ENGENSEC
Educating the Next generation experts in Cyber Security

Tempus

The project has been funded by the European Commission. The Education, Audiovisual and Culture Executive program (EACEA), TEMPUS IV. The content of this presentation reflects the opinion of the author.

Bundes-
kriminalamt

Сетевая безопасность

Андрей Чечулин
к.т.н., ведущий научный сотрудник
СПИИРАН

Что такое криминалистика?

Юристы: местные и международные законы

Специалисты по безопасности: методы сбора и анализа следов

Технические специалисты: аппаратные и программные средства

Что такое криминалистика?

Разработчики: SIEM, хранилища и т.д.

Ученые: Модели и методы

Нарушители: Как скрыть следы?

Что такое криминалистика?

Область использования

- Армия
- Полиция
- Частный сектор
- Наука

Источники данных

- Компьютеры (hard drives, memory, etc)
- Хранилища данных (USB, DVD, SD, etc)
- Мобильные устройства (smart phones, cameras, etc)
- Сеть (mail, file, access control, etc servers)

Что такое доказательство?

Доказательство – основной элемент криминалистики

Цифровое доказательство – обобщенный термин для описания информации или материалов, хранимых или передаваемых в цифровом виде для представления в суде

Свойства цифровых доказательств

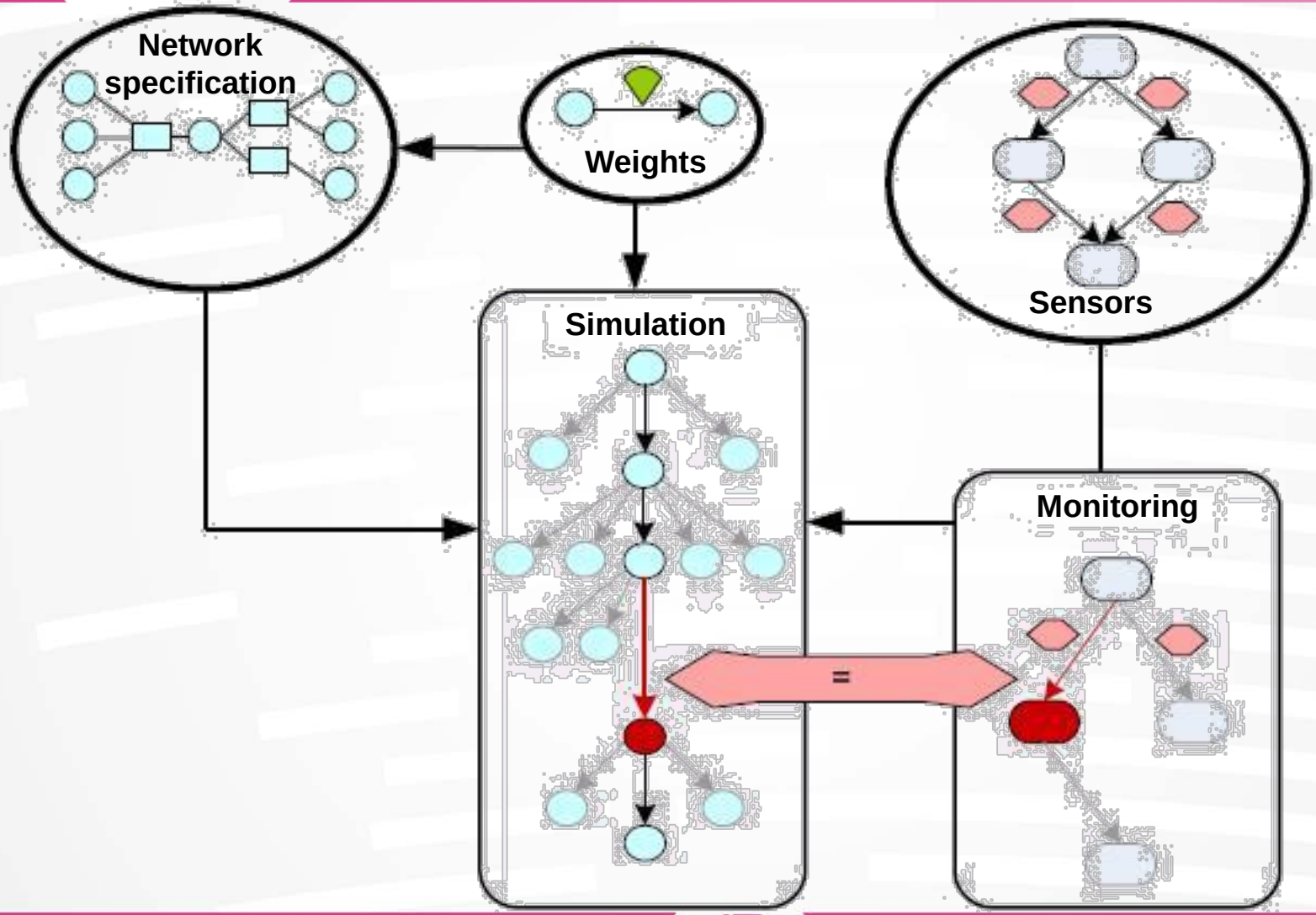
- Они должны быть связаны с действиями людей
- Они должны легко восприниматься в участниками судебного процесса напрямую или через специалистов
- Сбор и хранение должны соответствовать законам

Организации и разработчики

Figure 1. Magic Quadrant for Security Information and Event Management

Source: Gartner (July 2015)

Исследователи



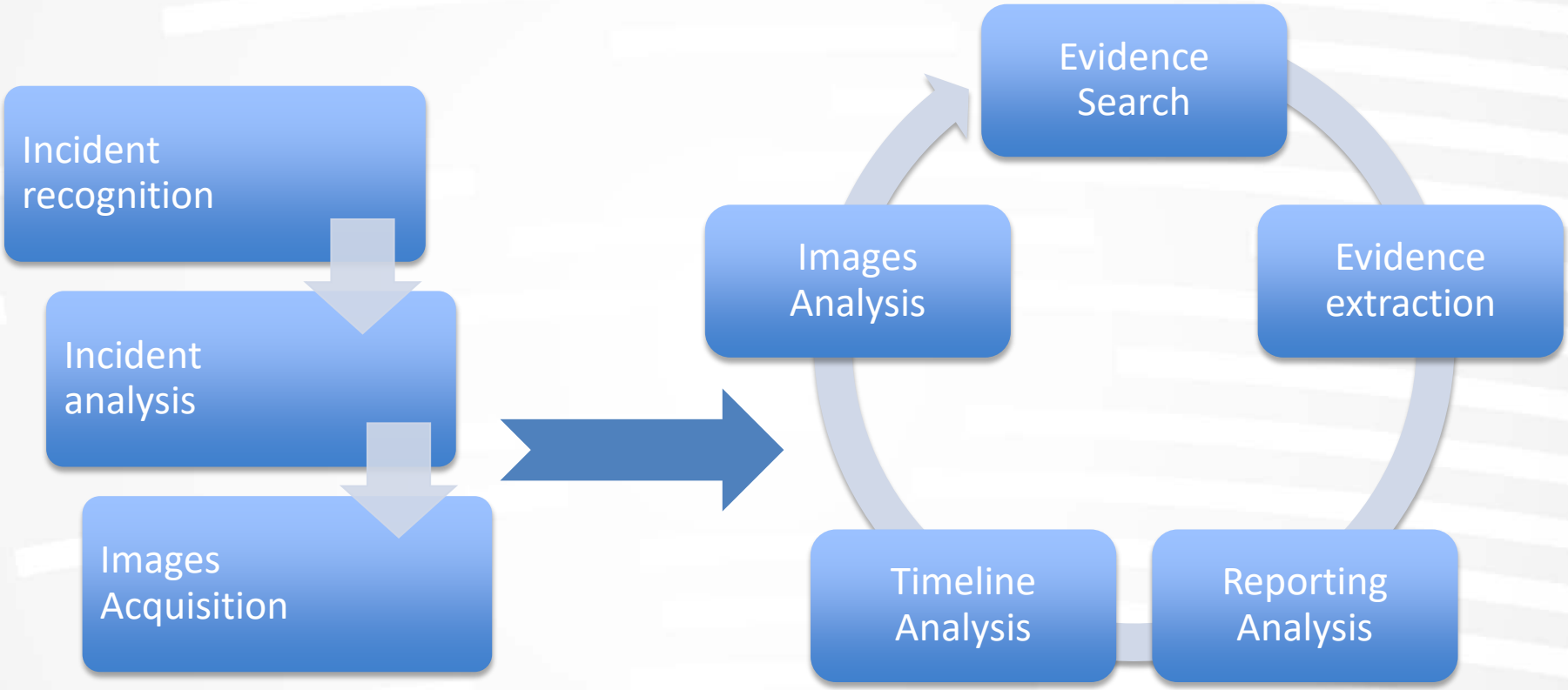
Вопросы

- Когда атака была обнаружена?
- Как атака была обнаружена?
  - Средствами ИБ?
  - Была ли она задокументирована?
  - От пользователей?
- Сервер или рабочая станция?
  - Если сервер, то есть ли зависимости сервисов?
  - Может ли атакованная машина быть отключена?
- Атака еще продолжается?
  - А нужно, чтобы она продолжалась?
- С кем мы должны говорить?
- О чем мы должны говорить?

Расследование

- Сбор данных (imaging, live forensic, logs gathering, etc)
- Извлечение доказательств (recovering files, searching for hidden traces, extracting logs, decrypt data, etc)
- Анализ доказательств (reconstructing of events, step by step analysis of the chain, creating time line, etc)
- Представление доказательств (report writing, presentation of the results for the curt)

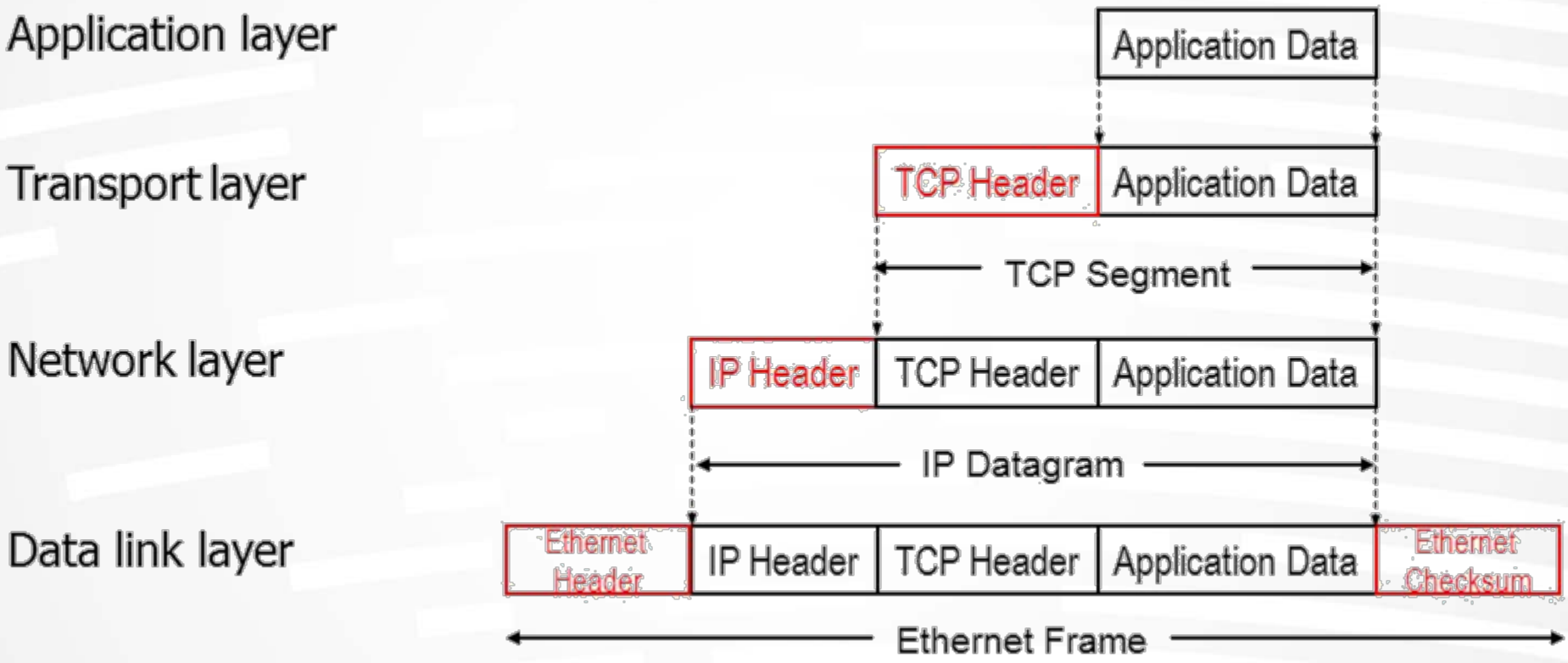
Цикл расследования



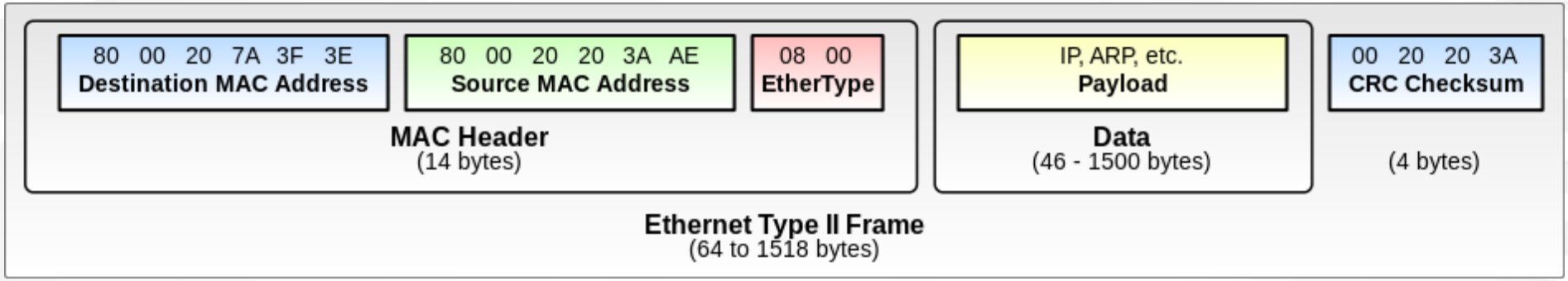
Протоколы

OSI Model				
	Data Unit	**Layer**		**Function**
Host Layers	Data	**7**	Application	Network process to application
		6	Presentation	Data representation, encryption and decryption
		5	Session	Interhost communication
	Segments	**4**	Transport	End-to-end connections and reliability, flow control
Network Layers	Packet	**3**	Network	Path determination and logical addressing
	Frame	**2**	Data Link	Physical addressing
	Bit	**1**	Physical	Media, signal and binary transmission

Протоколы


Application layer
Transport layer
Network layer
Data link layer
Application Data
TCP Header
Application Data
TCP Segment
IP Header
TCP Header
Application Data
IP Datagram
Ethernet Header
IP Header
TCP Header
Application Data
Ethernet Checksum
Ethernet Frame

Ethernet


80 00 20 7A 3F 3E
Destination MAC Address
80 00 20 20 3A AE
Source MAC Address
08 00
EtherType
MAC Header
(14 bytes)
IP, ARP, etc.
Payload
Data
(46 - 1500 bytes)
00 20 20 3A
CRC Checksum
(4 bytes)
Ethernet Type II Frame
(64 to 1518 bytes)

Internet protocol

Bit	+0..7		+8..15		+16..23	+24..31
0	Version	Header Length	DSCP	ECN	Total Length	
32	Identification				Flags	Fragment Offset
64	Time To Live		Protocol		Header Checksum	
96	Source IP Address					
128	Destination IP Address					
160	Options (if present)					
...	*Payload*					

Transmission Control Protocol

TCP Header

Offsets Octet		0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source port																Destination port															
4	32	Sequence number																															
8	64	Acknowledgment number (if ACK set)																															
12	96	Data offset				Reserved 0 0 0				NS	CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Window Size														
16	128	Checksum																								Urgent pointer (if URG set)							
20 ...	160 ...	Options (if *data offset* > 5. Padded at the end with "0" bytes if necessary.) ...																															

HTTP header

Request

GET / HTTP/1.1
Host: engensec.eu
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:47.0) Gecko/20100101 Firefox/47.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
X-Compress: 1
Proxy-Authorization: 9bf685378c35f7b9a320da2a9dcddd9ffbe670c4ccc0584c0ae897ebfbb9387b
DNT: 1
Connection: keep-alive

Answer

HTTP/1.1 200 OK
Server: Apache
X-Powered-By: PHP/5.6.23
X-Pingback: http://engensec.eu/xmlrpc.php
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8
Content-Length: 10725
Accept-Ranges: bytes
Date: Wed, 20 Jul 2016 23:05:34 GMT
X-Varnish: 1112361889
Age: 0
Via: 1.1 varnish
Connection: keep-alive

Пример. Фишинг

Исходные данные

Деньги жертвы были украдены через фишинговый веб-сайт

Пример. Фишинг

Исходные данные

Деньги жертвы были украдены через фишинговый веб-сайт

Следы

Domain registration info
Hosting info
Advertisements, spam messages, etc
Transaction information
Interaction with a victim (web-forms, email messages, etc)

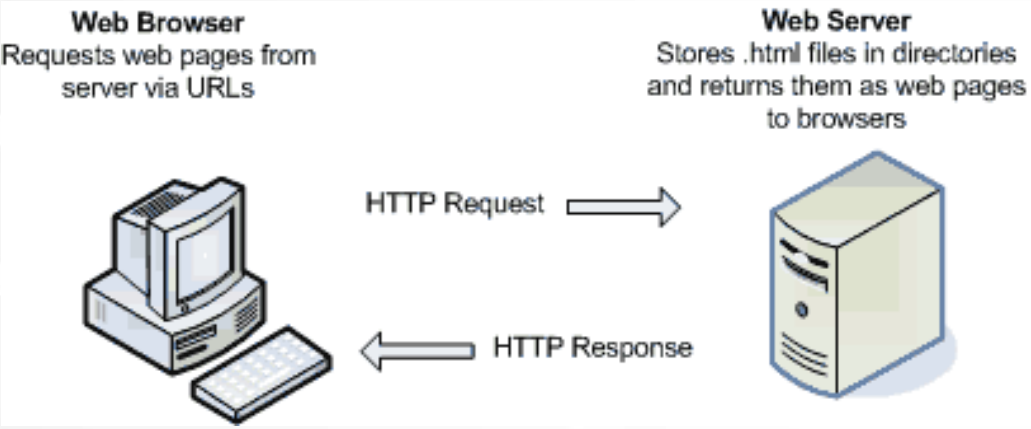
Пример ответа whois сервера:

From WHOIS.NIC.RU:
domain: COMSEC.SPB.RU
nserver: dns1.yandex.net.
nserver: dns2.yandex.net.
state: REGISTERED, DELEGATED
person: Private person
e-mail: ****@comsec.spb.ru
descr: Laboratory of Computer Security Problems of the St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science (SPIIRAS)
descr: 14 line, Vasil'evskiy island.
descr: Saint-Petersburg
descr: Russia
registrar: RU-CENTER
created: 2010.04.24
paid-till: 2017.07.02
source: RU-CENTER

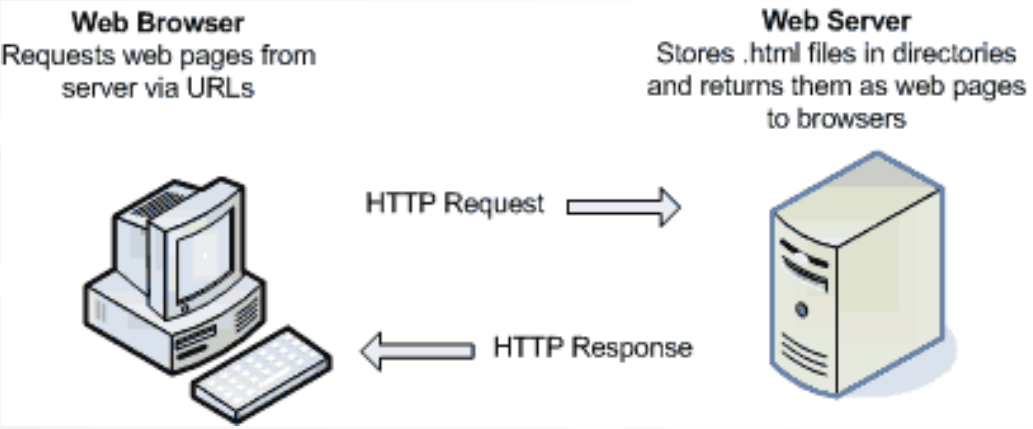
Перехват трафика

OSI Model				
	Data Unit	**Layer**		**Function**
Host Layers	Data	**7**	Application	Network process to application
		6	Presentation	Data representation, encryption and decryption
		5	Session	Interhost communication
	Segments	**4**	Transport	End-to-end connections and reliability, flow control
Network Layers	Packet	**3**	Network	Path determination and logical addressing
	Frame	**2**	Data Link	Physical addressing
	Bit	**1**	Physical	Media, signal and binary transmission

Где могут быть логи?



Где могут быть логи?



- Браузер
- Средства сетевой безопасности
- Антивирус
- Операционная система
- DNS сервера
- Сетевая безопасность
- Веб-сервер
- Приложения веб-сервера
- Баннеры и пр. реклама
- Следующий веб-сервер
- Прокси сервер
- СОРМ
- и т.д.

Софт для расследования

Этап сбора данных

•tcpdump, etc

Этап извлечения данных

•Wireshark, etc

Этап анализа данных

•Network Miner, etc

Этап представления данных

•Microsoft Power Point, Word, Open Office, etc

Контакты

Лаборатория проблем компьютерной безопасности
ФГБУН СПИИРАН:

- Почтовый адрес: 199178, Санкт-Петербург, 14-я линия В.О., д.39
- Телефон: +7(812)328-26-42
- Факс: +7(812)328-44-50
- URL: http://comsec.spb.ru

Международная лаборатория информационной безопасности киберфизических систем Университета ИТМО:

- Почтовый адрес : 191002 , Санкт-Петербург, Ломоносова д. 9

Автор:

- Чечулин Андрей, chechulin@comsec.spb.ru, http://comsec.spb.ru/chechulin