Fortbildungskatalog der Landespolizei Schleswig-Holstein

OZ 4000-4999 - Informationsmanagement

4000 – Anlassbezogene Fortbildung PD AFB

Zielgruppe	
Lehrinhalte	Aus Initiative des Fachbereiches IV werden sach- und themenbezogene Veranstaltungen zur Ausbildung/Fortbildung ausgeschrieben. Die Konkretisierung erfolgt mit der Ausschreibung Siehe Seminar Nr. 4001.
Lernziele	
Dauer	
Besondere Hinweise	

Zurück zum Inhalt

4035 – Merlin – Wahrnehmen von Führungsaufgaben

Zielgruppe	Führungskräfte, deren Mitarbeiterinnen und Mitarbeiter das Verfahren Merlin im Rahmen der Sachbearbeitung einsetzen oder zukünftig einsetzen sollen.
Lehrinhalte	• Philosophie des Verfahrens Merlin • Einsatzmöglichkeiten • Voraussetzungen für den Einsatz von Merlin im Rahmen eines Ermittlungsverfahrens • Verantwortung von Führungskräften in der Informationssicherheit • Abhängigkeiten zwischen Datenqualität und Analyse • Möglichkeiten der länderübergreifenden Ermittlungsunterstützung durch Merlin • Gewinnen von operativen und strategischen Führungsinformationen
Lernziele	Die Teilnehmerinnen und Teilnehmer kennen nach Abschluss des Seminars die Möglichkeiten und Grenzen des Verfahrens Merlin. Sie sind in der Lage, operative und strategische Informationen mit Hilfe des Verfahrens Merlin zu gewinnen und für ihre Führungsaufgaben zu nutzen. Die Teilnehmenden nehmen die Gewährleistung von Informationssicherheit als eine Führungsaufgabe war und kennen die Bedeutung der Datenqualität für das Ermittlungsverfahren.
Dauer	1 Tag
Besondere Hinweise	Die Teilnahme an dem Seminar führt zur Erteilung der Rolle 06 – Führungskräfte.

Zurück zum Inhalt

4050 –Vorgangsbearbeitung @rtus zur Wahrnehmung von Führungsaufgaben

Zielgruppe	Leiterinnen und Leiter und Vertreterinnen und Vertreter von @rtus-Dienststellen der Landespolizei Schleswig-Holstein
Lehrinhalte	• Verantwortung von Führungskräften in der Informationssicherheit • Philosophie Vorgangsbearbeitungssystem (VBS) @rtus • Datenverarbeitungsrechtliche Bestimmungen • Berechtigungskonzept unter @rtus • Funktions- und Datenberechtigungen im VBS @rtus • Dienst- und fachaufsichtliche Belange • Datenqualität im VBS @rtus im Hinblick auf Auswertung/Analyse
Lernziele	Die Leiterinnen und Leiter und Vertreterinnen und Vertreter sollen die Vorgangsbearbeitung mit ihren Möglichkeiten als IT-Fachanwendung kennen und für die eigene Dienststelle die erforderlichen, organisatorischen Maßnahmen treffen können, um die rechtlich einwandfreie Datenverarbeitung und effektive Aufgabenwahrnehmung im VBS @rtus zu gewährleisten. Die Teilnehmerinnen und Teilnehmer wissen, dass es zur Wahrnehmung ihrer Führungsaufgaben gehört, die Mitarbeiterinnen und Mitarbeiter über getroffene lokale Regelungen der Informationssicherheit sach- und zeitgerecht zu informieren.
Dauer	1 Tag
Besondere Hinweise	Voraussetzungen für die Seminarteilnahme: • Eigenschaft der Dienststellenleitung/Vertretung auf einer @rtus-Dienststelle • Einrichtung auf der Dienststelle im @rtus-Übungsbetrieb als Dienststellenleiter/Dienststellenleiter-Vertreter

Zurück zum Inhalt

4052 – @rtus-Recherche für Dienststellenleitungen

Zielgruppe	Leiterinnen und Leiter und Vertreterinnen und Vertreter von @rtus-Dienststellen der Landespolizei Schleswig-Holstein, die im Rahmen ihrer Aufgaben die Mitarbeiterinnen und Mitarbeiter der eigenen Dienststelle für die @rtus-Recherche einrichten und die @rtus-Recherche anwenden
Lehrinhalte	• Grundlagen der Informationssicherheit • Unterschiede @rtus Suche und @rtus-Recherche • Horizontale Blockverbunde/Nutzergruppen • Berechtigungskonzept unter @rtus und Führungsverantwortung • Datenverarbeitungsrechtliche Bestimmungen/Belehrung • Vorgangsstatus und Datenumfang • Datenqualität im Vorgangsbearbeitungssystem (VBS) @rtus im Hinblick auf Auswertung/Analyse und Qualitätssicherung • Arbeiten mit der Recherche
Lernziele	Die Leiterinnen und Leiter und Vertreterinnen und Vertreter sollen unter Berücksichtigung der rechtlichen Bestimmungen ihre Mitarbeiterinnen und Mitarbeiter für die @rtus-Recherche einrichten und Maßnahmen zur Verbesserung der Datenqualität treffen können. Sie sollen das Berechtigungskonzept anwenden und mit der Recherche arbeiten können.
Dauer	1 Tag
Besondere Hinweise	Voraussetzungen für die Seminarteilnahme: • Eigenschaft der Dienststellenleitung/Vertretung auf einer @rtus-Dienststelle und die Teilnahme am Seminar OZ 4050 (OZ 456) • Einrichtung auf der Dienststelle im @rtus-Übungsbetrieb als Dienststellenleiter/Dienststellenleiter-Vertreter

Zurück zum Inhalt

4053 – Wahrnehmung der Führungsaufgabe Dienst- und Fachaufsicht in @rtus

Zielgruppe	Dienstgruppenleiterinnen/Dienstgruppenleiter, Sachgebietsleiterinnen/Sachgebietsleiter, Leiterinnen/Leiter und die jeweiligen Vertreterinnen/Vertreter von @rtus Dienststellen der Landespolizei Schleswig-Holstein
Lehrinhalte	Verantwortung von Führungskräften • Informationssicherheit • Philosophie Vorgangsbearbeitungssystem (VBS) @rtus • Datenverarbeitungsrechtliche Bestimmungen • Datenqualität im VBS @rtus im Hinblick auf die Bedienung weiterer Dienste • Wahrnehmung der Dienst- und Fachaufsicht in @rtus im Rahmen der Ersterfassung ○ Umsetzung der Erfassungsrichtlinien • Wahrnehmung der Dienst- und Fachaufsicht in @rtus im Rahmen der Endbearbeitung • Aktuelle Themen zur Wahrnehmung der Dienst- und Fachaufsicht in @rtus
Lernziele	Die Lehrgangsteilnehmerinnen und Lehrgangsteilnehmer sollen die Belange der Dienst- und Fachaufsicht kennen. In ihrem Arbeitsbereich sollen sie die Aufgabe der Dienst- und Fachaufsicht in ihrer Führungsfunktion verantwortungsvoll wahrnehmen. Die Teilnehmerinnen und Teilnehmer wissen, dass es zur Wahrnehmung ihrer Führungsaufgaben gehört, die Mitarbeiterinnen und Mitarbeiter über getroffene Regelungen der Datenverarbeitung zeitnah und sachgerecht zu informieren. Sie beachten die Grundlagen der Informationssicherheit und kennen die Bedeutung der Datenqualität für den Informationsverarbeitungsprozess.
Dauer	1 Tag
Besondere Hinweise	Voraussetzung ist eine persönliche Zugangsberechtigung +1-Arbeitsplatz Polizei.

Zurück zum Inhalt

4122 – Anwender Digitalfunk BOS

Zielgruppe	Alle Mitarbeiterinnen und Mitarbeiter der Landespolizei Schleswig-Holstein, die den Digitalfunk BOS praktisch anwenden und bereits für den Einsatz des analogen BOS-Funks im Rahmen der Ausbildung (mD/gD) qualifiziert wurden.
Lehrinhalte	• Informationssicherheit und Datenschutz in Bezug auf den Digitalfunk BOS • Möglichkeiten durch den Digitalfunk in der polizeilichen Einsatzverwendung • Veränderung von Arbeitsweisen und Taktik in der polizeilichen Praxis • Rufgruppensystematiken • Zusammenarbeit mit anderen Länderpolizeien und BOS • Einsatz der Endgeräte • Verwendung von Statusmeldungen • Gateway- und Repeaterbetrieb • Praktische Übungen am Gerät
Lernziele	Die Lehrgangsteilnehmerinnen und Lehrgangsteilnehmer sollen die Eigenschaften und die Funktionalitäten der Endgeräte im Digitalfunk BOS kennen und diese bei der Bewältigung polizeilicher Einsatzlagen handlungssicher, taktisch richtig und rechtlich einwandfrei einsetzen können. Weiterhin sollen die Teilnehmerinnen und Teilnehmer die themenspezifischen Grundsätze der Informationssicherheit und die datenschutzrechtlichen Hintergründe im Umgang mit dem Digitalfunk BOS kennen.
Dauer	½ Tag
Besondere Hinweise	Die Teilnahme an dem Seminar OZ 4122 ist gemäß Betriebskonzept Digitalfunk BOS verpflichtend. Dieses Seminar ist lediglich eine Update-Schulung von Analog- auf Digitalfunk BOS. Für alle anderen Zielgruppen, die nicht in der Ausbildung für den BOS-Funk qualifiziert wurden, wird ab Mai 2016 ein gesondertes zweitägiges Seminar (Digitalfunk BOS für Beschäftigte der Landespolizei) konzipiert und regelmäßig angeboten.

Zurück zum Inhalt

4123 – Digitale Sprechfunkkommunikation für Beschäftigte der Landespolizei (TVL)

Zielgruppe	Beschäftigte der Landespolizei (TVL), die in ihrem Aufgabenbereich den Digitalfunk BOS einsetzen sollen.
Lehrinhalte	• Grundlagen für den Einsatz von Sprechfunkgeräten • Abwicklung des Sprechfunkverkehrs nach PDV 810.2 • Physikalische Grundlagen der Funkkommunikation • Struktur des Digitalfunknetzes in SH und dem Bund • Funkmeldesysteme, GPS und Statusmeldungen • Rufnamensystematik und Begrifflichkeiten • Informationssicherheit und Datenschutz • Bedienung der Funkgeräte MTP 850 und MTM 800 FuG • Taktische Anwendungsmöglichkeiten • Informationsmanagement mit der Regionalleitstelle (RLS) • Praktische Übungen mit den Endgeräten
Lernziele	Die Teilnehmerinnen und Teilnehmer sollen die Grundlagen der Sprechfunkkommunikation bei der Landespolizei kennen. Sie sollen die Fertigkeiten zur sicheren Handhabung der verwendeten Endgeräte für den Digitalfunk BOS erlernen. Sie sollen die Kommunikation nach den Vorgaben der PDV 810.2 beherrschen. Sie sollen die taktische Bedeutung des Digitalfunks BOS verstehen und regelrecht an der Sprechfunkkommunikation teilnehmen können. Sie sollen die im Zusammenhang mit dem Digitalfunk BOS bestehenden Datenschutzbestimmungen kennen und die Möglichkeiten der sicheren Informationsverarbeitung nach den Grundsätzen der Informationssicherheit beherrschen. Sie sollen die Rolle der RLS als zentrale Kommunikationskomponente für die Einsatzbewältigung kennen.
Dauer	1 ½ Tag
Besondere Hinweise	Nur für Mitarbeiterinnen und Mitarbeiter der Landespolizei, die bisher noch nicht für die Sprechfunkkommunikation der BOS qualifiziert wurden.

Zurück zum Inhalt

4170 – Produktorientierte Arbeitszeiterfassung (PA)/Flexible Personaleinsatzplanung (FP) mit SP-EXPERT – Anwenderinnen und Anwender

Zielgruppe	Alle Mitarbeiterinnen und Mitarbeiter der Landespolizei Schleswig-Holstein, die Zugang zu einem LSK-Arbeitsplatz haben.
Lehrinhalte	• Grundlagen der Informationssicherheit • Passwortverfahren/Kennwortrichtlinie • Anmelden am Citrix-Client und an SP-EXPERT • Ansichten der Anwenderinnen und Anwender • Wunschdienste eintragen und übernehmen • Sinn und Zweck der Produkterfassung • Anmeldung am Modul Produkterfassung • Datenbankkollisionen • Auswahl des Erfassungsdatums • Die eigene Produkterfassungskonfiguration • Praktisches Arbeiten mit der Erfassungsmaske • Mitarbeiter mit F-Berechtigungen und ihre Möglichkeiten
Lernziele	Die Anwenderinnen und Anwender sollen unter rechtskonformer Anwendung des Arbeitszeitrechts und dazu ergangener Rechtsprechung die Software SP-EXPERT zur flexiblen Personaleinsatzplanung (FP) und Produktorientierten Arbeitszeiterfassung unter Berücksichtigung ihrer Kontenstände planen und als Produkte erfassen können. Sie kennen die Grundlagen der Informationssicherheit und sind sich der Bedeutung der Datenqualität für den Informationsverarbeitungsprozess bewusst, sind über die landeseinheitlichen Regelungen zur Informationssicherheit informiert und wissen, wo sie zu Fragen Informationen erhalten können (IT-Regelwerk im Intrapol; CheckIT).
Dauer	½ Tag (Für nicht geübte IT- Anwenderinnen und Anwender wird dieser Lehrgang auch ganztägig angeboten.)
Besondere Hinweise	Voraussetzung ist eine eigene LSK-Zugangskennung. Beschult wird standardmäßig mit der aktuellen Programmversion.

Zurück zum Inhalt

4171 – Produktorientierte Arbeitszeiterfassung (PA)/Flexible Personaleinsatzplanung (FP) mit SP-EXPERT für Dienstplanerinnen und Dienstplaner

Zielgruppe	Mitarbeiterinnen und Mitarbeiter der Landespolizei Schleswig-Holstein, die mit der Dienstplanung ihrer Dienststelle beauftragt sind.
Lehrinhalte	• Grundlagen, Verantwortung und Aufgaben in der Informationssicherheit • Passwortverfahren/Kennwortrichtlinie • Anmelden am Citrix-Client und an SP-EXPERT • Ansichten und Möglichkeiten der Anwenderinnen und Anwender • Produkterfassung • MA mit F-Berechtigungen und ihre Möglichkeiten • Planungsphasen und zeitliche Vorgaben • Fenstereinstellungen und Ansichten des Monatsplanes • Durchführung der Vorplanung • Dienstplan genehmigen • IST-Planung • Abwesenheiten und Regelverletzungen • Buchungen anzeigen und nachvollziehen • Mitarbeiterwechsel • Makros mit Erläuterungen • Bearbeitung von Stammdaten • Berichtswesen
Lernziele	Die Dienstplanerinnen und Dienstplaner sollen mit der Software SP-EXPERT zur flexiblen Personaleinsatzplanung (FP) und Produktorientierten Arbeitszeiterfassung unter rechtskonformer Anwendung des Arbeitszeitrechts und dazu ergangener Rechtsprechung die Arbeitszeit der Mitarbeiterinnen und Mitarbeiter ihrer Dienststelle planen, alle Kontenstände überblicken, die Produkterfassung in den Fristen kontrollieren sowie den Datenabfluss an das LBesA durchführen können. Darüber hinaus sollen sie andere Nutzerinnen und Nutzer ihrer Dienststelle unterstützen können und über die Möglichkeiten des Systems für die Wahrnehmung von Führungsaufgaben im Rahmen der Dienstplanung informiert sein. Sie sollen die Grundlagen sowie die Verantwortung und Aufgaben von Führungskräften in der Informationssicherheit kennen und für ihren Arbeitsbereich anwenden können.
Dauer	4 Tage

Besondere Hinweise	Voraussetzung sind eine eigene LSK-Zugangskennung und Erfahrungen in der Dienstplanung. Die Themen der Lehrgänge OZ: 4170 (0470) und OZ: 4072 (OZ 0472) sind Bestandteil dieses Lehrgangs. Es findet eine Erfolgskontrolle statt, die über die Zuweisung der Planer-Berechtigung in SP-EXPERT entscheidet. Die Möglichkeit einer einmaligen Nachprüfung innerhalb von 4 Wochen ist vorgesehen.

Zurück zum Inhalt

4173 – Produktorientierte Arbeitszeiterfassung (PA)/Flexible Personaleinsatzplanung (FP) mit SP-EXPERT für Funktionswechsler (F-Kennung)

Zielgruppe	Leiterinnen und Leiter von Polizeidienststellen in Schleswig-Holstein sowie Mitarbeiterinnen und Mitarbeiter mit Führungsaufgaben in Organisationseinheiten dieser Dienststellen (z. B. Truppführer, DGL), die diese Aufgabe neu übernommen haben.
Lehrinhalte	• Grundlagen der Informationssicherheit • Synopse der Benutzerrechte • Monatsplanansichten der F-Kennungen • Dienstplanung/-änderung im genehmigten Plan mit der F-Kennung • Buchungen im genehmigten Plan • Arbeiten mit Schichtdienstbesetzungsstärken • Makros • Ziele der Produkterfassung • Nutzung des Moduls Produkterfassung mit der F-Kennung • Wahrnehmung der Dienstaufsicht • Abgrenzung zu Planeraufgaben und -möglichkeiten • Arbeitszeit- und datenschutzrechtliche Regelungen/Bestimmungen
Lernziele	Mitarbeiterinnen und Mitarbeiter mit einer F-Kennung in SP-EXPERT sollen die Dienstplanung im genehmigten Plan durchführen sowie ihre Dienstaufsicht im Rahmen der flexiblen Personaleinsatzplanung und produktorientierten Arbeitszeiterfassung für ihre Mitarbeitergruppe bzw. Organisationseinheit wahrnehmen können. Sie sollen die Grundlagen der Informationssicherheit und die zum Thema Arbeitszeit in Beziehung stehenden Erlasse kennen.
Dauer	1 Tag
Besondere Hinweise	Voraussetzungen sind eine persönliche Zugangsberechtigung +1-Arbeitsplatz Polizei. Die Teilnahme am OZ 4170 ist nicht erforderlich.

Zurück zum Inhalt

4174 – Umgang mit Mehrarbeit bei Tarifbeschäftigten in SP-EXPERT

Zielgruppe	Dienstvorgesetzte und Planer in SP-Expert, die in ihrer Aufgabenwahrnehmung Tarifbeschäftigte betreuen.
Lehrinhalte	• Voraussetzungen für Eintragungen, die systemseitig zu finanziellen Zulagen und zu (vergütbarer) Mehrarbeit führen • Voraussetzungen für Eintragungen, die nicht automatisch zum Erwerb vergütbarer Mehrarbeit führen • Korrekte Anwendung von „B-Makros“ • Auswirkungen in der Planungsansicht (Regelverletzungen zur Unterstützung der Fürsorge- und Aufsichtspflicht) • Abbau von Mehrarbeit • Buchungen • Planer-Bericht „Beschäftigte“
Lernziele	Mitarbeiterinnen und Mitarbeiter mit einer F-Kennung oder Planer, in deren Zuständigkeitsbereich Tarifpersonal beschäftigt ist sollen erkennen, unter welchen Umständen vor dem Hintergrund des jeweiligen Arbeitsvertrages Mehrarbeit entsteht. Weiterhin erfassen die Teilnehmenden die Bestimmungen aus dem TV-L und den landesinternen Regelungen zum fristgerechten Abbau von Mehrarbeit.
Dauer	½ Tag
Besondere Hinweise	Voraussetzung ist eine eigene LSK-Zugangskennung und die vorangegangene Teilnahme am OZ 4171 (0471), 4072 (0472) oder 4173 (0473).

Zurück zum Inhalt

4180 – EPSweb – Einsatzprotokollierung und Lagedarstellung bei besonderen Einsatzlagen

Zielgruppe	Alle Mitarbeiterinnen und Mitarbeiter der Landespolizei Schleswig-Holstein, die eine Tätigkeit bei einer Regionalleitstelle, einem Führungsstab und zugleich in einer besonderen Aufbauorganisation versehen sollen.
Lehrinhalte	• Das White-Board-Prinzip • Benutzerverwaltung • Anlage und Verwaltung von Einsätzen • Berechtigungs- und Dienststellenstruktur • Einsatzabläufe • Protokollerfassung und Protokollbearbeitung • Informationssteuerung • Datenaustausch • Verwaltung von Anlagen • Arbeiten in mehreren Einsätzen • Erstellung grafischer Befehle
Lernziele	Die Teilnehmerinnen und Teilnehmer sollen für ihre Tätigkeit in einem Führungsstab zur Bewältigung von besonderen Einsatzlagen das Verfahren EPSweb zur Lageprotokollierung und Einsatzdokumentation beherrschen. Sie sollen die Möglichkeiten des Verfahrens EPSweb für die Einsatzorganisation und die Informationsgewinnung sowie Informationssteuerung kennen.
Dauer	1 Tag
Besondere Hinweise	Kenntnisse über Aufbau und Arbeitsweise eines Führungsstabes sind wünschenswert.

Zurück zum Inhalt

4261 – +1-Zugangslehrgang

Zielgruppe	Mitarbeiterinnen und Mitarbeiter der Landespolizei, die im Rahmen ihrer dienstlichen Aufgaben erstmalig den polizeilichen +1-Arbeitsplatz mit Vollzugriff nutzen und ihre Dienstzeiten mit SP-EXPERT verwalten sollen.
Lehrinhalte	• Grundlagen der Informationssicherheit • Datenverarbeitungsrechtliche Bestimmungen • Tarifrecht und Ergonomie • Passwortverfahren • Desktop des polizeilichen +1-Arbeitsplatzes • Gestaltung des elektronischen Arbeitsplatzes, Ablagestrukturen • Übersicht über die Office-Produkte auf dem Standardarbeitsplatz, Grundlagen der Bürokommunikation und Terminverwaltung • Personalmanagement mit SP-EXPERT für AnwenderInnen
Lernziele	Die Anwenderinnen und Anwender sollen unter Berücksichtigung der datenverarbeitungsrechtlichen Bestimmungen die Grundfunktionen des polizeilichen +1-Arbeitsplatzes kennen und das Passwortverfahren sicher anwenden können. Zusätzlich sollen sie die Bürokommunikation, speziell die Kommunikation per E-Mail gemäß E-Mail-Richtlinie, und die Terminverwaltung vornehmen können. Die Teilnehmerinnen und Teilnehmer sind über die getroffenen landeseinheitlichen Regelungen zur Informationssicherheit informiert und wissen, wo sie zu Fragen/Informationen erhalten können (IT-Regelwerke im Intrapol). Ferner erhalten sie die Einweisung im Personalmanagementsystem SP-EXPERT als Anwender mit der entsprechenden Zugangsberechtigung.
Dauer	1 Tag
Besondere Hinweise	

Zurück zum Inhalt

4270 – Owi21

Zielgruppe	Alle Mitarbeiterinnen und Mitarbeiter der Landespolizei, die mit der selbständigen, elektronischen Erfassung von Verkehrsordnungswidrigkeiten beauftragt sind.
Lehrinhalte	• Grundlagen der Informationssicherheit • Zuteilung der Berechtigung zum IT-Verfahren Owi21 • Rechtsgrundlagen für die Speicherung personenbezogener Daten • Richtlinien für die Aufnahme und Bearbeitung von Ordnungswidrigkeiten im Straßenverkehr • Eingabe von Datensätzen mit und ohne Personalien • Änderung von Datensätzen • Veränderung und Löschung von Fällen
Lernziele	Selbständige und rechtlich einwandfreie Erfassung von Verkehrsordnungswidrigkeiten im IT-Verfahren Owi21
Dauer	½ Tag
Besondere Hinweise	Voraussetzung ist eine persönliche Zugangsberechtigung +1-Arbeitsplatz Polizei.

Zurück zum Inhalt

4280 – LSK Anwenderbetreuer/innen -Administration-

Zielgruppe	Mitarbeiterinnen und Mitarbeiter der Landespolizei, die im Rahmen ihrer Aufgaben für die Anwenderbetreuung eingesetzt werden oder für diese Aufgabe vorgesehen sind.
Lehrinhalte	• Grundlagen der Informationssicherheit und des Datenschutzes • IT-Betriebskonzept (Grundlagen/Regelungswerk/Formularwesen) • Hardwareinstallation (+1-Arbeitsplatz Polizei und Cybercrime) sowie Geräteverwaltung (GvZ) • Netzwerk-Infrastruktur im Bereich des +1-Arbeitsplatzes Polizei • Funktionen, Aufbau und Struktur des Active-Directory • Ablagestrukturen • Rechte und Berechtigungen in den Gruppenablagen • Datensicherungskonzept (+1-Arbeitsplatz Polizei und Cybercrime) • Störungsbeseitigung (Rollen und Arbeitsmittel der beteiligten Fachdienste) • Zusammenarbeit mit den Fachdienststellen des LPA 2
Lernziele	Die Anwenderbetreuerinnen und Anwenderbetreuer sollen die Nutzer der polizeilichen Fachanwendungen auf den Dienststellen bei der Arbeit im System unterstützen und beraten können. Sie sollen daraus entstehende Probleme (z. B. Schulungsbedarfe) analysieren und der Dienststellenleitung melden. Sie sollen ferner in der Lage sein, eine Gruppenablagestruktur mit entsprechenden Berechtigungen im Filesystem aufzubauen bzw. zu pflegen. Die Teilnehmerinnen und Teilnehmer sind über die landeseinheitlichen Regelungen zur Informationssicherheit informiert und kennen die Fundstellen des IT-Regelwerks im Intrapol.
Dauer	3 Tage
Besondere Hinweise	Voraussetzung ist eine persönliche Zugangsberechtigung +1-Arbeitsplatz Polizei.

Zurück zum Inhalt

4310 – Vorgangsbearbeitung @rtus-Anwenderbetreuer/innen für LSK-Anwenderbetreuer/innen

Zielgruppe	Anwenderbetreuerinnen und Anwenderbetreuer von LSK-Dienststellen der Landespolizei, die das Vorgangsbearbeitungssystem (VBS) @rtus nutzen und im Rahmen ihrer Aufgaben für die Anwenderbetreuung der VBS @rtus eingesetzt werden.

Lehrinhalte	• Grundlagen der Informationssicherheit
	• @rtus-Philosophie
	• Überblick @rtus
	  ○ VBS @rtus
	  ○ @rtus-Forms
	  ○ @rtus Recherche
	• datenverarbeitungsrechtliche Bestimmungen
	• @rtus Berechtigungskonzept
	• Funktions- und Datenberechtigungen
	• Vorgangsbearbeitung in der Rolle Sachbearbeitung
	• elektronische Sachfahndung
	• INPOL-Merkblatt und elektronische Kriminalakte
	• polizeiliche Kriminalstatistik
	• Verwaltung/Registratur und Organisation.
	Datenqualität im VBS @rtus im Hinblick auf Auswertung/Analyse

Lernziele	Die Anwenderbetreuer/innen sollen unter Berücksichtigung der datenverarbeitungsrechtlichen Bestimmungen die Grundfunktionen der polizeilichen Vorgangsbearbeitung zur Bewältigung polizeilicher Aufgabenstellungen anwenden können. Sie sollen die Möglichkeiten des VBS @rtus kennen, um die Dienststellenleitung bei den erforderlichen, organisatorischen Maßnahmen zu unterstützen. Ferner sollen sie Anwenderinnen und Anwender bei der polizeilichen Vorgangsbearbeitung mit dem VBS @rtus unterstützen. Sie beachten die Grundlagen der Informationssicherheit und kennen die Bedeutung der Datenqualität für den Informationsverarbeitungsprozess.
Dauer	2 Tage
Besondere Hinweise	Voraussetzung ist die Eigenschaft der Anwenderbetreuung auf einer LSK-Dienststelle.

Zurück zum Inhalt

4320 – Vorgangsbearbeitung @rtus -Sachbearbeitung-

Zielgruppe	Mitarbeiterinnen und Mitarbeiter der Landespolizei, die im Rahmen ihrer dienstlichen Aufgaben erstmalig die polizeiliche Vorgangsbearbeitung als Sachbearbeiter auf einem LSK-Arbeitsplatz nutzen sollen.

Lehrinhalte	• Grundlagen der Informationssicherheit
	• Datenverarbeitungsrechtliche Bestimmungen
	• @rtus-Philosophie
	• Arbeiten mit den polizeilichen Vordrucken im Vorgangsbearbeitungssystem (VBS) @rtus und in @rtus forms
	• Erfassen von Objekten
	  ○ im Dokument
	  ○ strukturiert
	• Bearbeiten von Ersuchen
	• elektronische Sachfahndung
	• INPOL-Merkblatt und elektronische Kriminalakte
	• PIAV Meldebogen
	• Visualisierung
	• Aufzeichnungen
	• polizeiliche Kriminalstatistik
	• Vorgangsabgabe vorbereiten
	• @rtus-Recherche
	Datenqualität im VBS @rtus im Hinblick auf Auswertung/Analyse

Lernziele	Die Anwenderinnen und Anwender sollen unter Berücksichtigung der datenverarbeitungsrechtlichen Bestimmungen die Grundfunktionen der polizeilichen Vorgangsbearbeitung zur Bewältigung polizeilicher Aufgabenstellungen als Sachbearbeiter anwenden können. Sie beachten die Grundlagen der Informationssicherheit und kennen die Bedeutung der Datenqualität für den Informationsverarbeitungsprozess.
Dauer	3 Tage
Besondere Hinweise	Voraussetzung ist eine persönliche Zugangsberechtigung +1-Arbeitsplatz Polizei.

Zurück zum Inhalt

4321 – @rtus INPOL-Merkblatt und elektronische Kriminalakte

Zielgruppe	Mitarbeiterinnen und Mitarbeiter der Landespolizei, die im Rahmen ihrer dienstlichen Aufgaben vornehmlich als Ermittlungstätigkeit die polizeiliche Vorgangsbearbeitung auf einem +1-Arbeitsplatz Polizei in diesen erweiterten Funktionen nutzen sollen.
Lehrinhalte	• Grundlagen der Informationssicherheit • Merkblattspezifische Rechtsgrundlagen • Erstellung eines INPOL-Merkblattes • Anlage und Nutzen einer elektronische Kriminalakte • Qualitätssicherung • Datenqualität im Vorgangsbearbeitungssystem (VBS) @rtus im Hinblick auf Auswertung/Analyse
Lernziele	Die Mitarbeiter/innen der Landespolizei sollen unter Berücksichtigung der rechtlichen Bestimmungen der Datenverarbeitung die Funktionen des INPOL-Merkblattes und der elektronischen Kriminalakte unter @rtus zur Bewältigung polizeilicher Aufgabenstellungen rechtssicher anwenden können. Sie beachten die Grundlagen der Informationssicherheit und kennen die Bedeutung der Datenqualität für den Informationsverarbeitungsprozess.
Dauer	½ Tag
Besondere Hinweise	Voraussetzungen für die Seminarteilnahme: • eine persönliche Zugangsberechtigung +1-Arbeitsplatz Polizei • @rtus-Grundkenntnisse als Sachbearbeiter

Zurück zum Inhalt

4330 – Vorgangsbearbeitung @rtus -Verwaltung-

Zielgruppe	Mitarbeiterinnen und Mitarbeiter der Landespolizei, die im Rahmen ihrer dienstlichen Aufgaben erstmalig die polizeiliche Vorgangsbearbeitung als Verwalter auf einem LSK-Arbeitsplatz nutzen sollen.
Lehrinhalte	• Grundlagen der Informationssicherheit • datenverarbeitungsrechtliche Bestimmungen • @rtus-Philosophie • Vorgangsein- und -ausgänge • strukturierte Erfassung von Objekten • Bearbeiten von Ersuchen • Berechtigungskonzept • Vorgangsverwaltung mit der Registratur • Datenqualität im Vorgangsbearbeitungssystem (VBS) @rtus im Hinblick auf Auswertung/Analyse
Lernziele	Die Anwenderinnen und Anwender sollen unter Berücksichtigung der rechtlichen Bestimmungen der Datenverarbeitung die Grundfunktionen der polizeilichen Vorgangsbearbeitung zur Bewältigung polizeilicher Aufgabenstellungen als Verwalter anwenden können. Sie beachten die Grundlagen der Informationssicherheit und kennen die Bedeutung der Datenqualität für den Informationsverarbeitungsprozess.
Dauer	1 Tag
Besondere Hinweise	Voraussetzung ist eine Zugangsberechtigung +1-Arbeitsplatz Polizei.

Zurück zum Inhalt

4340 – @rtus-Recherche für Anwenderbetreuer/innen

Zielgruppe	Anwenderbetreuerinnen und Anwenderbetreuer von @rtus-Dienststellen, die mit der Aufgabe der @rtus-Anwenderbetreuung beauftragt sind.
Lehrinhalte	• Grundlagen der Informationssicherheit • Unterschiede @rtus Suche und @rtus-Recherche • Horizontale Blockverbunde/Nutzergruppen • Berechtigungskonzept • Wahrnehmung der Aufgaben gem. Einführungserlass • Unterstützung der Dienststellenleitung • Tangierte Rechtsgrundlagen/Belehrung • Datenumfang und Vorgangsstatus • Datenqualität im Vorgangsbearbeitungssystem (VBS) @rtus im Hinblick auf Auswertung/Analyse • Qualitätssicherung • Arbeiten mit der Recherche
Lernziele	Die Anwenderbetreuerinnen und Anwenderbetreuer (AWB) sollen unter Berücksichtigung der rechtlichen Bestimmungen auf Weisung der Dienststellenleitung Mitarbeiterinnen und Mitarbeiter für die @rtus-Recherche berechtigen und Maßnahmen zur Verbesserung der Datenqualität treffen können. Sie sollen das Berechtigungskonzept anwenden, mit der Recherche arbeiten können und den Datenumfang kennen. Ferner sollen sie die Nutzerinnen und Nutzer bei der Arbeit mit der @rtus-Recherche unterstützen.
Dauer	1 Tag
Besondere Hinweise	Voraussetzung ist die Eigenschaft der Anwenderbetreuung auf einer @rtus-Dienststelle und die Teilnahme am Seminar OZ 4310.

Zurück zum Inhalt

4342 – InfoZoom-Grundlagen zur Auswertung von PKS-Daten

Zielgruppe	Leiterinnen und Leiter von Kriminalpolizeistellen und Stabsbereiche 1.2 der Polizeidirektionen und deren Beauftrage.
Lehrinhalte	• Das Programm InfoZoom • Datenschutzrechtliche Aspekte bei Nutzung dieser Anwendung • Grundlagen der Bedienung • Allgemeine Funktionen: Diagramme, Datenexport • Grundlagen der Analyse • Allgemeine Praktische Übungen
Lernziele	Die Teilnehmenden sollen die Grundlagen und Funktionen der Anwendung InfoZoom ausschließlich zum Zweck der individuellen Auswertung und Analyse der aktuellen polizeilichen Kriminalstatistik anwenden können und die Möglichkeiten der Nutzung kennen.
Dauer	½ Tag
Besondere Hinweise	Die Anwendung InfoZoom steht standardmäßig nicht auf jedem LSK-Arbeitsplatz zur Verfügung, sondern wird vom LPA auf Antrag explizit zugewiesen.

Zurück zum Inhalt

4386 – EPOST 810

Zielgruppe	Mitarbeiterinnen und Mitarbeiter der Landespolizei, die im Rahmen ihres Dienstes EPOST 810 bedienen sollen.
Lehrinhalte	• Grundlagen der Informationssicherheit • Kenntnisse der PDV 810.1 • Zusatzregelung zum Betrieb von EPOST 810 für die Polizei SH • Die Oberfläche von EPOST 810 • An- und Abmelden • Erstellen, Empfangen und Senden von Nachrichten • Gesendete Nachrichten anzeigen lassen • Recherchieren von Nachrichten • Umleitungen aktivieren und deaktivieren
Lernziele	Beherrschung des Führungs- und Einsatzmittels EPOST 810 unter Beachtung der Grundlagen der Informationssicherheit.
Dauer	½ Tag
Besondere Hinweise	Voraussetzung ist die Teilnahme am LSK-Zugangslehrgang OZ 4260 (OZ 450)

Zurück zum Inhalt

4510 – Merlin – Sachbearbeitung in Ermittlungsverfahren

Zielgruppe	Mitarbeiterinnen und Mitarbeiter von Dienststellen, die das Verfahren Merlin im Rahmen der Sachbearbeitung nutzen sollen.
Lehrinhalte	• IT-Betriebskonzept, Systematik der Verfahrensanbindungen • Grundlagen der Informationssicherheit • Berechtigungskonzept und Rollen • Anlegen, Bearbeiten und Verwalten von Entitäten und Verknüpfungen • Bedeutung der Datenqualität für ein Ermittlungsverfahren • einfache Möglichkeiten der Visualisierung • Druckfunktionen • einfache Such- und Recherchefunktionen • Datenpflege und Datenbereinigung • Durchführung und Bearbeitung von Anschlussinhaberfeststellungen • Bearbeiten von TKÜ-Maßnahmen
Lernziele	Die Teilnehmerinnen und Teilnehmer können nach Abschluss des Seminars das Verfahren Merlin mit der Rolle Sachbearbeiter (alle fachlichen Rechte) aufgabenorientiert nutzen, sowie taktisch und rechtlich richtig anwenden. Sie sind über die landeseinheitlichen Regelungen zur Informationssicherheit informiert. Sie wissen, wie Informationen zu aktuellen Fragestellungen erlangt werden können (Regelwerke im Intrapol).
Dauer	3 Tage
Besondere Hinweise	Die Teilnahme an dem Seminar berechtigt zur Nutzung der Rolle 01 – Sachbearbeiter (alle fachlichen Rechte).

Zurück zum Inhalt

4511 – Merlin-Workshop: Telekommunikationsüberwachung

Zielgruppe	Mitarbeiterinnen und Mitarbeiter von Kriminalpolizeidienststellen, die das Verfahren Merlin im Rahmen der Sachbearbeitung nutzen und dabei Erfahrung im Bearbeiten und Verwalten von TKÜ-Maßnahmen in Merlin haben.
Lehrinhalte	• Grundlagen der Informationssicherheit • Anlegen und Verwalten von TKÜ-Maßnahmen • Bedeutung der Datenqualität für das weitere Verfahren • Aufgaben und Möglichkeiten der TKÜ-Zentrale im LKA • Erstellen und Bearbeiten von AIF-Maßnahmen • Bearbeiten von Gesprächsprotokollen • Druckfunktionen, Auswerteberichte • Unterstützung der Ermittlungen über das GIS-Modul • Neue Funktionen im TKÜ-Modul • Selbstständiges Lösen von Problemen
Lernziele	Die Teilnehmerinnen und Teilnehmer nutzen nach Abschluss des Seminars die Möglichkeiten des TKÜ-Moduls in dem Verfahren Merlin professionell aus und können es unter Beachtung der Grundlagen der Informationssicherheit taktisch und rechtlich richtig anwenden. Die Teilnehmerinnen und Teilnehmer sind in der Lage, laufende TKÜ-Maßnahmen auszuwerten und Problemstellungen selbstständig zu lösen.
Dauer	1 Tag
Besondere Hinweise	Bedingung für die Teilnahme an diesem Seminar ist eine erfolgte Teilnahme an dem Seminar OZ 4510 – Merlin – Sachbearbeitung in Ermittlungsverfahren, sowie Handlungssicherheit in der Anwendung des Verfahrens Merlin. Die Teilnahme an dem Seminar führt NICHT zur Erteilung einer Rolle.

Zurück zum Inhalt

4512 – Merlin-Workshop: Ermittlungsverfahren professionell unterstützen

Zielgruppe	Mitarbeiterinnen und Mitarbeiter von Kriminalpolizeidienststellen, die das Verfahren Merlin im Rahmen der Sachbearbeitung anwenden und durch ihre bisherige Erfahrungen in Merlin in der Lage sind, neue Funktionen zu erlernen und anzuwenden.
Lehrinhalte	• Koordinierung der Eingangsbedingungen zum erfolgreichen Begleiten eines Ermittlungsverfahrens in Merlin • Grundlagen der Informationssicherheit • Abhängigkeiten zwischen Datenqualität und Analyse • Datenpflege und Datenbereinigung • Datenexport • Abgleich von externen Informationen mit dem Datenbestand in Merlin • Neue Funktionen im Verfahren Merlin • Erarbeiten von Möglichkeiten zur individuellen Problemlösung
Lernziele	Die Teilnehmerinnen und Teilnehmer können nach Abschluss des Seminars die speziellen Funktionen des Verfahrens Merlin zielgerichtet, sowie taktisch und rechtlich richtig einsetzen. Die Teilnehmenden unterstützen nach Abschluss des Seminars ihre Dienststelle durch kreative Nutzung des Verfahrens Merlin im Rahmen von Ermittlungsverfahren. Sie beachten die Grundlagen der Informationssicherheit und kennen die Bedeutung der Datenqualität für den Informationsverarbeitungsprozess.
Dauer	1 Tag
Besondere Hinweise	Bedingung für die Teilnahme an diesem Seminar ist eine erfolgte Teilnahme an dem Seminar OZ 4510 – Merlin – Sachbearbeitung in Ermittlungsverfahren, sowie Handlungssicherheit in der Anwendung des Verfahrens Merlin. Die Teilnahme an dem Seminar führt NICHT zur Erteilung einer Rolle.

Zurück zum Inhalt

4513 – Merlin – Spurenintensive Ermittlungen

Zielgruppe	Mitarbeiterinnen und Mitarbeiter von Dienststellen, die das Verfahren Merlin im Rahmen der Sachbearbeitung anwenden und durch die Möglichkeiten Merlins bei spurenintensiven Ermittlungen professionell unterstützen sollen.
Lehrinhalte	• Grundlagen der Informationssicherheit • Einsatz des Soko-Moduls • Hinweisaufnahme und -bearbeitung • Anlegen, Bearbeiten und Verwalten von Spuren und Aufträgen • Abhängigkeiten zwischen Datenqualität und Analyse • Steuerung für die Bearbeitung von Spuren, Ermittlungsunterspuren und Aufträgen • einfache Analyse der Spurenlage • Druckfunktionen und Visualisierung
Lernziele	Die Teilnehmerinnen und Teilnehmer kennen nach Abschluss des Seminars das Soko-Modul des Verfahrens Merlin und können es unter Beachtung der Grundlagen der Informationssicherheit taktisch und rechtlich richtig anwenden. Die Teilnehmenden sind in der Lage durch die Nutzung des Verfahrens Merlin die Ermittlungen bei spurenintensiven Verfahren zu unterstützen.
Dauer	1,5 Tage
Besondere Hinweise	Bedingung für die Teilnahme an diesem Seminar ist eine erfolgte Teilnahme an dem Seminar OZ 4510 – Merlin – Sachbearbeitung in Ermittlungsverfahren, sowie Handlungssicherheit in der Anwendung des Verfahrens Merlin. Die Teilnahme an dem Seminar führt NICHT zur Erteilung einer Rolle.

Zurück zum Inhalt

4515 – Merlin-Workshop: Auffrischen von Kenntnissen

Zielgruppe	Mitarbeiterinnen und Mitarbeiter von Kriminalpolizeidienststellen, die das Verfahren Merlin im Rahmen der Sachbearbeitung anwenden sollen und deren Teilnahme an einem Seminar OZ4510 – Merlin – Sachbearbeitung in Ermittlungsverfahren schon einige Zeit zurückliegt.
Lehrinhalte	• Systematik der Verfahrensanbindungen, Berechtigungskonzept und Rollen • Grundlagen der Informationssicherheit • Anlegen, Bearbeiten und Verwalten von Entitäten und Verknüpfungen • Bedeutung der Datenqualität für die Analyse • Datenpflege und Datenbereinigung • Druckfunktionen • einfache Such- und Recherchefunktionen • Neue Funktionen im Verfahren Merlin
Lernziele	Die Teilnehmerinnen und Teilnehmer können nach Abschluss des Seminars ihre bereits erworbenen Kenntnisse unter Beachtung der Grundlagen der Informationssicherheit wieder zielgerichtet, sowie taktisch und rechtlich richtig anwenden. Die Teilnehmenden sind in der Lage, die grundsätzlichen Möglichkeiten einer Sachbearbeiterin/eines Sachbearbeiters wieder auszuschöpfen, obwohl sie seit längerem nicht mehr mit dem Verfahren Merlin gearbeitet haben.
Dauer	1 Tag
Besondere Hinweise	Bedingung für die Teilnahme an diesem Seminar ist eine erfolgte Teilnahme an dem Seminar OZ 4510 – Merlin – Sachbearbeitung in Ermittlungsverfahren. Die Teilnahme an dem Seminar führt NICHT zur Erteilung einer Rolle.

Zurück zum Inhalt

4520 – Merlin – Hinweisaufnahme für Unterstützungskräfte

Zielgruppe	Mitarbeiterinnen und Mitarbeiter von Polizeidienststellen, die zur Bewältigung von Hinweiseingängen bei Großverfahren, Schadenslagen oder im Rahmen einer BAO einsetzt werden sollen.
Lehrinhalte	• IT-Betriebskonzept • Grundlagen der Informationssicherheit • Systematik der Verfahrensanbindungen • Berechtigungskonzept und Rollen • Hinweisaufnahme • Bedeutung der Datenqualität für das Verfahren
Lernziele	Die Teilnehmerinnen und Teilnehmer können nach Abschluss des Seminars mit der Rolle Hinweisaufnahme in Merlin Hinweise erfassen, die im Rahmen eines Großverfahrens (MK, EG, BAO, etc.) eingehen, kennen die Bedeutung der Datenqualität für ein Verfahren und beachten die Grundlagen der Informationssicherheit.
Dauer	½ Tag
Besondere Hinweise	Die Teilnahme an dem Seminar führt zur Erteilung der Rolle 07 – Hinweisaufnahme.

Zurück zum Inhalt

4530 – Merlin – Asservatenverwaltung für Sachbearbeiter Spurensicherung (LKA und BKI/K6)

Zielgruppe	Mitarbeiterinnen und Mitarbeiter des LKA und der BKI/K6, die das Verfahren Merlin im Rahmen der Sachbearbeitung anwenden und zukünftig Asservate in Merlin verwalten sollen.
Lehrinhalte	• IT-Betriebskonzept, Systematik der Verfahrensanbindungen, Grundlagen der Informationssicherheit • Berechtigungskonzept und Rollen • Anlegen, Bearbeiten und Verwalten von Entitäten und Verknüpfungen • Abhängigkeiten zwischen Datenqualität und Analyse • Anlegen und Verwalten von Kategorien • Anlegen und Verwalten von Asservaten • Umsetzung der ermittlungsrelevanten Rahmenbedingungen • KTU-Objekte und KTU-Ergebnisse • Druckfunktionen und Visualisierung
Lernziele	Die Teilnehmerinnen und Teilnehmer kennen nach Abschluss des Seminars die Grundfunktionen und das Asservatenmodul des Verfahrens Merlin und können diese unter Beachtung der Grundlagen der Informationssicherheit taktisch und rechtlich richtig anwenden. Die Teilnehmenden unterstützen ihre Dienststelle bei der Erfassung und Verwaltung von Asservaten und sind in der Lage kriminaltechnische Untersuchungen anzufordern.
Dauer	2 Tage
Besondere Hinweise	Die Teilnahme an dem Seminar führt zur Erteilung der Rolle 03 – Sachbearbeiter Spurensicherung.

Zurück zum Inhalt

4531 – Merlin – Asservatenverwaltung für Sachbearbeiter

Zielgruppe	Mitarbeiterinnen und Mitarbeiter von Kriminalpolizeidienststellen, die das Verfahren Merlin im Rahmen der Sachbearbeitung anwenden und zukünftig Asservate in Merlin verwalten sollen.
Lehrinhalte	• Grundlagen der Informationssicherheit • Anlegen und Verwalten von Kategorien • Anlegen und Verwalten von Asservaten • Umsetzung der ermittlungsrelevanten Rahmenbedingungen • KTU-Objekte und KTU-Ergebnisse • Druckfunktionen und Visualisierung
Lernziele	Die Teilnehmerinnen und Teilnehmer kennen nach Abschluss des Seminars das Asservatenmodul des Verfahrens Merlin können dies unter Beachtung der Grundlagen der Informationssicherheit taktisch und rechtlich richtig anwenden. Die Teilnehmenden unterstützen ihre Dienststelle bei der Erfassung und Verwaltung von Asservaten und sind in der Lage, kriminaltechnische Untersuchungen anzufordern.
Dauer	1 ½ Tage
Besondere Hinweise	Bedingung für die Teilnahme an diesem Seminar ist eine erfolgte Teilnahme an dem Seminar OZ 4510 – Merlin – Sachbearbeitung in Ermittlungsverfahren, sowie Handlungssicherheit in der Anwendung des Verfahrens Merlin. Die Teilnahme an dem Seminar führt NICHT zur Erteilung einer Rolle.

Zurück zum Inhalt

4541 – Merlin – Analyse von Datenbeständen

Zielgruppe	Mitarbeiterinnen und Mitarbeiter von Kriminalpolizeidienststellen, die das Verfahren Merlin im Rahmen der Sachbearbeitung anwenden und im Rahmen von Ermittlungsverfahren den Datenbestand in Merlin auswerten und analysieren sollen.
Lehrinhalte	• Abhängigkeiten zwischen Datenqualität und Analyse • Umfassende Möglichkeiten der Analyse von Datenbeständen • Abgleichsuche, Ähnlichkeitssuche, Volltextrecherche • Abgleich von externen Informationen mit dem Datenbestand in Merlin (Listenabgleich) • Komplexe Recherche • Export von Analyseergebnissen • Umsetzen ermittlungsrelevanter Fragestellungen in adäquate Recherchen in Merlin
Lernziele	Die Teilnehmerinnen und Teilnehmer kennen nach Abschluss des Seminars die Recherche- und Analysefunktionen des Verfahrens Merlin können diese unter Beachtung der Grundsätze der Informationssicherheit taktisch und rechtlich richtig anwenden. Die Teilnehmenden sind in der Lage ermittlungsrelevante Fragestellungen zu bearbeiten und Ergebnisse durch professionelle Nutzung des Verfahrens Merlin zu liefern.
Dauer	2 ½ Tage
Besondere Hinweise	Bedingung für die Teilnahme an diesem Seminar ist eine erfolgte Teilnahme an dem Seminar OZ 4510 – Merlin – Sachbearbeitung in Ermittlungsverfahren, sowie Handlungssicherheit in der Anwendung des Verfahrens Merlin. Das Seminar schließt mit einer schriftlichen Lernerfolgskontrolle ab. Die Teilnahme an dem Seminar führt NICHT zur Erteilung einer Rolle.

Zurück zum Inhalt

4550 – Merlin – Anwenderbetreuung und Verfahrensadministration

Zielgruppe	Mitarbeiterinnen und Mitarbeiter von Dienststellen, die für ihre Dienststellen: • Merlin-Verfahren administrieren sollen, • die die rollenspezifischen Berechtigungen des Verfahrensbetreuers im Rahmen der Sachbearbeitung für die Verfahren der Dienststelle einsetzen sollen, • die Anwenderinnen und Anwender, die das Verfahren Merlin im Rahmen der Sachbearbeitung einsetzen, als Verfahrensbetreuer unterstützen und beraten sollen.
Lehrinhalte	• Zentrale Fachadministration Merlin beim LPA • Grundlagen der Informationssicherheit • Anwenderbetreuung und Verfahrensadministration • Verfahrenseinrichtung • Admin-Tool • Kataloge • Import und Export von Datenbeständen • Schemabearbeitung und -verwaltung • Recherche- und Analysefunktionen
Lernziele	Die Teilnehmerinnen und Teilnehmer können nach Abschluss des Seminars Verfahren einrichten und Anwender mit funktionsspezifischen Rollen zuweisen. Sie beherrschen den Import von angelieferten Datenbeständen externer Stellen und können diese verfahrensgerecht aufbereiten. Die Teilnehmenden beherrschen den Funktionsumfang des Verfahrens Merlin und sind in der Lage, die Anwenderinnen und Anwender beim Einsatz des Verfahrens Merlin zu unterstützen. Sie sind über die landeseinheitlichen Regelungen zur Informationssicherheit informiert. Sie wissen, wie Informationen zu aktuellen Fragestellungen erlangt werden können (IT-Regelwerk im Intrapol; CheckIT).
Dauer	1 Woche
Besondere Hinweise	Die Teilnehmerinnen und Teilnehmer sollen erfahrene Verwender des Fallbearbeitungssystems Merlin sein und das Verfahren mit seinen verschiedenen Modulen handlungssicher einsetzen können. Die Teilnahme an dem Seminar berechtigt zur Nutzung der Rolle **90 –**

	Verfahrensbetreuer und führt zur Erteilung der Berechtigung **RSCADMIN**.

Zurück zum Inhalt

4612 –Cybercrime – Eine Einführung

Zielgruppe	Alle Mitarbeiterinnen und Mitarbeiter von Polizeidienststellen.
Lehrinhalte	• Grundsätze der Informationssicherheit • Cybercrime – Definition und Hintergründe • Bearbeitungs- und Ermittlungsmöglichkeiten bei der Polizei Schleswig-Holstein • Fallbeispiele und technische Hintergründe • Viren, Trojaner, Würmer • Hacking, Cracking & Co. • Phishing & Scramming • Internetbetrug • Ransomware • Anonymous, LulzSec & andere Gruppierungen • Einsatzmöglichkeiten mit LSK, Auswerterechner und Internetrechercherechner
Lernziele	Die Teilnehmerinnen und Teilnehmer kennen nach Abschluss des Seminars die technischen, taktischen und rechtlichen Bedeutungen von aktuellen Fällen der Cybercrime. Die Teilnehmerinnen und Teilnehmer können Sachverhalte erkennen, bewerten und im Rahmen der polizeilichen Zuständigkeiten einordnen. Sie kennen die Grundsätze der Informationssicherheit und sind sich der Bedeutung der Datenqualität für den Informationsverarbeitungsprozess bewusst.
Dauer	1 Tag
Besondere Hinweise	An dem Seminar kann ohne Vorkenntnisse teilgenommen werden. Die Inhalte werden dem aktuellen Geschehen angepasst. Das Seminar eignet sich auch, um vorhandenes Wissen aufzufrischen. Das Seminar kann an jedem Ort durchgeführt werden.

Zurück zum Inhalt

4620 – Auswertung strukturierter Massendaten mit Standardanwendungen

Zielgruppe	Alle Sachbearbeiterinnen und Sachbearbeiter der Schutz- und Kriminalpolizei, die im Rahmen ihrer Ermittlungen mit umfangreichen Datenbeständen konfrontiert werden und Sicherheit in der Handhabung, Aufbereitung und Auswertung umfangreicher Datenbestände (strukturierte Massendaten) erlangen wollen.
Lehrinhalte	• Konvertierung von Dateiformaten • Aufbereitung von Datenbeständen • Sortierung, Filterung und Auswertung von Datenbeständen mit Standardanwendungen • Sicherung und Aufbereitung von Arbeitergebnissen • Bedeutung der Datenqualität für die Landespolizei
Lernziele	Die Teilnehmerinnen und Teilnehmer können umfangreiche Datenbestände sicher handhaben. Sie sind fähig, die erstellten oder erlangten Daten in die richtigen Formate und Strukturen umzuwandeln, um eine Auswertung mit den unterschiedlichen zur Verfügung stehenden Standardanwendungen durchzuführen. Die ermittelten Ergebnisse können gesichert und zur weiteren Verarbeitung in der Sachbearbeitung verwendet werden.
Dauer	4 Tage
Besondere Hinweise	

Zurück zum Inhalt

4630 – Microsoft Betriebssysteme im Fokus polizeilicher Ermittlungen (Grundlagen)

Zielgruppe	Sachbearbeiterinnen und Sachbearbeiter der IuK-Kriminalität im engeren Sinne, Mitarbeiterinnen und Mitarbeiter der IT-Beweissicherung und der forensischen IT.
Lehrinhalte	• Grundlagen der Informationssicherheit • Dateisysteme unter Microsoft Windows • Struktur des Betriebssystems • Unterschiede zu Linux • Benutzerverwaltung und Berechtigungsstrukturen • Ermittlungsarbeit mit der Befehlszeile • Microsoft Windows Betriebssysteme als Client oder Server in Netzwerken • Ermittlungsorientierte Auswertung und Analyse eines sichergestellten Microsoft Windows Betriebssystems
Lernziele	Die Teilnehmerinnen und Teilnehmern haben nach Teilnahme an diesem Seminare Kenntnisse über Administration, Einsatzmöglichkeiten und Bedienung von Microsoft Windows Betriebssystemen. Dadurch können sie im Rahmen von Ermittlungen der IuK-Kriminalität diese IT-Systeme untersuchen und auswerten, um auftragsorientiert kriminalistische Fragestellungen zu beantworten. Sie beachten die Grundlagen der Informationssicherheit und kennen die Bedeutung der Datenqualität für den Informationsverarbeitungsprozess.
Dauer	1 Woche
Besondere Hinweise	Die Teilnahme an oder vergleichbare Kenntnisse der folgenden Seminare werden zwingend vorausgesetzt: • OZ 4705 – Internetnutzung zur Wahrnehmung dienstlicher Aufgaben, • OZ 4615 – IuK-Kriminalität in der Sachbearbeitung, • OZ 4710 – Einsatz von Auswerterechnern zur Ermittlungsunterstützung.

Zurück zum Inhalt

4640 – IuK-Kriminalität – Linux-Betriebssysteme im Fokus polizeilicher Ermittlungen (Grundlagen)

Zielgruppe	Sachbearbeiterinnen und Sachbearbeiter der IuK-Kriminalität im engeren Sinne, Mitarbeiterinnen und Mitarbeiter der IT-Beweissicherung und der forensischen IT.
Lehrinhalte	• Grundlagen der Informationssicherheit • Dateisysteme unter Linux • Struktur des Betriebssystems • Unterschiede zu Microsoft Windows • Benutzerverwaltung und Berechtigungsstrukturen • Ermittlungsarbeit mit der Befehlszeile • Linux als Client oder Server in Netzwerken • Ermittlungsorientierte Auswertung und Analyse eines sichergestellten Linux-Systems
Lernziele	Die Teilnehmerinnen und Teilnehmern haben nach Teilnahme an diesem Seminare Kenntnisse über Administration, Einsatzmöglichkeiten und Bedienung von Linux-Betriebssystemen. Dadurch können sie im Rahmen von Ermittlungen der IuK-Kriminalität diese IT-Systeme untersuchen und auswerten, um auftragsorientiert kriminalistische Fragestellungen zu beantworten. Sie beachten die Grundlagen der Informationssicherheit und kennen die Bedeutung der Datenqualität für den Informationsverarbeitungsprozess.
Dauer	1 Woche
Besondere Hinweise	Die Teilnahme an oder vergleichbare Kenntnisse der folgenden Seminare werden zwingend vorausgesetzt: • OZ 4705 – Internetnutzung zur Wahrnehmung dienstlicher Aufgaben, • OZ 4615 – IuK-Kriminalität in der Sachbearbeitung, • OZ 4710 – Einsatz von Auswerterechnern zur Ermittlungsunterstützung.

Zurück zum Inhalt

4641 – IuK-Kriminalität – Linux-Betriebssysteme im Fokus polizeilicher Ermittlungen (Aufbau)

Zielgruppe	Sachbearbeiterinnen und Sachbearbeiter der IuK-Kriminalität im engeren Sinne, Mitarbeiterinnen und Mitarbeiter der IT-Beweissicherung und der forensischen IT.
Lehrinhalte	• Auffrischen der Kenntnisse aus dem Grundkurs • Struktur des Betriebssystems in Netzwerken • Unterschiede zu MS Windows® u. MS Server® • Benutzerverwaltung und Berechtigungsstrukturen im Netzwerk • Ermittlungsarbeit im Netzwerk mit der Befehlszeile • Samba Integration • Apache Webserver • MySQL Datenbanksysteme
Lernziele	Die Teilnehmerinnen und Teilnehmer haben nach Teilnahme an diesem Seminar Kenntnisse über Administration, Einsatzmöglichkeiten und Bedienung von Linux-Betriebssystemen in einer Client-Server Netzwerkumgebung. Dadurch sind sie im Rahmen von polizeilichen Ermittlungen in der Lage, diese IT-Systeme unter forensischen Gesichtspunkten zu untersuchen und auszuwerten, und auftragsorientiert kriminalistische Fragestellungen zu beantworten.
Dauer	1 Woche
Besondere Hinweise	Das Seminar schließt mit einer schriftlichen Lernerfolgskontrolle ab. Im Rahmen des Seminars werden SUSE- und UBUNTU-Distributionen genutzt.

Zurück zum Inhalt

4650 – Netzwerke und Server im Fokus polizeilicher Ermittlungen

Zielgruppe	Sachbearbeiterinnen und Sachbearbeiter der IuK-Kriminalität im engeren Sinne, Mitarbeiterinnen und Mitarbeiter der IT-Beweissicherung und der forensischen IT.
Lehrinhalte	• kabelgebundene und kabellose Netzwerke • Netzwerkarten und –topologien • Netzwerkhardware (Netzwerkkarte, Repeater, Hub, Switch, Bridge, Router) • Technologien zur LAN-WAN-Kopplung: ISDN, DSL, X.25 • Protokolle: TCP/IP, UDP, IPv4 und IPv6; OSI-Schichtenmodell • Aufbau einer Domäne • zentralisierte Administration der Benutzer und Zugriff auf Ressourcen, sowie Verwendung von Gruppenrichtlinien • Netzwerkdienste: DNS und DHCP, Fernzugriff mit RAS und VPN • Webserver
Lernziele	Die Teilnehmerinnen und Teilnehmer haben nach Teilnahme an diesem Seminar Kenntnisse über Administration, Einsatzmöglichkeiten und Analyse von Netzwerkumgebungen. Dadurch sind sie im Rahmen von polizeilichen Ermittlungen in der Lage, diese IT-Systeme unter forensischen Gesichtspunkten zu untersuchen und auszuwerten, sowie auftragsorientiert kriminalistische Fragestellungen zu beantworten.
Dauer	4 Tage
Besondere Hinweise	Die Teilnahme an oder vergleichbare Kenntnisse der folgenden Seminare werden zwingend vorausgesetzt: • OZ 4705 – Internetnutzung zur Wahrnehmung dienstlicher Aufgaben, • OZ 4615 – IuK-Kriminalität in der Sachbearbeitung, • OZ 4710 – Einsatz von Auswerterechnern zur Ermittlungsunterstützung. Das Seminar schließt mit einer schriftlichen Lernerfolgskontrolle ab.

Zurück zum Inhalt

4660 – IuK-Kriminalität – Ethical Hacking – Angriffe auf IT

Zielgruppe	Sachbearbeiterinnen und Sachbearbeiter der IuK-Kriminalität im engeren Sinne, Mitarbeiterinnen und Mitarbeiter der IT-Beweissicherung und der forensischen IT.
Lehrinhalte	• Bedeutung der Informationssicherheit • Angriffe auf verteilte Systeme über drahtgebundene und drahtlose Verbindungen • Vorbereiten • Planen • Durchführen • Exploits in Systemen finden und nutzen • Kryptografie und Steganografie • Datensicherung und die Möglichkeiten der Überwindung • Praktische Übungen • Möglichkeiten und Grenzen der polizeilichen Ermittlungsarbeit
Lernziele	Die Teilnehmerinnen und Teilnehmer kennen nach erfolgreichem Abschluss die geläufigsten Angriffsmethoden im Bereich IuK-Kriminalität in Theorie und Praxis und sind in der Lage die Bedeutung der Informationssicherheit einem Außenstehenden zu erläutern. Sie versetzen sich durch den Erwerb vergleichbarer Kompetenzen in die Lage der Angreifer. Sie erkennen die jeweiligen Möglichkeiten und Ansatzpunkte für polizeiliche Ermittlungen und wissen, an welchen Stellen ermittlungsrelevante Spuren hinterlassen werden.
Dauer	1 Woche
Besondere Hinweise	Die Teilnahme an nachfolgend genannten Lehrgängen oder vergleichbare Kenntnisse der folgenden Inhalte werden zwingend vorausgesetzt: • OZ 4705 – Internetnutzung zur Wahrnehmung dienstlicher Aufgaben, • OZ 4615 – IuK-Kriminalität in der Sachbearbeitung, • OZ 4710 – Einsatz von Auswerterechnern zur Ermittlungsunterstützung, • Ermittlungs- und/oder Auswertungserfahrung im Bereich IuK-Kriminalität, • Kenntnisse der einschlägigen, auch englischsprachigen Fachtermini, • Kenntnisse Microsoft Windows und Linux OS.

	Kenntnisse in den Bereichen: • Funktion des Internets und seiner Dienste, • Netzwerkgrundlagen und –topologie, • DHCP, DNS, • OSI-Referenzmodell, • TCP/IP, UDP, ICMP. Das Seminar schließt mit einer schriftlichen Lernerfolgskontrolle ab.

Zurück zum Inhalt

4661 – IuK-Kriminalität – WLAN – Drahtlose Netzwerke als Ziel krimineller Handlungen

Zielgruppe	Sachbearbeiterinnen und Sachbearbeiter der IuK-Kriminalität im weiteren und im engeren Sinne, Mitarbeiterinnen und Mitarbeiter der IT-Beweissicherung und der forensischen IT.
Lehrinhalte	• Angriffe auf verteilte Systeme über drahtlose Verbindungen • Vorbereiten • Planen • Durchführen • rechtliche Relevanz durchgeführter Angriffe • Bedeutung der Informationssicherheit • Kryptografie und Steganografie • Datensicherung und die Möglichkeiten der Überwindung • Praktische Übungen • Möglichkeiten und Grenzen der polizeilichen Ermittlungsarbeit
Lernziele	Die Teilnehmerinnen und Teilnehmer kennen nach erfolgreichem Abschluss die geläufigsten Methoden, mit denen verteilte Systeme über drahtlose Verbindungen angegriffen werden und können dadurch die Bedeutung der Informationssicherheit einschätzen. Sie versetzen sich durch den Erwerb vergleichbarer Kompetenzen in die Lage der Angreifer. Sie erkennen die jeweiligen Möglichkeiten und Ansatzpunkte für polizeiliche Ermittlungen und wissen, an welchen Stellen ermittlungsrelevante Spuren hinterlassen werden.
Dauer	2 Tage
Besondere Hinweise	Die Teilnahme an nachfolgend genannten Lehrgängen oder vergleichbare Kenntnisse der folgenden Inhalte werden zwingend vorausgesetzt: • OZ 4705 – Internetnutzung zur Wahrnehmung dienstlicher Aufgaben, • OZ 4615 – IuK-Kriminalität in der Sachbearbeitung, • OZ 4710 – Einsatz von Auswerterechnern zur Ermittlungsunterstützung, • Ermittlungs- und/oder Auswertungserfahrung im Bereich IuK-Kriminalität, • Kenntnisse der einschlägigen, auch englischsprachigen Fachtermini, • Kenntnisse Microsoft Windows und Linux OS. Kenntnisse in den Bereichen: • Funktion des Internets und seiner Dienste,

	• Netzwerkgrundlagen und –topologie, • DHCP, DNS, • OSI-Referenzmodell, • TCP/IP, UDP, ICMP. Das Seminar schließt mit einer schriftlichen Lernerfolgskontrolle ab.

Zurück zum Inhalt

4670 – IuK-Kriminalität – Grundlagen der forensischen Datenanalyse für ITB und SB IuK i. e. S.

Zielgruppe	Sachbearbeiterinnen und Sachbearbeiter der IuK-Kriminalität im engeren Sinne, Mitarbeiterinnen und Mitarbeiter der IT-Beweissicherung und der forensischen IT. Sachbearbeiterinnen und Sachbearbeiter, die das Verfahren Auswerterechner sicher beherrschen, im Rahmen ihrer dienstlichen Aufgaben Datenträger auswerten und eine lückenlose Beweisführung im Strafprozess anstreben.
Lehrinhalte	• Bedeutung der Informationssicherheit • Datensicherung als Grundlage einer forensischen Datenanalyse • Vorbereiten • Planen • Durchführen • Grundprinzipien der forensischen IuK • Datenintegrität herstellen und nachweisen • Bedeutung der Datenqualität für die Analyse • Analyse der gesicherten Datenträger • Einsatz von Open Source Produkten • Erstellen von Auswerteberichten und Gutachten • Grundsätze der Gutachtenerstellung • Aussagen treffen und validieren • Aufbereitung der Ergebnisse • Möglichkeiten und Grenzen der forensischen Datenanalyse
Lernziele	Die Teilnehmerinnen und Teilnehmer kennen nach erfolgreichem Abschluss die Grundsätze der forensischen Datenanalyse und die Bedeutung der Datenqualität im Analyseprozess. Sie können hersteller- und plattformunabhängig Datenträger analysieren, Aussagen zu kriminalistischen Fragestellungen treffen und einfache Gutachten oder Auswerteberichte fertigen. Dabei beachten Sie die Grundlagen der Informationssicherheit.
Dauer	5 Tage
Besondere Hinweise	Die Teilnahme an nachfolgend genannten Lehrgängen oder vergleichbare Kenntnisse der folgenden Inhalte werden zwingend vorausgesetzt: • OZ 4705 – Internetnutzung zur Wahrnehmung dienstlicher Aufgaben, • OZ 4615 – IuK-Kriminalität in der Sachbearbeitung, • OZ 4710 – Einsatz von Auswerterechnern zur

	Ermittlungsunterstützung, • Ermittlungs- und/oder Auswertungserfahrung im Bereich IuK-Kriminalität, • Kenntnisse der einschlägigen, auch englischsprachigen Fachtermini, • Kenntnisse Microsoft Windows und Linux OS. Kenntnisse in den Bereichen: • Funktion des Internets und seiner Dienste, • Netzwerkgrundlagen und –topografie, • DHCP, DNS, • OSI-Referenzmodell, • TCP/IP, UDP, ICMP. Das Seminar schließt mit einer schriftlichen Lernerfolgskontrolle ab.

Zurück zum Inhalt

4680 – Forensische Auswertung von Beweismitteln mit X-Ways Forensics (Grundlagen)

Zielgruppe	Mitarbeiterinnen und Mitarbeiter der IT-Beweissicherung und Sachbearbeitung IuK-Kriminalität von Landes- und Bundesbehörden, sowie Fachlehrerinnen und Fachlehrer des FB IV der PD AFB, die zukünftig mit der Auswertesoftware X-Ways Forensics arbeiten sollen.
Lehrinhalte	• Grundsätze der Informationssicherheit • Installation des Programms XWF und Einrichten einer Ordnerstruktur • Programmfunktionen und Navigation in der Benutzeroberfläche • Erstellen und Einsatz von HashSets • Erstellen von Verwalten von Fällen • Erstellen von Images und Dateicontainern • Export von Dateien • Erweitern des Dateiüberblicks und Einsatz von Filtern • Suchfunktionen und Grundlagen GREP für die Analyse von Beweismitteln • Analyse der Windows Registry auf sichergestellten Datenträgern • Analyse von Bild-, Video- und E-Maildateien mittels Add-ons von Drittanbietern • Problemlösung und Grenzen der Ermittlungsarbeit
Lernziele	Die Teilnehmerinnen und Teilnehmer sind nach erfolgreichem Abschluss in der Lage, digitale Beweismittel nach den Grundsätzen der forensischen Datenanalyse mit der Auswertesoftware X-Ways Forensics zu analysieren. Sie können Aussagen zu kriminalistischen Fragestellungen treffen und einfache Gutachten oder Auswerteberichte fertigen. Dabei beachten Sie die Grundsätze der Informationssicherheit.
Dauer	1 Woche
Besondere Hinweise	Voraussetzungen: • Eine eigene gültige Lizenz der Auswertesoftware X-Ways Forensics incl. Dongle. • Die erfolgreiche Teilnahme am Seminar OZ 4670 - Grundlagen der forensischen Datenanalyse oder vergleichbare Kenntnisse, insbesondere: o Betriebssysteme und deren Funktion o Dateisysteme o Grundlagen der Computerforensik o Grundlagen von Datennetzen.

	Das Seminar wird mit einer schriftlichen Lernerfolgskontrolle abgeschlossen. Die Softwarelizenz wird **nicht** durch den FB IV bereitgestellt. Auf Teilnehmerinnen und Teilnehmer, die X-Ways mit einer nicht mehr updatefähigen Lizenz verwenden **kann** bei eventuellen Programmfehlern und Übungen **im Unterricht keine Rücksicht genommen werden.** Die Teilnehmenden können mit einer eigenen HDD im Wechselrahmen die persönliche Arbeitsumgebung am Auswerterechner nutzen und diese bei Seminarende wieder mit an den eigenen Arbeitsplatz nehmen.

Zurück zum Inhalt

4681 – Forensische Auswertung von Beweismitteln mit X-Ways Forensics (Aufbau)

Zielgruppe	Mitarbeiterinnen und Mitarbeiter der IT-Beweissicherung und Sachbearbeitung IuK-Kriminalität von Landes- und Bundesbehörden, sowie Fachlehrerinnen und Fachlehrer des FB IV der PD AFB, die bereits seit längerem mit der Auswertesoftware X-Ways Forensics arbeiten.
Lehrinhalte	• Grundsätze der Informationssicherheit • Auffrischen der essentiellen Grundfunktionen (Fallverwaltung, Filter, Sortieren etc.) • Wiederherstellung gelöschter Daten • FAT Suchtechniken mit Schwerpunkt Regular Expressions • Internet und E-Mail Auswertung • Windows Registry • Dokument Metadaten • Hash-Analysen • HDD Sektorenanalyse • Datenschablonen • Analyse von Link-Dateien
Lernziele	Die Teilnehmerinnen und Teilnehmer sind nach erfolgreichem Abschluss in der Lage, digitale Beweismittel nach den Grundsätzen der forensischen Datenanalyse mit der Auswertesoftware X-Ways Forensics zu analysieren. Sie können Aussagen zu kriminalistischen Fragestellungen treffen und einfache Gutachten oder Auswerteberichte fertigen. Die Teilnehmenden sind in der Lage, weitergehende Funktionen der Auswertesoftware ordnungsgemäß zu nutzen und können dadurch problematische Ermittlungsfälle unter forensischen Gesichtspunkten bearbeiten. Dabei beachten Sie die Grundsätze der Informationssicherheit.
Dauer	1 Woche
Besondere Hinweise	Voraussetzungen: • Eine gültige Lizenz der Auswertesoftware X-Ways Forensics incl. Dongle, • Die erfolgreiche Teilnahme am Seminar OZ 4680 – X-Ways Forensics - Forensische Auswertung von Beweismitteln (Grundlagen), • ein intensives Eigenstudium der im Grundlagenseminar ausgegebenen Schulungsunterlagen und des in der Software enthaltenen Handbuchs des Herstellers vor der Teilnahme an

	diesem Seminar. Das Seminar wird mit einer schriftlichen Lernerfolgskontrolle abgeschlossen. Die Softwarelizenz wird **nicht** durch den FB IV bereitgestellt. Auf Teilnehmerinnen und Teilnehmer, die X-Ways mit einer nicht mehr updatefähigen Lizenz verwenden **kann** bei eventuellen Programmfehlern und Übungen **im Unterricht keine Rücksicht genommen werden.** Die Teilnehmenden können mit einer eigenen HDD im Wechselrahmen die persönliche Arbeitsumgebung am Auswerterechner nutzen und diese bei Seminarende wieder mit an den eigenen Arbeitsplatz nehmen.

Zurück zum Inhalt

4685 – Forensische Datenanalyse in der Sachbearbeitung mit X-Ways Investigator

Zielgruppe	Sachbearbeiterinnen und Sachbearbeiter von Landes- und Bundesbehörden, die die Auswertesoftware X-Ways Investigator einsetzen und selbstständig, aufbereitete Datensicherungen analysieren sollen.

Lehrinhalte	• Bedeutung der Informationssicherheit
	• Grundlagen der Informationsverarbeitung
	  ○ Betriebssysteme, Dateisysteme, Dateitypen
	  ○ Fachtermini und deren Bedeutung
	• Grundlagen Netzwerktechnik
	  ○ IP-Adresse, DHCP, DNS, Routing
	  ○ Verbindungen und Datenverkehr im Internet
	• Grundlagen der forensischen Datenanalyse
	  ○ Speichern und Löschen von Daten
	  ○ Prozesse in der IuK-Forensik
	• Bedeutung von Hashwerten
	  ○ Spurensuche und -analyse auf Datenträgern
	• Ermittlungsarbeit mit X-Ways Investigator
	  ○ Programmoberfläche und -funktionen
	  ○ Bedienung und Arbeitsabläufe
	  ○ Anlegen und Verwalten eines Falles
	  ○ Bewertung von Ergebnissen
	  ○ Erstellen von Berichten
	  ○ Grenzen der Ermittlungsarbeit

Lernziele	Die Teilnehmerinnen und Teilnehmer kennen nach erfolgreicher Teilnahme die Bedeutung der Computerforensik in der polizeilichen Sachbearbeitung. Sie sind in der Lage, die durch die IT-Beweissicherung aufbereiteten Datensicherungen mit der Auswertesoftware X-Ways Investigator zu analysieren, kriminalistische Fragestellungen zu beantworten und einen Auswertebericht zu verfassen. Dabei beachten sie die Grundsätze der Informationssicherheit.
Dauer	1 Woche
Besondere Hinweise	Voraussetzungen: • Die Teilnahme am Seminar OZ 4610 (OZ 445) – IuK-Kriminalität – Anzeigenaufnahme/Erster Angriff, • Eine gültige Lizenz der Auswertesoftware X-Ways Investigator, • Grundkenntnisse in der Funktionsweise von Microsoft Windows

	als grafische Erweiterung des Betriebssystems (GUI), • Bereitschaft zum Eigenstudium auch außerhalb des Seminars. Das Seminar wird mit einer schriftlichen Lernerfolgskontrolle abgeschlossen. Die Softwarelizenz wird **nicht** durch den FB IV bereitgestellt. Auf Teilnehmerinnen und Teilnehmer, die X-Ways mit einer nicht mehr updatefähigen Lizenz verwenden **kann** bei eventuellen Programmfehlern und Übungen **im Unterricht keine Rücksicht genommen werden.** Die Teilnehmenden können mit einer eigenen HDD im Wechselrahmen die persönliche Arbeitsumgebung am Auswerterechner nutzen und diese bei Seminarende wieder mit an den eigenen Arbeitsplatz nehmen.

Zurück zum Inhalt

4686 – Ermittlungen Kinderpornografie mit der Auswertesoftware URANOS

Zielgruppe	Sachbearbeitung Kinderpornografie LKA 242 – Ansprechstelle KiPo
Lehrinhalte	• Grundsätze der Informationssicherheit • Bedeutung der Computerforensik • Konzept der Anwendung URANOS • Programmbedienung und Benutzeroberfläche • Programmfunktionen und –grenzen • Analyse aufbereiteter Datenträger • Hashdatenbanken • Arbeitsabläufe beim LKA und BKA • Auswerteberichte und Verwaltung der Daten Zusammenarbeit mit der IT-Beweissicherung
Lernziele	Die Teilnehmenden kennen nach Abschluss des Seminars die technischen, taktischen und rechtlichen Bedeutungen der Software URANOS für die digitalen Ermittlungen im Phänomenbereich Kinderpornografie. Die Teilnehmenden können Bild- und Videodaten in aufbereiteten Datenträgern analysieren und in die standardisierten Verfahrensabläufe einbringen. Sie können die Software URANOS im Rahmen der dienstlichen Möglichkeiten handhabungssicher anwenden. Sie kennen die Grundsätze der Informationssicherheit und sind sich der Bedeutung der Datenqualität für den Informationsverarbeitungsprozess bewusst.
Dauer	1 Tag
Besondere Hinweise	Die Inhalte dieses Seminars entsprechen den fachspezifischen Inhalten des Tag 4 im OZ 2170. Teilnehmende, die bereits am OZ 2170 teilgenommen haben, gehören nicht mehr zur Zielgruppe des OZ 4686.

Zurück zum Inhalt

4687 – Auswertung von aufbereiteten Asservaten mit X-Ways CTR

Zielgruppe	Mitarbeitende der Landespolizei Schleswig-Holstein, die das Verfahren Auswerterechner einsetzen.

Lehrinhalte	• Grundsätze der Informationssicherheit
	• Zusammenarbeit mit der IT-Beweissicherung
	• Ermittlungsarbeit mit X-Ways CTR
	  ○ Programmoberfläche und -funktionen
	  ○ Bedienung und Arbeitsabläufe
	  ○ Anlegen und Verwalten eines Falles
	  ○ Bewertung von Ergebnissen
	  ○ Erstellen von Berichten
	Grenzen der Ermittlungsarbeit

Lernziele	Die Teilnehmenden kennen nach Abschluss des Seminars die technischen, taktischen und rechtlichen Bedeutung der Software X-Ways CTR für die digitalen Ermittlungen. Die Teilnehmenden können einfache digitale Spurenlagen in aufbereiteten Datenträgern analysieren und in die standardisierten Verfahrensabläufe einbringen. Sie können die Software X-Ways CTR im Rahmen der dienstlichen Möglichkeiten anwenden. Sie kennen die Grundsätze der Informationssicherheit und sind sich der Bedeutung der Datenqualität für den Informationsverarbeitungsprozess bewusst.
Dauer	1 Tag
Besondere Hinweise	

Zurück zum Inhalt

4688 – Auswertung von Internet- und Kommunikationsdaten mit XRY Reader und IEF Reader

Zielgruppe	Mitarbeitende der Landespolizei Schleswig-Holstein, die das Verfahren Auswerterechner einsetzen.

Lehrinhalte	• Grundsätze der Informationssicherheit
	• Zusammenarbeit mit der IT-Beweissicherung
	• Ermittlungsarbeit mit der Auswertesoftware XRY Reader und Internet Evidence Finder (IEF Reader)
	  ○ Programmoberfläche und -funktionen
	  ○ Bedienung und Arbeitsabläufe
	  ○ Suchfunktionen
	  ○ Auswertung von Internet- und Kommunikationsdaten auf aufbereiteten Datensicherungen
	  ○ Bewertung von Ergebnissen
	Grenzen der Ermittlungsarbeit

Lernziele	Die Teilnehmenden kennen nach Abschluss des Seminars die technischen, taktischen und rechtlichen Bedeutung der Software XRY-Reader und IEF-Reader für die digitalen Ermittlungen. Die Teilnehmenden können die durch die IT-Beweissicherung aufbereiteten Ergebnisse auswerten und in die standardisierten Verfahrensabläufe einbringen. Sie können die Software XRY-Reader und IEF-Reade im Rahmen der dienstlichen Möglichkeiten anwenden. Sie kennen die Grundsätze der Informationssicherheit und sind sich der Bedeutung der Datenqualität für den Informationsverarbeitungsprozess bewusst.
Dauer	1 Tag
Besondere Hinweise	Die Teilnahme am „OZ 4710 – Einsatz von Auswerterechnern zur Ermittlungsunterstützung“ wird vorausgesetzt.

Zurück zum Inhalt

4690 – Cybercrime Netzwerk- und Internetgrundlagen – Bedeutung für Ermittlungsverfahren verstehen

Zielgruppe	Alle Mitarbeiterinnen und Mitarbeiter von Polizeidienststellen.

Lehrinhalte	• Grundsätze der Informationssicherheit
	• Adressierungsmerkmale in Netzwerken
	  ○ IP-Adresse
	  ○ Protokolle
	  ○ Ports
	  ○ URL
	• Domain Name System (DNS)
	• Routing
	• Bewertung der Informationen
	• Virtuelle Netzwerke
	• Netzwerke in Firmenumgebungen
	• Einsatzmöglichkeiten mit LSK, Auswerterechner und Internetrechercherechner

Lernziele	Die Teilnehmerinnen und Teilnehmer kennen nach Abschluss des Seminars die technischen, taktischen und rechtlichen Bedeutungen der Adressierungsmerkmale in Netzwerken. Die Teilnehmenden können Adressierungsmerkmale feststellen, sichern, bewerten und Verantwortliche feststellen. Durch Kenntnis über die Zusammenhänge sind sie in der Lage, die richtigen einsatztaktischen, -technischen und rechtlichen Maßnahmen zu treffen und effizient umzusetzen. Sie kennen die Grundsätze der Informationssicherheit und sind sich der Bedeutung der Datenqualität für den Informationsverarbeitungsprozess bewusst.
Dauer	1 Tag
Besondere Hinweise	

Zurück zum Inhalt

4691 – Cybercrime Webseiten analysieren und Verantwortliche feststellen

Zielgruppe	Alle Mitarbeiterinnen und Mitarbeiter von Polizeidienststellen.

Lehrinhalte	• Grundsätze der Informationssicherheit
	• Kommunikationsplattformen im Internet
	  ○ Blogs, Foren, Homepages
	  ○ Soziale Neztwerke
	• Verantwortlichkeit im Internet
	  ○ Holder, admin-c, tech-c
	  ○ Provider
	• Whois-Abfragen durchführen und bewerten
	• Serverstrukturen
	  ○ URL
	  ○ Speicherstrukturen
	• Shared Hosting
	• Seitenquelltext bewerten
	• Internetarchive finden und nutzen
	• Einsatzmöglichkeiten mit LSK, Auswerterechner und Internetrechercherechner

Lernziele	Die Teilnehmerinnen und Teilnehmer kennen nach Abschluss des Seminars die technischen, taktischen und rechtlichen Hintergründe von publizierten Inhalten in Netzwerken. Die Teilnehmenden können Inhalte und Zusatzinformationen feststellen, sichern und bewerten und Verantwortliche feststellen. Durch Kenntnis über die Zusammenhänge sind sie in der Lage, die richtigen einsatztaktischen, -technischen und rechtlichen Maßnahmen zu treffen und effizient umzusetzen. Sie kennen die Grundsätze der Informationssicherheit und sind sich der Bedeutung der Datenqualität für den Informationsverarbeitungsprozess bewusst.
Dauer	1 Tag
Besondere Hinweise	Die Inhalte des „OZ 4690 – Cybercrime – Netzwerk- und Internetgrundlagen – Bedeutung für Ermittlungsverfahren verstehen“ müssen von den Teilnehmern beherrscht werden.

Zurück zum Inhalt

4692 – Cybercrime E-Mails analysieren und zurückverfolgen

Zielgruppe	Alle Mitarbeiterinnen und Mitarbeiter von Polizeidienststellen.

Lehrinhalte	• Grundsätze der Informationssicherheit
	• E-Mail als Kommunikationsmittel
	  ○ Aufbau
	  ○ Headerinformationen
	• Verantwortlichkeiten im Internet ermitteln
	  ○ Provider
	• E-Mails zurückverfolgen
	• Anonymisierungsdienste und Einmal-Email
	• Gesicherte E-Maildateien auswerten
	• Zusammenarbeit mit Providern
	Einsatzmöglichkeiten mit LSK, Auswerterechner und Internetrechercherechner

Lernziele	Die Teilnehmerinnen und Teilnehmer kennen nach Abschluss des Seminars die technischen, taktischen und rechtlichen Hintergründe des E-Maildatenverkehrs in Netzwerken. Die Teilnehmenden können Spuren und Headerinformationen erkennen, sichern, bewerten und Verantwortliche feststellen. Durch Kenntnis über die Zusammenhänge sind sie in der Lage, die richtigen einsatztaktischen, -technischen und rechtlichen Maßnahmen zu treffen und effizient umzusetzen. Sie kennen die Grundsätze der Informationssicherheit und sind sich der Bedeutung der Datenqualität für den Informationsverarbeitungsprozess bewusst.
Dauer	1 Tag
Besondere Hinweise	Die Inhalte des „OZ 4690 – Cybercrime – Netzwerk- und Internetgrundlagen – Bedeutung für Ermittlungsverfahren verstehen“ müssen von den Teilnehmenden beherrscht werden.

Zurück zum Inhalt

4693 – Cybercrime Internetchat und Messenger – Kommunikationsverläufe auswerten

Zielgruppe	Alle Mitarbeiterinnen und Mitarbeiter von Polizeidienststellen.

Lehrinhalte	• Grundsätze der Informationssicherheit
	• Grundfunktionen von Chatprogrammen
	• Skype, Facebook, MSN, Twitter, ICQ
	  ○ Wo liegen welche Daten?
	  ○ Welche Informationen können ausgewertet werden?
	  ○ Zusammenarbeit mit Provider
	• Protokolldaten analysieren
	• Einsatz von Auswertesoftware
	• Bewertung von Ermittlungsergebnissen
	• Einsatzmöglichkeiten mit LSK, Auswerterechner und Internetrechercherechner

Lernziele	Die Teilnehmerinnen und Teilnehmer kennen nach Abschluss des Seminars die technischen, taktischen und rechtlichen Hintergründe von Chat und Messengerdiensten in Netzwerken. Die Teilnehmenden können Spuren und Hintergrundinformationen erkennen, sichern bewerten und Verantwortliche feststellen. Durch Kenntnis über die Zusammenhänge sind sie in der Lage, die richtigen einsatztaktischen, -technischen und rechtlichen Maßnahmen zu treffen und effizient umzusetzen. Sie kennen die Grundsätze der Informationssicherheit und sind sich der Bedeutung der Datenqualität für den Informationsverarbeitungsprozess bewusst.
Dauer	1 Tag
Besondere Hinweise	Die Inhalte des „OZ 4690 – Cybercrime – Netzwerk- und Internetgrundlagen – Bedeutung für Ermittlungsverfahren verstehen“ müssen von den Teilnehmenden beherrscht werden.

Zurück zum Inhalt

4694 – Cybercrime P2P-Netzwerke und 1-Click-Hosting – (Urheber) Rechtsverletzungen im Internet nachvollziehen

Zielgruppe	Alle Mitarbeiterinnen und Mitarbeiter von Polizeidienststellen.

Lehrinhalte	• Grundsätze der Informationssicherheit
	• Grundfunktionen und Bedeutung
	• eMule, Bittorrent, KaZaa & Co.
	  ○ Wo liegen welche Daten?
	  ○ Welche Informationen können ausgewertet werden?
	  ○ Zusammenarbeit mit Provider
	• 1-Click-Hosting und Streaming
	• Nachweis der Tatbestandsmerkmale
	• Datenspuren in Netzwerken, Servern und Endgeräten bewerten
	• Umgang mit sichergestellten Asservaten
	• Einsatz von Auswertesoftware
	• Bewertung von Ermittlungsergebnissen
	• Einsatzmöglichkeiten mit LSK, Auswerterechner und Internetrechercherechner

Lernziele	Die Teilnehmerinnen und Teilnehmer kennen nach Abschluss des Seminars die technischen, taktischen und rechtlichen Hintergründe von P2P-Netzwerken, Streaming und 1-Click-Hosting. Die Teilnehmenden können Spuren und Hintergrundinformationen erkennen, sichern bewerten und Verantwortliche feststellen. Durch Kenntnis über die Zusammenhänge sind sie in der Lage, die richtigen einsatztaktischen Maßnahmen zu treffen und effizient umzusetzen. Sie kennen die Grundsätze der Informationssicherheit und sind sich der Bedeutung der Datenqualität für den Informationsverarbeitungsprozess bewusst.
Dauer	1 Tag
Besondere Hinweise	Die Inhalte des „OZ 4690 – Cybercrime – Netzwerk- und Internetgrundlagen – Bedeutung für Ermittlungsverfahren verstehen“ müssen von den Teilnehmenden beherrscht werden.

Zurück zum Inhalt

4695 – Cybercrime Cloud Computing – Beweismittel im Internet finden und sichern

Zielgruppe	Alle Mitarbeiterinnen und Mitarbeiter von Polizeidienststellen.
Lehrinhalte	• Grundsätze der Informationssicherheit • Grundfunktionen von Chatprogrammen • Dropbox, iCloud & Co. • Recherchemöglichkeiten • Nutzung von Smartphones • Welche Informationen können ausgewertet werden? • Datenspuren in Netzwerken, Servern und Endgeräten bewerten • Umgang mit sichergestellten Asservaten • Einsatz von Auswertesoftware • Bewertung von Ermittlungsergebnissen • Einsatzmöglichkeiten mit LSK, Auswerterechner und Internetrechercherechner
Lernziele	Die Teilnehmerinnen und Teilnehmer kennen nach Abschluss des Seminars die technischen, taktischen und rechtlichen Hintergründe des Speichern/Auslagern von Daten auf weltweit verteilten Servern über das Internet (Cloud Computing). Die Teilnehmenden können Spuren und Hintergrundinformationen erkennen, sichern, bewerten und Verantwortliche feststellen. Durch Kenntnis über die Zusammenhänge sind sie in der Lage, die richtigen einsatztaktischen, -technischen und rechtlichen Maßnahmen zu treffen und effizient umzusetzen. Sie kennen die Grundsätze der Informationssicherheit und sind sich der Bedeutung der Datenqualität für den Informationsverarbeitungsprozess bewusst.
Dauer	1 Tag
Besondere Hinweise	Die Inhalte des „OZ 4690 – Cybercrime – Netzwerk- und Internetgrundlagen – Bedeutung für Ermittlungsverfahren verstehen“ müssen von den Teilnehmenden beherrscht werden.

Zurück zum Inhalt

4696 – Cybercrime Umgang mit Verschlüsselung in polizeilichen Ermittlungen

Zielgruppe	Alle Mitarbeiterinnen und Mitarbeiter von Polizeidienststellen.
Lehrinhalte	• Grundsätze der Informationssicherheit • Hintergründe und Anwendungsfälle • Stärken und Schwächen von Algorithmen • Passwortsicherheit • EFS, Bitlocker, Truecrypt • Verschlüsselung in der Telekommunikation (Skype) • Besonderheiten bei der Durchsuchung • Steganografie • Möglichkeiten und Grenzen der ITB
Lernziele	Die Teilnehmerinnen und Teilnehmer kennen nach Abschluss des Seminars die technischen, taktischen und rechtlichen Hintergründe von digitaler Verschlüsselung und Steganografie. Durch Kenntnis über die Zusammenhänge sind sie in der Lage, die richtigen einsatztaktischen, -technischen und rechtlichen Maßnahmen zu treffen und effizient umzusetzen. Sie kennen die Grundsätze der Informationssicherheit und sind sich der Bedeutung der Datenqualität für den Informationsverarbeitungsprozess bewusst.
Dauer	1 Tag
Besondere Hinweise	Die Inhalte des „OZ 4690 – Cybercrime – Netzwerk- und Internetgrundlagen – Bedeutung für Ermittlungsverfahren verstehen“ müssen von den Teilnehmenden beherrscht werden.

Zurück zum Inhalt

4707 – Ermittlungen in Sozialen Netzwerken

Zielgruppe	Mitarbeiterinnen und Mitarbeiter der Landespolizei.
Lehrinhalte	• Bedeutungen und Funktion der Sozialen Netzwerke • Netzwerkgrundlagen • Anonymisierung • Provideranfragen • iana.org • Welche Informationen können anlassabhängig von der Polizei genutzt werden • Anlegen von Ermittlungsaccounts, hier Facebook, unter Beachtung der Einstellungen und rechtliche Voraussetzungen • Möglichkeiten der Verschleierung IP-Adresse im Internet via LSK-CITRIX • OSINT Recherche • Facebook Portal • Sicherung der Ergebnisse und deren Beweiswert im Strafverfahren • Ermittlungsübungen und Einsatz des Internetrechercherechners
Lernziele	Die Teilnehmenden sind nach Abschluss des Seminars über die Bedeutung und Hintergründe aktueller Internetanwendungen des Themenbereiches „Soziale Netzwerke“ informiert. Die Teilnehmenden sind in der Lage, offene, nichtoffene und verdeckte Ermittlungen in SNS zu unterscheiden, rechtlich zu begründen und im zulässigen Rahmen praktisch durchzuführen. Nach Abschluss des Seminars haben die Teilnehmerinnen und Teilnehmer Ermittlungsaccounts bei mindestens einem SNS. Sie können diese unter Kenntnis der für die Landespolizei Schleswig-Holstein gültigen Rechtsvorschriften erfolgreich einsetzen und beachten dabei die Grundsätze der Informationssicherheit.
Dauer	2 Tage
Besondere Hinweise Stand: Aug. 18	Es sind keine besonderen Vorkenntnisse erforderlich.

Zurück zum Inhalt

4710 – Einsatz von Auswerterechnern zur Ermittlungsunterstützung

Zielgruppe	Mitarbeiterinnen und Mitarbeiter der Landespolizei, die das Verfahren Auswerterechner S/K/WSP einsetzen **und** die durch den AWB-Auswerterechner begleitete Lernphase absolviert haben.
Lehrinhalte	• Grundlagen der Informationssicherheit • Das Verfahren Auswerterechner S/K/WSP und Zuständigkeiten • Zusammenarbeit mit dem AWB-Auswerterechner, der IT-Beweissicherung und dem LPA 2 • Hard- und Softwareausstattung • Behandlung, Aufbereitung und Auswertung von Daten, Datenträgern und Datenträgersicherungen • Auswerterechner richtig einrichten • Umgang mit E-Mails, Bild- und Videodaten als Beweismittel • FTK-Imager, DocFetcher, XNView, Quickview Plus, Mailstore Home, URANOS, Truecrypt • Sicherung der Ergebnisse und Auswerteberichte • Rechtliche Regelungen für die Landespolizei Schleswig-Holstein • Ermittlungsübungen
Lernziele	Die Teilnehmenden können nach der Schulung das Verfahren Auswerterechner technisch, taktisch und rechtlich einwandfrei einsetzen, um bei der Bearbeitung von Ermittlungsverfahren eine Aufspürung, Sicherung und beweiskräftige Darstellung von relevanten Daten durchzuführen. Die Teilnehmenden werden nach erfolgreichem Abschluss des Seminars zum Verfahren Auswerterechner S/K/WSP zugelassen.
Dauer	3 Tage
Besondere Hinweise	**Pflichtlehrgang mit Lernerfolgskontrolle** – führt bei erfolgreichem Abschluss zur Zulassung zum Verfahren Auswerterechner S/K/WSP und berechtigt zur selbständigen Nutzung des Auswerterechners im Rahmen von polizeilichen Ermittlungen. Kann erst nach Absolvieren der durch einen AWB-Auswerterechner begleiteten Lernphase belegt werden. Die Dienststelle muss zwingend mit einem Auswerterechner S/K/WSP ausgestattet sein.

Zurück zum Inhalt

4711 – AWB Auswerterechner (S/K/WSP)

Zielgruppe	Mitarbeiterinnen und Mitarbeiter der Landespolizei, die als AWB-Auswerterechner das Verfahren Auswerterechner (S/K/WSP) administrieren sollen.
Lehrinhalte	• Grundlagen der Informationssicherheit • Das Verfahren Auswerterechner S/K/WSP und Zuständigkeiten • Zusammenarbeit mit der IT-Beweissicherung und dem LPA 2 • Hard- und Softwareausstattung • Behandlung, Aufbereitung und Auswertung von Daten, Datenträgern und Datenträgersicherungen • Auswerterechner richtig einrichten • Umgang mit E-Mails, Bild- und Videodaten als Beweismittel • FTK-Imager, DocFetcher, XNView, Quickview Plus, Mailstore Home, URANOS, Truecrypt, X-Ways CTR, XRY Reader, Internet Evidence Finder • Umgang mit Updates und Problemlösung • Betreuung von Nutzenden im Rahmen des IT-Schulungsteilkonzeptes Auswerterechner • Durchführung von Dienstunterrichten • Rechtliche Regelungen für die Landespolizei Schleswig-Holstein • Ermittlungsübungen
Lernziele	Die Teilnehmenden können nach der Schulung das Verfahren Auswerterechner technisch, taktisch und rechtlich einwandfrei einsetzen, um bei der Bearbeitung von Ermittlungsverfahren eine Aufspürung, Sicherung und beweiskräftige Darstellung von relevanten Daten durchzuführen. Sie können als Anwenderbetreuerin/Anwenderbetreuer (AWB) die Nutzenden des Verfahrens Auswerterechner anleiten, unterstützen und Hilfestellungen geben. Die Teilnehmenden werden nach erfolgreichem Abschluss des Seminars zum Verfahren Auswerterechner S/K/WSP in der Rolle eines AWB zugelassen.
Dauer	4 Tage
Besondere Hinweise	**Pflichtlehrgang mit Lernerfolgskontrolle** – führt bei erfolgreichem Abschluss zur Zulassung zum Verfahren Auswerterechner S/K/WSP als AWB. Berechtigt gemäß Erlass zur Administration des Verfahrens Auswerterechner S/K/WSP und zur Betreuung der Nutzenden.

	Die Belegung dieses Lehrgangs sollte ausstattungsbegleitend erfolgen.

Zurück zum Inhalt

4771 – Polizeiliche Informationssysteme im Intranet/Extranet

Zielgruppe	Alle Mitarbeiterinnen und Mitarbeiter der Landespolizei als Nutzer der polizeilichen Informationssysteme
Lehrinhalte	• Theoretische und praktische Unterweisung in Bedienung, Inhalt, Aufbau und praktischen Einsatzmöglichkeiten der verschiedenen Informationssysteme im Intra- und Extranet (RAKK, EuFID, FINAS, DOKIS, LUNA, HaNS, FeD u. a.) • Grundlagen der Informationssicherheit
Lernziele	Die Teilnehmerinnen und Teilnehmer sollen die Einsatzmöglichkeiten und Leistungsmerkmale der Verfahren kennen sowie diese unter Berücksichtigung rechtlicher Vorschriften und einsatztaktischer Gesichtspunkte anwenden können. Sie beachten dabei die Grundlagen der Informationssicherheit.
Dauer	1 Tag
Besondere Hinweise	

Zurück zum Inhalt

4800 – Grundlehrgang Polizeiliche Informationssysteme

Zielgruppe	Alle Mitarbeiterinnen und Mitarbeiter der Landespolizei als Nutzer der polizeilichen Informationssysteme.
Lehrinhalte	• Theoretische und praktische Unterweisung in Bedienung, Inhalt, Aufbau und praktischen Einsatzmöglichkeiten der verschiedenen polizeilichen Informationssysteme und der Informationssysteme anderer Behörden (INPOL, ZEVIS, EWO, FADA, Justiz-Online, AZR, RAKK, EuFID, DOKIS, LUNA, HaNS) • Datenschutz und Grundlagen der Informationssicherheit • Die verschiedenen Passwortverfahren
Lernziele	Die Teilnehmerinnen und Teilnehmer sollen die Einsatzmöglichkeiten und Leistungsmerkmale der Verfahren kennen sowie diese unter Berücksichtigung rechtlicher Vorschriften und einsatztaktischer Gesichtspunkte anwenden können. Die Teilnehmenden sind über die für den getroffenen landeseinheitlichen Regelungen zur Informationssicherheit informiert und wissen, wo sie zu Fragen Informationen erhalten können (IT-Regelwerk im Intrapol; CheckIT).
Dauer	2 Tage
Besondere Hinweise	Nach dem Lehrgang erfolgt die Zuteilung einer Zugangskennung, soweit diese für die Nutzung der unterschiedlichen Verfahren erforderlich ist.

Zurück zum Inhalt

4810 – EDDI-Datenerfassung - Grundlehrgang

Zielgruppe	Laut Richtlinie Erkennungsdienst Digital in der jeweils gültigen Fassung.
Lehrinhalte	• Anforderungen an die Datenqualität von ED-Behandlungen • Praktische Durchführung einer ED-Behandlung mit der Fachanwendung Erkennungsdienst Digital (EDDI) • Rechtsgrundlagen zur ED-Behandlung • Vorladung und Vollzug • Richtlinien und Dienstanweisungen • Anlage und Änderung von elektronischen Kriminalakten • Prüffristen und Umwidmung von ED-Behandlungen • Abnahme und Digitalisierung von Finger- und Handflächenabrücken • Digitalisierung von Dokumenten • Digitale Fotografie von Personen und körperlichen Merkmalen • Lichtbildrecherche, Zeugeneinsichtnahme, Recherche ohne Zeugen • Grundlagen der Informationssicherheit
Lernziele	Die Teilnehmerinnen und Teilnehmer sollen die Einsatzmöglichkeiten und Leistungsmerkmale der Fachanwendung kennen sowie diese unter Berücksichtigung rechtlicher Vorschriften und einsatztaktischer Gesichtspunkte anwenden können. Sie sollen die Bedeutung der Datenqualität für die taktische polizeiliche Arbeit erkennen. Die Teilnehmenden sind über die für den getroffenen landeseinheitlichen Regelungen zur Informationssicherheit informiert und wissen, wo sie zu Fragen Informationen erhalten können (IT-Regelwerk im Intrapol; CheckIT).
Dauer	2 Tage in Modulen
Besondere Hinweise	**Die Teilnehmerinnen und Teilnehmer müssen über eine Zugangsberechtigung für INPOL verfügen!** Die Teilnahme führt zur Erteilung einer Zugangsberechtigung für die EDDI-Datenerfassung **und** die EDDI-Lichtbildrecherche.

Zurück zum Inhalt

4821 – EDDI-Lichtbildrecherche

Zielgruppe	Mitarbeiterinnen und Mitarbeiter der Kriminalpolizei sowie nicht nur vorübergehend abgeordnete Mitarbeiterinnen und Mitarbeiter der Schutz- und Wasserschutzpolizei
Lehrinhalte	• Ermittlung eines unbekannten Tatverdächtigen anhand von Personenbeschreibungen • Rechtsgrundlagen für Lichtbildvorlagen • Grundlagen der Informationssicherheit • Subjektive/objektive Personenbeschreibung bei der ED-Behandlung • Auswertung von Zeugenaussagen (Personenbeschreibungen) • Taktischer Umgang mit den Suchkriterien • Auswertung der Suchergebnisse • Protokollierung • Abgrenzung zur Personenrecherche
Lernziele	Die Teilnehmerinnen und Teilnehmer sollen die Einsatzmöglichkeiten und Leistungsmerkmale der Lichtbildrecherche kennen sowie diese unter Berücksichtigung rechtlicher Vorschriften und einsatztaktischer Gesichtspunkte anwenden können. Die Teilnehmenden sind über die für den getroffenen landeseinheitlichen Regelungen zur Informationssicherheit informiert und wissen, wo sie zu Fragen Informationen erhalten können (IT-Regelwerk im Intrapol; CheckIT).
Dauer	½ Tag
Besondere Hinweise	Die Teilnehmerinnen und Teilnehmer müssen über praktische Erfahrungen in der Anwendung der Informationssysteme sowie über eine Zugangskennung für INPOL verfügen.

Zurück zum Inhalt

4840 – INPOL-Fall Dezentralisierung MA ELST und Kripo

Zielgruppe	Mitarbeiterinnen und Mitarbeiter von Einsatzleitstellen sowie alle Mitarbeiterinnen und Mitarbeiter der Kriminalpolizei
Lehrinhalte	• Grundlagen der Informationssicherheit • Allgemeine Erläuterungen zu Inpol-Fall • Aufbau des Systems und Navigation im System • Erfassungsregeln • Datenschutzrechtliche Bestimmungen • Darstellung und Erklärung der unterschiedlichen Recherchemöglichkeiten • Praktische Übungen und Recherchen
Lernziele	Die Lehrgangsteilnehmerinnen und Lehrgangsteilnehmer sollen die unterschiedlichen Recherchen eigenverantwortlich durchführen um Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung aufzuklären oder zu verhüten. Sie sollen unter Beachtung rechtlicher Vorschriften mittels systematischer Informationsverdichtung neue Erkenntnisse für polizei- und ermittlungstaktisches Vorgehen gewinnen, insbesondere durch Erkennen von relevanten Personen, Personengruppierungen, Institutionen, Objekten und Sachen und durch Erkennen von Verflechtungen/Zusammenhängen zwischen Personen, Personengruppierungen, Institutionen, Objekten und Sachen. Die Teilnehmerinnen und Teilnehmer sind über die für den getroffenen landeseinheitlichen Regelungen zur Informationssicherheit informiert und wissen, wo sie zu Fragen Informationen erhalten können (IT-Regelwerk im Intrapol; CheckIT).
Dauer	2 Tage
Besondere Hinweise	Die praktischen Rechercheübungen werden im Datenbestand der Schulungsumgebung durchgeführt. Die Befähigung zum Arbeiten im System Inpol-Fall gilt für die Recherchen in den jeweiligen frei geschalteten Anwendungen.

Zurück zum Inhalt

4850 – INPOL–Fall Datenerfassung/-pflege und Recherche

Zielgruppe	Mitarbeiterinnen und Mitarbeiter des LKA SH, die in ihren Dienststellen die Datenerfassung/-pflege und Recherche in Inpol Fall vornehmen.
Lehrinhalte	• Grundlagen der Informationssicherheit • Einführung in das Thema/Aufbau Inpol Fall • Bildschirmaufbau und Navigation im System • Erstellung und Bearbeitung von Verfahren und Vorgängen • Rechtliche Bestimmungen • Erstellung und Bearbeitung von Objekten • Anlegen von Beziehungen • Erfassung eines Geschäftsvorfalles • Praktische Rechercheübungen in den unterschiedlichen Suchen • Sonstiges/Extras
Lernziele	Die Lehrgangsteilnehmerinnen und Lehrgangsteilnehmer sollen Sachverhalte selbständig aufbereiten, die Dateneingaben eigenverantwortlich vornehmen sowie Recherchen durchführen um Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung aufzuklären oder zu verhüten. Sie sollen unter Beachtung rechtlicher Bestimmungen mittels systematischer Informationsverdichtung neue Erkenntnisse für polizei- und ermittlungstaktisches Vorgehen gewinnen, insbesondere durch Erkennen von relevanten Personen, Personengruppierungen, Institutionen, Objekten und Sachen und durch Erkennen von Verflechtungen/Zusammenhängen zwischen Personen, Personengruppierungen, Institutionen, Objekten und Sachen. Die Teilnehmerinnen und Teilnehmer sind über die für den getroffenen landeseinheitlichen Regelungen zur Informationssicherheit informiert und wissen, wo sie zu Fragen Informationen erhalten können (IT-Regelwerk im Intrapol; CheckIT).
Dauer	3 Tage
Besondere Hinweise	Die praktischen Übungen zur Datenerfassung und –pflege und zur Recherche werden im Datenbestand der Schulungsumgebung durchgeführt. Die Befähigung zum Arbeiten im System Inpol Fall gilt für die jeweiligen frei geschalteten Anwendungen.

Zurück zum Inhalt

4851 – INPOL–Fall Recherche

Zielgruppe	Mitarbeiterinnen und Mitarbeiter des LKA SH, die in ihren Dienststellen Recherchen und Standardauswertungen in Inpol Fall vornehmen.
Lehrinhalte	• Struktur des Dokumentationssystems Inpol Fall • Bildschirmaufbau und Navigation • Grundlagen der Erfassung • Datenschutzrechtliche Bestimmungen • Grundlagen der Informationssicherheit • Darstellung und Erklärung der unterschiedlichen Recherchemöglichkeiten • Praktische Übungen und Recherchen • Standardauswertungen im Datenbestand anhand von praktischen Ü-bungen
Lernziele	Die Teilnehmerinnen und Teilnehmer sollen die Einsatzmöglichkeiten und Leistungsmerkmale der INPOL Fall Recherche kennen sowie diese unter Berücksichtigung rechtlicher Vorschriften und einsatztaktischer Gesichtspunkte anwenden können. Sie sollen befähigt werden, Recherchen und Standardauswertungen in Inpol Fall durchzuführen. Weiterhin sollen die Teilnehmenden mit Hilfe der Abfragen/Recherchen und der Standardauswertungen Ermittlungs- und Auswertungsunterstützung leisten. Die Teilnehmerinnen und Teilnehmer sind über die für den getroffenen landeseinheitlichen Regelungen zur Informationssicherheit informiert und wissen, wo sie zu Fragen Informationen erhalten können (IT-Regelwerk im Intrapol; CheckIT).
Dauer	2 Tage
Besondere Hinweise	Die praktischen Übungen zur Recherche und zu Standardauswertungen werden im Datenbestand der Schulungsumgebung durchgeführt. Die Befähigung zum Recherchieren und zur Standardauswertung im System Inpol Fall gilt für die jeweiligen frei geschalteten Anwendungen.

Zurück zum Inhalt