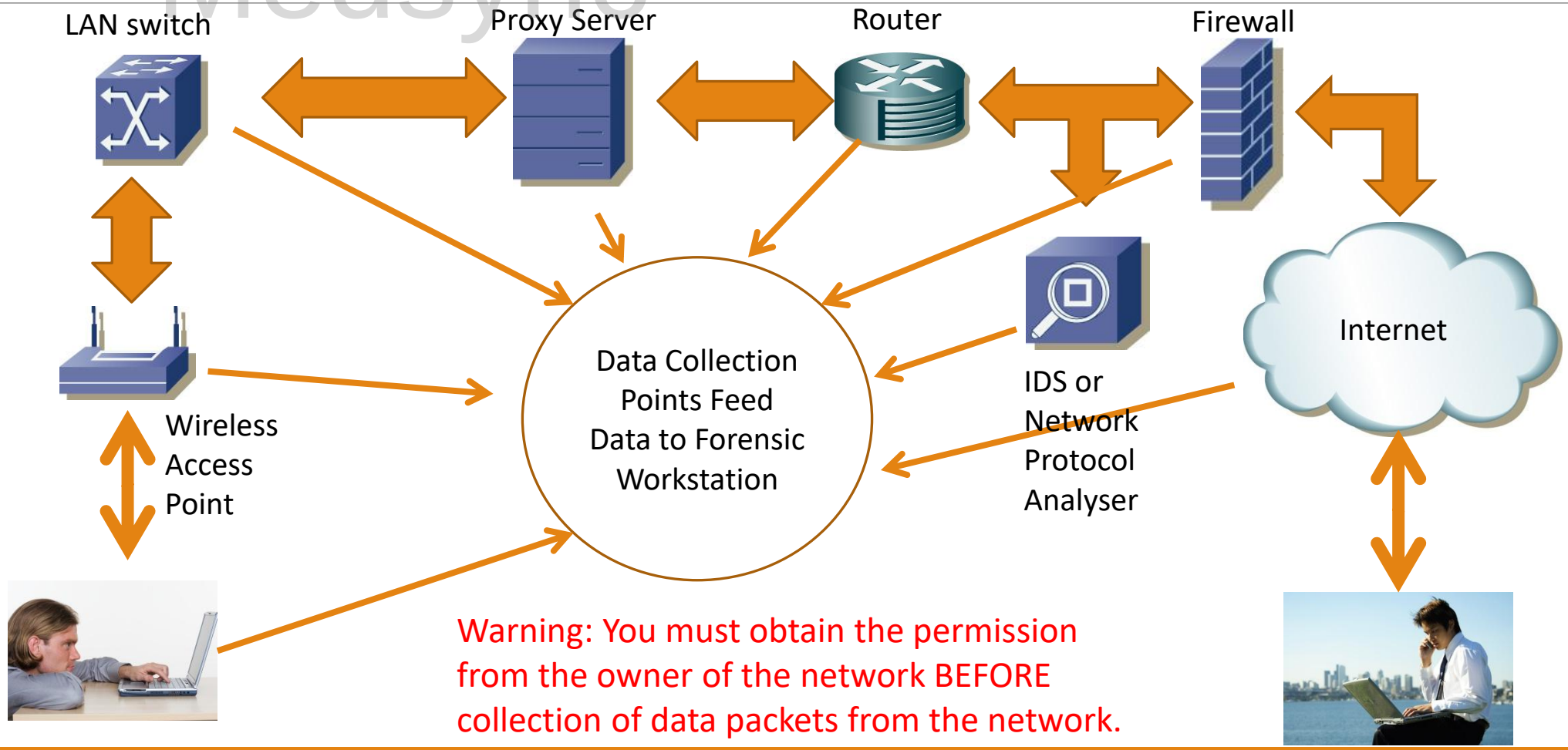
Acquire the data

- How to do it?

Verify the integrity of the data

- Hash values required

Network Data Collection Points



Warning: You must obtain the permission from the owner of the network BEFORE collection of data packets from the network.

What Kind of Network Traffic Data?

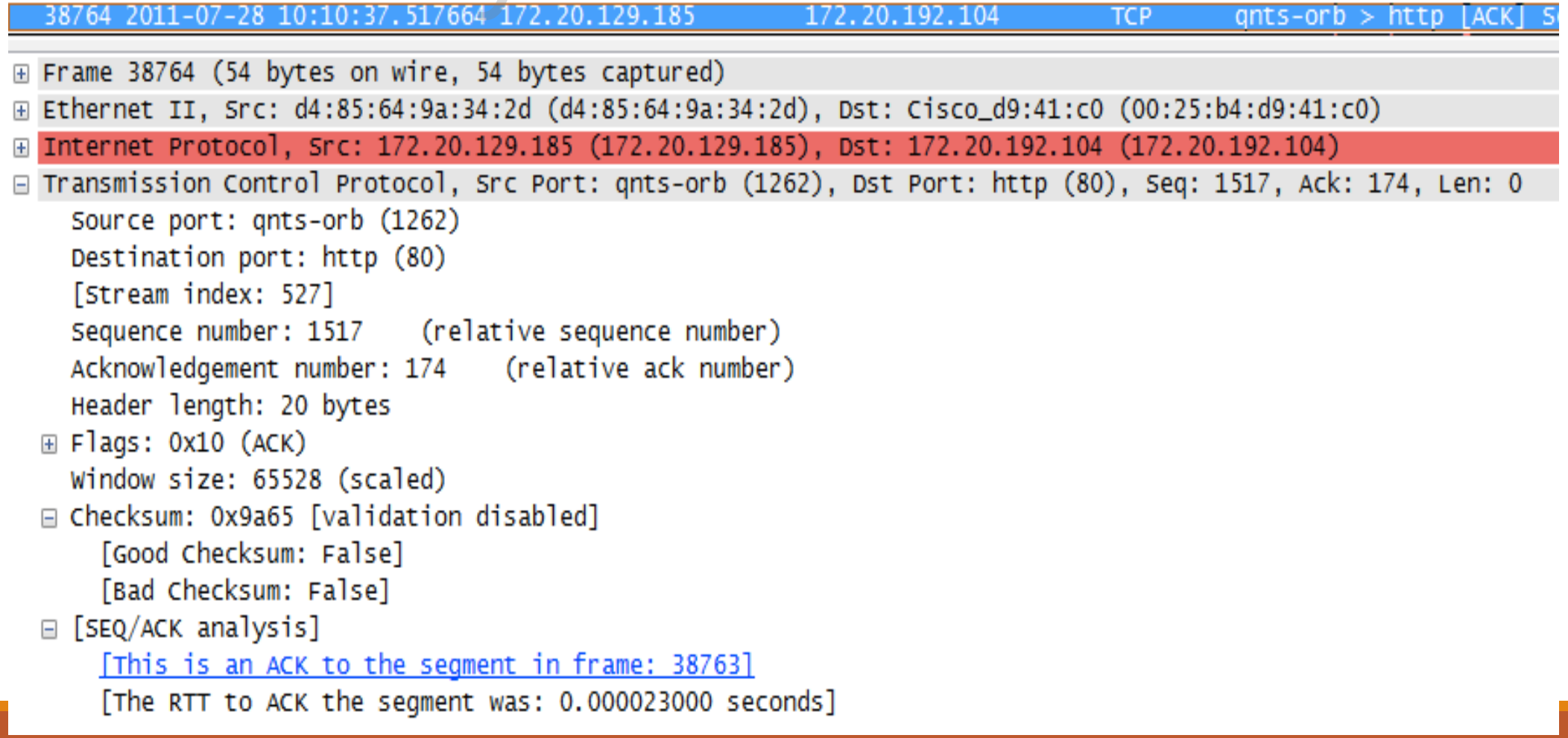
Full-Packet Capture

- Run a network monitoring or a network protocol analyser tool such as wireshark, tcpdump, tshark
  - e.g. tshark –w fullcapture.pcap
- Suitable for small amount of data only

Where to run it?

- At the end point, a network server such as proxy server to collect
  - Broadcast traffic, such as ARP and BROWSER, and
  - Unicast traffic sent and received at the end point
- At a forensic PC connected to the mirror port of a Internet Router, to collect
  - Unicast traffic between computers in the untrusted Internet and the computers in the trusted intranet

HTTP Protocol - Unicast Traffic



Network Evidence in Different Layers

Application

- This layer sends and receives data for particular applications, such as Domain Name System (DNS), Hypertext Transfer Protocol (HTTP), and Simple Mail Transfer Protocol (SMTP).

Transport

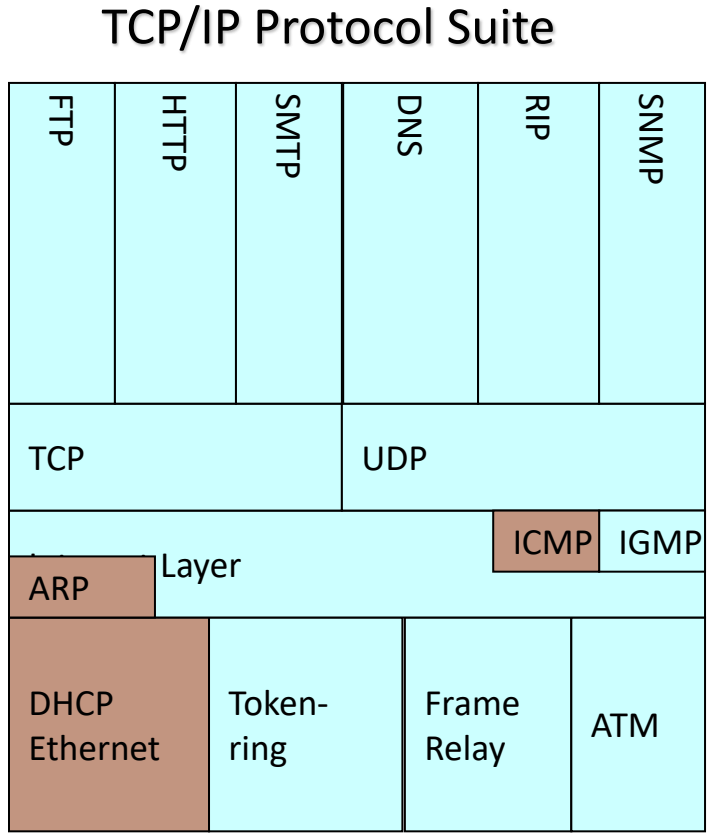
- This layer provides connection-oriented or connectionless services for transporting application layer services between networks. The transport layer can optionally ensure the reliability of communications. Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are commonly used transport layer protocols.

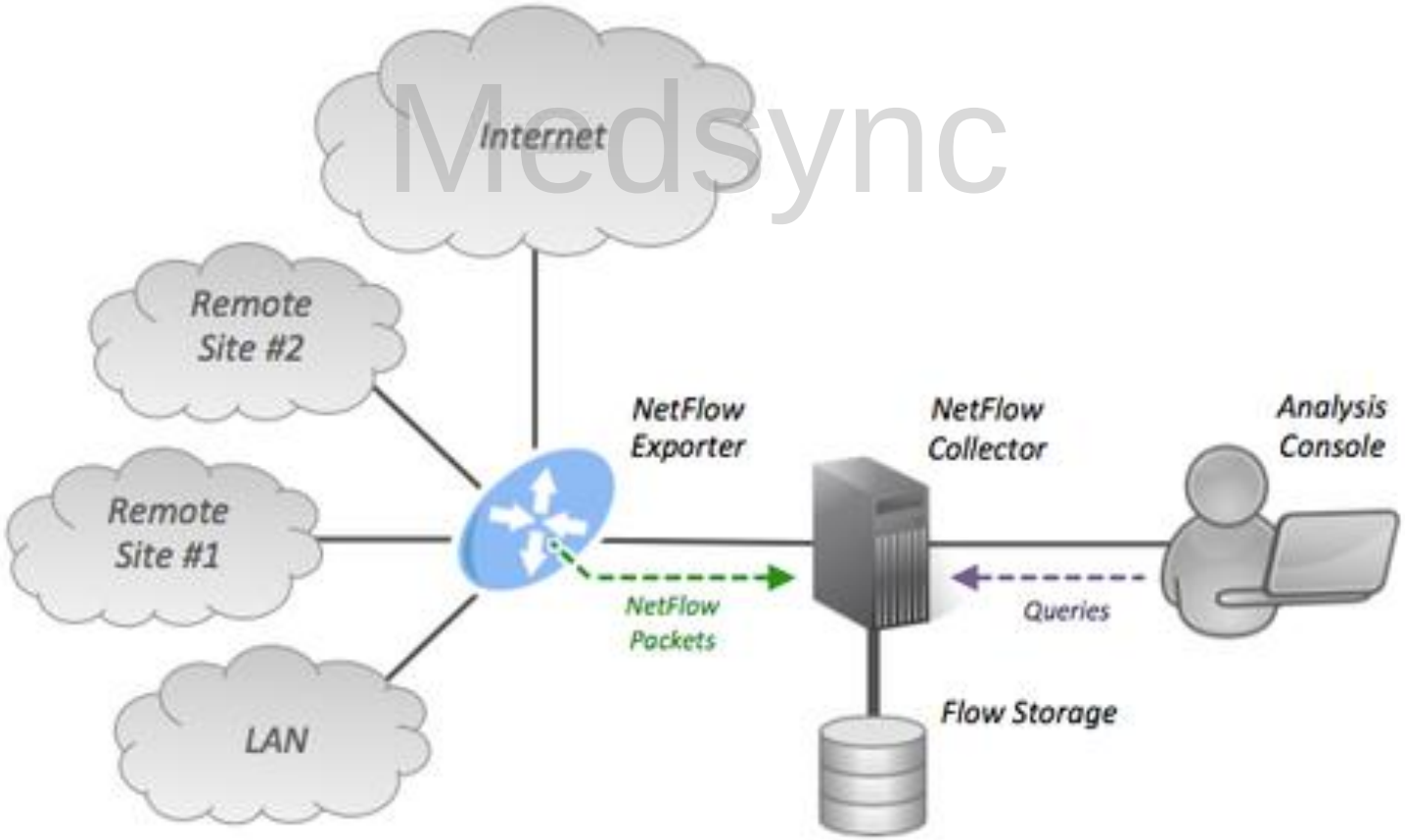
Network

- This layer routes packets across networks. IP is the fundamental network layer protocol for TCP/IP. Other commonly used protocols at the network layer are Internet Control Message Protocol (ICMP) and Internet Group Management Protocol (IGMP).

Data Link

- This layer handles communications on the physical network components. The best known data link layer protocol is Ethernet.

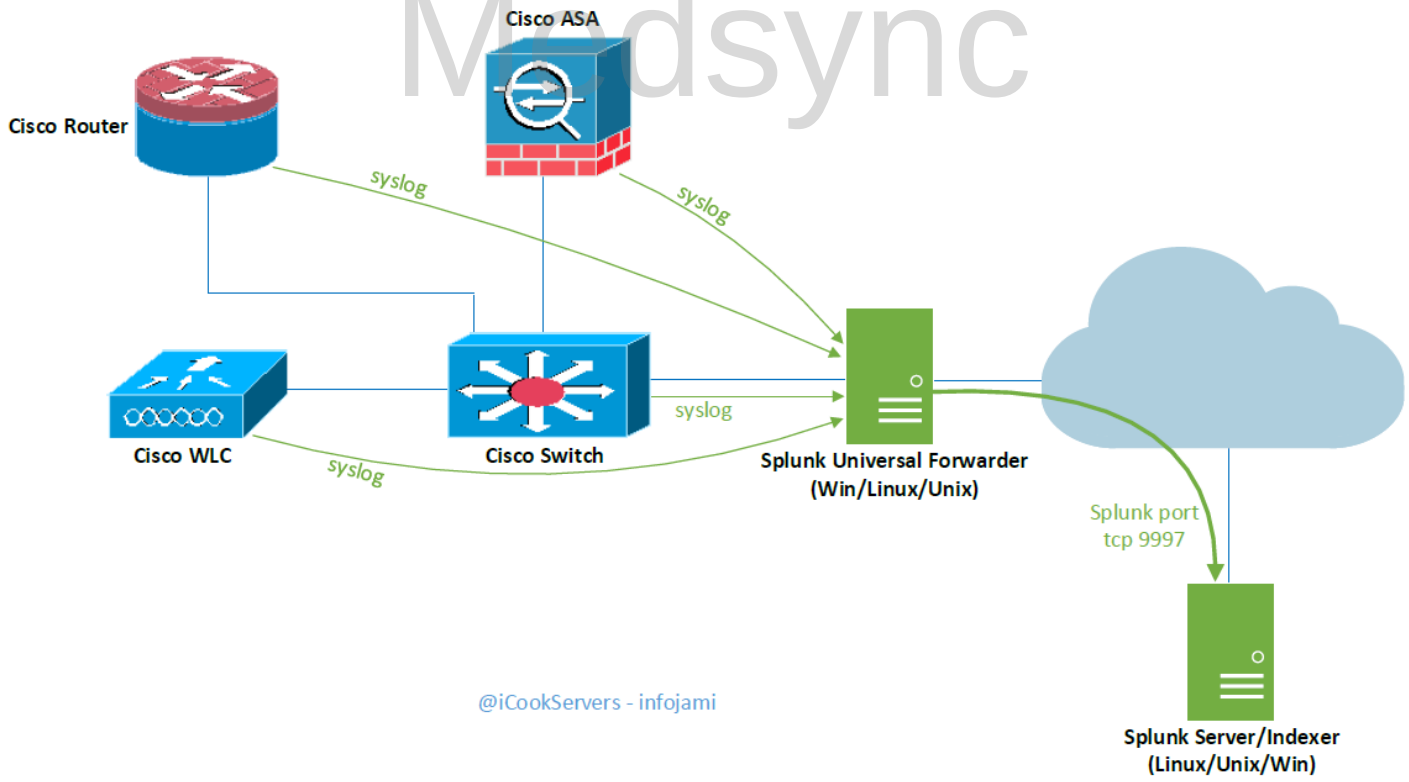




What Kind of Network Traffic Data?

Protocol Header Capture

- Use NetFlow to capture only the content of the protocol headers but not the protocol data
  - NetFlow is a feature that was introduced on Cisco routers around 1996 that provides the ability to collect IP network traffic as it enters or exits an interface.
- Supports advanced data analytics



What Kind of Network Traffic Data?

Network Events

- Run a security information and event management (SIEM) servers, such as Splunk, to collect, examine and analysis network events (evidence)
- Syslog from various network devices, e.g. routers, firewalls, IDS, proxy servers, LAN switches and WiFi Access Points

Network Traffic Forensics

Network forensic analysis relies on all of the layers.

1. When analysts begin to examine data, they typically have limited information most likely an IP address of interest and perhaps protocol and port information. This is enough information to support searching common data sources for more information.
2. In most cases, the application layer contains the actual activity of interest. Most attacks are against vulnerabilities in applications, and nearly all misuse involves misuse of applications.
3. Analysts need IP addresses so that they can identify the hosts that may have been involved in the activity. The hosts may also contain additional data that would be of use in analyzing the activity.
4. Some events of interest may not have relevant application-level data (e.g., a distributed denial of service attack designed to consume all network bandwidth), most do; network forensics provides important support to the analysis of application-layer activities.

Network Traffic Forensics

Evidence in Network Routers

- Routing table
- Access Control List (ACL)
- Blocked incoming/outgoing packets (not meeting ACL rules)
- Error logs
- Optional information
  - Packets forwarded
  - Routing information shared with other routers

Evidence in Network Switches

- MAC addresses of computers connected at each switch port
- Date and time each MAC address was last detected at a particular port
- IP addresses of computers connected at each port
- Hostnames of computers connected at each port
- History logs on blocked broadcast traffic
- Error logs

Network Traffic Forensics

Evidence in Firewalls

- Firewalls Rules
  - TCP/IP filtering rules
  - Users, application restriction rules
  - User groups and their security policies
- Blocked incoming and outgoing network traffic
  - Most firewalls send event logs to a network log server for archive purpose.

Evidence in Proxy Servers

- Internet browsing history of each user and computer in the company intranet
- Black-listed websites
- Decrypted SSL connection application data between the attackers' computers in Internet and the victim computers in the company Intranet.

Social Media Forensics

Social Media

- Facebook
- Twitter
- Instagram
- LinkedIn
- Gmail
- YouTube

Credit: https://www.wordstream.com/social-media-marketing

Data Acquisition and Duplication

Evidence can be collected from information that is available in public

- Unethical to create a fake account for the purpose of accessing someone's information

Information can be commonly found during the process of a computer or cell phone examination

- In Internet history and unallocated space
- Username or an email address can be used to find information about a person online

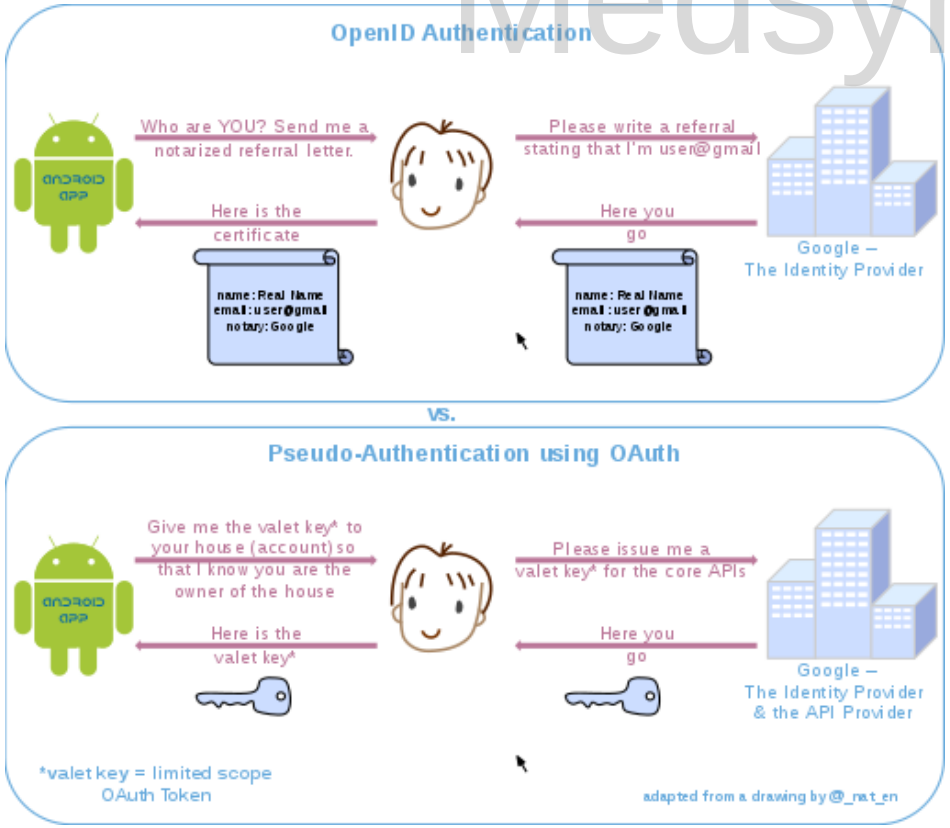
Getting information from the service provider

- Requires a criminal subpoena
- Foreign Intelligence Surveillance Act, US
  - Google, Microsoft, Facebook, Twitter and Apple revealed US surveillance requests
- Facebook Global Government Request Report

Acquisition Challenges

- Most artifacts are stored in websites
- Require forensic examiners to develop applications to capture
- Websites provide limited logical acquisition via Application Programme Interface (API)

OAuth 2.0 Protocol



OAuth2.0 (RFC6749) allows users to share their private resources such as contact lists and photos stored on one site, say flickr, with another site, say Facebook, without having to handout their credentials.

Examiners use it to get their data acquisition applications authenticated to social media websites and get authorization on acquiring users' data

What will be your approach?

It was reported hacker got into one of the 10 Internet facing web servers. Some web contents had been deleted and modified. You are asked to acquire evidence data related to this case.

Question: Do you have a few hours to plan for a comprehensive data acquisition?

Live Response

When a computer is involved in an incident, the administrator may not be able to remove the system from the network because a proper backup server cannot be swapped its place.

The traditional forensic duplication cannot be executed.

The time allowed to acquire data is from 5 to 30 minutes

There is a need to collect volatile and non-volatile data during a live response

The live response data is collected by running a series of commands

Data Acquisition and Duplication in Live Response

Identify possible sources of data
- Network connections
- Current processes
- Current opened files
- Current memory contents

Develop a plan to acquire the data
- Likely Value – Network connections, current processes and open files are high value evidence
- Volatility – All these data could be vanished in minutes
- Amount of Effort Required – A quick logical acquisition of live system data required tested user-defined scripts and reliable software tools

Acquire the data
- How to do it?

Verify the integrity of the data
- Hash values are to be computed during the acquisition and verified after the acquisition

Live Response Script

Sample Windows Live Response commands in an VB script

- date /T| nc -w 2 %1% 2222
- time /T| nc -w 2 %1% 2222
- netstat -abno | nc -w 5 %1% 2222
- fport.exe | nc -w 5 %1% 2222
- psloggedon.exe | nc -w 2 %1% 2222
- psfile.exe | nc -w 5 %1% 2222
- nbtstat -c | nc -w 5 %1% 2222
- netstat -rn | nc -w 5 %1% 2222
- pslist.exe | nc -w 5 %1% 2222
- psservice.exe | nc -w 20 %1% 2222
- at | nc -w 2 %1% 2222
- psinfo -h -s -d | nc -w 5 %1% 2222
- NTLast | nc -w 5 %1% 2222
- date /T| nc -w 2 %1% 2222
- time /T| nc -w 2 %1% 2222

What does it do?

The script sends volatile data from the computer under attack to a forensic computer at port 2222 with IP stated in %1% (note: nc is netcat.exe)

- date/time - Start date/time of the acquisition
- netstat and fport - current TCP/UDP network connections
- psloggedon – who logged on currently
- psfile – shows files opened remotely
- pslist – running processes information
- psservice – active services status and dependencies
- at – show scheduled tasks
- psinfo - kernel build, registered organization and owner, number of processors
- NTLast – shows security events log
- date/time – End date/time of the acquisition

Triage

Triage originated in World War I by French doctors treating the battlefield wounded at the aid stations behind the front.

At its most primitive, those responsible for the removal of the wounded from a battlefield or their care afterwards have divided victims into three categories

- Those who are likely to live, regardless of what care they receive;
- Those who are likely to die, regardless of what care they receive;
- Those for whom immediate care might make a positive difference in outcome.

Triage in Cyber Forensics

A process in which things are ranked in terms of importance or priority.

Essentially, those items, pieces of evidence or potential containers of evidence that are the most important or the most volatile need to be dealt with first.

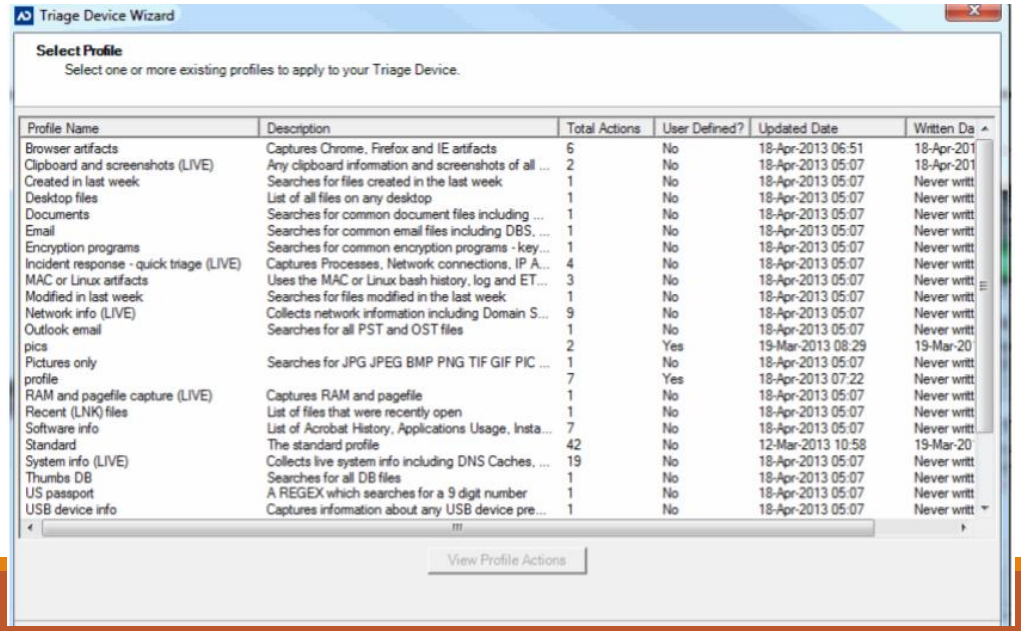
Challenges

- Short planning and execution time
- Require users to conduct data acquisition

Solutions

- Well-tested and prepared forensic tools and scripts
- Easy-to-use forensic tools (hardware and software) for inexperienced users

Source: Computer Forensics Field Triage Process Model, Conference on Digital Forensics, Security and Law, 2006



Triage Forensic Capabilities

Specially designed and tested for targeted systems

Ease of use

Portable (CD, DVD, USB Flash)

Cater for computers in

- power-on (live mode) or
- power-off (boot mode)

Summary

Network Data Acquisition

- Where and what
- Evidence at various network devices

Social Media Data Acquisition

- Limited Logical Acquisition
- Oauth Protocol

Live response

- Short planning time
- Well-prepared portable tools

Triage

- Easy-to-use forensic tools for operators
- Identify significant computers from a number of suspected computers

References

1. Guide to Integrating Forensic Techniques into Incident Response SP800-86 NIST, csrc.nist.org
2. Hacking Exposed Computer Forensics Second Edition, Aaron Philipp, 2010, McGraw-Hill
3. Digital Forensics for Legal Professionals, Larry E. Daniel, Lars E. Daniel, 2012, Syngress
4. https://accessdata.com/products-services/ad-triage
5. Guide to Integrating Forensic Techniques into Incident Response SP800-86 NIST, csrc.nist.org