



**COLEGIO DE
INGENIEROS
DEL PERU**

PERICIAS INFORMÁTICAS Y LOS ATAQUES CIBERNÉTICOS

**Ing. CIP Víctor Barrientos Rodríguez
CIP 060996**



**COLEGIO DE
INGENIEROS
DEL PERU**



CV

1. Ingeniero de Sistemas de la UNI egreso 1995 y titulo 1999.
2. Maestro de Ingeniería de Sistemas.
3. **Curso de Hacker U.telaviv Israel.**
4. Curso de Peritos en el Centro de Peritajes del Colegio de Ingenieros (2018)
5. **Perteneiente al Centro del Peritajes del colegio de Ingenieros de Perú.**
6. **Perito de Perteneiente al Poder Judicial Lima Sur y Lima Este**
7. 25 Años de experiencia en desarrollo de software o sistemas de Información.
8. Curso ETH-ECCOUNCIL Docente Informático en Web, Java, Python y C.
9. Trabajo haciendo software en Java Web - PHP - .Net



Objetivos Webinar

- 1. Introducción de los Ciberataques**
- 2. Tipos de Ataques Cibernéticos**
- 3. Ley de Delitos Informáticos**
- 4. Conceptos de Pericias Informáticas**
- 5. Las Herramientas que utiliza el perito.**
- 6. Denuncias.**
- 7. Recomendaciones**



Introducción

- Nuestra vida diaria gira alrededor de actividades cada vez más digitalizadas
- Las áreas se encuentran informatizadas: desde Cadenas de suministro, distribución, transporte, transacciones financieras, actividades educativas, trámites gubernamentales, servicios de médicos, el suministro de agua y energía, entre un sin número de actividades, operan en la actualidad a través de tecnologías digitales.



Introducción

- La creciente ataques informáticos generando daños económicos.
- Las políticas de ciberseguridad son fundamentales para salvaguardar los derechos de los ciudadanos en el ámbito digital, tales como la **privacidad**, la **propiedad**, así como para **aumentar la confianza** de los ciudadanos en las tecnologías digitales.
- Según BID, los crímenes pueden pasar el 1% del producto interno bruto (PIB) en algunos países.
- En el caso de los ataques a la infraestructura crítica, esta cifra podría alcanzar hasta el 6% del PIB.



Que es la Ciberdelincuencia

Es una Palabra que no esta definido en la RAE.

En el X Congreso de Naciones Unidas sobre Prevención del delito y Tratamiento del Delincuente, celebrado en Viena, abril del 2000, se realizó una importante distinción que contribuye a una mejor precisión del concepto.

- La Ciberdelincuencia **comportamiento ilícito** realizado mediante operaciones electrónicas **que atentan contra la seguridad de sistemas informáticos y datos** que se procesan.
- La Ciberdelincuencia comportamiento **ilícito cometido por medio de un sistema informático** o una red de computadores.



La Economía Subterránea

En los últimos años, los ataques se han vuelto no solo más complejos, sino también más fáciles de realizar, debido a la comercialización de componentes y servicios de ataque.

1. Mercados abiertamente accesible para todos (La Dark Web) destaca por el uso del anonimato y la venta del mercado de productos ilícitos.
2. Comprar 1000 hosts comprometidos por \$200.
3. Servidores proxy: 150 por \$25 /mes.
4. Si buscas cuentas (Twitter, Facebook, Google):
1000 cuentas por menos de \$30.
4. Seguidores en Twitter:
\$23 / 1000 Seguidores



La Economía Subterránea

Pueden comprar servicios:

1. Ataque DDoS contra una víctima en particular,
2. Solucionadores de captcha,
3. SIM para teléfonos móviles,
4. Malware personalizado y payload para ciberAtaques y
5. También credenciales pertenecientes a usuarios reales.

Delitos Informáticos Perú

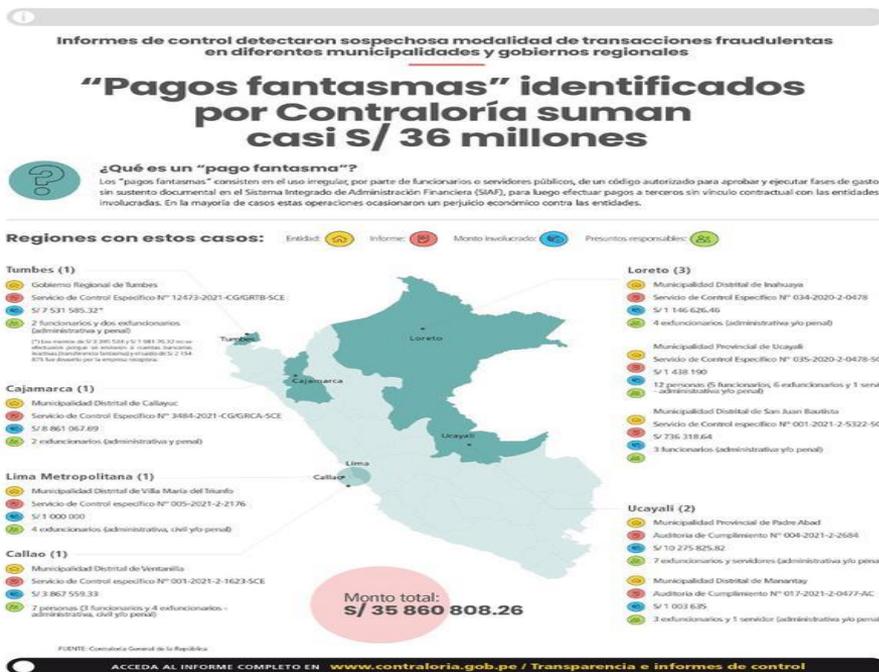
1. Robos cibernéticos de más de 36 millones de soles haciendo uso del SIAF

elcomercio.pe/videos/pais/detienen-a-delincuentes-ciberneticos-que-pretendian-robar-5-millones-de-la-municipalidad-

País | Informativo

Detienen a delincuentes cibernéticos que pretendían robar 5 millones de la Municipalidad de San Borja

Un grupo de delincuentes cibernéticos fue detenido por la Policía Nacional tras intentar robar 5 millones de soles a la Municipalidad de San Borja. Los sujetos realizaron 24 transferencias bancarias a la cuenta de una empresa constructora. Fuente: [América TV]



2. Robos cibernéticos sobre el bono universal, Yanapay entre otros:

elbocon.pe/trends/segundo-bono-familiar-universal-delincuentes-emplean-esta-modalidad-para-robar-informacion-de-beneficiarios-bono-bono-universal-bono-de-760-soles-n

Segundo Bono Familiar Universal: delincuentes emplean esta modalidad para robar información de beneficiarios

La Policía Nacional informó que a la fecha 1.200 denuncias fueron por transferencias bancarias fraudulentas. Indicó que delincuentes cibernéticos buscan obtener la información de beneficiarios del Bono Familiar Universal, cuyo segundo pago inicia este sábado 10 de octubre.



Delitos Informáticos Perú

3. Transferencias bancarias entre particulares.

larepublica.pe/sociedad/2021/11/30/robos-ciberneticos-denuncian-retiro-de-cuentas-bancarias-entre-mas-de-13000-y-34000-



SOCIEDAD

30 NOV 2021 | 10:09 h

Robos cibernéticos: denuncian retiro de cuentas bancarias entre más de 13.000 y 34.000 soles

Dos ciudadanos sufrieron el robo de sus ahorros por medio de transferencias en sus cuentas bancarias.

- Resultados Elecciones Regionales 2022, EN VIVO: Quien va ganando en la Segunda Vuelta, según ONPE
- Elecciones regionales EN VIVO | Cuándo se conocerán los resultados y ganadores en Callao, Cusco y regiones



**COLEGIO DE
INGENIEROS
DEL PERU**

Delitos Informáticos Perú

4. Transferencias bancarias:

trome.pe/actualidad/compran-chip-a-nombre-de-joven-y-le-vacian-su-cuenta-con-todos-sus-ahorros-le-robaron-mas-de-s6200-entel-banco-pichincha-ciberdelincuencia

☰ Menú | 🔍

trome

REGÍSTRATE

ACTUALIDAD

Síguenos en Google News



Compran chip a nombre de joven y le vacían su cuenta con todos sus ahorros: Le robaron más de S/6,200

Daysi Cruz se convirtió en una nueva víctima de los ciberdelincuentes, que se hicieron pasar por ella para adquirir un nuevo chip, asociado a su aplicativo bancario, para robarle sus ahorros y dinero de la CTS.



Técnicas de los Hackers – ECH-ECCOUNCIL

06	System Hacking
07	Malware Threats
08	Sniffing
09	Social Engineering
10	Denial-of-Service
11	Session Hijacking
12	Evading IDS, Firewalls, and Honeypots
13	Hacking Web Servers
14	Hacking Web Applications
15	SQL Injection
16	Hacking Wireless Networks
17	Hacking Mobile Platforms
18	IoT and OT Hacking



Técnicas de los Hackers

- ✓ Buffer Overflow –Stack Overflow- Debilidad de los Programas
- ✓ Sniffing
- ✓ Vulnerabilidad de la Red Interna
- ✓ Vulnerabilidad de la web
- ✓ Malware
- ✓ Denial of Service
- ✓ Hijacking
- ✓ Firewall
- ✓ SqlInjeccion.
- ✓ Automatizacion de los Ataques – Metasploit
- ✓ Ataque a servicios IOT

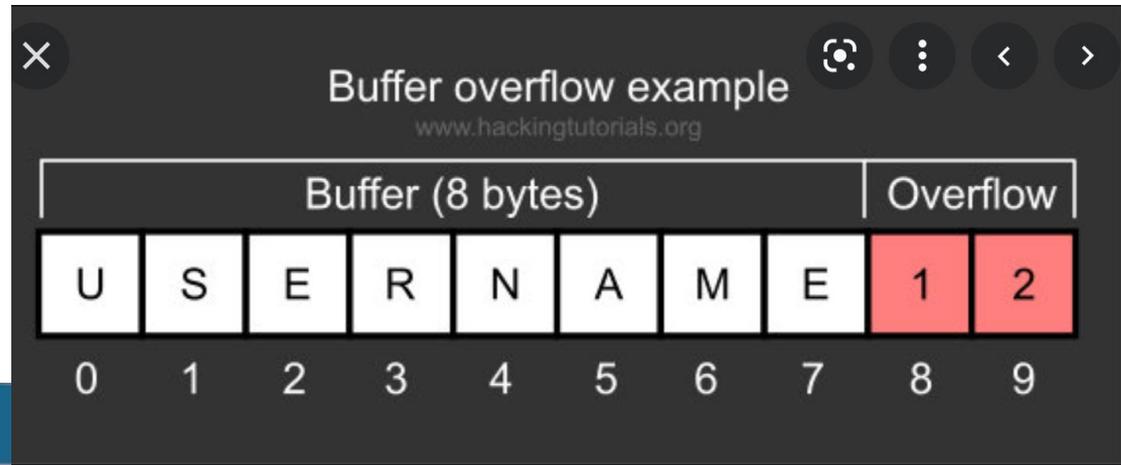


Métodos o técnicas que usan los Hackers

1. Buffer Overflow o stack overflow

Lenguaje C, Software de Programacion Base de los SO, han sido creado con alguna debilidad técnicamente el Buffer Overflow o StackOverflow quiere decir que:

1. Buffer Overflow: accede a la memoria.
2. Stack Overflow: Orden de Ejecución de llamadas de la Pila





Métodos o técnicas que usan los Hackers

Stack Overflow

```
void hello() {  
    char name[8];  
    gets(name);  
    printf("Hello, %s!\n", name);  
}
```

D a a a a a a n 0

RETURN
ADDRESS

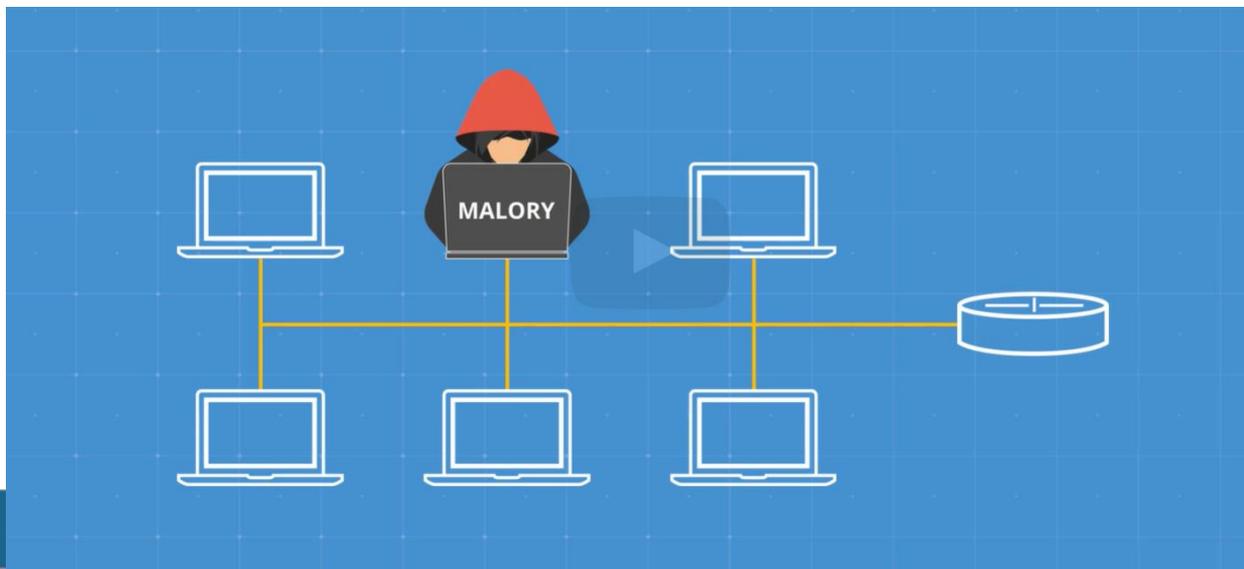
CRASH!



Métodos o técnicas que usan los Hackers

2. Vulnerabilidad Red

- ✓ Técnica de Hombre en el Medio.
- ✓ Envenenamiento de DNS, Envenenamiento de ARP





Métodos o técnicas que usan los Hackers

2. Vulnerabilidad Red

- ✓ Técnica de Hombre en el Medio.
- ✓ Envenamamiento de DNS, envenamamiento de ARP





Métodos o técnicas que usan los Hackers

3. Vulnerabilidad web

a) Cliente Ataca Servidor

1. Sql Injection, instrucciones de base de datos.

b) Servidor Ataca Cliente

1. **Cross-Site Request Forgery.**

c) Cliente Ataca Cliente

1. **Cross-Site Scripting**, or XSS.



Métodos o técnicas que usan los Hackers



CODE INJECTION

User input is embedded into code, that is then executed as-is



LOGIN IF

USERNAME == ' OR 1 == 1 //' AND PASSWORD == '\$PASSWORD'





Métodos o técnicas que usan los Hackers

4. Malware programas maliciosos.

1. **Virus:** Son programas que infectan los archivos de la computadora.
2. **Gusanos:** Programas que se transmiten de una pc a otra.
3. **Ransoware:** programas que encripta los archivos de la computadora para pedir un rescate.
4. **Spyware:** Los spywares son piezas de software maliciosas que intentan robar información personal. Esto no solo es interesante para piratas informáticos malintencionados, sino también para empresas o gobiernos.



Virus de la Historia

- **ILoveYou.** Lanzado en el año 2000, causó pérdidas y daños que en la actualidad ascienden a más de 5.500 millones de dólares. Este virus se enviaba a través de correos electrónicos con el asunto «ILOVEYOU».
- **Mydoom.** Virus informático que afecta a ordenadores con el sistema operativo de Windows. Fue emitido por primera vez en 2004 y se propaga por correo electrónico mediante un archivo adjunto. Según diversas fuentes, todavía está activo, aunque de forma minoritaria.
- **Anna Kournikova.** Emitido por primera vez en 2001 a través del envío por *email* de una supuesta imagen de la tenista que le da nombre. Una vez abierto el archivo, el virus se enviaba a todos los contactos que encontraban en la libreta de direcciones de Outlook.
- **Zeus.** Detectado por primera vez en 2007, iba dirigido a dispositivos con Microsoft Windows. Este virus se hizo famoso por su uso para robar credenciales, contraseñas, datos bancarios e información de carácter sensible.



Gusanos de la Historia

Gusano Morris

Este gusano informático fue lanzado por Robert Morris en 1988. Liberó el código sin saber que estaba plagado de bugs que causarían una variedad de problemas a los anfitriones afectados. El gusano Morris causó pérdidas financieras – que oscilaban entre los 10 y los 100 millones de dólares – en miles de ordenadores sobrecargados que funcionaban con UNIX y gusano d Storm.

El Gusano Storm

Es un gusano de correo electrónico de 2007, y las víctimas recibieron correos electrónicos con un mensaje falso. Se informó de una ola sin precedentes de gusanos Storm que se cree que ha matado a cientos de personas en toda Europa. Durante 10 años, se enviaron más de 1.200 millones de correos electrónicos infectados con el Gusano Storm. Los expertos estiman que todavía hay al menos un millón de ordenadores infectados cuyos propietarios no saben que están infectados.

Gusano SQL

Este gusano informático era único en su método de propagación. Generó una serie de direcciones IP aleatorias y se envió a ellas con la esperanza de que no estuvieran protegidas por un software antivirus. Poco después de que el gusano SQL se propagara en 2003, más de 75.000 ordenadores infectados se vieron envueltos, sin saberlo, en [ataques DDoS](#) en varios sitios web importantes.



Malware

6. **Troyano:** Programas que parecen inofensivos pero que al descargar son malignos.
7. **Rootkits:** Son malware que constantemente se esconden y crean puertas abiertas en la computadora.
8. **Session hijacking**
Cuando inicie sesión en una aplicación, debe ser el único que se haga cargo de la sesión. Sin embargo, un ataque de secuestro de sesión facilita que un atacante acceda a su sesión.



Informe de amenazas – Symantec 2016

1. 429 Millones de Identidades Expuestas
2. 53% de todos los Email son Spam
3. 431 Millones de variantes de malware descubiertos.
4. 1 en 3172 WebSite se encontraron con Malware.
5. 78% de los webSite son vulnerables.
6. Mas de un Millón de ataques bloqueados por dia.



Incidencias relevantes en Ciberseguridad.

1. El segundo incidente del que hablaremos hoy es el Ataque que sufrió PlayStation 2011. Esta fue una de las violaciones de seguridad de datos más grandes de la historia en ese momento. Según algunos informes, se expusieron hasta cien millones de cuentas (Credenciales , nombre de Usuario, Correo Electrónico, dirección fecha de nacimiento, Tarjeta de Crédito).
2. Violaciones de datos incluyen las que afectan a Yahoo. (2013 y 2014) con mil quinientos millones de cuentas.
3. eBay (2014) que afectó a ciento cuarenta y cinco millones de cuentas.
4. La lista de servicios afectados es bastante grande e incluye Amazon, PayPal, Twitter y Airbnb, BBC, la CNN, Fox News, New York Times, The Guardian,el Wall Street Journal y Wired.Y también servicios de entretenimiento, como HBO y Netflix; sitios de juegos,como PlayStation Network y Xbox.



Software FinFisher-Software Espia.

1. FinSpy - software espía llamado "FinFisher", creado y comercializado por una compañía británica llamada Gamma Group, que presentó a FinFisher como una nueva forma para que la policía y las agencias de inteligencia monitoreen a los criminales y espías. Descubrieron que se vendió a varios gobiernos y estos hacían espionajes desde Egipto, Morocco, Malaysia, Saudi Arabia, Uganda, Egypt, Oman, Turkey, Uzbekistan, Nigeria, Ethiopia, Sudan, Kazakhstan, Azerbaijan, Bahrain, and Albania, not to mention three American clients: the F.B.I., the Drug Enforcement Administration, and the Department of Defense.



Reporte de kaspersky-2021 - PERÚ

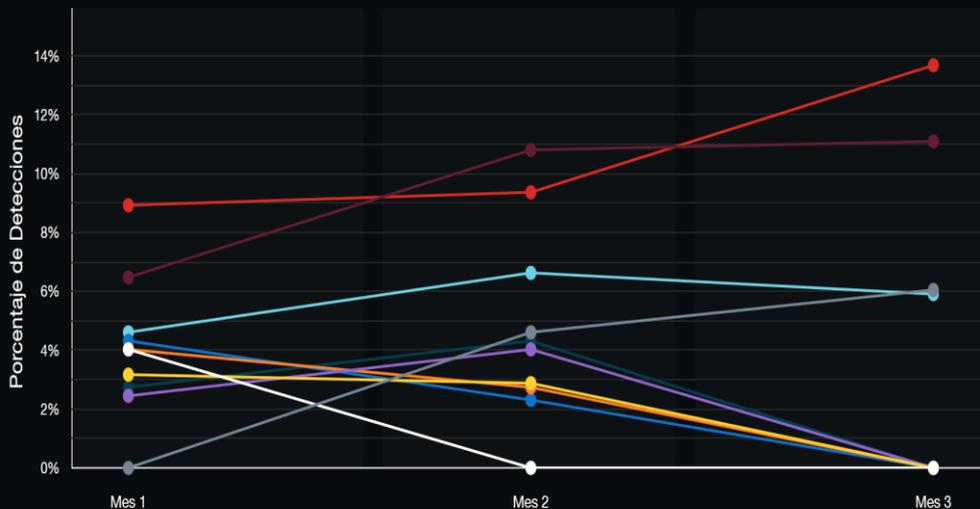




Reporte de Fortinet Peru-2021

FortiGuard Virus Detecciones

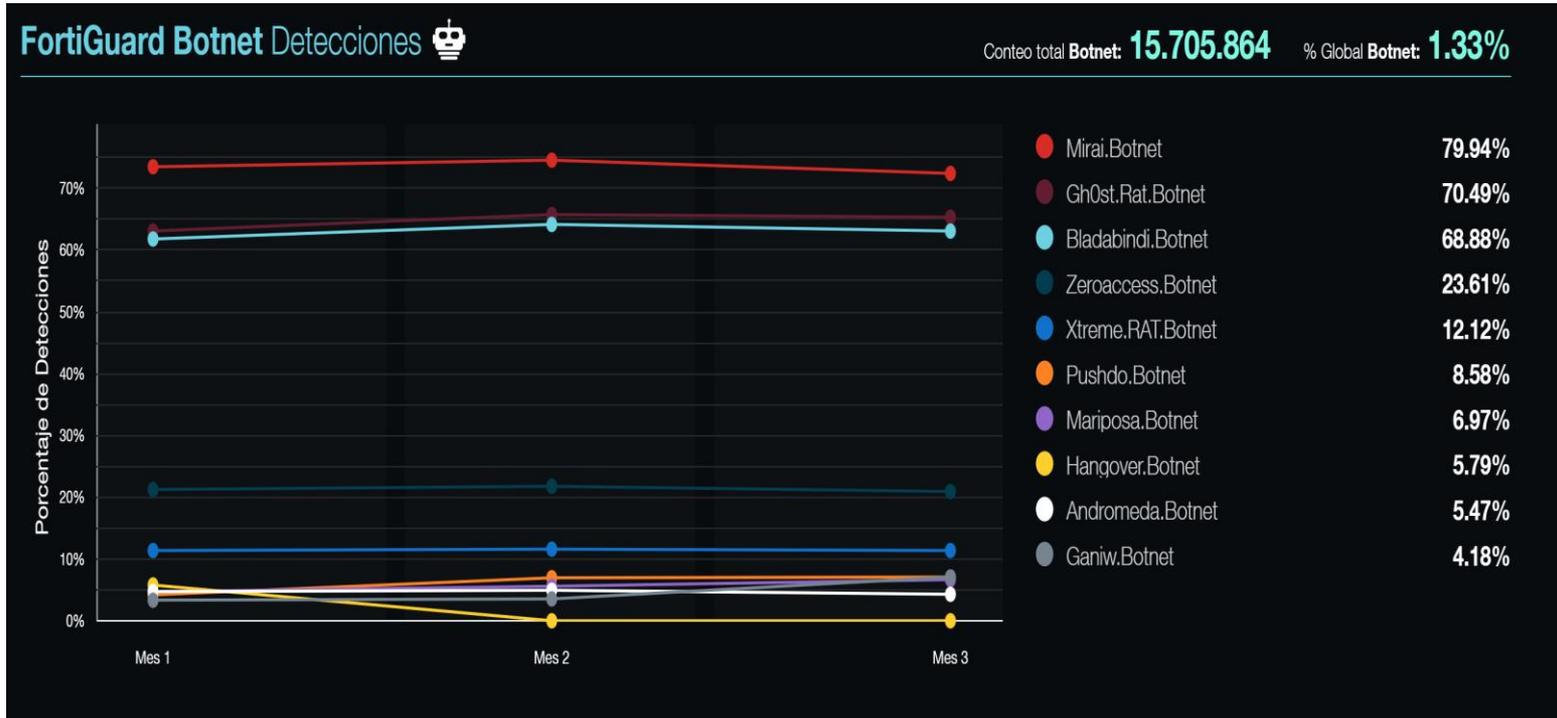
Conteo total Virus: **3.514.206** % Global Virus: **1.07%**



JS/ScrInject.B!tr	15.27%
HTML/ScrInject.B!tr	14.7%
JS/Nemucod.AMO!tr	9.65%
JS/Agent.79EE!tr	6.05%
W32/GenKryptik.DPIE!tr	5.48%
MSOffice/CVE_2017_11882.B!exploit	5.33%
RTF/CVE_2017_11882.BX!exploit	5.04%
PHP/Rst.CO!tr.bdr	4.76%
MSIL/Kryptik.SHS!tr	4.61%
MSIL/GenKryptik.EWC!tr	4.61%



Reporte de Fortinet Peru-2021

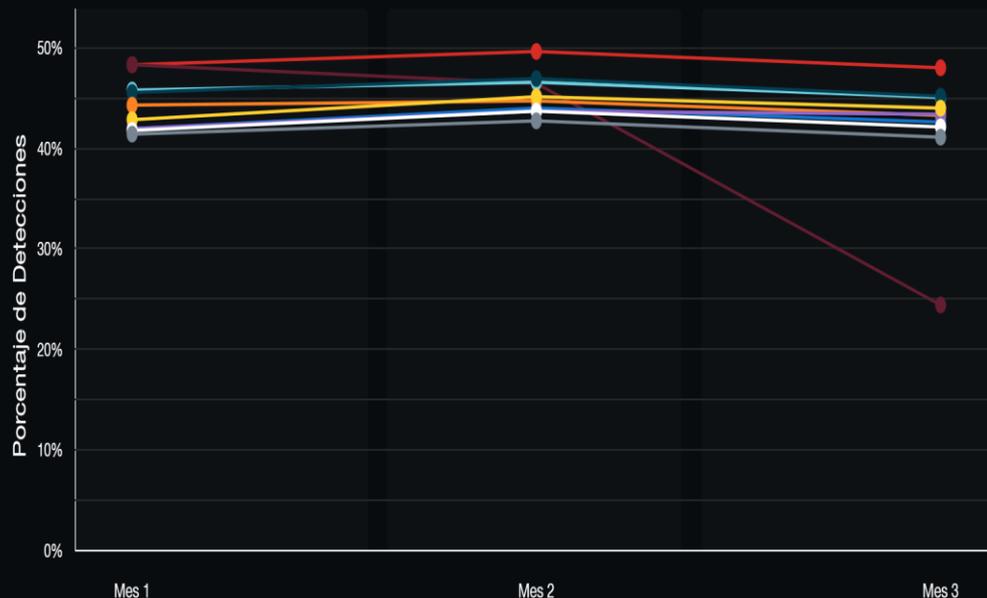




Reporte de Fortinet Peru-2021

FortiGuard Exploit Detecciones

Conteo total Exploit: **781.449.474** % Global Exploit: **0.64%**



- NETGEAR.DGN1000.CGI.Unauthenticated... **51.74%**
- Shenzhen.TVT.DVR.Remote.Code.Execution **50.06%**
- ThinkPHP.Controller.Parameter.Remote.Co... **48.68%**
- Dasan.GPON.Remote.Code.Execution **48.62%**
- Apache.Axis2.Default.Password.Access **47.78%**
- PHPUnit.Eval-stdin.PHP.Remote.Code.Exe... **47.36%**
- PHP.CGI.Argument.Injection **47.06%**
- D-Link.Devices.HNAP.SOAPAction-Header... **46.76%**
- ThinkPHP.Request.Method.Remote.Code.E... **46.64%**
- Joomla!.Core.Session.Remote.Code.Execu... **46.28%**



CiberCrimen

Estos son algunos ejemplos de los diferentes tipos de cibercrimen:

1. Fraude por correo electrónico e Internet.
2. Fraude de identidad (en caso de robo y uso de información personal).
3. Robo de datos financieros o de la tarjeta de pago.
4. Robo y venta de datos corporativos.
5. Ciberextorsión (amenazar con un ataque para exigir dinero).
6. Ataques de ransomware (un tipo de ciberextorsión).
7. Cryptojacking (en el que los hackers consiguen criptomoneda con recursos que no les pertenecen).
8. Ciberespionaje (en el que los hackers acceden a datos gubernamentales o empresariales).
9. La mayor parte del cibercrimen se divide en dos categorías principales:
10. Actividad delictiva *dirigida* a las computadoras.
11. Actividad delictiva que *utiliza* computadoras para cometer otros delitos.
12. El cibercrimen *dirigido* a las computadoras suele implicar virus y otros tipos de malware.



**COLEGIO DE
INGENIEROS
DEL PERU**

La Ley de Delitos Informáticos

En el año 2013, se promulga la Ley 30096 y su modificatoria Ley 30171

Su objetivo es prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos e informáticos y mediante la utilización de tecnologías de la información o de la comunicación.



La Ley de Delitos Informáticos

DELITOS CONTRA DATOS Y SISTEMAS INFORMÁTICOS:

Art. 2: Acceso ilícito,

Art. 3: atentado a la integridad de datos informáticos,

Art. 4: Atentado a la integridad de sistemas informáticos.

Reprimida con pena privativa de libertad no menor de uno ni mayor de **seis años**.

DELITOS INFORMÁTICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES

Art. 5. Propositiones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos. Se sanciona con pena privativa de libertad **no menor de cuatro ni mayor de ocho años**.



**COLEGIO DE
INGENIEROS
DEL PERU**

La Ley de Delitos Informáticos

DELITOS INFORMÁTICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES

Art. 6. Tráfico ilegal de datos.

Art. 7. intercepción de datos informáticos. Reprimida con pena privativa de libertad no menor de tres ni mayor de **seis años**.

DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO

Art. 8: Fraude informático. Reprimida con pena privativa de libertad no menor de tres ni mayor de **ocho años**.



**COLEGIO DE
INGENIEROS
DEL PERU**

La Ley de Delitos Informáticos

DELITOS CONTRA LA FE PÚBLICA:

Art. 9: Suplantación de identidad. Reprimida con pena privativa de libertad no menor de tres ni mayor de **cinco años**".

Disposiciones comunes:

Art. 10: **Abuso de mecanismos y dispositivos informáticos**. Reprimida con pena privativa de libertad no menor de uno ni mayor de **cuatro años**



Estadísticas - DIVINDAT PNP

Tabla 1. Denuncias de delitos informáticos investigados por la DIVINDAT. 2013-2020

DELITO	2013	2014	2015	2016	2017	2018	2019	2020	TOTAL	%
Abuso de mecanismos y dispositivos informáticos	14	3	6	4	5	1	2	19	54	0.4%
Abuso de mecanismos y dispositivos informáticos	14	3	6	4	5	1	2	19	54	
Suplantación de identidad	10	101	114	134	132	227	247	572	1537	12.6%
Suplantación de identidad	10	101	114	134	132	227	247	568	1533	
Suplantación de identidad virtual								4	4	
Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos	9	9			29	94	49	100	290	2.4%
Contra la indemnidad sexual de menores								2	2	
Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos	9	9			29	94	49	98	288	
Contra datos y sistemas informáticos	38	62	47	47	104	126	159	177	760	6.2%
Acceso ilícito	11	42	1	1	49	84	129	151	468	
Acceso ilícito a una base de datos								2	2	
Atentado a integridad de datos informáticos	21	4	30	22	40	26	5	9	157	
Atentado a la integridad de sistemas informáticos	6	16	16	24	15	9	5	9	100	
Atentado contra la integridad de datos y sistemas informáticos						7	20	6	33	
Contra la intimidad y el secreto de las comunicaciones						3	2	8	13	0.1%
Interceptación de datos								2	2	
Interceptación de datos personales								1	1	
Tráfico ilegal de datos						3	2	5	10	
Fraude informático	298	334	414	610	1219	1928	2097	2615	9515	78.2%
Clonación de tarjeta	83	42	46	44	30	120	25	4	394	4
Compras fraudulentas por internet						287	431	261	979	10
Operaciones y transferencia electrónicas y/o de fondos no autorizados	215	292	368	566	1189	1521	1641	2350	8142	86
TOTAL	369	509	581	795	1489	2379	2556	3491	12169	100.0%

Adaptado de informe N° 237-2020-DIRINCRI-PNP/DIVINDAT-SEC, de fecha 14 de septiembre de 2020 y de información remitida por el Coronel Orlando Mendieta, jefe de DIVINDAT, a la OFAEC de fecha 20 de enero de 2021.



Estadísticas Ministerio Público

Tabla 4. Delitos informáticos según tipo subgenérico

DELITO SUBGENÉRICO	2013	2014	2015	2016	2017	2018	2019	2020	TOTAL	%
Sin especificar			57	643	1513	2431	4415	1325	10384	48%
Contra el patrimonio	99	535	812	614	931	1657	3228	1138	9014	42%
Contra la fe pública		2	7	45	123	160	335	116	788	4%
Contra datos y sistemas informáticos		2	16	41	118	159	281	79	696	3%
Contra la indemnidad y libertad sexuales			4	35	68	137	115	25	384	2%
Contra la intimidad y el secreto de las comunicaciones			6	25	49	72	68	40	260	1%
Disposiciones comunes		1	5	7	39	32	62	15	161	0.7%
TOTAL	99	540	907	1410	2841	4648	8504	2738	21687	100.0%

Adaptado de reporte de la Oficina de Racionalización y Estadística,
remitido a la OFAEC a través de correo electrónico de fecha 18 de agosto de 2020.



La Prueba Pericial

1. ¿Qué se entiende por prueba pericial?

Es una actividad procesal realizada por unos sujetos que tienen una condición especial debido a los conocimientos científicos, técnicos, artísticos o experiencia en un determinado campo, vale decir, conocimientos especializados que poseen.

El fiscal –impelido por una necesidad de conocimiento– debe recurrir u ordenar la intervención en el proceso del experto o especialista, que en el área respectiva, posea el conocimiento del cual aquél carece, y que está en perfecta posibilidad de estudiar, descubrir o valorar uno o varios elementos de prueba –hechos, cosas o fenómenos que el caso presenta–, para lo cual se requieren, de manera ostensible, determinados conocimientos artísticos, científicos o técnicos, es decir, conocimientos propios de una formación o capacidad especializada[1].



Que es un Perito

1. Todo **Perito** es un **Testigo Experto** que debe exponer sus hallazgos, opiniones y conclusiones dentro de los límites del juicio. Testificando la base científica de hallazgos, análisis y conclusiones. Demostrar el conocimiento científico asociado con sus áreas de especialización.



Que es Informática Forense

1. Llamado cómputo forense, computación forense, análisis forense digital, examinación forense digital o Forensic.
2. Es la Aplicación de técnicas informáticas y/o científicas utilizadas en la obtención de datos útiles que, potencialmente, podrían convertirse en evidencia o prueba en un **proceso judicial o Arbitraje**.
3. El peritaje informático es una especialización cuyo objetivo es asesorar a jueces, abogados o empresas durante procesos judiciales, con todo lo relacionado a temas informáticos. Hay un experto que se encarga de hacer las evaluaciones pertinentes.



**COLEGIO DE
INGENIEROS
DEL PERU**

Base Legal

1. Ley 28858 – Ley del Ingeniero. 26/Julio/2006
2. El Código Procesal Civil
3. El Código Procesal Penal



Quienes son Peritos

**LEY QUE COMPLEMENTA LA LEY N° 16053,
LEY QUE AUTORIZA A LOS COLEGIOS DE
ARQUITECTOS DEL PERÚ Y AL COLEGIO
DE INGENIEROS DEL PERÚ PARA
SUPERVISAR A LOS PROFESIONALES
DE ARQUITECTURA E INGENIERÍA
DE LA REPÚBLICA**

Artículo 1º.- Requisitos para el ejercicio profesional

Todo profesional que ejerza labores propias de Ingeniería y de docencia de la Ingeniería, de acuerdo a la Ley que autoriza a los Colegios de Arquitectos del Perú y al Colegio de Ingenieros del Perú para supervisar a los profesionales de Arquitectura e Ingeniería de la República, N° 16053, requiere poseer grado académico y título profesional otorgado por una universidad nacional o extranjera debidamente revalidado en el país, estar colegiado y encontrarse habilitado por el Colegio de Ingenieros del Perú. Son ámbitos del ejercicio profesional del ingeniero, entre otros, los siguientes:

- a) Las labores de realización de estudios técnicos, propuestas u ofertas técnicas, anteproyectos, esquemas técnicos, proyectos, **absolución de consultas y asesorías técnicas, avalúos, peritajes,** planificación y esquemas de funcionamiento de obras y servicios de ingeniería, informes técnicos, planos, mapas, cálculos, presupuestos y valuaciones con todos sus anexos, croquis, minutas, estudios preliminares y estudios definitivos; gerencias, supervisiones, inspecciones y auditorías especializadas; coordinaciones y direcciones de obras, procesos de ingeniería o sus servicios conexos; operación, mantenimiento y reparación de las mismas, incluyendo los aspectos informáticos y de sistemas, gestión de calidad, medio ambiente, estudios de impacto ambiental, entre otras. Estas labores deben ser efectuadas, firmadas y refrendadas por profesionales inscritos



Base Legal Código Procesal Civil

TITULO VIII: Medios probatorios (Artículo 188 al 304)

Capítulo I: Disposiciones generales (Artículo 188 al 201)

Capítulo II: Audiencia de pruebas (Artículo 202 al 212)

Capítulo III: Declaración de partes (Artículo 213 al 221)

Capítulo IV: Declaración de testigos (Artículo 222 al 232)

Capítulo V: Documentos (Artículo 233 al 261)

Capítulo VI: Pericia (Artículo 262 al 271)

Capítulo VII: Inspección Judicial (Artículo 272 al 274)

Capítulo VIII: Sucedáneos de los medios probatorios (Artículo 275 al 283)

Capítulo IX: Prueba anticipada (Artículo 284 al 299)

Capítulo X: Cuestiones probatorias (Artículo 300 al 304)



Base Legal Código Procesal Civil

Capítulo VI: Pericia

Artículo 262.- Procedencia

La pericia procede cuando la apreciación de los hechos controvertidos requiere de conocimientos especiales de naturaleza científica, tecnológica, artística u otra análoga.

Artículo 263.- Requisitos

Al ofrecer la pericia se indicarán con claridad y precisión, los puntos sobre los cuales versará el dictamen, la profesión u oficio de quien debe practicarlo y el hecho controvertido que se pretende esclarecer con el resultado de la pericia. Los peritos son designados por el Juez en el número que considere necesario.

Artículo 264.- Perito de parte

Las partes pueden, en el mismo plazo que los peritos nombrados por el Juez, presentar



Base Legal Código Procesal Penal

SECCIÓN II: La Prueba (artículo 155 al 252)

Título I: Preceptos Generales (artículo 155 al 159)

Título II: Los Medios de Prueba (artículo 160 al 201-A)

Capítulo I: La Confesión (artículo 160 al 161)

Capítulo II: El Testimonio (artículo 162 al 171)

Capítulo III: La Pericia (artículo **172** al 181)

Capítulo IV: El Careo (artículo 182 al 183)

Capítulo V: La Prueba Documental (artículo 184 al 188)

Capítulo VI: Los otros Medios de Prueba (artículo 189 al 201)

Subcapítulo I: El Reconocimiento (artículo 189 al 191)

Subcapítulo II: La Inspección Judicial y la Reconstrucción (artículo 192 al 194)

Subcapítulo III: Las Pruebas Especiales (artículo 195 al 201-A)

Título III: La Búsqueda de Pruebas y Restricción de Derechos (artículo 202 al 241)



Base Legal Código Procesal Penal

CAPÍTULO III: LA PERICIA

Artículo 172.- Procedencia

1. La pericia procederá siempre que, para la explicación y mejor comprensión de algún hecho, se requiera conocimiento especializado de naturaleza científica, técnica, artística o de experiencia calificada.
2. Se podrá ordenar una pericia cuando corresponda aplicar el artículo 15 del Código Penal. Ésta se pronunciará sobre las pautas culturales de referencia del imputado.
3. No regirán las reglas de la prueba pericial para quien declare sobre hechos o circunstancias que conoció espontáneamente aunque utilice para informar las aptitudes especiales que posee en una ciencia, arte o técnica. En este caso regirán las reglas de la prueba testimonial.

Artículo 173 - Nombramiento



Delitos Informáticos

1. **Los delitos informáticos** o cibernéticos es toda aquella [acción antijurídica](#) que se realiza en el entorno digital.(Computadora, Teléfonos, Tablet, Raspberry, IoT, Convergencia Digital, Domótica etc.).
2. Para las investigaciones en delitos cibernéticos: los detectives dependen en gran medida de las **evidencias digitales**.
3. El objetivo final de una investigación forense es identificar, analizar y reconstruir eventos pasados , las actividades y presentar evidencia admisible en el **Poder Judicial**.
4. Se requiere de procedimientos adecuados y tecnologías que utiliza el investigador forense **para trabajar en evidencia digital sin alterar los datos (Contaminada)**



Evidencias Digitales

5. La evidencias Digitales se encuentra en la Memoria Volátil y No Volátil. Existen diferentes Herramientas para cada tipo de memoria.
6. Por cada tipo de Sistemas Operativos el procedimiento es diferente.
7. También existe la contraparte llamada análisis forense anti-digital o ADF, que son tecnologías diseñadas para frustrar el descubrimiento de dicha información. Con el objetivo manipular, borrar u ofuscar datos digitales.

Metodología de la Informática Forense

Según la ISO/IEC 27037:2012, « Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence», s/f, <https://www.iso.org/standard/44381.html> (consultada el 26 de septiembre del 2021).

- 1. Identificación** evidencia digital
- 2. Adquirir** evidencia sin modificaciones o corrupciones
- 3. Preservar** que la evidencia recuperada no se modifique al que se le incauto.
- 4. Analizar** los datos sin ninguna alteración
- 5. Dictamen Pericial**



Adquisición y Preservación

1. Adquisición de Datos Volátiles
2. Adquisición de Datos No Volátiles
3. Cadena de Custodia y código Hash



Adquisición y Preservación

Dispositivo de
almacenamiento
(Disco duro)



**SOFTWARE
FORENSE**

Disco duro
externo



Código hash:

85CB7009E7DA5D6C2FDD4F607284461C



Herramientas del Perito -Adquisición

Herramientas Libres

1. FTK Imager.
2. OsForensic
3. Autopsy
4. Bulk_extractor
5. Kali Linux
6. Caine
7. Volatility
8. AndreKiller.
9. Entre Otros

Herramientas Pagadas

1. Encase Forensic
2. Ftk Imager
3. Cellebrite UFED
4. XRY Office Complete
5. SantoKU
6. Magnet Forensic
7. Amped Forensic



Copia de Información bit a bit mediante Duplicadores

TableAU Forensic



Fulcrum Management





COLEGIO DE
INGENIEROS
DEL PERU

Software Proprietario de Analisis Forense PC

Encase Forensic

The screenshot displays the Encase Forensic software interface. The main window shows a file system tree on the left, a table of files in the center, and a hex view of a selected file at the bottom.

File System Tree (Left):

- 192.168.137.11-0-HDD
 - \$Extend
 - \$Recycle.Bin
 - Boot
 - Documents and Settings
 - PerfLogs
 - Program Files
 - Program Files (x86)
 - ProgramData
 - Recovery
 - System Volume Information
 - Users
 - Windows
 - addins
 - appcompat
 - AppPatch



**COLEGIO DE
INGENIEROS
DEL PERU**

Adquisición de Teléfonos

1. Cellebrite UFED
2. XRY Office Complete
3. SantoKU
4. Magnet Forensic



Adquisicion de Camaras de Video Vigilancia.

1. AMPED Software
2. DVR examiner





**COLEGIO DE
INGENIEROS
DEL PERU**

Adquisición de Cámaras de Video Vigilancia.

The screenshot displays the Amped FIVE software interface for video processing. The main window shows a blurred video frame of a car. A zoomed-in view of the license plate is shown on the right. The interface includes a 'Filters' panel with 'Motion Deblurring' selected, a 'Tools (Point)' panel, and a 'History' panel showing 'Chain 1' with 'Image Loader 1' and 'Nonlinear Deblurring 2'. The bottom status bar shows 'Frame 0 (00:00:00.000)' and 'car.jpg (1600 x 1200)'. The Windows taskbar at the bottom shows various application icons.



Análisis

1. Visualizar la Metadata del Sistema Operativo
2. Analizar los programas informáticos.
3. Análisis de Artefactos dependiendo del tipo de

Pericia :

1. Pagefile,
2. \$LogFile,
3. \$MFT
4. \$Journal
5. FileSystem
6. Los Registros de Windows
7. Hora del Sistema
8. Los archivos Borrados



Análisis

9. Los Cokies
10. Los URL
11. Memoria RAM
12. Los procesos ejecutados
13. Los procesos dependientes
14. Registros de Acceso Remoto.
15. Registros a Nivel de Bios.



Ftk Imager

AccessData FTK Imager 4.3.1.1

File View Mode Help

Evidence Tree

- Partition 2 [99899MB]
 - NONAME [NTFS]
 - [orphan]
 - [root]
 - \$BadClus
 - \$Extend
 - \$Recycle.Bin
 - \$Secure
 - \$UpCase
 - ARCHIVOS DE PERSONAL.rar
 - ARCHIVOS_DE_PERSONAL
 - Brief
 - Clip53
 - CLIPPER5
 - Config.Msi
 - Documents and Settings
 - epson
 - Instalador CONTROL
 - Instalador CONTROL.rar
 - ipress - octubre2018
 - LJM428f-M429f_UWWWL_Full_WebPac
 - LJM428f-M429f_V3_DriveronlyWebpac
 - Ms documentos
 - MSIa56.tmp
 - MSOCache
 - Nueva carpeta
 - Nueva carpeta (2)
 - progra
 - Program Files
 - ProgramData
 - Recovered data 10-27-2020 at 15_43_
 - Recovery
 - SIS_PER
 - System Volume Information
 - Thumbs.db
 - Users
 - Windows

File List

Name	Size	Type	Date Modified
SIS_PER	1	Directory	29/10/2020 00:06:00
System Volume Information	1	Directory	1/06/2021 21:45:44
Users	1	Directory	23/10/2020 15:21:53
Windows	1	Directory	4/05/2021 12:54:26
\$AttrDef	3	Regular File	21/04/2012 02:14:39
\$BadClus	0	Regular File	21/04/2012 02:14:39
\$Bitmap	3,122	Regular File	21/04/2012 02:14:39
\$Boot	8	Regular File	21/04/2012 02:14:39
\$I30	40	NTFS Index All...	8/06/2021 07:58:49
\$LogFile	65,536	Regular File	21/04/2012 02:14:39
\$MFT	858,624	Regular File	21/04/2012 02:14:39
\$MFTMirr	4	Regular File	21/04/2012 02:14:39
\$Secure	1	Regular File	21/04/2012 02:14:39
\$TXF_DATA	1	NTFS Logged ...	8/06/2021 07:58:49
\$UpCase	128	Regular File	21/04/2012 02:14:39
\$Volume	0	Regular File	21/04/2012 02:14:39
ARCHIVOS DE PERSONAL.rar	379,596	Regular File	18/08/2017 14:07:50
autoexec.bat	1	Regular File	22/11/2014 16:20:10
Brief	1	NTFS INDEX Entry	
config.sys	0	Regular File	18/02/2010 17:34:28
Disco local (D:) - Acceso directo.Ink	1	Regular File	11/12/2020 20:45:26

```

00 30 00 00 00 01 00 00 00-00 10 00 00 01 00 00 00
10 10 00 00 00 28 00 00 00-28 00 00 00 01 00 00 00
20 00 00 00 00 00 00 00-18 00 00 00 03 00 00 00
30 05 00 00 00 00 00 00-00-
  
```

Activar Windows
Ve a Configuración para activar Windows.

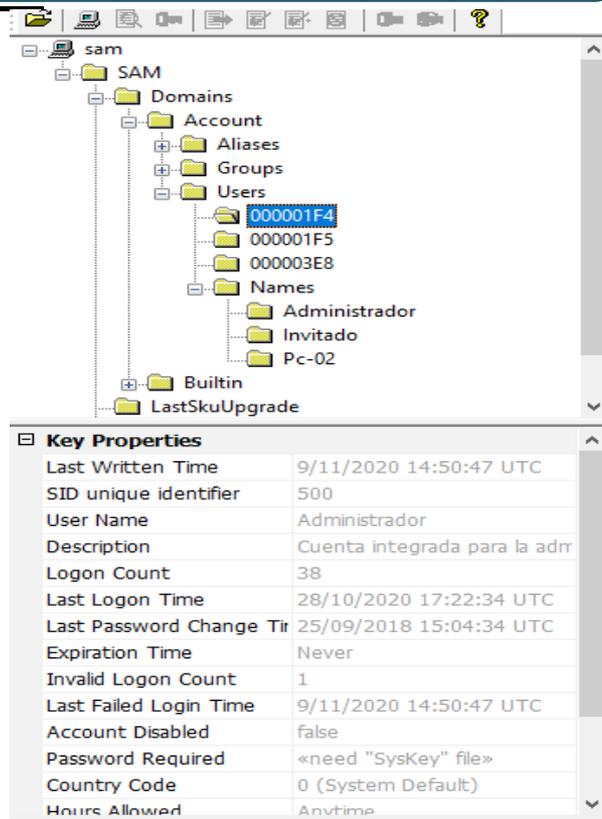
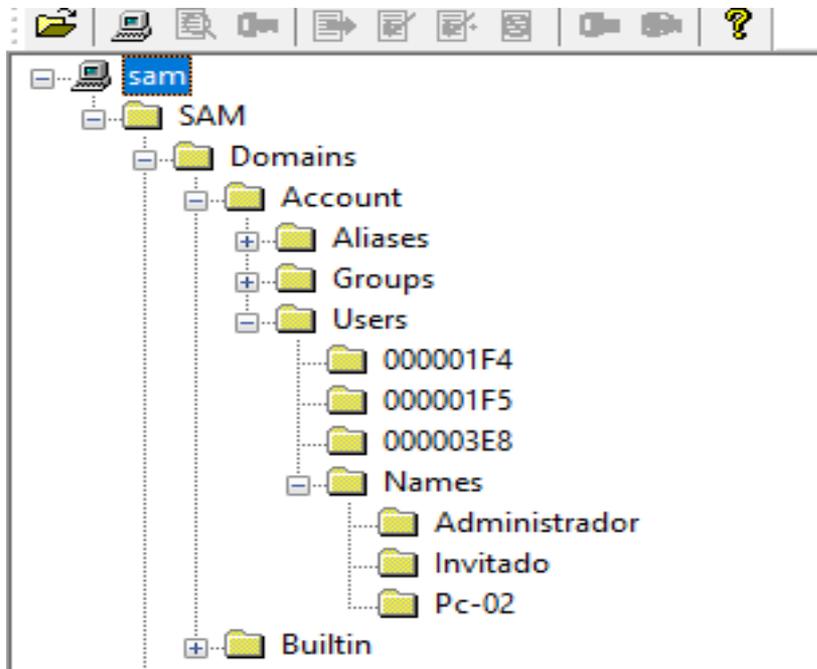
Listed: 57 Selected: 0 HBTRRHH.001/Partition 2 [99899MB]/NONAME [NTFS]/[root]

Cursor pos = 0

18°C Nublado 11:51 2/07/2021

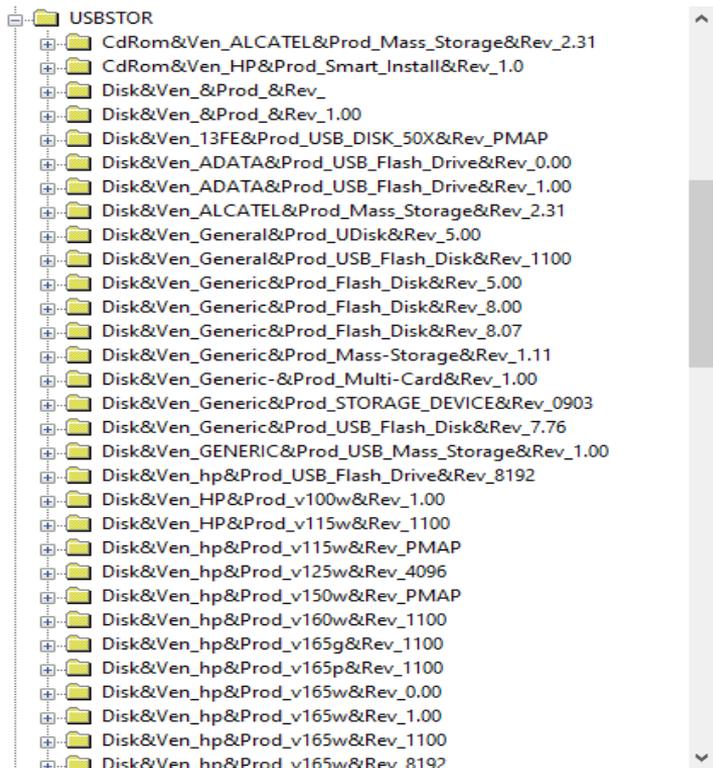


Herramientas del Perito – Access Visor de RegEdit





Herramientas del Perito – Access Visor de RegEdit – Ultima Conexión del USB





Herramientas del Perito – Access Visor de RegEdit – Visualizar conexión del ANYDESK

AccessData FTK Imager 4.5.0.3

File View Mode Help

Evidence Tree

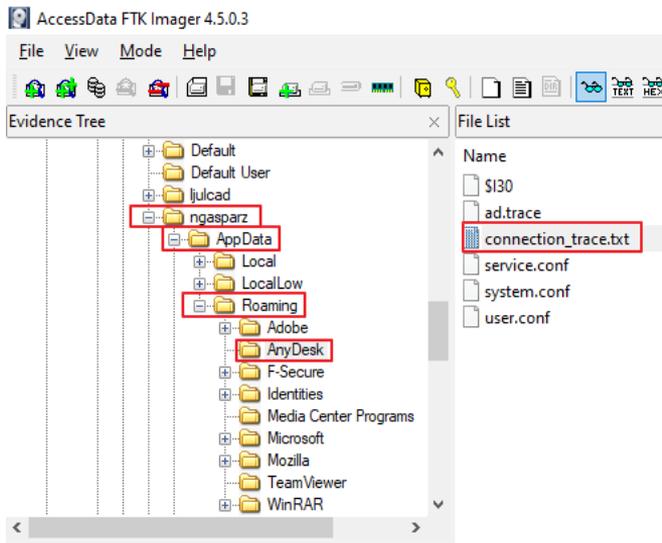
- Default
- Default User
- ljulcad
- ngasparz
- AppData
 - Local
 - LocalLow
 - Roaming
 - Adobe
 - AnyDesk
 - F-Secure
 - Identities
 - Media Center Programs
 - Microsoft
 - Mozilla
 - TeamViewer
 - WinRAR

File List

Name	Size	Type	Date Modified
\$I30	4	NTFS Index All...	12/04/2020 20:03:59
ad.trace	934	Regular File	20/04/2020 13:45:42
connection_trace.txt	2	Regular File	13/04/2020 00:46:52
service.conf	3	Regular File	12/04/2020 21:35:32
system.conf	1	Regular File	20/04/2020 13:45:42
user.conf	1	Regular File	20/04/2020 13:45:32



Herramientas del Perito – Access Visor de RegEdit – Visualizar conexión del ANYDESK



```

error 2020-04-13 00:47:17.462      back 1888 2144      base.dyn_library - Could not load library shcore.dll (0x
error 2020-04-13 00:47:17.478      back 1888 3656      base.dyn_library - Could not load library shcore.dll (0x
error 2020-04-13 00:47:17.494      back 1888 3988      base.dyn_library - Could not load library shcore.dll (0x
error 2020-04-13 00:47:17.510      back 1888 3124      base.dyn_library - Could not load library shcore.dll (0x
error 2020-04-13 00:47:17.527      back 1888 3648      base.dyn_library - Could not load library shcore.dll (0x
error 2020-04-13 00:47:17.544      back 1888 2144      base.dyn_library - Could not load library shcore.dll (0x
error 2020-04-13 00:47:17.560      back 1888 3656      base.dyn_library - Could not load library shcore.dll (0x
error 2020-04-13 00:47:17.577      back 1888 4072      base.dyn_library - Could not load library shcore.dll (0x
error 2020-04-13 00:47:17.594      back 1888 2144      base.dyn_library - Could not load library shcore.dll (0x
error 2020-04-13 00:47:17.611      back 1888 5704      base.dyn_library - Could not load library shcore.dll (0x
error 2020-04-13 00:47:17.627      back 1888 4072      base.dyn_library - Could not load library shcore.dll (0x
error 2020-04-13 00:47:17.644      back 1888 3656      base.dyn_library - Could not load library shcore.dll (0x
error 2020-04-13 00:47:17.661      back 1888 2144      base.dyn_library - Could not load library shcore.dll (0x
error 2020-04-13 00:47:17.678      back 1888 3124      base.dyn_library - Could not load library shcore.dll (0x
error 2020-04-13 00:47:17.695      back 1888 3648      base.dyn_library - Could not load library shcore.dll (0x
error 2020-04-13 00:47:17.712      back 1888 3988      base.dyn_library - Could not load library shcore.dll (0x
error 2020-04-13 00:47:17.729      back 1888 4072      base.dyn_library - Could not load library shcore.dll (0x
error 2020-04-13 00:47:17.746      back 1888 3280      base.dyn_library - Could not load library shcore.dll (0x
error 2020-04-13 00:47:17.763      back 1888 5704      base.dyn_library - Could not load library shcore.dll (0x
error 2020-04-13 00:47:17.779      back 1888 3124      base.dyn_library - Could not load library shcore.dll (0x
error 2020-04-13 00:47:17.796      back 1888 3280      base.dyn_library - Could not load library shcore.dll (0x
error 2020-04-13 00:47:17.812      back 1888 3124      base.dyn_library - Could not load library shcore.dll (0x
error 2020-04-13 00:47:17.828      back 1888 2144      base.dyn_library - Could not load library shcore.dll (0x
error 2020-04-13 00:47:17.844      back 1888 3280      base.dyn_library - Could not load library shcore.dll (0x
error 2020-04-13 00:47:17.860      back 1888 3124      base.dyn_library - Could not load library shcore.dll (0x
error 2020-04-13 00:47:17.876      back 1888 3656      base.dyn_library - Could not load library shcore.dll (0x
error 2020-04-13 00:47:17.892      back 1888 3648      base.dyn_library - Could not load library shcore.dll (0x
error 2020-04-13 00:47:17.908      back 1888 3124      base.dyn_library - Could not load library shcore.dll (0x
error 2020-04-13 00:47:17.925      back 1888 3656      base.dyn_library - Could not load library shcore.dll (0x
error 2020-04-13 00:47:17.942      back 1888 4072      base.dyn_library - Could not load library shcore.dll (0x
error 2020-04-13 00:47:17.959      back 1888 3280      base.dyn_library - Could not load library shcore.dll (0x
error 2020-04-13 00:47:17.976      back 1888 3988      base.dyn_library - Could not load library shcore.dll (0x
error 2020-04-13 00:47:17.993      back 1888 2144      base.dyn_library - Could not load library shcore.dll (0x
error 2020-04-13 00:47:18.010      back 1888 4072      base.dyn_library - Could not load library shcore.dll (0x
error 2020-04-13 00:47:18.027      back 1888 3988      base.dyn_library - Could not load library shcore.dll (0x

```



Herramientas del Perito – Access Visor de RegEdit – Visualizar eventos

Propiedades de evento: Evento 21, TerminalServices-LocalSessionManager

General Detalles

Servicios de Escritorio remoto: inicio de sesión correcto:

Usuario: HBELENTRUJILLO\ngasparz
Identificador de sesión: 1
Dirección de red de origen: LOCAL

Nombre de registro: Microsoft-Windows-TerminalServices-LocalSessionManager/Operational

Origen: TerminalServices-LocalSessic Registrado: 15/10/2020 06:35:51

Id. del 21 Categoría de tarea: Ninguno

Nivel: Información Palabras clave:

Usuario: SYSTEM Equipo: PER_CTRLTIEMPOS.hbelentrujillo.gob.pe

Código de operación: Información

Más información: [Ayuda Registro de eventos](#)

Copiar Cerrar



Herramientas del Perito – Visualizar PageFile

Belkasoft Evidence Center X | v.1.7.7432 VERSIÓN DE PRUEBA | Análisis de pagefile.sys

Reporte | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021

Tablares | **Artefactos**

Reporte | Estructura | Visión general

- [-] SLogFile.copy0 (1)
 - [-] Chats (1)
- [-] pagefile.sys.copy0 (7826)
 - [-] Archivos de sistema (222)
 - [-] Enlace de archivo (222)**
 - [-] Chats (2)
 - [-] Correos (1)
 - [-] Imágenes (559)
 - [-] Miniaturas (4)
 - [-] Navegadores (7018)
 - [-] Chrome (Carved) (4464)
 - [-] Internet Explorer (Carved) (40)
 - [-] Opera (Carved) (2514)
 - [-] Otros archivos (20)

Elementos: 222 | Elementos actualizados (de 222 a 222) | Actualizar

<input type="checkbox"/>	<input type="checkbox"/>	xcu...	Tamaño de archivo...	Hora de acceso al a...	Hora de creación d...	↓ Hora
<input type="checkbox"/>	<input type="checkbox"/>		32768	28/10/2020 22:01:19	21/04/2012 02:14:34	28/10/20
<input type="checkbox"/>	<input type="checkbox"/>		327680	3/11/2020 17:25:35	28/10/2020 16:50:31	3/11/202
<input type="checkbox"/>	<input type="checkbox"/>		40960	28/10/2020 16:50:51	28/10/2020 16:50:51	28/10/20
<input type="checkbox"/>	<input type="checkbox"/>		4096	5/11/2020 16:16:59	2/09/2020 03:39:07	5/11/202
<input type="checkbox"/>	<input type="checkbox"/>		0	4/11/2020 13:44:10	4/11/2020 13:41:47	4/11/202
<input type="checkbox"/>	<input type="checkbox"/>		0	4/11/2020 05:00:00	4/11/2020 21:00:56	4/11/202
<input type="checkbox"/>	<input type="checkbox"/>		4096	5/11/2020 12:55:36	5/11/2020 12:53:39	5/11/202

Propiedades

Está eliminado	Sí
Archivo	
Nombre del archivo	common_000026F79938.Ink
Ruta	common_000026F79938.Ink
Desplazamiento (bytes)	653760824
Tamaño del archivo (bytes)	559
Guardado en la base de datos	No
Metadatos	
Tamaño de archivo de destino (bytes)	24117248
Atributo del archivo	The link target is a directory
Hora de acceso al archivo de destino (UTC)	3/11/2020 14:58:00
Hora de creación	28/10/2020



Herramientas del Perito – Visualizar \$LOGFILE

< Imager 4.5.0.3

File Help

File List

Name	Size	Type
Windows	1	Direct
\$AttrDef	3	Regul
\$BadClus	0	Regul
\$Btmmap	3,122	Regul
\$Boot	8	Regul
\$I30	40	Regul
\$LogFile	65,536	Regul
\$MFT	858,624	Regul
\$MFTI	4	Regul
\$Sec	1	Regul
\$STX	1	Regul
\$UpCase	128	Regul
\$Volume	0	Regul
ARCHIVOS DE PERSONAL.rar	379,596	Regul
autoexec.bat	1	Regul
Brief	\$I30 IN	Regul
config.sys	0	Regul
Disco local (D) - Acceso directo.lnk	1	Regul
GDIA1220	48	Regul

NTFS Log Tracker v1.6

Regul Target Path : C:\Users\Gabriel\Desktop\logfile\LogFile.copy0

Regul \$LogFile File Path : C:\Users\Gabriel\Desktop\logfile\LogFile.copy0

Regul \$UsnJrnl File Path : C:\Users\Gabriel\Desktop\logfile\\$.copy0

Regul Source Files Folder Path :

Regul NTFS (for UsnJrnl Record Carving) : Carving Alignment : 8

Regul Option

Regul SMFT File Path : C:\Users\Gabriel\Desktop\logfile\SMFT.copy0

Regul Open SQLite DB File

Regul SQLite DB File Path :

Regul Search

Regul \$LogFile \$UsnJrnl \$LogFile(Search Result) \$UsnJrnl(Search Result)

Page : (1 / 1)

LSN	EventTime(UTC-5)	Event	Detail	File/Directory Name	Full Path(from \$MFT)	Create Time	Modified Time
72449185339	2021-05-28 09:46:17	File Creation		NOD885.tmp	Windows(Temp)\NOD885.tmp	2021-05-28 09:46:17	2021-05-28 09:46:17
72449186130	2021-05-28 09:46:17	File Deletion		NOD885.tmp	Windows(Temp)\NOD885.tmp	2021-05-28 09:46:17	2021-05-28 09:46:17
72449187685	2021-05-28 09:46:17	File Creation		NOD808A.tmp	Windows(Temp)\NOD808A.tmp	2021-05-28 09:46:17	2021-05-28 09:46:17
72449188933	2021-05-28 09:46:17	File Deletion		NOD808A.tmp	Windows(Temp)\NOD808A.tmp	2021-05-28 09:46:17	2021-05-28 09:46:17
72449189164	2021-05-28 09:46:18	File Creation		NOD90A7.tmp	Windows(Temp)\NOD90A7.tmp	2021-05-28 09:46:18	2021-05-28 09:46:18
72449189975	2021-05-28 09:46:18	File Deletion		NOD90A7.tmp	Windows(Temp)\NOD90A7.tmp	2021-05-28 09:46:18	2021-05-28 09:46:18
72449190206	2021-05-28 09:46:18	File Creation		NOD9JFF.tmp	Windows(Temp)\NOD9JFF.tmp	2021-05-28 09:46:18	2021-05-28 09:46:18
72449191391	2021-05-28 09:46:19	File Deletion		NOD9JFF.tmp	Windows(Temp)\NOD9JFF.tmp	2021-05-28 09:46:18	2021-05-28 09:46:18
72449193033		Writing Content of Non-Resident File	Data Runs(in Volume) : 19379170...	NOD84FB.tmp	Windows(Temp)\NOD84FB.tmp		
72449193167	2021-05-28 09:46:27	File Creation		NOD84FB.tmp	Windows(Temp)\NOD84FB.tmp	2021-05-28 09:46:27	2021-05-28 09:46:27
72449193509		Writing Content of Non-Resident File	Data Runs(in Volume) : 641271(16)	NOD84FB.tmp	Windows(Temp)\NOD84FB.tmp		
72449193868	2021-05-28 09:46:27	File Deletion		NOD84FB.tmp	Windows(Temp)\NOD84FB.tmp	2021-05-28 09:46:27	2021-05-28 09:46:27
72449194217	2021-05-28 09:46:29	File Creation		NOD8A68.tmp	Windows(Temp)\NOD8A68.tmp	2021-05-28 09:46:29	2021-05-28 09:46:29
72449199152		Writing Content of Non-Resident File	Data Runs(in Volume) : 19372177...	NOD8A68.tmp	Windows(Temp)\NOD8A68.tmp		
72449202402	2021-05-28 09:46:30	File Deletion		NOD8A68.tmp	Windows(Temp)\NOD8A68.tmp	2021-05-28 09:46:29	2021-05-28 09:46:29

\$LogFile Record Count : 10594 \$UsnJrnl Record Count : 359417

Created by Junghoon Oh(blueangell275@gmail.com)



Herramientas del Perito – Analizar SQL

Ejm: Geolocalización

```
select distinct
    a.perano, a.permes,
    b.trarev, rrhh.f_per_obtiene_nomemp('01',b.trarev) aperev
from pensiones.pen_t_prerem a, pensiones.pen_t_precau b
where (a.perano>=2010 and a.perano<=2021)
and a.perano=b.perano and a.permes=b.permes
and a.codinst=b.codinst and a.codper=b.codper
and b.estado <> 0 and b.trarev is not null
order by a.perano asc, a.permes asc;
```



Herramientas del Perito – Analizar SQL

SQLyog Enterprise Trial - MySQL GUI - [MySql/v1 - root@localhost*]

File Edit Favorites DB Table Objects Tools PowerTools Window Help

root@localhost

- bd_tambini_202007
- db1
- db2
- dbiclassq
- dbicrmv01
- information_schema
- mysql
- performance_schema
- phpmyadmin
- test

Query QueryBuilder SchemaDesigner

Autocomplete: [Tab]->Next Tag, [Ctrl+Space]->List Matching Tags, [Ctrl+Enter]->List All Tags.

```
1 SELECT L1.TELEFONO_A, S1.SENTIDO, L1.TELEFONO_B,  
2 concat( substring(L1.FECHA_HORA_P,1,4),'/' , substring(L1.FECHA_HORA_P,5,2) , '/' , substring(L1.FECHA_HORA_P,7,2) , ' ', substring(L1.FECHA_HORA_P,9,2) ) as FECHA_HORA,  
3 from llamadas_vl L1, sentido S1  
4 where L1.SENTIDO_P=S1.CODIGO  
5 and L1.estado_reg in (1,8)  
6 and L1.id in (  
7 SELECT L1.id  
8 from llamadas_vl L1, titular t, persona p, sentido S  
9 where t.telefono IN (L1.TELEFONO_AP, L1.TELEFONO_BP )  
10 and p.PERSONA=t.PERSONA  
11 and p.PERSONA in ('P1')  
12 and L.SENTIDO_P=S.CODIGO  
13 and L.estado_reg in (1,8)  
14 and substring(l.fecha_hora_p,1,12) between "201709150000" and "201709231159"  
15 INTERSECT  
16 SELECT L1.id  
17 from llamadas_vl L1, titular t, persona p, sentido S  
18 where t.telefono IN (L1.TELEFONO_AP, L1.TELEFONO_BP )  
19 and p.PERSONA=t.PERSONA  
20 and p.PERSONA in ('P2')  
21 and L.SENTIDO_P=S.CODIGO  
22 and L.estado_reg in (1,8)  
23 and substring(l.fecha_hora_p,1,12) between "201709150000" and "201709231159"  
24  
25  
26 ORDER BY L1.FECHA_HORA_P ASC  
27
```

1 Result 2 Messages 3 Table Data 4 Objects 5 History

(Read Only)

TELEFONO_A	SENTIDO	TELEFONO_B	FECHA_HORA	DURACION	CELDA_ORIGEN	NOMBRE_CELDA	DIRECCION_CELDA	DISTRITO
------------	---------	------------	------------	----------	--------------	--------------	-----------------	----------



Herramientas del Perito – Jail Break

Iphone

```
192.168.1.11 - PuTTY
-sh: lsdf: command not found
iPhone-de-Christian:~ root# Lsof
-sh: lsdf: command not found
iPhone-de-Christian:~ root# netstat
Active Internet connections
Proto Recv-Q Send-Q Local Address Foreign Address (state)
tcp4 0 0 192.168.1.11.ssh 192.168.1.5.49962 ESTABLISHED
tcp4 0 0 192.168.1.11.53036 172.217.192.154.443 ESTABLISHED
tcp4 0 0 192.168.1.11.53035 64.62.210.2.443 ESTABLISHED
tcp4 0 0 192.168.1.11.53034 142.250.0.157.443 ESTABLISHED
tcp4 0 0 192.168.1.11.53033 142.250.0.157.443 ESTABLISHED
tcp4 0 0 192.168.1.11.53032 142.250.0.155.443 ESTABLISHED
tcp4 0 0 192.168.1.11.53031 172.217.192.155.443 ESTABLISHED
tcp4 0 0 192.168.1.11.53030 142.250.0.155.443 ESTABLISHED
tcp4 0 0 192.168.1.11.53029 64.62.210.2.443 ESTABLISHED
tcp4 0 0 192.168.1.11.53026 192.183.215.91.443 TIME_WAIT
tcp4 0 0 192.168.1.11.53019 157.185.158.198.80 ESTABLISHED
tcp4 0 0 192.168.1.11.53017 157.185.158.198.443 ESTABLISHED
tcp4 0 0 192.168.1.11.53016 157.185.158.198.443 ESTABLISHED
tcp4 0 0 192.168.1.11.53011 40.102.34.34.443 ESTABLISHED
tcp4 0 0 192.168.1.11.52851 17.57.144.36.5223 ESTABLISHED
udp4 0 0 *.* **
udp4 0 0 *.* **
udp6 0 0 *.mdns **
udp4 0 0 *.mdns **
udp4 0 0 *.* **
Active Multipath Internet connections
Proto/ID Flags Local Address Foreign Address (state)
icm6 0 0 *.* **
Active LOCAL (UNIX) domain sockets
Address Type Recv-Q Send-Q Inode Conn Refs Nextref Addr
8fb38071 stream 0 0 0 8fb3bbd1 0 0 /var/run/mDNSResponder
8fb3bbd1 stream 0 0 0 8fb38071 0 0
8fb3a659 stream 0 0 0 0 0 0
8fb386b1 stream 0 0 0 8fb38779 0 0 /var/run/mDNSResponder
8fb38779 stream 0 0 0 8fb386b1 0 0
8fb38909 stream 0 0 0 8fb3b659 0 0 /var/run/mDNSResponder
8fb3b659 stream 0 0 0 8fb38909 0 0
8fb389d1 stream 0 0 0 8fb394c1 0 0 /var/run/mDNSResponder
8fb394c1 stream 0 0 0 8fb389d1 0 0
8fb3adcl stream 0 0 0 8fb3acf9 0 0 /var/run/mDNSResponder
8fb3acf9 stream 0 0 0 8fb3adcl 0 0
8fb38e29 stream 0 0 0 8fb38cf1 0 0 /var/run/mDNSResponder
8fb38cf1 stream 0 0 0 8fb38e29 0 0
8fb3aaa1 stream 0 0 0 8fb3a9d9 0 0
8fb3a9d9 stream 0 0 0 8fb3aaa1 0 0
8fb38db9 stream 0 0 0 8fb38e81 0 0
8fb38e81 stream 0 0 0 8fb38db9 0 0
8fb38f49 stream 0 0 0 8fb39011 0 0
8fb39011 stream 0 0 0 8fb38f49 0 0
8fb390d9 stream 0 0 0 8fb3a911 0 0
8fb3a911 stream 0 0 0 8fb390d9 0 0
```



Herramientas del Perito – Rootear un Android

Cat /proc/partitions

Open terminal cmd (terminal2)

```
Adb forward tcp:8888 tcp:8888
```

```
nc 127.0.0.1 8888 > xxxx1.dd
```

```
nc 127.0.0.1 8888 > xxxx1.dd
```

Terminal1:

```
dd if=/dev/block/mmcblk0 | busybox nc -l -p 8888
```

va copiando

```
dd if=/dev/block/mmcblk0p1 | busybox nc -l -p 8888
```

```
ncat 127.0.0.1 8888 >particio0p1.dd
```

```
dd if=/dev/block/mmcblk0p2 | busybox nc -l -p 8888
```

```
ncat 127.0.0.1 8888 >particio0p2.dd
```

```
adb.exe pull /sdcard/forensics/20201027.1044 D:\PERICIA\SOFTWARE\platform-tools\particiones
```



Herramientas del Perito – Ubicar la IP

The screenshot shows a web browser window with the URL `iplocation.net/ip-lookup`. The page displays geolocation data for the IP address 17.57.144.36, which is identified as belonging to Apple Inc. in Cupertino, California. The browser's taskbar at the bottom shows several open windows, including a terminal window with the command `putty -64bit-0.75-L...gpg`.

enough? Please read geolocation accuracy info to learn why.
Do you have a problem with IP location lookup? Report a problem.

Geolocation data from IP2Location (Product: DB6, updated on 2021-5-1)

IP Address	Country	Region	City
17.57.144.36	United States of America	California	Cupertino

ISP

ISP	Organization	Latitude	Longitude
Apple Inc.	Not Available	37.3166	-122.0465

Geolocation data from ipinfo.io (Product: API, real-time)

IP Address	Country	Region	City
17.57.144.36	United States	California	Cupertino

ISP

ISP	Organization	Latitude	Longitude
Apple Inc.	Apple Inc. (apple.com)	37.3230	-122.0322

Geolocation data from DB-IP (Product: Full, 2021-5-1)

IP Address	Country	Region	City
17.57.144.36	United States	California	Cupertino

IP TOOLS

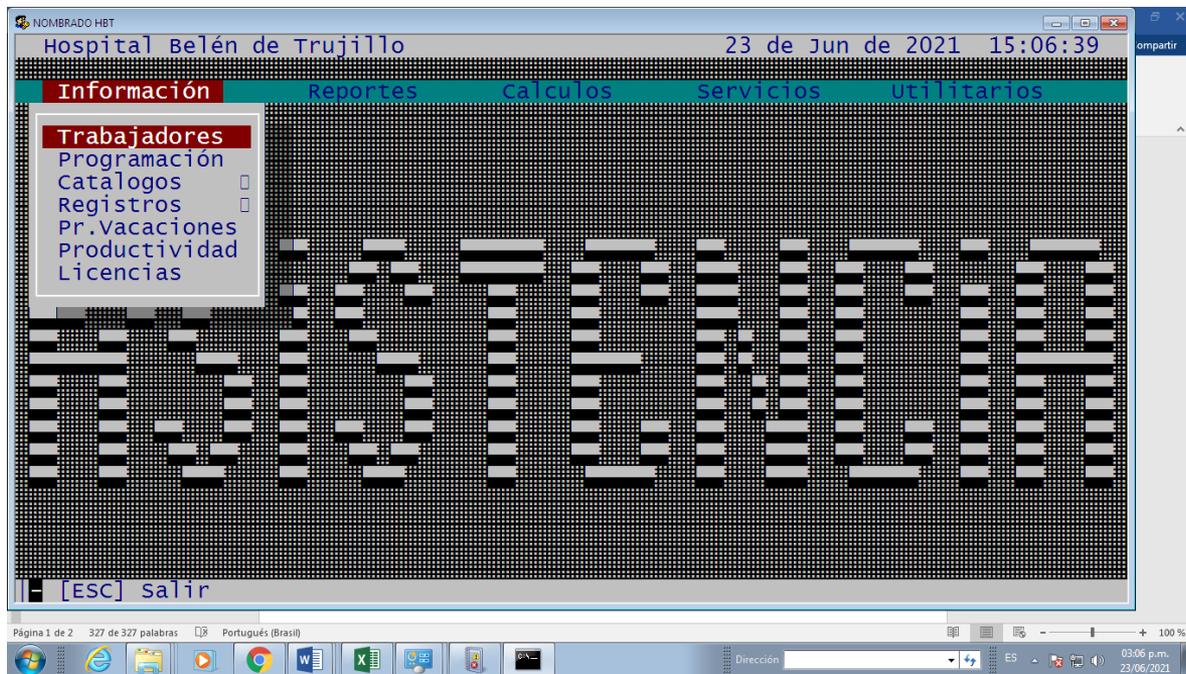
- Trace Email Source
- Verify Email Address
- Proxy Check
- Subnet Calculator
- IP-to-Integer Converter

DOMAIN TOOLS

- Who is Hosting a Website
- Alexa Traffic Rank Checker
- Domain Age Checker
- Domain DNS Lookup



Analizar aplicaciones Informáticas





Analizar aplicaciones Informáticas

s_FMV_0530 > Archivos > Archivos Jefferson > Backup Pases Calidad > STP > v6.16.20130424 > Instaladores > STP > Util

<input type="checkbox"/> Nombre	Fecha de modificación	Tipo	Tamaño
img	24/04/2013 16:28	Carpeta de archivos	
Anexo31bAjustes.aspx	27/11/2012 10:52	ASP.NET Server Pa...	37 KB
Anexo31bAjustesListar.aspx	27/11/2012 10:57	ASP.NET Server Pa...	22 KB
Anexo31bCierre.aspx	27/11/2012 10:15	ASP.NET Server Pa...	22 KB
<input checked="" type="checkbox"/> ExportarArchivoInterbank.aspx	08/02/2011 16:41	ASP.NET Server Pa...	9 KB
Formulario_Modal_Ajuste.aspx	30/11/2012 10:51	ASP.NET Server Pa...	4 KB
Formulario_Modal_Ajuste_E.aspx	30/11/2012 10:48	ASP.NET Server Pa...	5 KB
FormularioActualizar.aspx	04/02/2013 10:25	ASP.NET Server Pa...	59 KB
FormularioBuscarAct.aspx	13/08/2012 13:49	ASP.NET Server Pa...	19 KB
FormularioBuscarEstadoAct.aspx	16/01/2012 11:07	ASP.NET Server Pa...	19 KB
FormularioCaducidad.aspx	29/09/2009 16:44	ASP.NET Server Pa...	9 KB
FormularioEstadoAct.aspx	03/10/2011 10:42	ASP.NET Server Pa...	26 KB
FormularioTraslado.aspx	26/05/2011 11:22	ASP.NET Server Pa...	8 KB
FormularioVerAct.aspx	14/08/2012 15:34	ASP.NET Server Pa...	35 KB
GenerarArchivoSunarp.aspx	14/06/2011 17:10	ASP.NET Server Pa...	25 KB
GenerarSunarpListar.aspx	14/06/2011 10:56	ASP.NET Server Pa...	12 KB
ImportarArchivoInterbank.aspx	16/12/2009 13:01	ASP.NET Server Pa...	10 KB
UC_FormularioListarAnexo.ascx	19/10/2012 11:15	ASP.NET User Con...	15 KB
UC_FormularioListarAnexoE.ascx	19/10/2012 11:15	ASP.NET User Con...	15 KB



Analizar aplicaciones Informáticas

The image shows a screenshot of a Visual Basic code editor window. The main window displays the code for a module named 'Inicializar'. The code includes variable declarations, a function 'inicializar()', and two event procedures: 'cmdAceptar_Click()' and 'CARGA EL PERIODO ACTIVO'. A 'Guardar proyecto como' (Save Project As) dialog box is open in the foreground, showing the file name 'CAC_MATRIWEB.vbp' and the file type 'Proyecto (.vbp)'. The dialog also shows a file explorer view with folders like 'BACKUP', 'clases', 'Crear Instalador', 'FormatReport', 'formularios', and 'ib', and files like 'modulos', 'reportes', 'SCRIPTS', and 'CAC_MATRIWEB.vbp'.

```
Dim binLogeo As Boolean
Function inicializar() As Boolean
Me.Show vbModal
inicializar = binLogeo
End Function
Private Sub cmdAceptar_Click()
If Trim(txtUsuario.Text) = "" Then
MsgBox "Debe ingresar el usuario", vbInformation, "ACCESO"
txtUsuario.SetFocus
Exit Sub
End If
If Trim(txtClave.Text) = "" Then
MsgBox "Debe ingresar la clave", vbInformation, "ACCESO"
txtClave.SetFocus
Exit Sub
End If
Dim objUser As New cls_Usuario
Dim bUser As New bea_PERSONAL
Dim rsU As ADODB.Recordset
Dim strPerfil As String

'CARGA EL PERIODO ACTIVO
Dim objAdm As New cls_Administrador
Dim rsAdm As ADODB.Recordset
objAdm.setCONEXION PstrConexion
Set rsAdm = objAdm.obtPeriodoCargaActivo
If rsAdm.RecordCount > 0 Then
'SI ES MAYOR A 1
If rsAdm.RecordCount > 1 Then
```



Informe Pericial

VICTOR BARRIENTOS RODRIGUEZ

Perito Judicial, Perito Forense e Ingeniero de Sistemas - CIP
Nómina de Peritos Judiciales – REPEJ. Corte Superior de Justicia de Lima Sur y Lima Este

VICTOR BARRIENTOS RODRIGUEZ

Perito Judicial, Perito Forense e Ingeniero de Sistemas - CIP
Nómina de Peritos Judiciales – REPEJ. Corte Superior de Justicia de Lima Sur y Lima Este

OPERITAJE INFORMATICO DE PARTE: Comprobación del borrado de información de una computadora portátil asignada a un ex trabajador de la Compañía xxxx Consulting S. A.

Emitido por:
VICTOR SAUL BARRIENTOS RODRIGUEZ
INGENIERO DE SISTEMAS
CIP Nro. 060996 – Perito Judicial

28 de Septiembre del 2,020

PERITO JUDICIAL, NOMINA DE PERITOS JUDICIALES
REPEJ Nro. 30-00070-2019, REVALIDADO AL PERIODO 2019-2020 – DE LA CORTE
SUPERIOR DE JUSTICIA DE LIMA SUR.

PERITO - MIEMBRO ACTIVO EN EL CENTRO DE PERITAJE "GUILLERMO VAUDENAY
REYES" DEL CONSEJO DEPARTAMENTAL DE LIMA DEL COLEGIO DE INGENIEROS DEL
PERU

Domicilio Legal: Nicolas de Pierola 611 dpto 401 Lima Cercado
Teléfono Móvil Nro. 942818949
e-mail: victor.barrientosr@cjp.org.pe

CONTENIDO

1.	RESPONSABLE DE LA PERICIA	3
2.	SOLICITANTE	3
3.	ACERCA DE EMPRESA A	3
4.	OBJETO DE LA PERICIA, ALCANCE Y DESCRIPCIÓN DEL SERVICIO	3
4.1.	OBJETIVO	3
4.2.	ALCANCE Y DESCRIPCIÓN DEL SERVICIO DE PERITAJE	3
5.	ANTECEDENTES	4
6.	METODOLOGÍA	4
7.	HERRAMIENTAS A UTILIZAR	5
8.	FUENTES	5
9.	INSPECCIÓN FÍSICA	5
10.	ANÁLISIS	5
11.	DICTAMEN PERICIAL	6
ANEXOS		
	GLOSARIO DE TÉRMINOS	9
	ANEXO 01: CERTIFICADO DE HABILIDAD	10
	ANEXO 02: CARNET DEL PERITO JUDICIAL	12
	ANEXO 03: ADQUISICIÓN DEL DISCO DURO	14
	ANEXO 04: ANÁLISIS DE ARTEFACTO DE DISCO DURO NTFS	17
	ANEXO 05: ANÁLISIS DEL ARTEFACTO DE REGISTER Y USUARIOS	19
	ANEXO 06: ANÁLISIS DEL ARTEFACTO CORREO ELECTRÓNICO	27
	ANEXO 07: ANÁLISIS DEL ARTEFACTO HISTORY Y ARCHIVOS	31
	ANEXO 08: ANÁLISIS DEL ARTEFACTO ONEDRIVE	33
	ANEXO 09: ANÁLISIS DE ARTEFACTOS DEL RECICLY.BIN	35
	ANEXO 10: IDENTIFICACIÓN DE ARCHIVOS BORRADOS DE MAYO A JULIO DEL 2020	40
	ANEXO 11: DIFERENCIA DE ARCHIVOS DE ONE DRIVE Y ARCHIVOS DEL DISCO DURO	42
	ANEXO 12: RELACIÓN DE ARCHIVOS IDENTIFICADOS QUE HAN SIDO BORRADOS	44
	ANEXO 13: CAPTURA DE IMÁGENES DEL ONEDRIVE DE ARCHIVOS BORRADOS	44

Como se postula a Perito

1. Colegio de Ingenieros
2. Poder Judicial, mediante convocatorias.



google.com/search?q=perito+poder+judicial&oq=perito+poder+judicial&aqs=chrome..69i57j0i512j0i22i30i18.3558j0j7&sc

perito poder judicial

<https://www.pj.gob.pe> > wps > wcm > connect > C... PDF

CONVOCATORIA PERITOS -2022.I 1 - Poder Judicial

10 dic 2021 — -P-CSJAN/PJ, convoca al proceso de Evaluación de **Peritos Judiciales** para el periodo 2022 en el Distrito Judicial de Ancash. I.- OBJETO DE LA ...

Otras personas también buscaron

- lista de peritos del poder judicial 2022
- convocatoria peritos judiciales 2022
- oficina de peritos del poder judicial
- repej poder judicial 2022
- repej poder judicial
- peritos judiciales arequipa 2022

<https://scc.pj.gob.pe> > wps > wcm > connect > CO... PDF

CONVOCATORIA+PERITOS+2023+2024.pdf - Poder Judicial

27 oct 2022 — SELECCIÓN DE **PERITOS JUDICIALES** DE LA CORTE SUPERIOR DE JUSTICIA DE ANCASH. PARA EL AÑO **JUDICIAL 2023 - 2024**. Plaza de Armas S/N Tercer...

<https://csjarequipa.pj.gob.pe> > main > nomina-de-peritos

Nomina de Peritos Judiciales - Corte Superior de Justicia de ...

Nomina de **Peritos Judiciales REPEJ - 2021**. RESOLUCION ADMINISTRATIVA N° 000272-2021-P-CSJAR-PJ. Central Telefónica (054) 382520. De 8:00 a 13:00 hrs.



Recomendaciones para evitar el Ataque

- ✓ Actualice regularmente su sistema operativo
- ✓ Instale un Antivirus y
- ✓ Instale un Firewall
- ✓ Instalar en su equipo algún tipo de software anti-spyware
- ✓ Utilice contraseñas seguras
- ✓ Navegue por páginas web seguras y de confianza.
- ✓ Sea cuidadoso al utilizar programas de acceso remoto
- ✓ Ponga especial atención en el tratamiento de su correo electrónico
- ✓ No abra mensajes de correo de remitentes desconocidos.
- ✓ Desconfíe de aquellos e-mails en los que entidades bancarias,
- ✓ No propague aquellos mensajes de correo con contenido dudoso
- ✓ En general, es fundamental estar al día de la aparición de nuevas técnicas que amenazan la seguridad de su equipo informático, para tratar de evitarlas o de aplicar la solución más efectiva posible.



**COLEGIO DE
INGENIEROS
DEL PERU**

Preguntas?